

| | |
|---|-----|
| 1. Specificaties | 2 |
| 1.1 Begrippenlijst | 3 |
| 1.2 Overzicht interacties, versies en systeemrollen | 4 |
| 1.3 Benodigde UZI-middelen | 8 |
| 1.4 AORTA on FHIR specificaties - 0.7.22 | 9 |
| 1.4.1 Leeswijzer AoF - 0.7.x | 10 |
| 1.4.2 Changelog AoF - 0.7.x | 11 |
| 1.4.3 Globaal ontwerp - 0.7.x | 22 |
| 1.4.3.1 MedMij Flows - 0.7.x | 24 |
| 1.4.3.2 Zorgaanbieder Flows - 0.7.x | 25 |
| 1.4.4 Interfaces - 0.7.x | 26 |
| 1.4.4.1 Interfaces Common - 0.7.x | 27 |
| 1.4.4.2 Token specificaties - 0.7.x | 30 |
| 1.4.4.3 AORTA FHIR-profielen - 0.7.x | 42 |
| 1.4.4.4 AORTA Stelsel Interfaces - 0.7.x | 43 |
| 1.4.4.5 Adressering Server Interfaces - 0.7.x | 44 |
| 1.4.4.6 Autorisatie Server Interfaces - 0.7.x | 48 |
| 1.4.4.7 MAP Server Interfaces - 0.7.x | 56 |
| 1.4.4.8 Resource Broker Interfaces - 0.7.x | 58 |
| 1.4.4.9 Resource Server Interfaces - 0.7.x | 69 |
| 1.4.4.10 Transformatie Server Interfaces - 0.7.x | 78 |
| 1.4.4.11 Workflow Interfaces - 0.7.x | 89 |
| 1.4.5 Use cases - 0.7.x | 90 |
| 1.4.5.1 UC Resource Client - 0.7.x | 91 |
| 1.4.5.2 UC Resource Server - 0.7.x | 94 |
| 1.4.5.3 UC Workflow - 0.7.x | 104 |

Specificaties

Begrippenlijst

In de AORTA on FHIR (AoF) documentatie worden de volgende (AoF-specifieke) begrippen gehanteerd:

| Begrip | Omschrijving |
|--------------------|--|
| AoF | AORTA on FHIR. Project met als doelstelling om gegevensuitwisseling in het AORTA afsprakenstelsel te kunnen ondersteunen op basis van de FHIR standaard. |
| DVP Server | Een applicatierol van een Dienstverlener Persoon, zoals gedefinieerd in het MedMij afsprakenstelsel. |
| Resource Broker | Een set van systeemcomponenten die samen als een makelaar fungeren tussen Resource Clients (GBx-applicaties of DVP Servers) en Resource Servers (GBZ-applicaties). |
| GBx-applicatie | Een applicatie binnen een GBZ, een GBP of een GBK. |
| GBZ-applicatie | Een applicatie binnen een GBZ. |
| Autorisatie Server | Een systeemcomponent die autorisaties verleent aan Resource Clients om gegevens uit te mogen wisselen met Resource Servers, of met andere componenten. |

Overzicht interacties, versies en systeemrollen

- Benodigde systeemrollen voor Initiërende en Reagerende GBZ-applicaties (xIS'en)
- AORTA on FHIR versie 0.7
 - Interacties tot en met AoF versie 0.7
- AORTA on FHIR versie 0.6
 - Interacties tot en met AoF versie 0.6
 - Aanvullende of gewijzigde functies t.o.v. de vorige versie
- AORTA on FHIR versie 0.5.x
 - Interacties
 - Functies

Benodigde systeemrollen voor Initiërende en Reagerende GBZ-applicaties (xIS'en)

Een overzicht van alle systeemrollen die kunnen worden vervuld door initiërende en reagerende GBZ-applicaties is gegeven in:

- Overzicht Resource Client ([links toevoegen](#))
- Overzicht Resource Server

Een reagerende GBZ-applicatie zal typisch zowel acteren als resource client (bijvoorbeeld voor het aanmelden bij de VWI) en als resource server.

Om FHIR-interacties te kunnen ontvangen van de resource broker, is altijd de abstracte systeemrol *FHIR Verwerkend Systeem* vereist. De systeemrol *FHIR Verwerkend Systeem* vereist dat ook systeemrol *AORTA access_token Verwerkend Systeem* is geïmplementeerd. De abstracte systeemrol *FHIR Verwerkend Systeem* beschrijft functionaliteit die nodig is in de volgende concrete systeemrollen:

- *MedMij Opleverend Systeem*;
- *MedMij Ontvangend Systeem*;
- *Ontvankelijkheidsstatus Opleverend Systeem*.

Een xIS moet FHIR-interacties kunnen ontvangen wanneer:

- het één of meerdere gegevensdiensten ondersteund o.b.v. FHIR, OF
- het één of meerdere delen-gegevensdiensten ondersteund o.b.v. FHIR of HL7v3.

In het laatste geval moet namelijk altijd ook een custom FHIR-operation kunnen worden verwerkt, waarmee de ontvankelijkheidsstatus kan worden bepaald.

Onderstaande tabel geef een overzicht van de specifieke vereisten per functie(groep).

| Functie(groep) | Vereiste systeemrollen voor | |
|-------------------------------|---|---|
| | Initiërende GBZ-applicatie | Reagerende GBZ-applicatie |
| Alle | TKID Activerend Systeem | |
| | - | AORTA access_token Verwerkend Systeem |
| | - | capabilities Operation Verwerkend Systeem |
| MedMij Functie Verzamelen | N.v.t. | MedMij Opleverend Systeem |
| MedMij Functie Delen | N.v.t. | MedMij Ontvangend Systeem Ontvankelijkheidsstatus Opleverend Systeem |
| AORTA Opvragen gegevens | Patiënt Gegevens Raadplegend Systeem | Bronstelsysteem Patiëntgegevens |
| AORTA Versturen gegevens | Gegevens Versturend Systeem | Gegevens Ontvangend Systeem |
| AORTA Initiëren notified-pull | Notified-pull Initiërend Systeem Gegevens Versturend Systeem | Gegevens Ontvangend Systeem |
| AORTA Uitvoeren notified-pull | Patiënt Gegevens Raadplegend Systeem | Bronstelsysteem Patiëntgegevens |
| AORTA Taken en notificaties | Taak Aanvragend Systeem Gegevens Versturend Systeem | Taak Uitvoerend Systeem Gegevens Ontvangend Systeem |

Verder zijn voor MedMij gegevensdiensten en AORTA zorgtoepassingen vereist:

1. De van toepassing zijnde *<resource type> <interactietype> Verwerkend Systeem* systeemrollen, bijvoorbeeld Observation Search Verwerkend Systeem.

2. Indien van toepassing voor de gegevensdienst/toepassing de systeemrollen *FHIR Transaction Verwerkend Systeem* en/of *FHIR Batch Verwerkend Systeem*. Deze laatste twee systeemrollen vereisen technisch gezien altijd tenminste één <resource-type> <interactietype> Verwerkend Systeem systeemrol.

AORTA on FHIR versie 0.7

Interacties tot en met AoF versie 0.7

[Interacties en systeemrollen AoF 0.7.xlsx](#)

AORTA on FHIR versie 0.6

Interacties tot en met AoF versie 0.6

[Interacties en systeemrollen.xlsx](#)

Aanvullende of gewijzigde functies t.o.v. de vorige versie

| Omschrijving | Functie | | AORTA-systeemrol | |
|--|---------|------------|---------------------------------------|--|
| | ve | code | naam | |
| Kunnen ontvangen van gegevens in de context van de MedMij UC Delen. Op basis van welke criteria wordt deze systeemrol toegekend? Bespreken met Bart Hoenderboom | 0.6 | n.t.b. | MedMij Ontvangend Systeem | |
| Kunnen verwerken van een FHIR batch interactie. Een FHIR batch kan in theorie een willekeurige combinatie van FHIR-interacties bevatten, zoals create, read, update, delete en search. | 0.6 | BVS.FHIR.1 | FHIR Batch Verwerkend Systeem | |
| Kunnen verwerken van een FHIR transaction interactie. Een FHIR transaction kan in theorie een willekeurige combinatie van FHIR-interacties bevatten, zoals create, read, update, delete en search. | 0.6 | TVS.FHIR.1 | FHIR Transaction Verwerkend Systeem | |
| Kunnen verwerken van een JWT-based AORTA-access_token. | 0.6 | ATT.JWT.2 | AORTA access_token Verwerkend Systeem | |
| Kunnen activeren van een TKID(-set). | 0.6 | TKID.UIS.1 | TKID Activerend Systeem | |

AORTA on FHIR versie 0.5.x

Interacties

| AORTA FHIR-interactie | | | | | | AORTA-systeemrol | | Wordt gehanteerd in use case | Compatibel met MedMij gegevensdienst |
|-----------------------|--------------|---------------------|-------------------|---|-------------|--------------------------------|---|-------------------------------|--------------------------------------|
| m o d e | code | FHIR resourcetype | interactie versie | Heeft betrekking op de volgende ZIB's | FHIR versie | code | naam | | |
| client | update | CapabilityStatement | 0.5.0 | - | STU3 | CapabilityStatement.UIS.FHIR.1 | CapabilityStatement Update Initiërend Systeem | Activeren van kwalificaties | N.v.t. |
| server | capabilities | - | 0.5.2 | | STU3 | capabilities.OVS.FHIR.1 | capabilities Operation Verwerkend Systeem | Opleveren CapabilityStatement | N.v.t. |
| | search-type | Patient | 1.0 | Patiënt, burgerlijke staat, taalvaardigheid, zorgverlener, zorgaanbieder, juridische status, contactpersoon | | Patient.SVS.FHIR.1 | Patient Search Verwerkend Systeem | Opleveren BGGZ | 48, 50 |
| | search-type | Coverage | 1.0 | Betaler | | Coverage.SVS.FHIR.1 | Coverage Search Verwerkend Systeem | Opleveren BgGGZ | |

| | | | | | | | |
|-------------|----------------------------|-----|--|---------------------------------------|--|----------------------|-----------------|
| search-type | Consent | 1.0 | Behandelaanwijzing, wilsverklaring | Consent.SVS.FHIR.1 | Consent Search Verwerkend Systeem | | |
| search-type | Condition | 1.0 | Probleem | Condition.SVS.FHIR.1 | Condition Search Verwerkend Systeem | | |
| search-type | Procedure | 1.0 | Verrichting | Procedure.SVS.FHIR.1 | Procedure Search Verwerkend Systeem | | |
| search-type | Observation | 1.0 | Laboratoriumuitslag | Observation.SVS.FHIR.1 | Observation Search Verwerkend Systeem | | |
| | | | Drugsgebruik, alcoholgebruik, tabaksgebruik, woonsituatie, functionele of mentale status | | | | Opleveren BGZ |
| | | | Bloeddruk, lichaamsgewicht, lichaamslengte | | | | Opleveren BgGGZ |
| | | | Gezinsituatie, gezinssituatie kind, participatie in maatschappij, algemene meting | | | | |
| search-type | NutritionOrder | 1.0 | Voedingsadvies | NutritionOrder.SVS.FHIR.1 | NutritionOrder Search Verwerkend Systeem | Opleveren BGZ | 48 |
| search-type | Flag | 1.0 | Alert | Flag.SVS.FHIR.1 | Flag Search Verwerkend Systeem | | |
| search-type | AllergyIntolerance | 1.0 | Allergie intolerantie | AllergyIntolerance.SVS.FHIR.1 | AllergyIntolerance Search Verwerkend Systeem | | |
| search-type | MedicationStatement | 1.0 | Medicatiegebruik | MedicationStatement.SVS.FHIR.1 | MedicationStatement Search Verwerkend Systeem | | |
| search-type | MedicationRequest | 1.0 | Medicatieafpraak | MedicationRequest.SVS.FHIR.1 | MedicationRequest Search Verwerkend Systeem | | |
| search-type | MedicationDispense | 1.0 | Toedieningsafpraak | MedicationDispense.SVS.FHIR.1 | MedicationDispense Search Verwerkend Systeem | | |
| search-type | DeviceUseStatement | 1.0 | Medisch hulpmiddel | DeviceUseStatement.SVS.FHIR.1 | DeviceUseStatement Search Verwerkend Systeem | | |
| search-type | Immunization | 1.0 | Vaccinatie | Immunization.SVS.FHIR.1 | Immunization Search Verwerkend Systeem | | |
| search-type | Encounter | 1.0 | Contact | Encounter.SVS.FHIR.1 | Encounter Search Verwerkend Systeem | | |
| search-type | ProcedureRequest | 1.0 | Overdracht geplande zorgactiviteit | ProcedureRequest.SVS.FHIR.1 | ProcedureRequest Search Verwerkend Systeem | | |
| search-type | ImmunizationRecommendation | 1.0 | | ImmunizationRecommendation.SVS.FHIR.1 | ImmunizationRecommendation Search Verwerkend Systeem | | |
| search-type | DeviceRequest | 1.0 | | DeviceRequest.SVS.FHIR.1 | DeviceRequest Search Verwerkend Systeem | | |
| search-type | Appointment | 1.0 | | Appointment.SVS.FHIR.1 | Appointment Search Verwerkend Systeem | | |
| search-type | CarePlan | 1.0 | Hulp van anderen | CarePlan.SVS.FHIR.1 | CarePlan Search Verwerkend Systeem | Opleveren BgGGZ | 50 |
| search-type | DiagnosticReport | 1.0 | Tekstuitslag | DiagnosticReport.SVS.FHIR.1 | DiagnosticReport Search Verwerkend Systeem | | |
| search-type | CareTeam | 1.0 | - | CareTeam.SVS.FHIR.1 | CareTeam Search Verwerkend Systeem | | |
| search-type | DocumentManifest | 1.0 | -, patient, zorgverlener, zorgaanbieder | DocumentManifest.SVS.FHIR.1 | DocumentManifest Search Verwerkend Systeem | Opleveren documenten | 51 |
| search-type | DocumentReference | 1.0 | | DocumentReference.SVS.FHIR.1 | DocumentReference Search Verwerkend Systeem | | |
| read | Binary | 1.0 | | - | Binary.RVS.FHIR.1 | | |

Functies

| Functie | AORTA-systeemrol |
|---------|------------------|
|---------|------------------|

| Omschrijving | versie | code | naam |
|---|--------|---|--|
| Kunnen opleveren van gegevens in de context van de MedMij UC Verzamelen, waaronder het uitvoeren van MedMij beschikbaarheidstoets bij opvraag door patiënt. | 0.5.0 | DVZA. BES.2020 | MedMij Opleverend Systeem |
| Kunnen verwerken van een JWT-based AORTA-access_token. | 0.5.3 | ATT.JWT. 1 | AORTA access_token Verwerkend Systeem |
| Kunnen verwerken van een AORTA FHIR interactie, dus inclusief AORTA-specifieke vereisten m.b.t. verwerking access_token en andere HTTP-headers. Het gaat hierbij om de volgende FHIR-interacties: create, read, update, delete en search. Verwerking van een FHIR batch/transaction valt hier niet onder. | 0.5.3 | N.v.t. (abstracte systeemro l) | FHIR Verwerkend Systeem |

Benodigde UZI-middelen

Onderstaande figuur bevat de UZI-middelen, die nodig zijn in een GBZ, om vanuit een Resource Client een AORTA FHIR-interactie te kunnen initiëren. Er zijn dus verschillende opties. Op TLS-niveau is altijd een UZI-servercertificaat vereist.

Benodigde UZI-middelen bij Resource Client

| | |
|----------------------------------|--|
| Uitvoeren push of reguliere pull | AORTA SAML transactie_token, gesigned met een UZI-pas (zorgverlenerspas) |
| | AORTA SAML mandaat_token, gesigned met een UZI-pas (zorgverlenerpas) + AORTA SAML transactie_token, gesigned met een UZI-pas (zorgverlenerspas of medewerkerpas op naam) |
| | AORTA SAML mandaat_token, gesigned met een UZI-pas (zorgverlenerpas) + AORTA SAML transactie_token, gesigned met een UZI-servercertificaat + AORTA SAML inschrijf_token, gesigned met een UZI-pas (zorgverlenerpas of medewerkerpas op naam) |
| Aanmaken consent_token | signing met een UZI-servercertificaat |
| Uitvoeren pull na notificatie | AORTA SAML transactie_token, gesigned met een UZI-pas (zorgverlenerspas) + ontvangen AORTA SAML consent_token |
| | AORTA SAML mandaat_token, gesigned met een UZI-pas (zorgverlenerpas) + AORTA SAML transactie_token, gesigned met een UZI-pas (zorgverlenerspas of medewerkerpas op naam) + ontvangen AORTA SAML consent_token |
| | AORTA SAML mandaat_token, gesigned met een UZI-pas (zorgverlenerpas) + AORTA SAML transactie_token, gesigned met een UZI-servercertificaat + ontvangen AORTA SAML consent_token |

Push-interacties zijn: FHIR-create, FHIR-update, FHIR-delete. Pull-interacties zijn: FHIR-read, FHIR-search. Deze interacties kunnen al dan niet zijn gebundeld in een FHIR-batch of in een FHIR-transaction.

Doel van de verschillende tokens:

1. Met het transactietoken voor berichtauthenticatie wordt aan de ontvanger bewezen dat een bepaalde persoon of organisatie instaat voor de authenticiteit van een gegeven bericht.
2. Met een mandaattoken wordt aan de ontvanger bewezen dat een bepaalde persoon (mandaatverlener) lokaal in een GBZ een door een URI geïdentificeerde mandaatregel heeft vastgelegd, die geldig is binnen deze organisatie.
3. Met een inschrijftoken wordt aan de ontvanger bewezen dat een bepaalde persoon, binnen een bepaalde organisatie, een bepaald BSN heeft gevalideerd.
4. Met een consent_token wordt aan de ontvanger bewezen dat een bepaalde persoon, binnen een bepaalde organisatie, (veronderstelde) toestemming heeft gekregen van een patiënt om bepaalde gegevens beschikbaar te stellen voor opvraag door een andere zorgaanbieder.

Zie ook [de VZVZ website](#) voor meer informatie over vereenvoudigd gebruik UZI-pas.

AORTA on FHIR specificaties - 0.7.22

Leeswijzer AoF - 0.7.x

De volgende specificaties zijn van toepassing voor leveranciers van xIS'en.

Overzichten:

- [Globaal ontwerp](#) - deze bevat een overzicht van de betrokken systemen/componenten en een set sequence diagrammen, waarin de flow die wordt gevolgd voor verschillende interacties is beschreven. **MUST-READ om te begrijpen hoe AORTA on FHIR werkt.**
- [Overzicht interacties, versies en systeemrollen](#) - deze bevat een overzicht van alle (versies van) HL7-FHIR en HL7v3 interacties en van de bijbehorende AORTA systeemrollen waarvoor een xIS kan worden gekwalificeerd en geaccepteerd.

Programma's van Eisen:

- [Programma van Eisen GBx](#) - deze bevat generieke eisen die van toepassing zijn op GBx-applicaties en GBx'en.

Use cases:

- [UC Resource Client](#) (initieerend xIS of reagerend xIS) - deze bevat te realiseren use cases, van waaruit interacties worden gestart met de Resource Broker.
- [UC Resource Server](#) (reagerend xIS) - deze bevat te realiseren use cases, waarbij een onderverdeling is gemaakt tussen
 - use cases die worden getriggert door een FHIR-interactie (xIS'en die een HL7-FHIR koppelvlak bieden).
 - use cases die worden getriggert door een HL7v3-interactie (xIS'en die een HL7v3 koppelvlak bieden).
 - use cases of use case onderdelen die van toepassing kunnen zijn op zowel FHIR- als op HL7v3-koppelvlakken.
 - in de use cases wordt verwezen naar een informatieblok "Gegevensdienst-specifieke UC extensions en implementatiehandleidingen". Dit informatieblok kun je vinden op de use cases pagina en het bevat verwijzingen naar de implementatiehandleidingen die van toepassing is op een bepaalde uitwisseling (HL7v3 of HL7-FHIR).
- [UC Workflow](#) - deze bevat use case extensions en use case template m.b.t. de verwerking van Taken en Notificaties.

Interfaces:

- [Interfaces common](#)
 - generieke eisen voor interfaces.
 - te retourneren HTTP statuscodes, headers en FHIR OperationOutcomes in diverse situaties (de uitzonderingen in de use cases verwijzen naar deze afhandeling).
- [Token specificaties](#) - inhoud van de gebruikte tokens.
- [AORTA FHIR-profielen](#) - AORTA-specifieke toepassing van core FHIR-profielen die worden gebruikt in infrastructurele interacties (bijv. m.b.t. ACT/VWI).
- [AORTA Stelsel Interfaces](#) - bevat interface voor het verkrijgen van een AORTA Stelseltoken, met informatie over adressen van componenten die een rol vervullen in het AORTA-netwerk.
- [Autorisatie Server Interfaces](#) - bevat een aantal interfaces die moeten worden gebruikt door Resource Clients voor het verkrijgen van access_tokens, en door Resource Servers t.b.v. controle van access_tokens (metadata en JWKS).
- [Resource Broker Interfaces](#) - bevat interfaces voor Resource Clients
 - voor infrastructurele interacties, bijv. TKID-activatie en interacties m.b.t. ACT/VWI.
 - om FHIR-interacties te kunnen initiëren.
- [Resource Server Interfaces](#) - deze bevat alle FHIR- en HL7v3-interfaces die kunnen worden gerealiseerd door een xIS.
- [Transformatie Server Interfaces](#) - interfaces t.b.v. transformatie tussen HL7-v3 en HL7-FHIR (wordt slechts gebruikt door de Resource Broker).
- [Workflow Interfaces](#) - bevat interfaces t.b.v. het gebruik van Taken en Notificaties.

Wijzigingen voor reeds op AoF 0.6 aangesloten bronsystemen:

1. AORTA Stelseltoken
 - a. Periodiek ophalen van AORTA Stelseltoken bij de AORTA Stelselnode.
2. Resource Endpoint
 - a. FHIR version toegevoegd aan base-URL van Resource Server indien hoger dan STU3.
3. JWK
 - a. Issuer van AORTA access_token moet zijn opgenomen in het AORTA Stelseltoken.
 - b. Cache-control header toegevoegd aan metadata en jwks responses.
 - c. Bij selectie juiste JWK, naast kid, ook kty en use attribuut gebruiken.
 - d. Metadata en JWK moeten worden opgehaald via GZN.
4. AORTA access_token
 - a. Kunnen verwerken van een nieuwe versie van AORTA access_token.
 - b. FQDN van client_id in AORTA access_token moet worden getoetst m.b.v. het AORTA Stelseltoken.
 - c. Ontvangers van een AORTA access_token dienen geen replay detectie te doen op het token, omdat de scope van een token meerdere interacties kan bevatten, die ook sequentieel kunnen worden uitgevoerd.

Changelog AoF - 0.7.x

- [Versiegeschiedenis](#)
- [Wijzigingen in document set versie 0.7.22](#)
- [Wijzigingen in document set versie 0.7.21](#)
- [Wijzigingen in document set versie 0.7.20](#)
- [Wijzigingen in document set versie 0.7.19](#)
- [Wijzigingen in document set versie 0.7.18](#)
- [Wijzigingen in document set versie 0.7.17](#)
- [Wijzigingen in document set versie 0.7.16](#)
- [Wijzigingen in document set versie 0.7.15](#)
- [Wijzigingen in document set versie 0.7.14](#)
- [Wijzigingen in document set versie 0.7.13](#)
- [Wijzigingen in document set versie 0.7.12](#)
- [Wijzigingen in document set versie 0.7.11](#)
- [Wijzigingen in document set versie 0.7.10](#)
- [Wijzigingen in document set versie 0.7.9](#)
- [Wijzigingen in document set versie 0.7.8](#)
- [Wijzigingen in document set versie 0.7.7](#)
- [Wijzigingen in document set versie 0.7.6](#)
- [Wijzigingen in document set versie 0.7.5](#)
- [Wijzigingen in document set versie 0.7.4](#)
- [Wijzigingen in document set versie 0.7.3](#)
- [Wijzigingen in document set versie 0.7.2](#)
- [Wijzigingen in document set versie 0.7.1](#)
- [Verschillen tussen 0.6 en 0.7.0](#)
- [Wijzigingen in branch voor doorontwikkeling t.o.v. laatst gepubliceerde document set](#)

Versiegeschiedenis

| Versie | Vastgesteld op |
|--------|----------------|
| 0.7.22 | 9-dec-2022 |
| 0.7.21 | 1-dec-2022 |
| 0.7.20 | 11-nov-2022 |
| 0.7.19 | 21-okt-2022 |
| 0.7.18 | 30-sep-2022 |
| 0.7.17 | 12-sep-2022 |
| 0.7.16 | 5-sep-2022 |
| 0.7.15 | 25-aug-2022 |
| 0.7.14 | 28-jul-2022 |
| 0.7.13 | 22-jul-2022 |
| 0.7.12 | 15-jul-2022 |
| 0.7.11 | 30-jun-2022 |
| 0.7.10 | 16-jun-2022 |
| 0.7.9 | 2-jun-2022 |
| 0.7.8 | 23-mrt-2022 |
| 0.7.7 | 23-feb-2022 |
| 0.7.6 | 11-feb-2022 |
| 0.7.5 | 8-feb-2022 |
| 0.7.4 | 28-jan-2022 |
| 0.7.3 | 21-jan-2022 |
| 0.7.2 | 14-jan-2022 |
| 0.7.1 | 12-jan-2022 |

Wijzigingen in document set versie 0.7.22

| # | Document | Samenvatting van de wijziging | Relevant voor | Impact op eis |
|---|---|---|---|-------------------|
| 1 | Component Logging, UC Autorisatie Server ZA, UC ACT/VWI Server, UC Adressering Server, UC RB APR, UC MAP Server, UC RB LOG, UC Transformatie Server | Generalisatie van component logging eisen, en onderscheid gemaakt in logging per type client. | Autorisatie Server ZA, ACT/VWI Server, Adressering Server, Resource Broker APR, MAP Server, SDS Server. Resource Broker LOG, Transformatie Server | |
| 2 | Transformatie Server Interfaces | Transformatie-id optioneel gemaakt als input parameter bij transformatie requests, zodat de 0.7 interface backwards compatible is met de 0.6 interface. | Transformatie Server, Resource broker VnC | AOF.TS-I. TGP.100 |
| 3 | UC Resource Broker ZA, UC RB Common | Correctie volgorde toetsing geldigheid van request en match tussen scope van access_token en request. | UC Resource Broker ZA-in | |

Wijzigingen in document set versie 0.7.21

| # | Document | Samenvatting van de wijziging | Relevant voor | Impact op eis |
|---|---|---|--|---|
| 1 | AORTA FHIR-profielen | Aanpassing FHIR-profiel voor Task t.b.v. notified-pull n.a.v. landelijke ontwikkelingen + verwijzing naar profiel op Simplifier. Task profiel voor VWI-sync verwijderd. Valt buiten scope van AoF 0.7. | Resource Client, Resource Server. | AOF.FP. TP.100 AOF.FP. SYNC.100 AOF.FP. NTFP.100 AOF.FP. DEV.100 AOF.FP. ORG.100 AOF.FP. PAT.100 |
| 2 | Resource Broker Interfaces, Token specificaties | Aanpassing endpoint adres van RB ZA-in en RB VnC. | Resource Client, Resource Broker ZA-in, Resource Broker VnC. | AOF.RB-I. AFR.100 AOF.RB-I. VCI.50 AOF.RB-I. VCI.100 |

Wijzigingen in document set versie 0.7.20

| # | Document | Samenvatting van de wijziging | Relevant voor | Impact op eis |
|---|--------------------------|--|---|-----------------|
| 1 | Token specificaties | Consent_token aangepast: <ul style="list-style-type: none"> • NameID moet worden weggelaten bij handtekening met servercertificaat. • Verplicht attribuut AuthnStatement.@AuthnInstant toegevoegd. | Resource Client, Autorisatie Server ZA | AOF.TS.ACT. 100 |
| 2 | AORTA Stelsel Interfaces | Beschrijving uit te voeren controles op AORTA Stelseltoken | Resource Client, Resource Server, Resource Broker | |

Wijzigingen in document set versie 0.7.19

| # | Document | Samenvatting van de wijziging | Relevant voor | Impact op eis |
|---|---|--|--|------------------|
| 1 | Autorisatie Server Interfaces | Opvragen metadata en JWKS bij Autorisatie Server moet via GZN. | Autorisatie Server MedMij, Autorisatie Server ZA, Resource Broker, Resource Server | AOF.AS-I.MTD.100 |
| 2 | UC Autorisatie Server ZA | Bij ontvangst PKIo Authenticatietoken of AORTA transactietoken ook toetsen of de contextcode overeenkomt met het token exchange request. | Autorisatie Server ZA | |
| 3 | Token specificaties, UC Resource Server | Bij interactie gericht aan Resource Server, client_id in AORTA access_token vullen met role-id van RB VnC in plaats van met appID=1. Expliciet gemaakt dat toets op client_id in AORTA access_token bij Resource Server plaats moet vinden m.b.v. het AORTA Stelseltoken. | Autorisatie Server ZA, Autorisatie Server MedMij, Resource Server | AOF.TS.AAT.400 |
| 4 | Token specificaties | Slechts componenten/servers die direct interactie hebben met GBx-applicaties opnemen in AORTA Stelseltoken. Voor componenten die slechts interacties hebben met andere componenten, en niet met GBx-applicaties, worden de URL's vooralsnog via configuratiedata gedeeld. | Autorisatie Server ZA, Resource Broker ZA-in, Resource Broker VnC | AOF.TS.AST.300 |
| 5 | UC Adressering Server | Toets toegevoegd m.b.t. of een destination in staat is verkeer te verwerken in de context van MedMij en/of voor zorgaanbieder-zorgaanbieder uitwisseling. | Adressering Server | |

Wijzigingen in document set versie 0.7.18

| # | Document | Samenvatting van de wijziging | Relevant voor | Impact op eis |
|---|--|--|--|-----------------------------------|
| 1 | UC Resource Broker VnC | Aangegeven wat (voorlopig) niet in scope valt van AoF 0.7 na afspraken in de werkverdeling. | Resource Broker VnC | |
| 2 | Token Specificaties | Mandaatverlener en autorisatieregel/context attributen verwijderd uit consent_token. Worden door Autorisatie Server ZA niet gebruikt. | Resource Client, Autorisatie Server ZA | AOF.TS.ACT.200 |
| 3 | UC Resource Server | Correctie. Resource Server die documenten oplevert moet deze altijd zelf in PDF/A formaat aanleveren. Nog geen transformatie mogelijk door Resource Broker. | Resource Server | |
| 4 | Resource Broker Interfaces, Workflow Interfaces, UC Workflow, UC Resource Broker ACT, UC Resource Server, UC Resource Client | Onderdelen die niet worden gerealiseerd in AoF 0.7 verwijderd of gemarkeerd dat ze nog niet worden gebruikt: <ul style="list-style-type: none"> • RB ACT/VWI Interface • Taak Uitvoering Interface • Taak Notificatie Interface | RB ACT/VWI, Resource Server, Resource Client | |
| 5 | AORTA FHIR-profielen, Token Specificaties | Aanpassingen n.a.v. aanscherping notified-pull voor BgZ. <ul style="list-style-type: none"> • Slechts één consent_token per Task instance toestaan. • Client_id van consent_token bevat altijd URA en nooit een appID • appID toegevoegd aan alle query_strings in Task.input | Resource Client, Resource Server | AOF.TS.ACT.200 AOF.FP.NTFP.100 |
| 6 | UC Resource Broker Common, UC Resource Server | Ontvangers van een AORTA access_token dienen geen replay detectie te doen op het token, omdat de scope van een token meerdere interacties kan bevatten, die ook sequentieel kunnen worden uitgevoerd. | Resource Broker, Resource Server | |

Wijzigingen in document set versie 0.7.17

| # | Document | Samenvatting van de wijziging | Relevant voor | Impact op eis |
|---|----------------------|---|---|--|
| 1 | UC Resource Server | Verhelderd dat situatie "BSN nog niet geverifieerd" valt onder de beschikbaarheidsvoorwaarde (zowel voor opvraag door patiënt zelf als voor opvraag door een zorgverlener). | Resource Server | - |
| 2 | AORTA FHIR-profielen | Aanpassingen Task profiel n.a.v. opstellen voorbeelden. | Resource Client, Resource Broker, Resource Server | AOF.FP.SYNC.100 AOF.FP.NTFP.100 AOF.FP.ORG.100 AOF.FP.PAT.100 |

| | | | | |
|---|---|---|---|---|
| 3 | Token Specificaties, Resource Broker Interfaces | <p>Waar van toepassing vulling van _vrb_client_id met role van RB MedMij-in.</p> <p>Naast role name ook een role-id toegevoegd voor gebruik in tokens. Impact op vulling van diverse tokens.</p> <p>Waar van toepassing, toevoeging van FQDN van Resource Client (GBx-applicatie) aan _vrb_client_id, zodat toetsing van match tussen TLS Client en _vrb_client_id door RB ZA-in kan worden uitgevoerd zonder opnieuw het APR te hoeven raadplegen.</p> <p>Verheldering vulling van _vrb_client_id en client_id claims in AORTA access_token.</p> <p>Aanpassing hasConformance response, zodat ook FQDN van een client wordt geretourneerd.</p> | Resource Broker, Autorisatie Server ZA, Autorisatie Server MedMij, RB APR | <p>AOF.TS. AST.300</p> <p>AOF.TS. AAT.400</p> <p>AOF.RB-I. ARI.500</p> <p>AOF.TS. PAT.100</p> <p>AOF.TS. ATT.100</p> <p>AOF.TS. AMT.100</p> <p>AOF.TS. AIT.100</p> <p>AOF.TS. ACT.100</p> |
|---|---|---|---|---|

Wijzigingen in document set versie 0.7.16

| # | Document | Samenvatting van de wijziging | Relevant voor | Impact op eis |
|---|--|--|---|--|
| 1 | Resource Server Interfaces | Verhelderd dat bij \$is-allowed tenminste de ontvankelijkheidscriteria, zoals gespecificeerd in MedMij dienen te worden getoetst. | Resource Server | AOF.RS-I. ISA.100 |
| 2 | Zorgaanbieder Flows, Resource Broker Interfaces, UC Resource Broker APR, Adressering Server Interfaces | <p>Schrijven van toegangsllog door Resource Broker expliciet opgenomen in flow.</p> <p>Wijziging van APR API: van getApplication naar meer functionele aanroepen.</p> <p>Verhelderd dat Adressering Server voorsnog APR-data ophaalt via ZORG-AB.</p> <p>FQDN toegevoegd aan response van getRoutingInfo, zodat Autorisatie Server ZA deze in het access_token kan stoppen.</p> <p>Verhelderd dat response objecten door de Adressering Server worden geretourneerd in de volgorde waarin de interactions werden ontvangen in het request.</p> | Resource Broker APR, Autorisatie Server ZA, Adressering Server, Resource Client | <p>AOF.ADS-I.RII.100</p> <p>AOF.RB-I. ARI.500</p> <p>AOF.RB-I. ARI.600</p> |

Wijzigingen in document set versie 0.7.15

| # | Document | Samenvatting van de wijziging | Relevant voor | Impact op eis |
|---|---|--|--|---|
| 1 | Zorgaanbieder Flows, Resource Broker Interfaces, UC Resource Broker LOG, UC Resource Broker Common, Token Specificaties | Toevoeging RB-logging Interface t.b.v. Volgjezorg. | Resource Client, Resource Broker, Autorisatie Server ZA, AORTA Stelselnode | <p>AOF.RB-I. RBL.100</p> <p>AOF.RB-I. RBL.200</p> <p>AOF.TS. AST.300</p> <p>AOF.TS. AAT.400</p> |
| 2 | Transformatie Server Interfaces | Cache-control header toegevoegd aan metadata response. | Transformatie Server, Adressering Server | AOF.TS-I. MDI.100 |
| 3 | Adressering Server Interfaces, Interfaces Common | <p>Destination attribuut hoeft niet altijd aanwezig te zijn in routing info request. Het gebruik ervan daarnaast ook verhelderd.</p> <p>Verheldering omgang met versie van interacties.</p> <p>Verheldering uitzondering "Ongeldig request".</p> | Resource Client, Adressering Server, Autorisatie Server ZA | <p>AOF.ADS-I.RII.100</p> <p>AOF.GS-I. HTR.100</p> |

Wijzigingen in document set versie 0.7.14

| # | Document | Samenvatting van de wijziging | Relevant voor | Impact op eis |
|---|---|-------------------------------|---|--|
| 1 | MAP Server Interface, UC MAP Server, UC Autorisatie Server ZA | Beschrijving van MAP API. | Autorisatie Server ZA, MAP | AOF.MAP-I.MI.100 |
| 2 | Resource Broker Interfaces, UC Resource Broker APR | Beschrijving van APR API. | Adressering Server, Autorisatie Server ZA, RB APR | AOF.RB-I.ARI.100 AOF.RB-I.ARI.300 AOF.RB-I.ARI.400 |

Wijzigingen in document set versie 0.7.13

| # | Document | Samenvatting van de wijziging | Relevant voor | Impact op eis |
|---|--|---|---|--|
| 1 | Zorgaanbieder Flows, Token specificaties, UC Resource Broker VnC | Toevoegen FQDN van GBx-server aan aud claim van AORTA access_token, zodat RB VnC géén call meer hoeft uit te voeren naar het APR. | Autorisatie Server ZA, Autorisatie Server MedMij, RB VnC, Resource Server | AOF.TS.AAT.400 |
| 2 | Interfaces Common | Verhelderd dat alle interfaces worden aangeboden via AORTA-net (GZN), tenzij anders is vermeld in de specificatie van een interface. | - | AOF.GS-I.GEN.100 |
| 3 | Zorgaanbieder Flows, UC Resource Client, UC Autorisatie Server ZA, Autorisatie Server Interfaces | Aanpassing n.a.v. security-review: Naar GBx-clients wordt slechts een enkelvoudige token exchange response geretourneerd. Vooralsnog niet mogelijk om een array van responses te ontvangen. Eerst ervaring opdoen met array bij interne verwerking van token responses (t.b.v. FHIR-operation) in resource broker. | Resource Client, Autorisatie Server ZA | AOF.AS-I.ATE.200 |
| 4 | Autorisatie Server Interfaces | AORTA-ID header toegevoegd als verplichte header bij ieder request op de AORTA Token Interface. | Autorisatie Server MedMij, Autorisatie Server ZA, Resource Broker MedMij-in, Resource Client, Resource Broker VnC | AOF.AS-I.ATI.100 |
| 5 | Autorisatie Server Interfaces | Scope van AORTA token exchange request moet verplicht ook interactie-id-set bevatten. | Autorisatie Server ZA, Resource Client | AOF.AS-I.ATE.200 |
| 6 | MedMij Flows, Autorisatie Server Interfaces, Adressering Server Interfaces, UC Adressering Server, UC Resource Broker Common, UC Resource Broker MedMij-in | Aanpassingen t.b.v. integratie RSv1 en RSv2 van LSP+. Voorbeelden toegevoegd. | Autorisatie Server MedMij, RB MedMij-in, Adressering Server, Resource Client, Autorisatie Server ZA | AOF.AS-I.MTE.200 AOF.ADS-I.RII.100 |
| 7 | Zorgaanbieder Flows, Token specificaties, Autorisatie Server Interfaces | Hanteren role van interne componenten in Audience van AORTA SAML Assertions en in _vrb_aud claim van het AORTA access_token. Idem. in audience van token exchange request. | Autorisatie Server ZA, Autorisatie Server MedMij, Resource Broker Componenten | AOF.TS.AST.300 AOF.TS.PAT.100 AOF.TS.ATT.100 AOF.TS.AMT.100 AOF.TS.AIT.100 AOF.TS.ACT.100 AOF.TS.AAT.400 AOF.AS-I.ATE.200 |

Wijzigingen in document set versie 0.7.12

| # | Document | Samenvatting van de wijziging | Relevant voor | Impact op eis |
|---|----------|-------------------------------|---------------|---------------|
|---|----------|-------------------------------|---------------|---------------|

| | | | | |
|---|--|---|---|--|
| 1 | Token specificaties, Autorisatie Server Interfaces | acr claim in AORTA access_token dient slechts informatie te geven over het authenticatieniveau van het subject, niet van de actor. actor_token in AORTA token exchange request kan slechts een AORTA transactietoken zijn. | Resource Client, Autorisatie Server ZA, Resource Server | AOF.TS. AAT.400 AOF.AS-I. ATE.200 |
| 2 | Token specificaties | Formaat van FHIR interaction-id in PKI authenticatietoken en in transactietoken gelijk getrokken met formaat op andere plaatsen. | Resource Client, Autorisatie Server ZA | AOF.TS. PAT.200 AOF.TS. ATT.200 |

Wijzigingen in document set versie 0.7.11

| # | Document | Samenvatting van de wijziging | Relevant voor | Impact op eis |
|---|---|---|---|---|
| 1 | UC Adressering Server | Adressering Server levert ook applD voor instance-level interacties (read, update, delete). | Resource Client, AS-componenten, Adressering Server | |
| 2 | Token specificaties | Aanpassingen t.b.v. Corona Vaccinatie connector: <ul style="list-style-type: none"> Toestaan COA nummer in transactietoken, PKI authenticatietoken, inschrijftoken, consent_token en AORTA access_token. Toestaan hash van BSN in transactietoken, PKI authenticatietoken, consent_token en AORTA access_token. | Resource Client, AS-componenten, Resource Server | AOF.TS. PAT.200 AOF.TS. ATT.200 AOF.TS. AIT.100 AOF.TS. ACT.200 AOF.TS. AAT.400 |
| 3 | Interfaces Common, AORTA Stelsel Interfaces, Token specificaties, UC Resource Server, UC Resource Broker Common, UC Resource Client | Introductie van AORTA Stelseltoken om te borgen dat slechts wordt gecommuniceerd met vertrouwde servers in het AORTA netwerk. Ook van toepassing bij ophalen van metadata /JWKS bij Autorisatie Server. | Resource Client, RB- componenten, AS-componenten, AORTA Stelselnode, Resource Server. | AOF.GS-I. GEN.100 |
| 4 | Zorgaanbieder Flows | Aanscherping van API-gebruik in de zorgaanbieder-zorgaanbieder flows | Resource Client, RB- componenten, AS-componenten | |

Wijzigingen in document set versie 0.7.10

| # | Document | Samenvatting van de wijziging | Relevant voor | Impact op eis |
|---|--|--|--|--|
| 1 | UC Resource Broker ZA-in, UC Resource Broker Common | Verheldering van autorisatietoets in componenten. | RB ZA-in, RB VnC | - |
| 2 | Autorisatie Server Interfaces, UC Autorisatie Server ZA | Bevinding n.a.v. security review: <ul style="list-style-type: none"> subject_token hoort een verplicht attribuut te zijn in een token exchange request. | Resource Client, AS ZA | AOF.AS-I. ATE.200 |
| 3 | Autorisatie Server Interfaces | Bevinding n.a.v. security review: <ul style="list-style-type: none"> Audience attribuut in MedMij token exchange request moet conform RFC 8693 worden herhaald indien meerdere audiences worden gevraagd. Dus geen comma-separated attribuut. | AS Medmij | AOF.AS-I. MTE.200 |
| 4 | UC Resource Server, UC Resource Broker Common | Bevinding n.a.v. security review: <ul style="list-style-type: none"> Bij selectie juiste JWK, naast kid, ook kty en use attribuut gebruiken. | RB *-in, RB VnC, Resource Server | - |
| 5 | Adressering Server Interfaces, Resource Server Interfaces, Token specificaties, UC Resource Broker VnC, UC Adressering Server, UC Autorisatie Server ZA, Zorgaanbieder Flows, UC Resource Broker ZA-in, UC Resource Client, UC Autorisatie Server Common | Toevoeging Adressering Server | Adressering Server, RB ZA-in, AS ZA, RB VnC, Resource Client | AOF.RS-I. FRI.200 AOF.TS. AAT.400 |

Wijzigingen in document set versie 0.7.9

| # | Document | Samenvatting van de wijziging | Relevant voor | Impact op eis |
|---|--|--|---------------|--|
| 1 | Transformatie Server Interface, UC Transformatie Server, UC Resource Broker VnC | <p>TS Metadata Interface toegevoegd.</p> <p>Protocol_in en protocol_out op generieke transformatie request interface aangevuld met een transformation-id. De protocol-velden wijzen namelijk niet eenduidig naar één mogelijke transformatie. Response bevat nu ook interaction-id van output bericht.</p> <p>Vulling contentVersion in response o.b.v. interaction-id in transformatieresponse bericht.</p> | LSP+, LSP | <p>AOF.TS-I. OTR.100</p> <p>AOF.TS-I. MDI.100</p> <p>AOF.TS-I. FTR.100</p> <p>AOF.TS-I. FOT.100</p> <p>AOF.TS-I. TGP.100</p> <p>AOF.TS-I. TGP.200</p> <p>AOF.TS-I. FAP.100</p> |
| 2 | Token specificaties | OID voor AORTA requestID toegevoegd | LSP, GBZ | <p>AOF.TS. ATT.200</p> <p>AOF.TS. PAT.200</p> |
| 3 | Token Specificaties, Resource Server Interfaces | ID van consent_token toegevoegd aan AORTA access_token, zodat consent_token zelf niet hoeft te worden doorgegeven aan resource servers (GBZ-applicaties). | LSP, GBZ | <p>AOF.TS. AAT.400</p> <p>AOF.RS-I. FRI.100</p> |
| 4 | Zorgaanbieder Flows, Autorisatie Server Interfaces, Resource Broker Interfaces, Resource Server Interfaces, Token Specificaties, UC Autorisatie Server ZA, UC Resource Broker Common, UC Resource Broker ZA-in, UC Resource Broker VnC, UC Resource Client, UC Resource Server | Wijziging flow i.v.m. te grote tokens. Token exchange nu door client. | LSP, GBZ | <p>AOF.AS-I. ATE.100</p> <p>AOF.AS-I. ATE.200</p> <p>AOF.TS. AAT.400</p> <p>AOF.RS-I. FRI.200</p> |

Wijzigingen in document set versie 0.7.8

| # | Document | Samenvatting van de wijziging | Relevant voor | Impact op eis |
|---|------------------------------|---|---------------|---|
| 1 | UC Resource Broker MedMij-in | Integratie functionaliteit van resource server v1 (generieke query en vertaling) in RB Medmij-in. | LSP+ | AOF.RBM.VMI.100 |
| 2 | Token specificaties | Namingsysteem van act.sub van het AORTA access_token, voor applID casus gecorrigeerd. | LSP, GBZ | AOF.TS.AAT.400 |
| 3 | AORTA FHIR-profielen | Ook gebruik van FHIR namingsystem notatie toestaan in profielen voor Device, Organization en Patient. | LSP, GBZ | <p>AOF.FP.DEV.100</p> <p>AOF.FP.ORG.100</p> <p>AOF.FP.PAT.100</p> |

Wijzigingen in document set versie 0.7.7

| # | Document | Samenvatting van de wijziging | Relevant voor |
|---|----------|-------------------------------|---------------|
|---|----------|-------------------------------|---------------|

| | | | |
|---|---|---|-----------|
| 1 | UC Resource Broker Common, UC Resource Broker MedMij-in, UC Resource Broker ZA-in | Toelichting op wijze van controleren of een request binnen de scope van een gegevensdienst of contextCode valt. | LSP+, LSP |
| 2 | UC Resource Broker Common, UC Resource Broker ACT, UC Resource Broker VnC, UC Resource Broker MedMij-in, UC Resource Broker ZA-in, UC Autorisatie Server ZA | <p>Hergebruik middels UC extensions voor RB:</p> <ul style="list-style-type: none"> • UC extension: Inhoudelijke toetsing request • UC extension: Toetsing tokens bij inkomend request • UC extension: Toetsing van een intern RB-request • UC extension: Toetsing scope van request • UC extension: Toetsing request en contextCode • UC extension: Adressering van request • UC extension: Screening van response <p>Token controles voor AS ZA ondergebracht in UC Autorisatie Server ZA.</p> | LSP |

Wijzigingen in document set versie 0.7.6

| # | Document | Samenvatting van de wijziging | Relevant voor |
|---|---|---|----------------|
| 1 | UC Resource Broker MedMij-in | Verwijderen algoritme voor afhandeling meervoudige scope. | LSP+ |
| 2 | AORTA FHIR-profielen | <p>Task.owner toegevoegd aan Task profiel voor notified-pull.</p> <p>Task kan meerdere consent_tokens bevatten.</p> <p>Organization kan een afdeling representeren.</p> | GBZ |
| 3 | Token specificaties | <p>Vulling van NotOnOrAfter in consent_token laten bepalen door zorgtoepassing.</p> <p>Consent_token mag ook worden getekend m.b.v. servercertificaat (vereenvoudigd gebruik UZI-pas).</p> <p>BSN in SAML tokens opnemen in urn:oid formaat.</p> | GBZ |
| 4 | Zorgaanbieder Flows, Resource Broker Interfaces, Resource Server Interfaces | Header toegevoegd voor doorgeven AORTA consent_token. | LSP, GBZ |
| 5 | Resource Server Interfaces, Resource Broker Interfaces | <p>FHIR version en, waar van toepassing "broker", toegevoegd aan base-URL voor:</p> <ul style="list-style-type: none"> • AORTA CapabilityStatement Interface • AORTA FHIR Resource Interface • AORTA FHIR Resource Broker Interface • Verzending & Consolidatie Interface • Actualiteitsregister Interface | LSP+, LSP, GBZ |
| 6 | Workflow Interfaces, UC Resource Broker ACT | <p>Notificatie kan in de HTTP body ook een Task instance bevatten.</p> <p>RB ACT includeert Task in notificatie en retourneert foutmelding bij een FHIR-read op Task.</p> | LSP, GBZ |
| 7 | UC Autorisatie Server ZA | <p>Slechts toestemming toetsen wanneer gegevens worden opgevraagd.</p> <p>Aanpassingen m.b.t. toetsing autorisatie voor interne componenten.</p> | LSP |
| 8 | UC Resource Broker ZA-in | <p>Toetsing op verplichte aanwezigheid inschrijftoken en mandaattoken, bij tekening met servercertificaat, verwijderd, zodat ook interacties kunnen worden verwerkt op vertrouwensniveau laag. Geldt voor transactietoken en consent_token.</p> <p>Aanpassingen m.b.t. toetsing autorisatie voor interne componenten.</p> | LSP |

Wijzigingen in document set versie 0.7.5

| # | Document | Samenvatting van de wijziging | Relevant voor |
|---|--|---|----------------|
| 1 | Autorisatie Server Interfaces | <p>Aanpassing n.a.v. security review:</p> <ul style="list-style-type: none"> • Cache-control header gespecificeerd voor metadata en jwks responses | LSP+, LSP, GBZ |
| 2 | Zorgaanbieder Flows, Token specificaties, Autorisatie Server Interfaces, Resource Broker Interfaces, UC Resource Server, UC Resource Broker Common, UC Resource Broker VnC, UC Resource Broker ACT | Flows voor routing naar interne RB componenten (LOG en ACT/WI) aangepast. | LSP |

Wijzigingen in document set versie 0.7.4

| # | Document | Samenvatting van de wijziging | Relevant voor |
|---|---|---|---------------|
| 1 | UC Resource Broker VnC | Toelichting op vulling AORTA-Version header in response. | LSP |
| 2 | UC Autorisatie Server ZA | Aanpassing gebruik van MAP. | LSP |
| 3 | Token specificaties, UC Resource Broker ZA-in | Ook toestaan dat een consent_token wordt uitgegeven m.b.v. vereenvoudigd gebruik UZI-pas. | LSP |

Wijzigingen in document set versie 0.7.3

| # | Document | Samenvatting van de wijziging | Relevant voor |
|---|--|--|----------------|
| 1 | Autorisatie Server Interfaces, Resource Broker Interfaces | Op te leveren logging aan CCDA aangepast n.a.v. security review: <ul style="list-style-type: none"> • jti claim van subject_token i.p.v. gehele subject_token • hash van authorization code i.p.v. code zelf | LSP+ |
| 2 | Token specificaties | Aanpassing mogelijke waarden voor attest claim. Eigen waarde voor toetsing consent_token toegevoegd, zodat een bronsysteem dit kan onderscheiden van een reguliere toestemming die is vastgelegd bij de bronhouder. | LSP |
| 3 | Autorisatie Server Interfaces | Metadata response voor AS ZA aangepast n.a.v. security review: <ul style="list-style-type: none"> • authorization_endpoint verwijderd | LSP |
| 4 | Resource Broker Interfaces | Aanpassing n.a.v. security review: <ul style="list-style-type: none"> • Bij meesturen van tokens het type aanduiden middels Bearer (dus conform standaard) en niet langer als SAML2-Bearer of JWT-Bearer. Het type kan worden bepaald door de samenstelling van de ontvangen string. • Cache-control headers verwijderd op interface van RB VnC. Zijn hier overbodig, omdat gebruik wordt gemaakt van de standaard Authorization header. | LSP+, LSP |
| 5 | Workflow Interfaces | Toevoeging Task.code aan notificaties m.b.t. een Task, zodat ontvangers op basis hiervan notificaties intern kunnen routeren. | LSP, GBZ |
| 6 | AORTA FHIR-profielen | Attribuut restriction.period toegevoegd aan Task voor notified-pull. | GBZ |
| 7 | Resource Broker ZA-in | Aanpassing n.a.v. security review: <ul style="list-style-type: none"> • CRL-controle specifiek gemaakt voor type ontvangen token. | LSP |
| 8 | UC Resource Server, UC Workflow, UC Autorisatie Server MedMij, UC Autorisatie Server ZA, UC Resource Broker MedMij-in, UC Resource Broker ZA-in, UC Resource Broker VnC, UC Resource Broker ACT, UC Transformatie Server | Aanpassing n.a.v. security review: <ul style="list-style-type: none"> • Logging in use case zodanig beschreven dat altijd alle requests en responses worden gelogd. | LSP+, LSP, GBZ |

Wijzigingen in document set versie 0.7.2

| # | Document | Samenvatting van de wijziging | Relevant voor |
|---|---|--|---------------|
| 1 | UC Resource Broker MedMij-in | Verheldering verwerking wanneer meerdere gegevensdiensten in scope van MedMij access_token. | LSP+ |
| 2 | UC Autorisatie Server ZA | Aanpassing MAP regel: gebruiksinteractie i.p.v. operatie. Aanpassing toets consent_token. | LSP |
| 3 | Token specificaties, UC Resource Broker ZA-in | Aanscherping consent_token. | LSP, GBZ |
| 4 | UC Resource Client, UC Resource Server | Aanpassing benodigde systeemrollen in overzichtsplaten. | GBZ |

Wijzigingen in document set versie 0.7.1

| # | Document | Samenvatting van de wijziging | Relevant voor |
|---|--|--|----------------|
| 1 | Globaal Ontwerp, Token Specificaties, AORTA FHIR-profielen, Autorisatie Server Interfaces, UC Workflow, UC Resource Client, UC Resource Server, UC Autorisatie Server ZA, UC Resource Broker Common, UC Resource Broker ZA-in, UC Resource Broker VnC, UC Resource Broker ACT. | Toevoeging notified-pull. | LSP, GBZ |
| 2 | Alle UC pagina's en Globaal Ontwerp. | Update ArchiMate modellen. Heeft geen inhoudelijke impact. | LSP+, LSP, GBZ |

Verschillen tussen 0.6 en 0.7.0

Onderstaande tabel bevat een overzicht van de wijzigingen in de 0.7.0 versie t.o.v. de laatste 0.6.x versie, die relevant zijn voor partijen die oorspronkelijk hebben gebouwd conform versie 0.6.x.

| # | Samenvatting van de wijziging | Relevant voor |
|---|---|--------------------------|
| 1 | ZA-ZA uitwisseling met ondersteuning van transactietoken, mandaattoken en inschrijftoken (dus inclusief mandatering en opvraag door systeem) <ul style="list-style-type: none"> ▪ organisatie-search, applicatie-search, create, read, update, batch en transaction ▪ introductie RB ZA-in, AS ZA | LSP, Initiërend GBZ |
| 2 | Toetsing MAP | LSP, Reagerend GBZ |
| 3 | Toetsing Mitz | LSP, Reagerend GBZ |
| 4 | ACT/VWI interacties <ul style="list-style-type: none"> • introductie RB-ACT | LSP, Initiërend GBZ |
| 5 | Notify t.b.v. ACT/VWI-sync | LSP, Initiërend GBZ |
| 6 | Nieuwe versie van AORTA access_token | LSP+, LSP, Reagerend GBZ |
| 7 | Aanpassing interface Resource Broker VnC | LSP+, LSP |

Wijzigingen in branch voor doorontwikkeling t.o.v. laatst gepubliceerde document set

| # | Document | Samenvatting van de wijziging | Relevant voor | Impact op eis | Status van de wijziging | Publicatie gepland in versie |
|---|----------------------------|---|---------------|---------------|---|------------------------------|
| 1 | Interfaces Common | Aanpassing en aanscherping foutafhandeling voor zoekparameters. | LSP+, GBZ | | Heeft ook impact op M MKP-258 . Navragen impact bij Itzos. | 0.8 |
| 2 | Resource Broker Interfaces | Aanpassing ACT/VWI interface. Regulier resource.id gaan gebruiken, en daarmee ook create en update. | LSP | | Gestart | 0.8 |

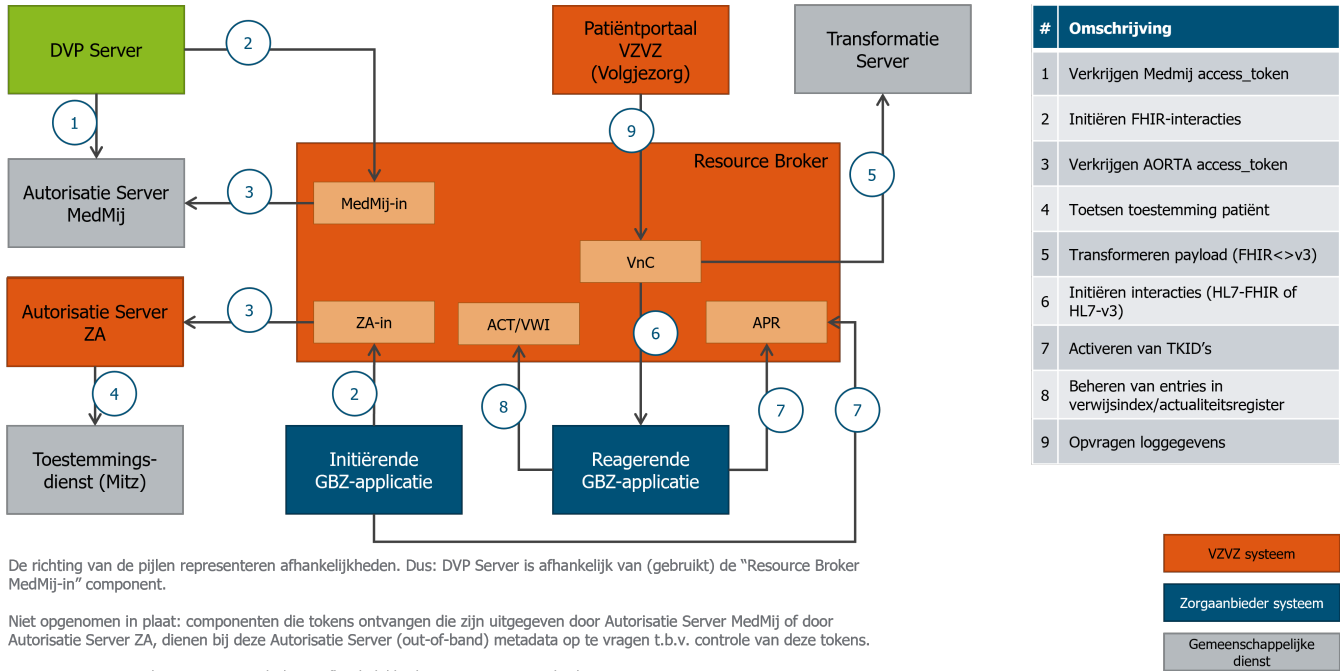
| | | | | | | |
|---|---|---|---|--|---------|-----|
| 3 | UC Resource Client, Adressering Server Interfaces, Autorisatie Server Interfaces, Resource Broker Interfaces, Token specificaties, SOAP Sender Interfaces UC Adressering Server, UC Autorisatie Server ZA, UC Resource Broker SDS, UC Resource Broker ZA-in, UC SOAP Sender, UC Resource Broker VnC | Aanpassingen t.b.v. AoF 0.8. | Resource Client, Adressering Server, Autorisatie Server ZA, Resource Broker | AOF.AS-I.ATE.200 AOF.TS.AAT.500 AOF.RB-I.SDI.100 AOF.SOAP-I.SI.100 AOF.ADS-I.RII.100 | Gestart | 0.8 |
| 4 | Token specificaties | Aanpassen scope van AORTA access_token naar SMART-on-FHIR v2. Ook fine-grained scope (t.b.v. FHIR operation). | | | Gereed | 0.8 |
| 5 | Interfaces Transformatie Server | Toevoeging van transformaties van v3 naar v3. | Transformatie Server, Resource Broker VnC | AOF.TS-I.PV3.200 AOF.TS-I.PV3.300 AOF.TS-I.PV3.500 AOF.TS-I.PV3.600 AOF.TS-I.PV3.700 | Gereed | 0.8 |
| 6 | Token specificaties | Consent_token mag slechts worden gesigned met een UZI-servercertificaat. | Resource Client, Autorisatie Server ZA | | Gereed | 0.8 |
| 7 | UC Resource Broker VnC, Interfaces Resource Server | Opvragen CapabilityStatement bij Resource Server moet werken voor zowel STU3 als voor R4. | UC Resource Broker VnC, Resource Server | | Gereed | 0.8 |

Globaal ontwerp - 0.7.x

- Vereenvoudigd overzicht van AORTA-on-FHIR
- Overzicht systemen en interfaces

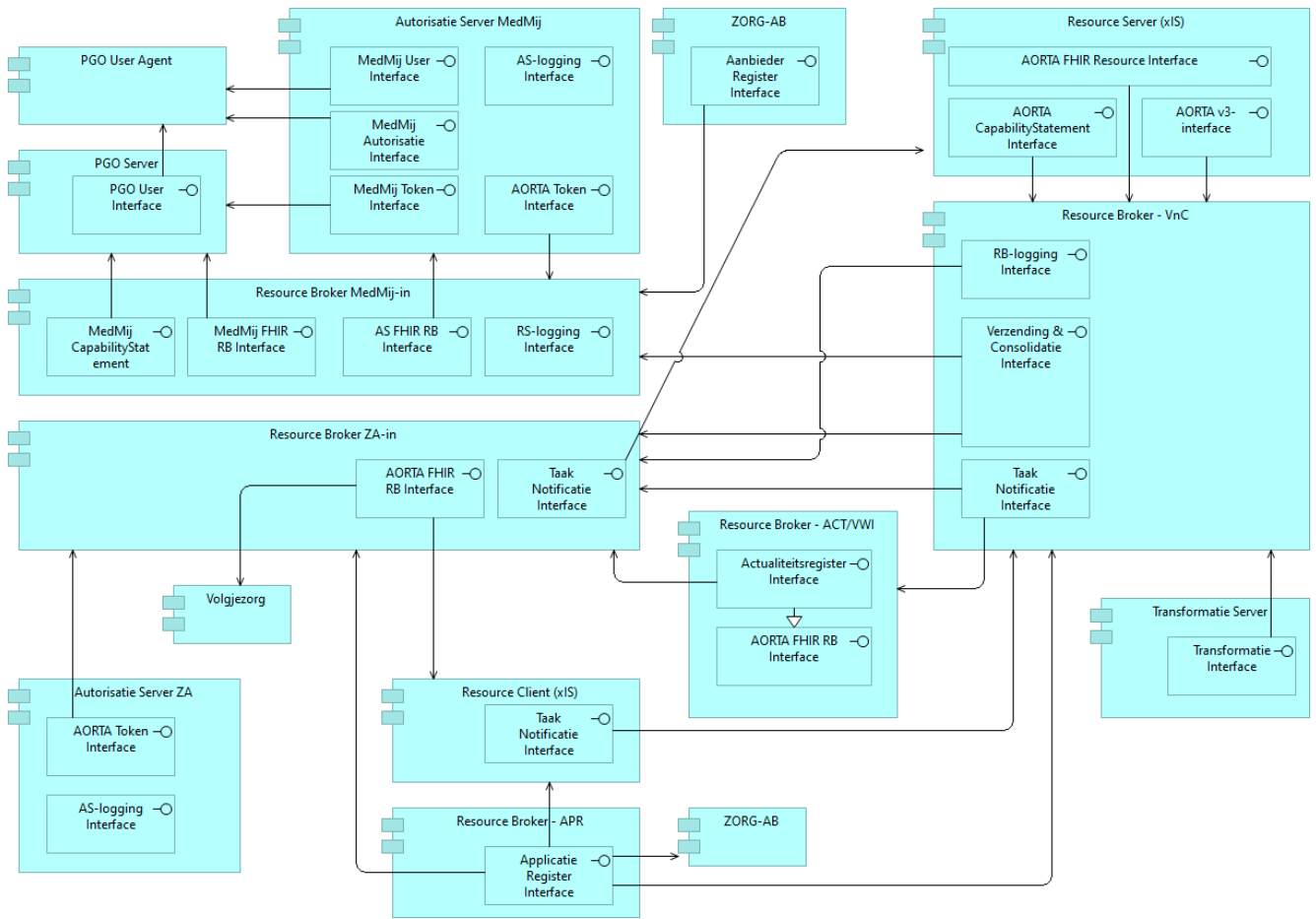
Vereenvoudigd overzicht van AORTA-on-FHIR

Onderstaande figuur toont een vereenvoudigde weergave van de AORTA-on-FHIR architectuur op systeem- en componentniveau.



Overzicht systemen en interfaces

Onderstaande figuur toont een overzicht van alle betrokken systemen en interfaces.



MedMij Flows - 0.7.x

- [MedMij autorisatieflow](#)
 - [Autorisatie MedMij](#)
- [MedMij resource flows](#)
 - [FHIR-interactie bij één organisatie](#)
 - [Uitvoeren van \\$is-allowed operation](#)

In alle diagrammen wordt aangegeven:

- welke interfaces worden gebruikt;
- vanuit welke use cases dit wordt gedaan;
- welke use cases middels deze interfaces worden gestart.

MedMij autorisatieflow

[Autorisatie MedMij](#)

MedMij resource flows

[FHIR-interactie bij één organisatie](#)

[Uitvoeren van \\$is-allowed operation](#)

Zorgaanbieder Flows - 0.7.x

- [Flows voor GBP/GBK](#)
 - [FHIR-search voor Toegangslog](#)
- [Flows voor ZA-ZA uitwisseling](#)
 - [FHIR-interactie bij één applicatie of organisatie - inclusief batch/transaction](#)
 - [Notified Pull](#)

In alle diagrammen wordt aangegeven:

- welke interfaces worden gebruikt;
- vanuit welke use cases dit wordt gedaan;
- welke use cases middels deze interfaces worden gestart.

Flows voor GBP/GBK

[FHIR-search voor Toegangslog](#)

Flows voor ZA-ZA uitwisseling

[FHIR-interactie bij één applicatie of organisatie - inclusief batch/transaction](#)

[Notified Pull](#)

1. [Aanmaken van taak door verzender bij en voor de ontvanger](#)
2. [Opragen van gegevens door de ontvanger, bij de verzender](#)

Interfaces - 0.7.x

Interfaces Common - 0.7.x

- [Generieke eisen voor alle server-to-server interfaces](#)
- [Mapping tussen OID en FHIR-based namingsystems](#)
- [HTTP-response](#)

Generieke eisen voor alle server-to-server interfaces

AOFGS-I.GEN.100.v3

De volgende eisen gelden voor alle server-to-server interfaces:

1. HTTP-requests en -responses worden verzonden conform HTTP versie 1.1.
2. Tenzij anders vermeld in de specificatie van een interface, worden interfaces slechts aangeboden op AORTA-net, dus via een GZN.
3. Alle HTTP-verkeer wordt verzonden binnen een TLS verbinding, waarbij verplicht gebruik wordt gemaakt van tweezijdige server authenticatie. Uitzonderingen hierop zijn:
 - a. Op de AORTA CapabilityStatement Interface wordt slechts server authenticatie vereist, maar mag de resource server ook client authenticatie vereisen.
 - b. Op de AS Metadata Interface wordt slechts server authenticatie toegepast.
4. TLS clients en TLS servers dienen tenminste TLS versie 1.2 te ondersteunen en mogen hierbij slechts gebruik maken van een ciphersuite uit de categorie "Goed", zoals genoemd in bijlage C van de [ICT-beveiligingsrichtlijnen voor Transport Layer Security \(TLS\)](#).
5. TLS clients en TLS servers maken bij voorkeur echter gebruik van een hogere TLS versie.
6. Server authenticatie vindt plaats middels PKI servercertificaten of, voor zorgaanbieders, m.b.v. UZI-servercertificaten.
7. Voor alle op FHIR gebaseerde interfaces gelden de [generieke eisen uit de MedMij informatiestandaarden](#). Dit betekent ondermeer dat zowel JSON als XML moet worden ondersteund.
8. Een request dat wordt gericht aan een type server die is opgenomen in de lijst met server rollen van het [AORTA Stelseltoken](#), mag slechts worden gericht aan een server die deze rol bijkiens het AORTA Stelseltoken ook daadwerkelijk heeft. Het geldende AORTA Stelseltoken dient periodiek te worden opgehaald via de [AORTA Stelsel Metadata Interface](#). De aangeven caching directives dienen hierbij te worden gevolgd. Voorbeelden:
 - a. Resource Broker VnC dient de base-URL van de Transformatie Server te verkrijgen via het AORTA Stelseltoken.
 - b. Bij controle van een AORTA access_token dient de issuer van het access_token te zijn opgenomen als een Autorisatie Server in het AORTA Stelseltoken.
 - c. Een Resource Client (xIS) dient de base-URL van Resource Broker ZA-in te verkrijgen via het AORTA Stelseltoken.

Mapping tussen OID en FHIR-based namingsystems

Onderstaande tabel bevat een mapping van de binnen AORTA on FHIR gehanteerde namingsystems.

| OID | URI | Description |
|-----------------------------------|---|--|
| 2.16.528.1.1007.3.1 | http://fhir.nl/fhir/NamingSystem/uzi-nr-pers | Uniek Zorgverlener Identificatienummer Personen |
| 2.16.528.1.1007.3.2 | http://fhir.nl/fhir/NamingSystem/uzi-nr-sys | UZI nummer van systeem, gekoppeld aan UZI services certificaat |
| 2.16.528.1.1007.3.3 | http://fhir.nl/fhir/NamingSystem/ura | UZI-register abonneenummer |
| 2.16.840.1.113883.2.4.3.11.8 | http://fhir.nl/fhir/NamingSystem/aorta-rolcode | Zie: https://www.nictiz.nl/wp-content/uploads/OID-ovrzicht-150819.pdf |
| 2.16.840.1.113883.2.4.3.11.25 | - | Organisatie-id in het kader van AORTA. |
| 2.16.840.1.113883.2.4.3.111.8 | - | AORTA Component rollen |
| 2.16.840.1.113883.2.4.3.111.1.5.1 | http://fhir.nl/fhir/NamingSystem/aorta-contextcode | AORTA contextcode |
| 2.16.840.1.113883.2.4.3.111.1.5.4 | - | AORTA requestID |
| 2.16.840.1.113883.2.4.6.1 | http://fhir.nl/fhir/NamingSystem/agb-z | Vektis AGB-z zorgverlener tabel |
| 2.16.840.1.113883.2.4.6.3 | http://fhir.nl/fhir/NamingSystem/bsn | Burgerservicenummer |
| 2.16.840.1.113883.2.4.6.6 | http://fhir.nl/fhir/NamingSystem/aorta-app-id | Applicatie ID binnen de AORTA infrastructuur |
| 2.16.840.1.113883.2.4.15.4 | http://fhir.nl/fhir/NamingSystem/aorta-gegevenssoort | AORTA gegevenssoort |
| 2.16.840.1.113883.2.4.15.111 | http://fhir.nl/fhir/NamingSystem/uzi-rolcode | UZI rolcode |
| - | http://fhir.nl/fhir/NamingSystem/aorta-taskcode | Codesysteem voor AORTA Task.code |

| | | |
|---|---|---|
| - | http://fhir.nl/fhir/NamingSystem/medmij-scope | Scope attribuut, zoals gehanteerd in de MedMij authorization flow |
|---|---|---|

HTTP-response

AOF.GS-I.HTR.100.v3

Wanneer een resource server een uitzondering/foutsituatie detecteert, dan dient het dit aan te geven in de HTTP-response. Een uitzondering kan op een aantal verschillende manieren worden gecommuniceerd, vaak ook middels een combinatie ervan:

- De HTTP statuscode;
- Een HTTP Authenticate response header;
- Een FHIR OperationOutcome, met hierin ondermeer de volgende attributen
 - issue.severity (verplicht), deze moet passend zijn voor de situatie en in lijn zijn met de geretourneerde HTTP statuscode;
 - issue.code (verplicht);
 - issue.details (optioneel in FHIR, maar indien aangegeven in onderstaande tabel verplicht te vullen conform de aangegeven valueset;
 - issue.diagnostics (optioneel in FHIR, optioneel binnen AORTA, waarbij altijd de beveiliging van de resource server in ogenschouw moet worden genomen).

De resource server retourneert fouten conform https://informatiastandaarden.nictiz.nl/wiki/MedMij:V2020.01/FHIR_IG#Handling_errors en <http://hl7.org/fhir/STU3/search.html#errors>. De te retourneren HTTP statuscode en mee te sturen aanvullende informatie, is opgenomen in onderstaande tabel.

In de bijbehorende use cases is gespecificeerd welke situaties gedetecteerd dienen te worden. Niet alle situaties zijn van toepassing op iedere use case.

| Gedetecteerde situatie | Response |
|---|--|
| Succes | statuscode 200 |
| Resource broker success | statuscode 200 <ul style="list-style-type: none"> • Wanneer één of meerdere van de achterliggende resource servers een fout heeft geretourneerd (anders dan het niet voldoen aan de MedMij beschikbaarheidsvoorwaarde), dan wordt voor ieder van deze resource servers een OperationOutcome toegevoegd met issue.severity "warning", issue.code "processing" en issue.diagnostics "<de betreffende appID>". |
| Ongeldig verzoek (de ontvangen interactie is ongeldig, voldoet niet aan de specificaties - deze situatie kan ook ontstaan doordat een verplichte header, niet zijnde een security token, ontbreekt of ongeldig is) | statuscode 400 <ul style="list-style-type: none"> • Wanneer een verplichte FHIR zoekparameter ontbreekt, dan wordt een OperationOutcome met issue.code "required" en de van toepassing zijnde issue.details geretourneerd • Wanneer een FHIR zoekparameter een ongeldige waarde heeft, dan wordt een OperationOutcome met issue.code "value" en de van toepassing zijnde issue.details geretourneerd; • Bij ontvangst van een FHIR zoekparameter die niet is gespecificeerd binnen de gegevensdienst wordt een OperationOutcome met issue.code "not-supported" en de van toepassing zijnde issue.details geretourneerd. • Wanneer een ontvangen FHIR resource instance ongeldig is, dan wordt een OperationOutcome met issue.code "invalid" en de van toepassing zijnde issue.details geretourneerd. • In deze situatie wordt, indien van toepassing, conform RFC 6750, ook een WWW-Authenticate HTTP response header met als auth-scheme "Bearer" en een error attribuut met waarde "invalid_request" geretourneerd. |
| Ongeldige notificatie | statuscode 400 |
| Een verplicht token ontbreekt | statuscode 401 <ul style="list-style-type: none"> • In deze situatie wordt geen nadere informatie over de opgetreden fout geretourneerd. |
| Ongeldig token (een ontvangen token is niet geldig, of kan niet worden gevalideerd) | statuscode 401 <ul style="list-style-type: none"> • In deze situatie wordt, conform RFC 6750, ook een WWW-Authenticate HTTP response header met als auth-scheme "Bearer" en een error attribuut met waarde "invalid_token" geretourneerd. • In deze situatie mag daarnaast ook een OperationOutcome met issue.code "security" worden geretourneerd. |

| | |
|---|--|
| Request van deze client mag niet worden verwerkt, bijvoorbeeld "de PGO server komt niet voor op de MedMij whitelist". | <p>statuscode 403</p> <ul style="list-style-type: none"> In deze situatie wordt geen nadere informatie over de opgetreden fout geretourneerd. |
| <p>De client beschikt niet over de juiste autorisatie, bijvoorbeeld</p> <ul style="list-style-type: none"> een xIS probeert een TKID te activeren voor een ander xIS. mismatch tussen BSN in AORTA access_token en BSN in ontvangen gegevens. | <p>statuscode 403</p> <ul style="list-style-type: none"> Indien een <code>Authorization</code> header werd gebruikt in het request, dan wordt in deze situatie, conform RFC 6750, een <code>WWW-Authenticate</code> HTTP response header met als auth-scheme "Bearer" en een <code>error</code> attribuut met waarde "access_denied" geretourneerd. Indien het een FHIR-request betreft, dan wordt in deze situatie (ook) een <code>OperationOutcome</code> met <code>issue.code</code> "forbidden" geretourneerd. |
| Niet voldaan aan (MedMij) beschikbaarheidsvoorwaarde | <p>statuscode 403</p> <ul style="list-style-type: none"> In deze situatie wordt, conform RFC 6750, een <code>WWW-Authenticate</code> HTTP response header met als auth-scheme "Bearer" en een <code>error</code> attribuut met waarde "access_denied" geretourneerd. In deze situatie wordt een <code>OperationOutcome</code> met <code>issue.code</code> "suppressed" geretourneerd. |
| Scope niet toereikend voor interactie | <p>statuscode 403</p> <ul style="list-style-type: none"> In deze situatie wordt, conform RFC 6750, ook een <code>WWW-Authenticate</code> HTTP response header met als auth-scheme "Bearer" en een <code>error</code> attribuut met waarde "insufficient_scope" geretourneerd. In deze situatie mag daarnaast ook een <code>OperationOutcome</code> met <code>issue.code</code> "forbidden" of "security" worden geretourneerd. |
| <p>FHIR resourcetype is niet gespecificeerd binnen de gegevensdienst, OF</p> <p>FHIR resourcetype of request type wordt niet ondersteund</p> | <p>statuscode 404</p> <ul style="list-style-type: none"> In deze situatie wordt een <code>OperationOutcome</code> met <code>issue.code</code> "not-supported" en de van toepassing zijnde <code>issue.details</code> geretourneerd. |
| resource-id niet bekend | <p>statuscode 404</p> <ul style="list-style-type: none"> In deze situatie wordt een <code>OperationOutcome</code> met <code>issue.code</code> "not-found" en de van toepassing zijnde <code>issue.details</code> geretourneerd. |
| Gevraagde <code>acceptVersion</code> in de AORTA-Version header wordt niet ondersteund | statuscode 406 |
| Gehanteerde <code>contentVersion</code> in de AORTA-Version header wordt niet ondersteund | statuscode 415 |
| Fout in server | statuscode 500 |
| Fout in achterliggende server | <p>statuscode 500</p> <ul style="list-style-type: none"> In deze situatie wordt, voor iedere resource server die een fout produceerde, een <code>OperationOutcome</code> toegevoegd met <code>issue.severity</code> "warning", <code>issue.code</code> "processing" en <code>issue.diagnostics</code> "<appID van betreffende resource server>". |
| Fout in achterliggende Mitz-dienst | <p>statuscode 500</p> <ul style="list-style-type: none"> In deze situatie wordt een <code>OperationOutcome</code> toegevoegd met <code>issue.severity</code> "error", <code>issue.code</code> "transient" en <code>issue.diagnostics</code> "Fout bij interactie met Mitz". |

Token specificaties - 0.7.x

- MedMij tokens
 - Inhoud en formaat van het MedMij access_token
- AORTA tokens
 - Inhoud en formaat van het AORTA stelseltoken
- GBP-tokens
 - SAML DigiD token
- GBK-tokens
 - SAML PKI Authenticatietoken
- GBZ-tokens
 - Inhoud en formaat van het SAML AORTA transactietoken
 - Inhoud en formaat van het SAML AORTA mandaattoken
 - Inhoud en formaat van het SAML AORTA inschrijftoken
 - Inhoud en formaat van het SAML AORTA consent_token
 - Inhoud en formaat van het AORTA access_token

MedMij tokens

Inhoud en formaat van het MedMij access_token

AOF.TS.MAT.100.v1

Het MedMij access_token is een JWT, die bestaat uit een header, een payload en een signature, waarbij gebruik wordt gemaakt van [JWS Compact Serialization](#).

AOF.TS.MAT.150.v1

De header van het token bevat de volgende attributen:

| Claim | Vaste waarde | Toelichting |
|-------|--------------|--|
| alg | RS256 | |
| typ | mat+JWT | "mat" is een afkorting voor MedMij access_token |
| kid | - | The identifier of the key-pair used to sign this JWT |

AOF.TS.MAT.200.v1

Het access_token wordt op basis van RS256 (RSA Signature met SHA-256), digitaal ondertekend met de private key van de Autorisatie Server. De signature wordt geplaatst over de header en de payload.

AOF.TS.MAT.300.v1

Het access_token bevat de volgende payload:

| Claim | Vaste waarde | Toelichting |
|-------|--------------|--|
| jti | - | Unieke ID van het token |
| ver | 1.0 | De versie van de tokendefinitie die wordt gehanteerd |
| iss | - | HTTPS-URL van de Autorisatie Server voor deze versie van het MedMij afsprakenstelsel (interfaceversie) |
| exp | - | Gelijk aan de waarde van <i>expires_in</i> in het <i>access token response</i> bericht |
| scope | - | Gelijk aan de <i>scope</i> in het <i>access token response</i> bericht. Wanneer een access_token wordt gegenereerd t.b.v. een interne \$is-allowed operation tussen Autorisatie Server en Resource Broker, dan wordt de scope gevuld met <ul style="list-style-type: none">• \$is-allowed/• gevolgd door de scope in het <i>access token response</i> bericht Bijvoorbeeld: "\$is-allowed/eenofanderezorgaanbieder-42" |

AORTA tokens

Inhoud en formaat van het AORTA stelseltoken

AOF.TS.AST.100.v1

Het AORTA stelseltoken is een JWT, die bestaat uit een header, een payload en een signature, waarbij gebruik wordt gemaakt van [JWS Compact Serialization](#).

AOF.TS.AST.150.v1

De header van het token bevat de volgende attributen:

| Claim | Vaste waarde | Toelichting |
|-------|--------------|---|
| alg | RS256 | |
| typ | aorta-st+JWT | "aorta-st" is een afkorting voor AORTA stelseltoken |
| x5c | - | De van toepassing zijnde keten van PKIX certificaten. Deze dient te worden gebruikt om de signature van het token te valideren. |

AOF.TS.AST.200.v1

Het token wordt op basis van RS256 (RSA Signature met SHA-256), digitaal ondertekend met de private key van de AORTA Stelselnode. De signature wordt geplaatst over de header en de payload.

AOF.TS.AST.300.v3

Het token bevat de volgende payload:

| Claim | Cardinaliteit | Vaste waarde | Toelichting |
|-----------------|---------------|--------------|---|
| jti | 1..1 | - | Unieke ID van het token |
| ver | 1..1 | 1.0 | De versie van de tokendefinitie die wordt gehanteerd |
| iss | 1..1 | - | HTTPS-URL van de AORTA Stelselnode |
| server | 0..n | - | Server object met subclaims. Eén object per server in het AORTA-stelsel. |
| server. role | 1..1 | - | String met de functionele rol van de server. Let op: een server met dezelfde rol kan met verschillende base-URL's meerdere keren voorkomen. |
| server. base | 1..1 | - | Base-URL van de server, bijv. <a href="https://<FQDN>/broker/fhir">https://<FQDN>/broker/fhir . |

Onderstaande tabel toont welke servers zijn opgenomen in het token:

| Role | Role-ID | Opgenomen in stelseltoken | Toelichting |
|----------|---------|---------------------------|--------------------------------------|
| as_za | 100 | ja | Autorisatie Server ZA |
| map | 120 | nee | Medisch Autorisatie Protocol Server |
| as_mm | 150 | ja | Autorisatie Server MedMij |
| rb_za_in | 200 | ja | Resource Broker ZA-in |
| rb_mm_in | 250 | ja | Resource Broker MedMij-in |
| rb_log | 300 | nee | Resource Broker LOG |
| rb_vnc | 400 | ja | Resource Broker VnC |
| rb_vwi | 500 | nee | Resource Broker VWI |
| rb_act | 550 | nee | Resource Broker Actualiteitsregister |

| | | | |
|--------|-----|-----|----------------------------|
| rb_sds | 600 | nee | Resource Broker SDS |
| rb_apr | 620 | ja | Resource Broker APR |
| adds | 640 | ja | Adressering Server |
| tds | 700 | nee | Transformatiedienst Server |

GBP-tokens

SAML DigiD token

Zie de [IH Berichtauthenticatie met DigiD](#) in de AORTA documentatie.

GBK-tokens

SAML PKI Authenticatietoken

AOF.TS.PAT.100.v2

Het PKI Authenticatietoken is een SAML Assertion en bevat de volgende elementen en attributen:

| Element/@Attribuut | Cardinaliteit | Vaste waarde | Toelichting |
|--|---------------|---|--|
| @ID | 1..1 | - | Unieke identificatie van de Assertion |
| @Version | 1..1 | "2.0" | Gebruikte SAML versie |
| @IssueInstant | 1..1 | - | Tijdstip van uitgifte van de Assertion. |
| Issuer | 1..1 | - | AppID van de initiërende GBK-applicatie. Formaat: "urn:oid:2.16.840.1.113883.2.4.6.6.<applicatie-id>" |
| Issuer.@Format | 1..1 | "urn:oasis:names:tc:SAML:2.0:nameid-format:entity" | |
| Subject.NameID | 1..1 | - | Bevat het serienummer van het certificaat, waarmee de Assertion is ondertekend. Formaat: "urn:cert:issuersn:CN=<common name>;<serienummer>" Zie ook: A Uniform Resource Name (URN) Namespace for Certificates . |
| Conditions.@NotBefore | 1..1 | - | |
| Conditions.@NotOnOrAfter | 1..1 | - | Richtlijn voor het verschil tussen NotBefore en Boorwater is 5 minuten. |
| Conditions.AudienceRestriction.Audience | 1..n | - | De volgende Audiences zijn altijd verplicht. <ul style="list-style-type: none"> De role van de Autorisatie Server ZA component, zoals benoemd in het AORTA Stelseltoken. Daarnaast verplicht bij interacties met een Resource Broker component: <ul style="list-style-type: none"> De role van de betreffende Resource Broker component, zoals benoemd in het AORTA Stelseltoken. Formaat: <ul style="list-style-type: none"> "urn:oid:2.16.840.1.113883.2.4.3.111.8.<role-id>" |
| AuthnStatement.@AuthnInstant | 1..1 | - | Tijdstip van authenticatie van de gebruiker (Subject). |
| AuthnStatement.AuthnContext.AuthnContextClassRef | 1..1 | "urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI" | |
| AttributeStatement | 1..1 | | Zie onderstaande tabel. |

AOF.TS.PAT.200.v4

In het AttributeStatement zijn de volgende Attributen opgenomen:

| @Name | Cardinaliteit | AttributeValue | |
|---------------------|---------------|------------------------------------|---|
| | | Vaste waarde | Toelichting |
| "patientIdentifier" | 0..1 | - | ID van de patient. Verplicht bij patiëntgebonden interacties. Anders afwezig. Formaat (één van de volgende): <ul style="list-style-type: none"> "urn:oid:2.16.840.1.113883.2.4.6.3.<BSN>" "urn:oid:2.16.840.1.113883.2.4.3.111.4.<Hash van BSN>" "urn:oid:2.16.840.1.113883.2.4.3.111.6.<COA nummer>" |
| "messageIdRoot" | 1..1 | "2.16.840.1.113883.2.4.3.111.15.4" | |
| "messageIdExt" | 1..1 | - | De waarde van het requestID dat zal worden meegestuurd in de AORTA-ID HTTP header. |
| "InteractionId" | 1..1 | - | Het interactie-id wordt als volgt samengesteld: " <code><type FHIR-interactie>:<FHIR resourcetype>:<contentVersion>:<request/response></code> " waarbij mogelijke type FHIR-interacties zijn gedefinieerd in de FHIR specificaties . OF " <code><\$<operation naam>:<contentVersion>:<request/response></code> " |
| "contextCodeSystem" | 1..1 | "2.16.840.1.113883.2.4.3.111.15.1" | |
| "contextCode" | 1..1 | - | De contextcode die aanduidt binnen welke (zorg)toepassing de FHIR-interactie wordt geïnitieerd, bijv. "LOG", of "ACT/VWI". |

AOF.TS.PAT.300.v1

De Assertion bevat ook een Signature die is geplaatst met behulp van de PKI pas van de GBK-medewerker.

AOF.TS.PAT.400.v1

Met het PKI Authenticatietoken wordt aan de ontvanger bewezen dat een bepaalde persoon of organisatie instaat voor de authenticiteit van een gegeven bericht.

GBZ-tokens

Inhoud en formaat van het SAML AORTA transactietoken

AOF.TS.ATT.100.v3

Het AORTA transactietoken voor berichtauthenticatie is een SAML Assertion en bevat de volgende elementen en attributen:

| Element/@Attribuut | Cardinaliteit | Vaste waarde | Toelichting |
|--------------------|---------------|--|---|
| @ID | 1..1 | - | Unieke identificatie van de Assertion |
| @Version | 1..1 | "2.0" | Gebruikte SAML versie |
| @IssueInstant | 1..1 | - | Tijdstip van uitgifte van de Assertion. |
| Issuer | 1..1 | - | URA van de initiërende organisatie, d.w.z. de organisatie aan de start van de keten. Formaat: "urn:oid:2.16.528.1.1007.3.3.<URA>" |
| Issuer.@Format | 1..1 | "urn:oasis:names:tc:SAML:2.0:nameid-format:entity" | |
| Subject.NameID | 1..1 | - | Bevat zowel de UZI van de geauthentiseerde zorgverlener /medewerker als mede diens rolcode. Formaat: "<UZI-nummer>:<UZI-rolcode>" Wanneer de handtekening is geplaatst met een servercertificaat, dan moet dit veld worden leeggelaten. |

| | | | |
|--|------|--|--|
| Subject.SubjectConfirmation. @Method | 1..1 | "urn:oasis:names:tc:SAML:2.0:cm:holder-of-key" | |
| Subject.SubjectConfirmation. SubjectConfirmationData.KeyInfo. X509Data | 1..1 | - | X.509 serial van de UZI-pas (zorgverlener of medewerker op naam) of van het servercertificaat waarmee de handtekening is geplaatst. |
| Conditions.@NotBefore | 1..1 | - | |
| Conditions.@NotOnOrAfter | 1..1 | - | Mag maximaal 1 minuut na @NotBefore liggen. |
| Conditions.AudienceRestriction. Audience | 1..n | - | De volgende Audiences zijn altijd verplicht. <ul style="list-style-type: none"> De role van de Autorisatie Server ZA component, zoals benoemd in het AORTA Stelseltoken. Daarnaast verplicht bij interacties met een andere zorgaanbieder: <ul style="list-style-type: none"> URA of applID van het Reagerend GBZ, afhankelijk van of een interactie is gericht aan een organisatie of aan een specifieke applicatie. Daarnaast verplicht bij interacties met een Resource Broker component: <ul style="list-style-type: none"> De role van de betreffende Resource Broker component, zoals benoemd in het AORTA Stelseltoken. Formaat: <ul style="list-style-type: none"> urn:oid:2.16.840.1.113883.2.4.6.6.<applicatie-id>", of "urn:oid:2.16.528.1.1007.3.3.<URA>", of "urn:oid:2.16.840.1.113883.2.4.3.111.8.<role-id>" |
| AuthnStatement.@AuthnInstant | 1..1 | - | Tijdstip van authenticatie van de gebruiker (Subject) of applicatie. |
| AuthnStatement.AuthnContext. AuthnContextClassRef | 1..1 | Ingeval van ondertekening met pas: "urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI" Ingeval van ondertekening met servercertificaat: "urn:oasis:names:tc:SAML:2.0:ac:classes:X509" | |
| AttributeStatement | 1..1 | | Zie onderstaande tabel. |

AOF.TS.ATT.200.v3

In het AttributeStatement zijn de volgende Attributen opgenomen:

| @Name | Cardinaliteit | AttributeValue | |
|---------------------|---------------|------------------------------------|--|
| | | Vaste waarde | Toelichting |
| "patientIdentifier" | 0..1 | - | ID van de patient. Verplicht bij patiëntgebonden interacties. Anders afwezig. Formaat (één van de volgende): <ul style="list-style-type: none"> "urn:oid:2.16.840.1.113883.2.4.6.3.<BSN>" "urn:oid:2.16.840.1.113883.2.4.3.111.4.<Hash van BSN>" "urn:oid:2.16.840.1.113883.2.4.3.111.6.<COA nummer>" |
| "messageIdRoot" | 1..1 | "2.16.840.1.113883.2.4.3.111.15.4" | |
| "messageIdExt" | 1..1 | - | De waarde van het requestID dat zal worden meegestuurd in de AORTA-ID HTTP header. |
| "InteractionId" | 1..1 | - | Het interactie-id wordt als volgt samengesteld: "<type FHIR-interactie>:<FHIR resourcetype>:<contentVersion>:<request/response>" waarbij mogelijke type FHIR-interacties zijn gedefinieerd in de FHIR specificaties . OF "\$<operation naam>:<contentVersion>:<request/response>" |
| "contextCodeSystem" | 1..1 | "2.16.840.1.113883.2.4.3.111.15.1" | |
| "contextCode" | 1..1 | - | De contextcode die aanduidt binnen welke (zorg)toepassing de FHIR-interactie word geïnitieerd, bijv. "BGZ", of "ACT/VWI". |

| | | | |
|-----------------------------|------|---|--|
| "autorisatieregel /context" | 0..1 | - | URI waar de autorisatieregel/context gevonden kan worden waarbinnen het mandaat gegeven wordt. Moet aanwezig zijn indien gebruik gemaakt is van een mandaat. Lokaal is vastgelegd dat een bepaald mandaat daadwerkelijk door een mandaatverlener is toegekend aan een bepaald persoon/systeem. |
| "applicationID" | 1..1 | - | ApplicatieID van de Resource Client (GBZ-applicatie). Formaat: "urn:oid:2.16.840.1.113883.2.4.6.6.<applicatie-id>" |

AOF.TS.ATT.300.v1

De Assertion bevat ook een Signature die is geplaatst met behulp van de UZI pas van de zorgverlener (Z) of de UZI medewerkerpas (N) van de medewerker. De handtekening dient geplaatst te zijn met behulp van het authenticatie certificaat op de pas. In het kader van "vereenvoudigd gebruik UZI-pas", mag de handtekening ook gezet worden met het servercertificaat (S) van de applicatie.

AOF.TS.ATT.400.v1

Met het transactietoken voor berichtauthenticatie wordt aan de ontvanger bewezen dat een bepaalde persoon of organisatie instaat voor de authenticiteit van een gegeven bericht. Wanneer hierbij gebruik is gemaakt van een verleend mandaat, dan bevat het token ook de URI van de van toepassing zijnde mandaatregel.

Inhoud en formaat van het SAML AORTA mandaattoken

AOF.TS.AMT.100.v2

Het AORTA mandaattoken is een SAML Assertion en bevat de volgende elementen en attributen:

| Element/@Attribuut | Cardinaliteit | Vaste waarde | Toelichting |
|---|---------------|--|--|
| @ID | 1..1 | - | Unieke identificatie van de Assertion |
| @Version | 1..1 | "2.0" | Gebruikte SAML versie |
| @IssueInstant | 1..1 | - | Tijdstip van registratie van het mandaat. |
| Issuer | 1..1 | - | De zorgverlener die het mandaat afgeeft. Formaat: "<UZI-nummer>:<UZI-rolcode>" |
| Issuer.@Format | 1..1 | "urn:oasis:names:tc:SAML:2.0:nameid-format:entity" | |
| Subject.NameID | 1..1 | - | De Organisatie (URA) waarbinnen het mandaat geldig is. Formaat: "urn:oid:2.16.528.1.1007.3.3.<URA>" |
| Subject.SubjectConfirmation.@Method | 1..1 | "urn:oasis:names:tc:SAML:2.0:cm:sender-vouches" | |
| Conditions.@NotBefore | 1..1 | - | |
| Conditions.@NotOnOrAfter | 1..1 | - | |
| Conditions.AudienceRestriction.Audience | 1..n | - | De volgende Audiences zijn verplicht. De role van de Autorisatie Server ZA component, zoals benoemd in het AORTA Stelseltoken. AppID van de Resource Client (GBZ-applicatie). Formaat: <ul style="list-style-type: none"> "urn:oid:2.16.840.1.113883.2.4.3.111.8.<role-id>" |
| AttributeStatement | 1..1 | | Zie onderstaande tabel. |

AOF.TS.AMT.200.v1

In het AttributeStatement zijn de volgende Attributen opgenomen:

| @Name | Cardinaliteit | AttributeValue | |
|-------|---------------|----------------|-------------|
| | | Vaste waarde | Toelichting |
| | | | |

| | | | |
|----------------------------|------|---|--|
| "autorisatieregel/context" | 1..1 | - | URI waar de autorisatieregel/context gevonden kan worden waarbinnen het mandaat gegeven wordt. |
|----------------------------|------|---|--|

AOF.TS.AMT.300.v1

De Assertion bevat ook een Signature die is geplaatst met behulp van de UZI pas van de zorgverlener (Z).

Met een mandaattoken wordt aan de ontvanger bewezen dat een bepaalde persoon (mandaatverlener) lokaal in een GBZ een door een URI geïdentificeerde mandaatregel heeft vastgelegd, die geldig is binnen deze organisatie.

Inhoud en formaat van het SAML AORTA inschrijftoken

AOF.TS.AIT.100.v3

Het AORTA inschrijftoken is een SAML Assertion en bevat de volgende elementen en attributen:

| Element/@Attribuut | Cardinaliteit | Vaste waarde | Toelichting |
|--|---------------|---|--|
| @ID | 1..1 | - | Unieke identificatie van de Assertion |
| @Version | 1..1 | "2.0" | Gebruikte SAML versie |
| @IssueInstant | 1..1 | - | Tijdstip van uitgifte van de Assertion. |
| Issuer | 1..1 | - | URA van de organisatie die de BSN-validatie heeft uitgevoerd. Formaat: "urn:oid:2.16.528.1.1007.3.3.<URA>" |
| Issuer.@Format | 1..1 | "urn:oasis:names:tc:SAML:2.0:nameid-format:entity" | |
| Subject.NameID | 1..1 | - | Bevat het gevalideerde patiënt ID. Formaat (één van de volgende): <ul style="list-style-type: none"> "urn:oid:2.16.840.1.113883.2.4.6.3.<BSN>" "urn:oid:2.16.840.1.113883.2.4.3.111.6.<COA nummer>" |
| Subject.SubjectConfirmation.@Method | 1..1 | "urn:oasis:names:tc:SAML:2.0:cm:sender-vouches" | |
| Subject.SubjectConfirmation.SubjectConfirmationData.KeyInfo.X509Data | 1..1 | - | X.509 serial van de UZI-pas (zorgverlener of medewerker op naam) waarmee de handtekening is geplaatst. |
| Conditions.@NotBefore | 1..1 | - | |
| Conditions.@NotOnOrAfter | 1..1 | - | Mag maximaal 1,5 jaar na @NotBefore liggen |
| Conditions.AudienceRestriction.Audience | 1..n | - | De volgende Audiences zijn verplicht. De role van de Autorisatie Server ZA component, zoals benoemd in het AORTA Stelseltoken. AppID van de Resource Client (GBZ-applicatie). Formaat: <ul style="list-style-type: none"> "urn:oid:2.16.840.1.113883.2.4.6.6.<applicatie-id>", of "urn:oid:2.16.840.1.113883.2.4.3.111.8.<role-id>" |
| AuthnStatement.@AuthnInstant | 1..1 | - | Tijdstip van BSN validatie. Dit mag t.b.v. het werkproces ook de 'timestamp' zijn van het moment van aanmaken van het inschrijftoken. |
| AuthnStatement.AuthnContext.AuthnContextClassRef | 1..1 | "urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI" | |

AOF.TS.AIT.200.v1

In het AttributeStatement zijn de volgende Attributen opgenomen:

| @Name | Cardinaliteit | AttributeValue | |
|-------|---------------|----------------|-------------|
| | | Vaste waarde | Toelichting |
| | | | |

| | | | |
|--------------|------|--|--|
| "Uitvoerder" | 1..1 | | Het UZI-nummer van de zorgverlener of medewerker die het token heeft ondertekend. Formaat: "urn:oid:2.16.528.1.1007.3.1.<UZI-nummer>" |
|--------------|------|--|--|

AOF.TS.AIT.300.v1

De Assertion bevat ook een Signature die is geplaatst met behulp van de UZI pas van de zorgverlener (Z) of de UZI medewerkerpas (N) van de medewerker.

Met een inschrijftoken wordt aan de ontvanger bewezen dat een bepaalde persoon, binnen een bepaalde organisatie, een bepaald BSN heeft gevalideerd.

Inhoud en formaat van het SAML AORTA consent_token

AOF.TS.ACT.100.v2

Het AORTA consent_token is een SAML Assertion en bevat de volgende elementen en attributen:

| Element/@Attribuut | Cardinaliteit | Vaste waarde | Toelichting |
|--|---------------|---|--|
| @ID | 1..1 | - | Unieke identificatie van de Assertion |
| @Version | 1..1 | "2.0" | Gebruikte SAML versie |
| @IssueInstant | 1..1 | - | Tijdstip van uitgifte van de Assertion. |
| Issuer | 1..1 | - | URA van de organisatie die de Assertion uitgeeft. Dit is tevens de organisatie waar de patiënt de toestemming aan heeft gegeven. Formaat: "urn:oid:2.16.528.1.1007.3.3.<URA>" |
| Issuer.@Format | 1..1 | "urn:oasis:names:tc:SAML:2.0:nameid-format:entity" | |
| Subject.NameID | 0..1 | - | Bevat zowel de UZI van de geauthentiseerde zorgverlener/medewerker alsmede diens rolcode. Formaat: "<UZI-nummer>:<UZI-rolcode>" Wanneer de handtekening is geplaatst met een servercertificaat, dan moet dit veld worden weggelaten. Let op: vanaf AoF 0.8 vervalt voor dit token de optie om een handtekening te plaatsen met de UZI pas. |
| Subject.SubjectConfirmation.@Method | 1..1 | "urn:oasis:names:tc:SAML:2.0:cm:sender-vouches" | |
| Subject.SubjectConfirmation.SubjectConfirmationData.KeyInfo.X509Data | 1..1 | - | X.509 serial van de UZI-pas (zorgverlener of medewerker op naam) of van het servercertificaat waarmee de handtekening is geplaatst. |
| Conditions.@NotBefore | 1..1 | - | Wordt bepaald door de (zorg)toepassing. |
| Conditions.@NotOnOrAfter | 1..1 | - | Wordt bepaald door de (zorg)toepassing. |
| Conditions.AudienceRestriction.Audience | 1..n | - | De volgende Audiences zijn verplicht. De role van de Autorisatie Server ZA component, zoals benoemd in het AORTA Stelseltoken. Formaat: <ul style="list-style-type: none"> "urn:oid:2.16.840.1.113883.2.4.3.111.8.<role-id>" |
| AuthnStatement.@AuthnInstant | 1..1 | - | Tijdstip van uitgifte van de Assertion. |
| AuthnStatement.AuthnContext.AuthnContextClassRef | 1..1 | "urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI" | |

AOF.TS.ACT.200.v3

In het AttributeStatement zijn de volgende Attributen opgenomen:

| @Name | Cardinaliteit | AttributeValue | |
|-------|---------------|----------------|-------------|
| | | Vaste waarde | Toelichting |
| | | | |

| | | | |
|---------------------|------|------------------------------------|---|
| "patientIdentifier" | 1..1 | - | Het ID van de patiënt, d.w.z. de persoon waarop de gegevens, waarvoor deze consent wordt verstrekt, betrekking hebben. Formaat (één van de volgende): <ul style="list-style-type: none"> "urn:oid:2.16.840.1.113883.2.4.6.3.<BSN>" "urn:oid:2.16.840.1.113883.2.4.3.111.4.<Hash van BSN>" "urn:oid:2.16.840.1.113883.2.4.3.111.6.<COA nummer>" |
| "contextCodeSystem" | 1..1 | "2.16.840.1.113883.2.4.3.111.15.1" | |
| "contextCode" | 1..1 | - | De contextcode die aanduidt welke set van gegevens beschikbaar mag worden gesteld bijv. "BGZ". |
| "clientID" | 1..1 | - | URA van het GBZ aan wie de Assertion wordt toegezonden om te gebruiken in een daaropvolgende pull-interactie. Formaat: <ul style="list-style-type: none"> "urn:oid:2.16.528.1.1007.3.3.<URA>" |

AOF.TS.ACT.300.v1

De Assertion bevat ook een Signature die is geplaatst met behulp van de UZI pas van de zorgverlener (Z) of de UZI medewerkerpas (N) van de medewerker. De handtekening dient geplaatst te zijn met behulp van het authenticatie certificaat op de pas. In het kader van "vereenvoudigd gebruik UZI-pas", mag de handtekening ook gezet worden met het servercertificaat (S) van de applicatie. **Let op: vanaf Aof 0.8 vervalt voor dit token de optie om een handtekening te plaatsen met de UZI pas.**

Met een consent_token wordt aan de ontvanger bewezen dat een bepaalde persoon, binnen een bepaalde organisatie, (veronderstelde) toestemming heeft gekregen van een patiënt om bepaalde gegevens beschikbaar te stellen voor opvraag door een andere zorgaanbieder.

Inhoud en formaat van het AORTA access_token

AOF.TS.AAT.100.v1

Het JWT-based AORTA access_token bestaat uit een header, een payload en een signature, waarbij gebruik wordt gemaakt van [JWS Compact Serialization](#).

AOF.TS.AAT.200.v2

De header van het token bevat de volgende attributen:

| Claim | Vaste waarde | Toelichting |
|-------|--------------|--|
| alg | RS256 | |
| typ | aorta-at+JWT | "aorta-at" is een afkorting voor AORTA access_token. |
| kid | - | The identifier of the key-pair used to sign this JWT |

AOF.TS.AAT.300.v1

Het token wordt op basis van RS256 (RSA Signature met SHA-256), digitaal ondertekend met de private key van de Autorisatie Server. De signature wordt geplaatst over de header en de payload.

AOF.TS.AAT.400.v6

De payload van het token is omschreven in onderstaande tabel.

| Claim | Cardinaliteit | Vaste waarde | Toelichting |
|-------|---------------|--------------|--|
| jti | 1..1 | - | jti bevat een globaal uniek ID van het betreffende token. Aanbevolen wordt om een UUID te gebruiken. |
| iat | 1..1 | - | iat bevat het tijdstip van uitgifte van dit token (aantal seconden sinds 1970-01-01T0:0:0Z gemeten in UTC). |
| iss | 1..1 | - | iss bevat de HTTPS-URL van de autorisatieserver die het token heeft uitgegeven. Op deze manier kan automatisch de juiste metadata, met daarin de juiste endpoints, worden opgehaald. |

| | | | |
|---------|------|---|---|
| sub | 1..1 | - | <p>Formaat: "<id-systeem> <id>"</p> <p>Het ID van de gebruiker, of van een systeem, die uitgifte van dit access_token legitimeert. De claim kan bevatten:</p> <ul style="list-style-type: none"> Het BSN van de persoon die een interactie initieert m.b.t. haar eigen gegevens, of die een ander persoon hiertoe heeft gemachtigd - sub bevat dan de string "http://fhir.nl/fhir/NamingSystem/bsn <bsn>" Het UZI-nummer van een zorgverlener - sub bevat dan de string "http://fhir.nl/fhir/NamingSystem/uzi-nr-pers <UZI-nummer>" Het applID van het systeem (indien het request zonder tussenkomst van een gebruiker is ingestuurd) - sub bevat dan de string "http://fhir.nl/fhir/NamingSystem/aorta-app-id <app-id>" |
| role | 0..1 | - | <p>Formaat: "<codesysteem> <rolcode>"</p> <p>De rolcode van de gebruiker die uitgifte van dit access_token legitimeert. De claim kan bevatten:</p> <ul style="list-style-type: none"> De rolcode die hoort bij een persoon, ofwel "http://fhir.nl/fhir/NamingSystem/aorta-rolcode P" De UZI-rolcode van een zorgverlener, ofwel "http://fhir.nl/fhir/NamingSystem/uzi-rolcode <UZI-rolcode>" <p>Verplicht indien de sub claim is gevuld met een ID van een persoon.</p> |
| act | 0..1 | - | <p>De act claim bevat een aantal subclaims en wordt opgenomen wanneer iets of iemand handelt namens een ander persoon. Zie ook RFC 8693 voor voorbeelden.</p> |
| act.sub | 1..1 | - | <p>Formaat: "<id-systeem> <id>"</p> <p>Het ID van de gebruiker of van het systeem die handelt namens de persoon, die is opgenomen in de sub claim. De claim kan bevatten:</p> <ul style="list-style-type: none"> Het BSN van een gemachtigd persoon die gegevens van een ander persoon opvraagt - sub bevat dan de string "http://fhir.nl/fhir/NamingSystem/bsn <bsn>" Het UZI-nummer van een zorgverlener of van een medewerker van een zorginstelling - sub bevat dan de string "http://fhir.nl/fhir/NamingSystem/uzi-nr-pers <UZI-nummer>" Het applID van het systeem (indien het request zonder tussenkomst van een gebruiker is ingestuurd) - sub bevat dan de string "http://fhir.nl/fhir/NamingSystem/aorta-app-id <app-id>" |
| acr | 1..1 | - | <p>De Authentication Context Class Reference. Geeft informatie over het niveau waarop de sub van het token is geauthenticeerd. Mogelijke waarden, zoals gespecificeerd binnen SAML zijn:</p> <ul style="list-style-type: none"> "urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport" (bijvoorbeeld DigiD-basis) "urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract" (bijvoorbeeld DigiD-midden) "urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard" (bijvoorbeeld DigiD-substantieel) "urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI" (bijvoorbeeld UZI-pas of DigiD-hoog) "urn:oasis:names:tc:SAML:2.0:ac:classes:X509" (servercertificaat) |
| attest | 1..1 | - | <p>Informatie over op welke grondslag of grondslagen dit token is gebaseerd. Het betreft een door spatie gescheiden set van strings. Mogelijk waarden:</p> <ul style="list-style-type: none"> "MAP" - het Medisch Autorisatie Protocol is toegepast. "TR" - toestemming van patiënt is vastgelegd in een toegelaten toestemmingsregister. "MedMij" - het token is uitgeven n.a.v. een conform MedMij afgegeven toestemmingsverklaring. "BRON" - toestemming is, door de patiënt of diens vertegenwoordiger, vastgelegd bij de bronhoudende zorgaanbieder zelf, en is daarom nog niet getoetst. "CNST" - toestemming mag door de bronhoudende zorgaanbieder worden verondersteld te zijn verkregen, bijvoorbeeld t. b.v. een verwijzing van de patiënt - deze is vastgelegd in een consent_token, en het juiste gebruik van dit token voor het ontvangen request is reeds getoetst. "LOG" - specifieke autorisatieregels m.b.t. de toegangsllog zijn toegepast. "ACT/VWI" - specifieke autorisatieregels m.b.t. toegang tot ACT/VWI-entries zijn toegepast. <p>Een voorbeeld van een attest claim is "MAP TR", waarmee dan wordt aangeduid dat het MAP is getoetst en dat toestemming is vastgelegd en getoetst in een toegelaten toestemmingsregister.</p> |
| nbf | 1..1 | - | <p>nbf bevat het tijdstip van uitgifte van dit token (aantal seconden sinds 1970-01-01T0:0:0Z gemeten in UTC).</p> |
| exp | 1..1 | - | <p>Wordt gevuld met de expiration time van het MedMij access_token of met de expiration time van het AORTA transactietoken naar aanleiding waarvan dit AORTA access_token wordt uitgegeven.</p> |
| aud | 1..1 | - | <p>Indien het token is bedoeld om een FHIR-interactie te initiëren bij een GBx-server:</p> <p>De aud van het token bevat het applID en de FQDN van de GBx-applicatie, die deze interactie gaat ontvangen. Formaat: ["<applID>", "<FQDN>"].</p> <p>Een applID heeft het formaat: "urn:oid:2.16.840.1.113883.2.4.6.6.<applicatie-id>". Aan iedere GBx-applicatie die is aangesloten op AORTA wordt een eigen <applicatie-id> toegekend.</p> <p>Indien het token is bedoeld om een FHIR-interactie te initiëren bij een Resource Broker component:</p> <p>De aud bevat de "<role van betreffende Resource Broker component>".</p> <p>Formaat van een role: "urn:oid:2.16.840.1.113883.2.4.3.111.8.<role-id>". Roles zijn gespecificeerd in het AORTA Stelseltoken.</p> |
| scope | 1..1 | - | <p>Voor de juiste vulling zie tekst onder deze tabel.</p> |

| | | | |
|-----------------------------|------|---|--|
| patient | 0..1 | - | <p>Het ID van de patiënt, d.w.z. de persoon waarop de gegevens, die worden uitgewisseld, betrekking hebben.</p> <p>Verplicht gevuld bij patiëntgebonden interacties.</p> <p>Formaat (één van de volgende):</p> <ul style="list-style-type: none"> • "urn:oid:2.16.840.1.113883.2.4.6.3.<BSN>" OF "http://fhir.nl/fhir/NamingSystem/bsn<bsn>" • "urn:oid:2.16.840.1.113883.2.4.3.111.4.<Hash van BSN>" • "urn:oid:2.16.840.1.113883.2.4.3.111.6.<COA nummer>" |
| client_id | 1..1 | - | <p>Dit attribuut bevat informatie over de partij die als resource client mag optreden en daarvoor dit token mag gebruiken.</p> <p>Indien een interactie, door RB VnC wordt geïnitieerd bij een Resource Server (GBZ-applicatie):</p> <p>client_id bevat de role van RB VnC, zoals gespecificeerd in het AORTA Stelseltoken.</p> <p>Indien een interactie, door een Resource Client (GBx-applicatie) via RB ZA-in wordt geïnitieerd bij een Resource Broker component (bijv. RB ACT):</p> <p>client_id bevat de role van RB ZA-in, zoals gespecificeerd in het AORTA Stelseltoken.</p> <p>Formaat van een role: "urn:oid:2.16.840.1.113883.2.4.3.111.8.<role-id>". Roles zijn gespecificeerd in het AORTA Stelseltoken.</p> |
| _vrb | 0..1 | - | <p>De _vrb claim bevat, in een aantal subclaims, VZVZ Resource Broker specifieke informatie over de afhandeling van interacties. Een resource server (GBZ-applicatie) mag deze claim desgewenst negeren.</p> <p>Deze claim is slechts aanwezig wanneer een interactie, via RB VnC, wordt geïnitieerd bij een resource server.</p> |
| _vrb. _vrb_aud | 1..1 | - | <p>Formaat: ["<role>", "<role>"]</p> <p>De role van alle Resource Broker componenten, die dit token in de keten tussen Resource Client en de uiteindelijke bestemming, mogen verwerken.</p> <p>Wanneer de uiteindelijke bestemming een Resource Broker component is, dan wordt deze component zelf niet opgenomen in de _vrb_aud claim, maar in de aud claim.</p> <p>Wanneer een interactie door RB VnC wordt geïnitieerd bij een resource server (GBZ-applicatie), dan bevat de _vrb_aud claim de role van RB ZA-in en die van RB VnC.</p> <p>Wanneer een interactie door RB ZA-in wordt geïnitieerd bij een andere Resource Broker component (bijv. RB ACT) dan bevat de _vrb_aud claim het role van de Resource Broker ZA-in component.</p> <p>Formaat van een role: "urn:oid:2.16.840.1.113883.2.4.3.111.8.<role-id>". Roles zijn gespecificeerd in het AORTA Stelseltoken.</p> |
| _vrb. _vrb_client_id | 1..1 | - | <p>Indien een interactie, door een Resource Client (GBx-applicatie) via RB ZA-in en RB VnC wordt geïnitieerd bij een Resource Server (GBZ-applicatie):</p> <p>_vrb_client_id bevat de role van RB ZA-in en de FQDN + appID van de Resource Client. Formaat: ["<role>", "<appID>", "<FQDN>"].</p> <p>Indien een interactie, door een Resource Client (GBx-applicatie) via RB ZA-in wordt geïnitieerd bij een Resource Broker component (bijv. RB ACT):</p> <p>_vrb_client_id bevat de FQDN + appID van de Resource Client. Formaat: ["<appID>", "<FQDN>"].</p> <p>Indien een interactie, door RB MedMij-in, via RB VnC wordt geïnitieerd bij een Resource Server (GBZ-applicatie):</p> <p>_vrb_client_id bevat de role van RB MedMij-in.</p> <p>Formaat van een appID: "urn:oid:2.16.840.1.113883.2.4.6.6.<applicatie-id>".</p> <p>Formaat van een role: "urn:oid:2.16.840.1.113883.2.4.3.111.8.<role-id>". Roles zijn gespecificeerd in het AORTA Stelseltoken.</p> |
| _vrb. _vrb_ion | 1..1 | - | <p>Een kenmerk van de organisatie die die het request heeft geïnitieerd (de "initiating organisation name"). In de MedMij use case gaat het om de OAuthclientOrganisatiennaam (naam van het PGO), zoals opgenomen in de MedMij OCL. In de ZA-ZA use case gaat het om de URA (formaat: "urn:oid:2.16.528.1.1007.3.3.<URA>").</p> |
| _vrb. _vrb_ter _scope | 1..1 | - | <p>De waarde van de scope parameter, zoals geretourneerd in het token exchange response. Indien van toepassing, dan bevat deze scope, per interactie, ook het van toepassing zijnde transformation-id.</p> |

| | | | |
|------------------------------|------|-----|---|
| _vrb. _vrb_co nsent_id | 0..1 | | Het ID kenmerk van het AORTA consent_token op basis waarvan dit AORTA access_token is uitgegeven. Slechts gevuld indien de attest claim de waarde "CNST" bevat. |
| ver | 1..1 | 2.0 | De versie van de tokendefinitie die wordt gehanteerd. |

AOF.TS.AAT.500.v2

De scope claim van het token wordt als volgt gevuld, waarbij verschillende scope-onderdelen door een spatie van elkaar worden gescheiden:

| Gegevensdienst / Interactie | Vulling van scope | Toevoeging op scope bij interactie vanuit MedMij | Toevoeging op scope bij interactie vanuit AORTA |
|--|---|--|---|
| Verzamelen Afspraken 2.0 | patient/Appointment.read | medmij. gegevensdienst .47 | nog niet beschikbaar |
| Verzamelen Basisgegevens zorg 3.0 | patient/Patient.read patient/Coverage.read patient/Consent.read patient/Condition.read patient/Observation.read patient/NutritionOrder.read patient/Flag.read patient/AllergyIntolerance.read patient /MedicationStatement.read patient/MedicationRequest.read patient/MedicationDispense.read patient /DeviceUseStatement.read patient/Immunization.read patient/Procedure.read patient/Encounter.read patient /ProcedureRequest.read patient/ImmunizationRecommendation.read patient/DeviceRequest.read patient /Appointment.read | medmij. gegevensdienst .48 | aorta. contextcode. BGZ |
| Verzamelen Basisgegevens GGZ 2.0 | patient/Patient.read patient/Coverage.read patient/Consent.read patient/Condition.read patient/Observation.read patient/CarePlan.read patient/Procedure.read patient/DiagnosticReport.read patient/CareTeam.read | medmij. gegevensdienst .50 | nog niet beschikbaar |
| Verzamelen Documenten 3.0 | patient/DocumentManifest.read patient/DocumentReference.read patient/Binary.read | medmij. gegevensdienst .51 | nog niet beschikbaar |
| Delen Meetwaarden vitale functies 2.0 | patient/Observation.write | medmij. gegevensdienst .53 | nog niet beschikbaar |
| Verzamelen Meetwaarden vitale functies 2.0 | patient/Observation.read | medmij. gegevensdienst. 52 | nog niet beschikbaar |
| Verzamelen verwijzingen naar vragenlijsten 2.0 | patient/Task.read | medmij. gegevensdienst .59 | nog niet beschikbaar |
| Delen antwoorden op vragenlijsten 2.0 | patient/Task.write patient/QuestionnaireResponse.write | medmij. gegevensdienst .60 | nog niet beschikbaar |
| \$is-allowed | patient\$is-allowed | - | n.v.t. |
| Interacties m.b.t. het actualiteitsregister en de verwijzindex | patient/DocumentManifest.write of patient/DocumentManifest.read of patient/delete-dossier | n.v.t. | - |
| Interacties m.b.t. de toegangsllog (RB-logging) | patient/AuditEvent.read | n.v.t. | - |
| Patiëntgebonden workflow interacties | patient/Task.write | - | - |

Met een access_token wordt aan de ontvanger bewezen dat aan een gegeven subject bepaalde toegangsrechten zijn verstrekt.

AORTA FHIR-profielen - 0.7.x

- [Algemeen](#)
- [FHIR-profiel van Task](#)
 - [Toepassing bij notified-pull](#)

Algemeen

De AORTA FHIR-profielen zijn gespecificeerd in een aantal tabellen. Attributen die wel zijn opgenomen een gehanteerd basisprofiel, maar niet in een AORTA-profiel, mogen worden gevuld conform het basisprofiel. Implementaties mogen deze echter negeren. Voor attributen die wel zijn opgenomen in een AORTA-profiel, gelden de specificaties uit het AORTA-profiel.

FHIR-profiel van Task

Toepassing bij notified-pull

AO.FP.NTFP.100.v3

Het [profiel van de Task](#), zoals gebruikt voor een notified-pull is hier beschreven (last updated on 30-11-2022 14:05:51).

Voorbeelden:

- <https://simplifier.net/vzvt/nl-vzvt-tasknotifiedpull-request-example>
- <https://simplifier.net/vzvt/nl-vzvt-tasknotifiedpull-request-example-with-department>

Bij Organization instances of references wordt op zorginstelling niveau een URA gehanteerd. Wanneer een Organization verwijst naar een onderdeel van een zorginstelling, dan wordt het type gevuld met een DepartmentSpecialty en wordt via partOf een relatie gelegd met de zorginstelling.

Het formaat van de valueString, zoals gebruikt voor input attributen van type "query_string" is als volgt:

- [appID]/[type]/[id], of
- [type]{?[parameters]}

Waarbij [type] het FHIR resourcetype aangeeft.

Middels [id] wordt de juiste resource instance geïdentificeerd.

Bij FHIR-read interacties wordt de juiste GBZ-applicatie ook aangegeven middels [appID].

Middels [parameters] kan de zoekopdracht worden verfijnd.

AORTA Stelsel Interfaces - 0.7.x

- [AORTA Stelsel Metadata Interface](#)

AORTA Stelsel Metadata Interface

De metadata van de AORTA Stelsel Server kan worden opgehaald op een aorta-base-URL die door VZVZ-beheer rechtstreeks, via een veilig kanaal, met aangesloten partijen wordt gecommuniceerd.

De metadata is opgenomen in een [AORTA Stelseltoken](#), en kan op de volgende wijze worden opgehaald:

```
GET [aorta-base-URL]/metadata
```

De response bevat de volgende headers:

- `Content-Type: application/json`
- `Cache-Control: must-revalidate, max-age=<max-age-aorta-stelseltoken>`
- `Pragma: no-cache`

Een client mag de verkregen response conform de `Cache-Control` header directives, zoals [beschreven in RFC 7234](#), cachen.

De waarde van `max-age-aorta-stelseltoken` is configureerbaar in de AORTA Stelsel Server. Initiële waarde is 14400 seconden (4 uur).

De response bevat de volgende attributen:

- `signed_metadata`

Wanneer een [AORTA Stelseltoken](#) wordt verkregen, dan dienen de volgende controles te worden uitgevoerd:

1. Of het token is uitgegeven door een voor mij vertrouwde partij, vertrouwde issuers van het AORTA Stelseltoken worden out-of-band aan betrokken partijen gecommuniceerd.
2. Of het certificaat, waarmee de handtekening is geplaatst, toebehoort aan de issuer van het AORTA Stelseltoken.
3. De juistheid van de digitale handtekening (signature), inclusief de geldigheid van het certificaat waarmee de handtekening is geplaatst. Hierbij worden ook maatregelen genomen om [bedreiging 2.1 uit RFC 8725](#) tegen te gaan.

Adressering Server Interfaces - 0.7.x

- [Routing Info Interface](#)
- [Voorbeelden van gebruik Routing Info Interface](#)
 - [Interactie vanuit MedMij](#)
 - [Initiatie vanuit GBx-client](#)
 - [Aanroep vanuit Autorisatie Server ZA](#)

Routing Info Interface

AOF.ADS-I.RII.100.v1

Het technische formaat van een *getRoutingInfo* request is:

```
POST [base endpointadres]/getRoutingInfo
Content-Type: application/json; charset=utf-8
AORTA-ID: initialRequestID=<UUID conform RFC4122>; requestID=<UUID conform RFC4122>

{
  "destination": {
    "code": "",
    "codeSystem": ""
  },
  "interaction": [{
    "id": "",
    "method": "",
    "url": "",
    "aortaVersion": ""
  }]
}
```

Het *initialRequestID* attribuut bevat het ID van het allereerste request in de hele keten en dient te worden opgenomen in de logbestanden van alle partijen in de keten, zodat bij foutopsporing de verschillende logbestanden aan elkaar kunnen worden gerelateerd. Het *requestID* is voor iedere request message uniek. In requests wordt deze gegenereerd door de client. Ook het *requestID* dient te worden opgenomen in de verschillende logbestanden, zodat altijd duidelijk is op welk bericht een log entry van toepassing is.

Input parameters:

| Name | Cardinality | Type | Toelichting |
|------------------------|-------------|-----------------------|--|
| destination | 0..1 | Object met attributen | Beoogde bestemming van de interactie. Vereist wanneer één van de ingestuurde interactions géén url attribuut bevat met daarin een applID. Wordt genegeerd wanneer alle ingestuurde interactions een url attribuut bevatten met daarin een applID. Wanneer één ingestuurde interaction een url attribuut bevat met een applID en een andere ingestuurde interaction wordt uitgedrukt middels een id attribuut, dan wordt de destination slechts gebruikt voor de interaction met het id attribuut. Voor de interaction met het url attribuut wordt dan de applID uit het url attribuut gebruikt. |
| destination.code | 1..1 | String | Beoogde bestemming van de interactie. Mogelijke waarden: <ul style="list-style-type: none"> • <applID> • <URA> |
| destination.codeSystem | 1..1 | String | Het gehanteerde codesysteem. Mogelijke waarden: <ul style="list-style-type: none"> • "urn:oid:2.16.840.1.113883.2.4.6.6" (applID) • "urn:oid:2.16.528.1.1007.3.3" (URA) |
| interaction | 1..n | Object met attributen | Structuur waaruit het interactie-id van ieder te adresseren bericht kan worden bepaald. Dient slechts te worden meegezonden indien interaction-id niet is gevuld. Een interactie dient op één van de volgende methoden te worden doorgegeven: <ol style="list-style-type: none"> 1. id (bijv. search:Observation:2.1:request) 2. method + url + aortaVersion (bijv. GET + Observation/127328348 + 2.1, nodig voor instance-level interacties) |

| | | | |
|--------------------------------------|----------|--|--|
| interacti on.id | 0.. 1 | String | Interactie-id van het te adresseren bericht, of van de te adresseren berichten. Het versie-deel in het id attribuut wordt gespecificeerd conform semver , dus bijvoorbeeld "1.0.0" of "2.x". De Adressering Server houdt bij het zoeken naar applicaties slechts rekening met het major nummer, omdat compatibiliteit hierdoor afdoende is geborgd. |
| interacti on. method | 0.. 1 | String met waarde GET POST PUT DELETE | De gebruikte HTTP method. |
| interacti on.url | 0.. 1 | String | De gebruikte URL, inclusief eventuele (zoek)parameters. |
| interacti on. aortaVe rsion | 0.. 1 | String | De gebruikte versie van de interactie. Het aortaVersion attribuut wordt gespecificeerd conform semver , dus bijvoorbeeld "1.0.0" of "2.x". De Adressering Server houdt bij het zoeken naar applicaties slechts rekening met het major nummer, omdat compatibiliteit hierdoor afdoende is geborgd. |

Het technische formaat van een *getRoutingInfo* response is:

```
200 OK
Content-Type: application/json; charset=utf-8

[ {
  "interactionId": "",
  "destinationInfo": [ {
    "destination": {
      "code": "",
      "codeSystem": ""
    },
    "fqdn": "",
    "transformationId": ""
  } ]
} ]
```

Output bestaat uit 0..n JSON objecten die, voor elk van de ontvangen interactions, de volgende inhoud bevatten. Deze objecten worden geretourneerd in de volgorde waarin de betreffende interactions werden ontvangen in het *getRoutingInfo* request.

| Name | Cardinality | Type | Toelichting |
|--------------------------------------|-------------|-----------------------|---|
| interactionId | 1..1 | String | Interactie-id van het te adresseren bericht, of van de te adresseren berichten. Wordt gevuld met de interactie waarmee de flow dient te worden vervolgd. Ook indien een transformatie is vereist. Het versie-deel van het interactionId wordt gevuld met het versie-deel in het ontvangen interactionId uit het request, of met het aortaVersion attribuut, zoals ontvangen in het request. |
| destinationInfo | 0..n | Object met attributen | Slechts aanwezig indien tenminste één geschikte GBx-applicatie is gevonden. |
| destinationInfo. destination | 1..1 | Object met attributen | Beoogde bestemming van de interactie. |
| destination.code | 1..1 | String | Beoogde bestemming van de interactie. Mogelijke waarden: <ul style="list-style-type: none"> • <appID> |
| destination. codeSystem | 1..1 | String | Het gehanteerde codesysteem. Mogelijke waarden: <ul style="list-style-type: none"> • "urn:oid:2.16.840.1.113883.2.4.6.6" (appID) |
| fqdn | 1..1 | String | FQDN van de GBx-applicatie. |
| destinationInfo. transformationId | 0..1 | String | Het ID van het uit te voeren transformatie algoritme. Slechts aanwezig indien de applicatie die het request moet beantwoorden, vereist dat eerst een transformatie wordt uitgevoerd. Wordt nooit gevuld wanneer de interactie een FHIR-operation is. |

Voorbeelden van gebruik Routing Info Interface

Interactie vanuit MedMij

Het technische formaat van een *getRoutingInfo* request is:

```

POST [base endpointadres]/getRoutingInfo
Content-Type: application/json; charset=utf-8
AORTA-ID: initialRequestID=<UUID conform RFC4122>; requestID=<UUID conform RFC4122>

{
  "destination": {
    "code": "382",
    "codeSystem": "urn:oid:2.16.528.1.1007.3.3"
  },
  "interaction": [{
    "id": "create:Observation:1.0:request"
  }]
}

```

Het technische formaat van een *getRoutingInfo* response is:

```

200 OK
Content-Type: application/json; charset=utf-8

[ {
  "interactionId": "create:Observation:1.0:request",
  "destinationInfo": [ {
    "destination": {
      "code": "5476",
      "codeSystem": "urn:oid:2.16.840.1.113883.2.4.6.6"
    },
    "fqdn": "bron.zorgaanbieder.nl",
    "transformationId": "1"
  } ]
} ]

```

In bovenstaande situatie is transformatie #1 vereist om de gevraagde FHIR-interactie af te kunnen leveren bij GBZ-applicatie #5476.

Initiatie vanuit GBx-client

Het technische formaat van een *getRoutingInfo* request is:

```

POST [base endpointadres]/getRoutingInfo
Content-Type: application/json; charset=utf-8
AORTA-ID: initialRequestID=<UUID conform RFC4122>; requestID=<UUID conform RFC4122>

{
  "destination": {
    "code": "592",
    "codeSystem": "urn:oid:2.16.528.1.1007.3.3"
  },
  "interaction": [ {
    "method": "GET",
    "url": "3287/MedicationRequest/23483147812",
    "aortaVersion": "1.0"
  }, {
    "method": "GET",
    "url": "4001/MedicationRequest/23483147813",
    "aortaVersion": "2.0"
  }, {
    "id": "search:Appointment:1.0:request"
  } ]
}

```

Het technische formaat van een *getRoutingInfo* response is:

```

200 OK
Content-Type: application/json; charset=utf-8

```

```
[{
  "interactionId": "read:MedicationRequest:1.0:request",
  "destinationInfo": [{
    "destination": {
      "code": "3287",
      "codeSystem": "urn:oid:2.16.840.1.113883.2.4.6.6"
    },
    "fqdn": "bron-1.zorgaanbieder.nl"
  }]
}, {
  "interactionId": "read:MedicationRequest:2.0:request"
}, {
  "interactionId": "search:Appointment:1.0:request",
  "destinationInfo": [{
    "destination": {
      "code": "3288",
      "codeSystem": "urn:oid:2.16.840.1.113883.2.4.6.6"
    },
    "fqdn": "bron-2.zorgaanbieder.nl",
    "transformationId": "3"
  }]
}]
```

In bovenstaande situatie is transformatie #3 vereist om de gevraagde Appointment interactie af te kunnen leveren bij GBZ-applicatie #3288. Er is géén transformatie vereist om de gevraagde MedicationRequest interactie af te kunnen leveren bij GBZ-applicatie #3287.

Aanroep vanuit Autorisatie Server ZA

Het technische formaat van een *getRoutingInfo* request is:

```
POST [base endpointadres]/getRoutingInfo
Content-Type: application/json; charset=utf-8
AORTA-ID: initialRequestID=<UUID conform RFC4122>; requestID=<UUID conform RFC4122>

{
  "destination": {
    "code": "3287",
    "codeSystem": "urn:oid:2.16.840.1.113883.2.4.6.6"
  },
  "interaction": [{
    "id": "search:MedicationRequest:1.0:request"
  }]
}
```

Het technische formaat van een *getRoutingInfo* response is:

```
200 OK
Content-Type: application/json; charset=utf-8

[{
  "interactionId": "search:MedicationRequest:1.0:request",
  "destinationInfo": [{
    "destination": {
      "code": "3287",
      "codeSystem": "urn:oid:2.16.840.1.113883.2.4.6.6"
    },
    "fqdn": "bron-1.zorgaanbieder.nl"
  }]
}]
```

In bovenstaande situatie is géén transformatie vereist om de gevraagde MedicationRequest interactie af te kunnen leveren bij GBZ-applicatie #3287.

Autorisatie Server Interfaces - 0.7.x

- Common Interfaces
 - AS Metadata Interface
 - Metadata
 - JWKS
 - AORTA Token Interface
 - MedMij Token Exchange
 - AORTA Token Exchange
 - AS-Logging Interface
 - Logging m.b.t. de MedMij Autorisatie Interface
 - Logging m.b.t. de MedMij User Interface
 - Logging m.b.t. de MedMij Token Interface
 - Logging m.b.t. de MedMij Introspection Interface (wordt uitgefaseerd met Resource Server v1)
 - Logging m.b.t. de AORTA Token Interface - MedMij Token Exchange
 - Logging m.b.t. de AORTA Token Interface - AORTA Token Exchange
- MedMij Interfaces
 - MedMij User Interface
 - MedMij Autorisatie Interface
 - MedMij Token Interface

Common Interfaces

AS Metadata Interface

Metadata

AOF.AS-I.MTD.200.v1

De metadata van de autorisatieserver kan, conform [RFC 8414](#), worden opgehaald op een well-known URL die kan worden geconstrueerd m.b.v. de <iss> claim uit het token (zie ook [section-3.1 van RFC8414](#)). Dit betekent dat bij een iss die gelijk is aan: <https://FQDN/some-path-extension>, de metadata kan worden verkregen bij: <https://FQDN/well-known/oauth-authorization-server/some-path-extension>.

De Authorization Server Metadata Response bevat de volgende attributen.

AOF.AS-I.MTD.300.v1

Autorisatie Server MedMij:

- issuer;
- authorization_endpoint;
- token_endpoint;
- jwks_uri;
- response_types_supported;
- signed_metadata.

AOF.AS-I.MTD.400.v1

Autorisatie Server ZA:

- issuer;
- token_endpoint;
- jwks_uri;
- response_types_supported;
- signed_metadata.

De response die wordt geretourneerd bevat daarnaast de volgende headers:

```
Cache-Control: must-revalidate, max-age=<max-age-metadata>
Pragma: no-cache
```

Een client mag verkregen metadata conform de Cache-Control header directives, zoals [beschreven in RFC 7234](#), cachen.

De waarde van max-age-metadata is configureerbaar in de autorisatie server. Initiële waarde is 14400 seconden (4 uur).

JWKS

AOF.AS-I.MTD.300.v1

De public key waarmee de digitale handtekening kan worden gecontroleerd wordt als een JWK beschikbaar gesteld. De URL waarop de JWK Set kan worden opgevraagd (`jwtks_uri`) maakt deel uit van de AS metadata response. Iedere JSON Web Key (JWK) in de set, die beschikbaar wordt gesteld op de `jwtks_uri`, bevat een `kid` parameter. De juiste JWK in de JWK Set wordt gevonden o.b.v. de waarde van het `kid` attribuut in de header van de ontvangen JWT.

De response die wordt geretourneerd na een HTTP GET op de `jwtks_uri` bevat naast de JWK Set de volgende headers:

```
Cache-Control: must-revalidate, max-age=<max-age-jwks>
Pragma: no-cache
```

Een client mag verkregen JWK's conform de `Cache-Control` header directives, zoals [beschreven in RFC 7234](#), cachen.

De waarde van `max-age-jwks` is configureerbaar in de autorisatie server. Initiële waarde is 14400 seconden (4 uur).

De JWK bevat de volgende attributen, waar de definitie van de attributen kan worden gevonden in [RFC 7517](#) en [RFC 7518](#):

- `"kty": "RSA"`
- `"alg": "RS256"`
- `"use": "sig"`
- `"kid": "<the identifier of the key-pair used to sign this JWT>"`
- `"x5c": "<de van toepassing zijnde keten van PKIX certificaten>"`
- `"n": "<the modulus value for the RSA public key>"`
- `"e": "<the exponent value for the RSA public key>"`

AORTA Token Interface

Middels deze interface kunnen AORTA `access_tokens` worden verkregen.

AOF.AS-I.ATI.100.v1

Bij iedere interactie die wordt geboden op de AORTA Token Interface, wordt in ieder HTTP-request, op de volgende wijze, een custom HTTP header meegezonden:

```
AORTA-ID: initialRequestID=<UUID conform RFC4122>; requestID=<UUID conform RFC4122>
```

MedMij Token Exchange

De MedMij Token Exchange Interface is gebaseerd op [OAuth token exchange](#).

AOF.AS-I.MTE.100.v1

Het MedMij Token Exchange endpoint is slechts benaderbaar voor de MedMij-in component van de resource broker.

AOF.AS-I.MTE.200.v2

De autorisatieserver ontvangt een *token exchange request* met de volgende attributen:

| Parameter | Cardinaliteit | Toelichting |
|-----------------------------------|---------------|--|
| <code>grant_type</code> | 1..1 | Vaste waarde "urn:ietf:params:oauth:grant-type:token-exchange". |
| <code>audience</code> | 1..1 | Waarde is "<appID van GBZ-applicatie>". Formaat: "urn:oid:2.16.840.1.113883.2.4.6.6.<applicatie-id>". |
| <code>requested_token_type</code> | 1..1 | Vaste waarde "urn:ietf:params:oauth:token-type:jwt". |
| <code>subject_token</code> | 1..1 | Het ontvangen MedMij access_token . |
| <code>subject_token_type</code> | 1..1 | Type aanduiding van het <code>subject_token</code> . Vaste waarde "urn:ietf:params:oauth:token-type:access_token". |

| | | |
|-------|------|--|
| scope | 1..1 | <p>Een string met daarin de gevraagde scope van autorisatie, die bestaat uit de volgende opeenvolgende delen, van elkaar gescheiden door een "~":</p> <ul style="list-style-type: none"> Een door spaties van elkaar gescheiden set van AORTA interaction-id's, bijvoorbeeld "search:Appointment:1.0:request"; De gegevensdienst, waarbinnen de interacties plaatsvinden, bijvoorbeeld "medmij.gegevensdienst.53". <p>Wanneer een transformatie is vereist voor een interactie, dan wordt dit in de scope aangegeven door het interactie-id uit te breiden met "<transformation-id>".</p> <p>Voorbeelden scope:</p> <ul style="list-style-type: none"> Opvragen van specifieke resources bij een GBZ-applicatie: "search:Coverage:1.0:request search:Patient:1.0:request~medmij.gegevensdienst.48". Aanmaken van resource bij een GBZ-applicatie, waarvoor transformatie is vereist: "create:Observation:1.0:request /1~medmij.gegevensdienst.53". |
|-------|------|--|

De autorisatieserver retourneert een *token exchange response* met de volgende attributen:

| Parameter | Cardinaliteit | Toelichting |
|---------------------|---------------|---|
| access_token | 1..1 | Een JWT-based AORTA access_token . |
| issued_token_type | 1..1 | Type aanduiding van de representatievorm van het uitgegeven access_token. Vaste waarde "urn:ietf:params:oauth:token-type:jwt". |
| token_type | 1..1 | Vaste waarde "Bearer". |
| expires_in | 1..1 | Geldigheid in seconden van het uitgegeven AORTA access_token , deze moet in overeenstemming zijn met de geldigheid van het ingewisselde MedMij access_token . |
| scope | 1..1 | Dezelfde string, zoals ontvangen in het token exchange request. |
| authenticatie_token | 1..1 | De DigiD SAML-Assertion, die wordt gecodeerd met behulp van base64url, conform RFC 4648 . |
| client_id | 1..1 | Het ID van de PGO Server waaraan het MedMij access_token is uitgereikt. |

Te hanteren error responses zijn eveneens beschreven in [RFC 8693](#).

AORTA Token Exchange

De AORTA Token Exchange Interface is gebaseerd op [OAuth token exchange](#).

AOE-AS-I.ATE.100.v2

Het AORTA Token Exchange endpoint is slechts benaderbaar voor de ZA-in component van de resource broker en voor GBx-applicaties die deel uitmaken van AORTA.

AOE-AS-I.ATE.200.v3

De autorisatieserver ontvangt een token exchange request met de volgende attributen:

| Parameter | Cardinaliteit | Toelichting |
|------------|---------------|---|
| grant_type | 1..1 | Vaste waarde "urn:ietf:params:oauth:grant-type:token-exchange" |
| client_id | 0..1 | <p>Het applID van de client die een FHIR-interactie wil initiëren. Hoefte slechts te worden meegezonden, wanneer het niet is opgenomen in het actor_token. Vooralsnog daarom slechts van toepassing voor interacties vanuit een GBP.</p> <p>Formaat: "urn:oid:2.16.840.1.113883.2.4.6.6.<applicatie-id>".</p> |

| | | |
|-------------------------|------|---|
| audience | 1..1 | <p>Bij geadresseerde interacties tussen GBZ'en:</p> <p>Waarde is "<appID van GBZ-applicatie>".</p> <p>Wanneer de client een FHIR-update of een FHIR-read interactie wil uitvoeren, dan is het juiste appID opgenomen in de base-URL van de betreffende resource instance, zoals eerder ontvangen. Instance-level interacties, zoals een read en een update dienen altijd te worden gericht aan één GBZ-applicatie, en nooit aan een URA.</p> <p>Wanneer de client een ander soortige FHIR-interactie wil uitvoeren, dan zijn er een aantal mogelijkheden:</p> <ol style="list-style-type: none"> 1. De client bepaalt zelf, m.b.v. de systeemrollen en conformances, zoals gevonden in ZORG-AB, en m.b.v. de transformatie server metadata, welk(e) GBZ-applicatie(s), eventueel na translatie, de betreffende interactie kan/kunnen ontvangen. 2. De client vraagt de Adressering Server, welk(e) GBZ-applicatie(s), eventueel na translatie, de betreffende interactie kan/kunnen ontvangen. <p>Bij interacties tussen een GBZ-applicatie en een Resource Broker component:</p> <p>Waarde is "<role van betreffende Resource Broker component>".</p> <p>Formaat van een appID: "urn:oid:2.16.840.1.113883.2.4.6.6.<applicatie-id>".</p> <p>Formaat van een URA: "urn:oid:2.16.528.1.1007.3.3.<URA>".</p> <p>Formaat van een role: "urn:oid:2.16.840.1.113883.2.4.3.111.8.<role-id>"</p> |
| request_ed_token_type | 1..1 | Vaste waarde "urn:iETF:params:oauth:token-type:jwt". |
| subject_token | 1..1 | <p><i>A security token that represents the identity of the party on behalf of whom the request is being made. Typically, the subject of this token will be the subject of the security token issued in response to the request.</i></p> <p>Wanneer geen actor_token aanwezig is, dan is het subject_token een AORTA SAML transactietoken, een SAML PKI Authenticatietoken, een SAML DigiD token.</p> <p>Wanneer wel een actor_token aanwezig is, dan is het subject token een AORTA SAML mandaattoken.</p> |
| subject_token_type | 1..1 | Type aanduiding van het subject_token. Vaste waarde "urn:iETF:params:oauth:token-type:saml2". Geeft aan dat het token een base64url-encoded SAML 2.0 Assertion is. |
| actor_token | 0..1 | <p><i>A security token that represents the identity of the acting party. Typically, this will be the party that is authorized to use the requested security token and act on behalf of the subject.</i></p> <p>Een actor_token is slechts aanwezig wanneer de acting party een andere is dan het subject.</p> <p>Een actor_token is altijd een AORTA SAML transactietoken. Het subject_token is in dat geval dan een AORTA SAML mandaattoken.</p> |
| actor_token_type | 0..1 | Type aanduiding van het actor_token. Vaste waarde "urn:iETF:params:oauth:token-type:saml2". Geeft aan dat het token een base64url-encoded SAML 2.0 Assertion is. |
| registration_token | 0..1 | Het registration_token is een AORTA SAML inschrijftoken . |
| registration_token_type | 0..1 | Type aanduiding van het registration_token. Vaste waarde "urn:iETF:params:oauth:token-type:saml2". Geeft aan dat het token een base64url-encoded SAML 2.0 Assertion is. |
| consent_token | 0..1 | Het consent_token is een AORTA SAML consent_token . |
| consent_token_type | 0..1 | Type aanduiding van het consent_token. Vaste waarde "urn:iETF:params:oauth:token-type:saml2". Geeft aan dat het token een base64url-encoded SAML 2.0 Assertion is. |

| | | |
|-------|------|--|
| scope | 1..1 | <p>Een string met daarin de gevraagde scope van autorisatie, die bestaat uit de volgende opeenvolgende delen, van elkaar gescheiden door een "~":</p> <ul style="list-style-type: none"> Een door spaties van elkaar gescheiden set van AORTA interaction-id's, bijvoorbeeld "search:Appointment:1.0:request"; De contextCode, waarbinnen de interacties plaatsvinden, bijvoorbeeld "aorta.contextcode.BGZOPV"; Een aanduiding van de situatie waarin de interactie plaatsvindt, "normaal" of "nood". Vooralnog is deze parameter gevuld met vaste waarde "normaal". <p>Voorbeelden scope:</p> <ul style="list-style-type: none"> Opvragen van specifieke resources bij een GBZ-applicatie: "search:Coverage:1.0:request search:Patient:1.0:request-aorta.contextcode.BGZOPV~normaal". Opvragen van loggegevens bij RB VnC: "search:AuditEvent:1.0:request-aorta.contextcode.LOGOPV~normaal". Aanmelden/bijwerken ACT/VWI: "update:DocumentManifest:1.1:request-aorta.contextcode.VWIREG~normaal". Aanvragen ACT/VWI-sync: "create:Task:2.0:request-aorta.contextcode.ACTSYNC~normaal". |
|-------|------|--|

Mogelijke combinaties van subject_token, actor_token, registration_token en consent_token zijn:

| Initiator | subject_token | actor_token | registration_token | consent_token |
|-----------|--|---|--|---|
| GBZ | AORTA SAML transactie_token, gesigned met een UZI-pas (zorgverlenerspas) | - | - | Aanwezig wanneer de initiator een "notified-pull" uitvoert. |
| | AORTA SAML mandaat_token, gesigned met een UZI-pas (zorgverlenerpas) | AORTA SAML transactie_token, gesigned met een UZI-pas (zorgverlenerspas of medewerkerpas op naam) | - | |
| | | AORTA SAML transactie_token, gesigned met een UZI-servercertificaat | - | Aanwezig. |
| | | | AORTA SAML inschrijf_token, gesigned met een UZI-pas (zorgverlenerpas) | - |
| GBK | SAML PKI Authenticatietoken | - | - | - |
| GBP | SAML DigiD token | - | - | - |

Voorbeeld van een token exchange request:

```

POST [base]/token
Content-Type: application/x-www-form-urlencoded
AORTA-ID: initialRequestID=<UUID conform RFC4122>; requestID=<UUID conform RFC4122>

grant_type=urn:iETF:params:oauth:token-type:token-exchange
&audience=urn:aoid:2.16.840.1.113883.2.4.6.6.352
&requested_token_type=urn:iETF:params:oauth:token-type:jwt
&subject_token=<base64url-encoded SAML Assertion>
&subject_token_type=urn:iETF:params:oauth:token-type:saml2
&actor_token=<base64url-encoded SAML Assertion>
&actor_token_type=urn:iETF:params:oauth:token-type:saml2
&registration_token=<base64url-encoded SAML Assertion>
&registration_token_type=urn:iETF:params:oauth:token-type:saml2
&consent_token=<base64url-encoded SAML Assertion>
&consent_token_type=urn:iETF:params:oauth:token-type:saml2
&scope=search:Coverage:1.0:request search:Patient:1.0:request-aorta.contextcode.BGZOPV~normaal

```

Een token exchange response bevat de volgende attributen:

| Parameter | Cardinaliteit | Toelichting |
|-------------------|---------------|--|
| access_token | 1..1 | Een JWT-based AORTA access_token . Er wordt één token uitgegeven met een audience element voor ieder te bevragen xIS van deze zorgaanbieder, die om kan gaan met het requested_token_type. |
| issued_token_type | 1..1 | Type aanduiding van de representatievorm van het uitgegeven access_token. Vaste waarde "urn:iETF:params:oauth:token-type:jwt". |
| token_type | 1..1 | Vaste waarde "Bearer". |
| expires_in | 1..1 | Geldigheid in seconden van het uitgegeven AORTA access_token . Deze bedraagt 20 seconden. |

| | | |
|-------|------|---|
| scope | 1..1 | <p>Dezelfde string, zoals ontvangen in het token exchange request, maar met daarin slechts de onderdelen die daadwerkelijk zijn toegekend.</p> <p>Wanneer een transformatie is vereist voor een interactie, dan wordt dit in de geretourneerde scope aangegeven door het interactie-id uit te breiden met "<transformation-id>".</p> <p>Voorbeelden van een geretourneerde scope:</p> <ul style="list-style-type: none"> • Opvragen van specifieke resources bij een GBZ-applicatie: "search:Coverage:1.0:request search:Patient:1.0:request~aorta.contextcode.BGZOPV~normaal". • Opvragen van resource bij een GBZ-applicatie, waarvoor transformatie is vereist: "search:Appointment:1.0:request/3~aorta.contextcode.AFSPROPV~normaal". |
|-------|------|---|

Te hanteren error responses zijn eveneens beschreven in [RFC 8693](#).

Voorbeeld van een token exchange response:

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8

{
  "access_token": "2YotnFZFEjrlzCsicMwPAA",
  "issued_token_type": "urn:ietf:params:oauth:token-type:jwt",
  "token_type": "Bearer",
  "expires_in": 20,
  "scope": "search:Appointment:1.0:request/3~aorta.contextcode.AFSPROPV~normaal"
}
```

AS-Logging Interface

AOF.AS-I.ALI.150.v1

Logbestanden die nodig zijn voor de managementrapportages kunnen, conform gemaakte afspraken in het DAP, middels een API, via HTTPS (TLS) door VZVZ-beheer worden opgehaald. Technisch formaat van de logbestanden is JSON.

De logging kan desgewenst worden opgesplitst in meerdere JSON-bestanden. Ieder JSON-bestand heeft wel altijd betrekking op interacties die plaats hebben gevonden conform één specifieke MedMij-release. Op deze manier kan in de rapportages een beeld worden gecreëerd van het gebruik van een bepaalde MedMij-release in de tijd.

De loggegevens die beschikbaar moeten worden gesteld zijn hieronder per interface van de Autorisatie Server beschreven.

Logging m.b.t. de MedMij Autorisatie Interface

AOF.AS-I.ALI.200.v1

Ontvangen authorization requests en de bijbehorende geretourneerde authorization responses of error responses:

- timestamp ontvangst
- sessie-id
- zorgaanbiedernaam
- gegevensdienst-id's en bijbehorende gegevensdienstnamen
- client_id en organisatiernaam
- timestamp tonen landingspagina
- timestamp redirect naar PGO Server
- een hash van de geretourneerde authorization code
- geretourneerde HTTP statuscodes en error-codes

Verzonden ZAB requests en de bijbehorende ontvangen ZAB responses of error responses:

- timestamp verzending
- sessie-id
- zorgaanbiedernaam
- timestamp ontvangst response
- ontvangen statuscode van ZAB
- ontvangen URA
- alle ontvangen appID's
- ontvangen error-codes

Authenticatie gebruiker:

- sessie-id
- timestamp redirect naar DigiD
- timestamp gebruiker terug van DigiD
- ontvangen statuscode van DigiD

Verzonden artefact resolve berichten en de bijbehorende geretourneerde artefact responses of error responses:

- timestamp verzending
- sessie-id
- timestamp ontvangst response
- status uit artefact response
- status van de ontvangen SAML-Assertion (duidt mogelijk op mis-use-case)
- ontvangen error-codes (duidt mogelijk op mis-use-case)

Logging m.b.t. de MedMij User Interface

AOF.AS-I.ALI.300.v1

Getoonde toestemmingspagina's en verleende of geweigerde toestemmingen:

- timestamp tonen
- sessie-id
- timestamp ontvangst keuze
- resultaat (toestemming of weigering)

Logging m.b.t. de MedMij Token Interface

AOF.AS-I.ALI.400.v1

Ontvangen access token requests en de bijbehorende geretourneerde access token responses of error responses:

- timestamp ontvangst
- sessie-id
- een hash van de ontvangen authorization code (wel zodanig dat deze kan worden gebruikt om een token request te relateren aan een authorization request)
- timestamp retour
- de jti claim van het geretourneerde access token
- geretourneerde gegevensdienst-id's (in scope attribuut)
- geretourneerde HTTP statuscodes en error-codes

Logging m.b.t. de MedMij Introspection Interface (wordt uitgefaseerd met Resource Server v1)

AOF.AS-I.ALI.500.v1

Ontvangen introspection requests en de bijbehorende geretourneerde introspection responses of error responses:

- timestamp ontvangst
- sessie-id
- de jti claim van het access token
- timestamp retour
- status token (actief of niet)
- geretourneerde HTTP statuscodes en error-codes

Logging m.b.t. de AORTA Token Interface - MedMij Token Exchange

AOF.AS-I.ALI.600.v1

Ontvangen token exchange requests en de bijbehorende geretourneerde token exchange responses of error responses

- sessie-id
- Inhoud van het ontvangen request
 - timestamp
 - de jti claim van het subject_token
 - subject_token_type
- Inhoud van de geretourneerde response
 - timestamp
 - de jti claim van het geretourneerde AORTA access_token
 - token_type
 - geretourneerde HTTP statuscodes en error-codes

Logging m.b.t. de AORTA Token Interface - AORTA Token Exchange

AOF.AS-I.ALI.700.v1

Volgt in een latere versie van AoF.

MedMij Interfaces

AOF.AS-I.MMI.100.v1

De autorisatieserver biedt een aantal MedMij interfaces. De autorisatieserver ondersteunt hierbij de volgende MedMij use cases:

- UC Verzamelen;
- UC Delen.

MedMij User Interface

AOF.AS-I.MMI.200.v1

Zie [MedMij User Interface](#).

MedMij Autorisatie Interface

AOF.AS-I.MMI.300.v1

De autorisatieserver biedt de Authorization interface, zoals gespecificeerd in de te ondersteunen releases van het MedMij afsprakenstelsel.

MedMij Token Interface

AOF.AS-I.MMI.400.v1

De autorisatieserver biedt het Token interface, zoals gespecificeerd in de te ondersteunen releases van het MedMij afsprakenstelsel.

MAP Server Interfaces - 0.7.x

- [MAP Interface](#)

MAP Interface

AOF.MAP-I.MI.100.v1

Het technische formaat van een *check* request is:

```
POST [base endpointadres]/check
Content-Type: application/json; charset=utf-8
AORTA-ID: initialRequestID=<UUID conform RFC4122>; requestID=<UUID conform RFC4122>

{
  "interactionId": [ "", "" ],
  "roleCode": {
    "code": "",
    "codeSystem": ""
  },
  "dataCategory": {
    "code": "",
    "codeSystem": ""
  }
}
```

Het *initialRequestID* attribuut bevat het ID van het allereerste request in de hele keten en dient te worden opgenomen in de logbestanden van alle partijen in de keten, zodat bij foutopsporing de verschillende logbestanden aan elkaar kunnen worden gerelateerd. Het *requestID* is voor iedere request message uniek. In requests wordt deze gegenereerd door de client. Ook het *requestID* dient te worden opgenomen in de verschillende logbestanden, zodat altijd duidelijk is op welk bericht een log entry van toepassing is.

Input parameters:

| Name | Cardinality | Type | Toelichting |
|-------------------------|-------------|--------|--|
| interactionId | 1..n | String | Interactie-id van het te verzenden bericht, of van de te verzenden berichten. |
| roleCode | 0..1 | String | Rolcode van de verantwoordelijke persoon voor de initiatie van de interactie-set. |
| roleCode.code | 1..1 | String | Het attribuut kan bevatten: <ul style="list-style-type: none">• De rolcode die hoort bij een persoon, ofwel "P"• De UZI-rolcode van een zorgverlener, ofwel "<UZI-rolcode>" |
| roleCode.codeSystem | 1..1 | String | OID. Toegestane waarden: <ul style="list-style-type: none">• "2.16.840.1.113883.2.4.3.11.8" (AORTA rolcode)• "2.16.840.1.113883.2.4.15.111" (UZI rolcode) |
| dataCategory | 0..1 | String | De contextcode die aanduidt binnen welke (zorg)toepassing de interacties worden geïnitieerd. Formaat: "urn:oid:2.16.840.1.113883.2.4.3.111.15.1.<contextcode>". |
| dataCategory.codeSystem | 1..1 | String | OID van het object "AORTA contextCodes". Waarde: "urn:oid:2.16.840.1.113883.2.4.3.111.15.1" |
| dataCategory.code | 1..1 | String | OID van de feitelijke contextcode die aanduidt binnen welke (zorg)toepassing de interacties worden geïnitieerd. |

Het technische formaat van een *check* response is:

```
200 OK
Content-Type: application/json; charset=utf-8

[ {
  "interactionId": "",
  "status": ""
} ]
```


Output bestaat uit 0..n JSON objecten die elk bestaan uit de volgende attributen:

| Name | Cardinality | Type | Toelichting |
|---------------|-------------|--------|---|
| interactionId | 1..1 | String | Interactie-id van het te verzenden bericht. |
| status | 1..1 | String | MAP autorisatiebesluit m.b.t. dit interactie-id. Mogelijke waarden: <ul style="list-style-type: none">• "Allow"• "Deny" |

Resource Broker Interfaces - 0.7.x

- Resource Broker LOG
 - RB-Logging Interface
- Resource Broker MedMij-in
 - AS FHIR Resource Broker Interface
 - MedMij CapabilityStatement Interface
 - MedMij FHIR Resource Broker Interface
 - Generiek
 - Ondersteunde MedMij gegevensdiensten
 - RS-Logging Interface
- Resource Broker ZA-in
 - AORTA FHIR Resource Broker Interface
- Resource Broker VnC
 - Verzending & Consolidatie Interface
 - Generiek
- Resource Broker APR
 - Applicatie Register Interface
 - Generiek
 - TKID-activatie
 - Bevragen Register
 - Toetsen conformances
 - Toetsen Mitz-status

Resource Broker LOG

RB-Logging Interface

AOF.RB-I.RBL.100.v1

Bij iedere interactie worden in het HTTP-request, de volgende additionele custom HTTP headers meegezonden:

- Authorization: Bearer <AORTA access_token>
- AORTA-ID: initialRequestID=<UUID conform RFC4122>; requestID=<UUID conform RFC4122>
- AORTA-Version: contentVersion=<versienummer>; acceptVersion=<versienummer>

Een token dat wordt meegezonden is in sommige gevallen een XML SAMLv2 Assertion, en in andere situaties een JSON Web Token (JWT). Een JWT bestaat uit een aantal base64 strings, die aan elkaar zijn gekoppeld met punten. Omdat een base64url geëncodeerde SAMLv2 Assertion geen punten kan bevatten, is de ontvanger altijd in staat om het type token bepalen. Een SAML Assertion dient altijd base64url te worden gecodeerd conform [RFC 4648](#). In het token, dat wordt ontvangen in een Authorization header, is informatie opgenomen over welke type inhoudelijk token het betreft en welke versie, dus bijvoorbeeld dat het gaat om een AORTA access_token.

Het attribuut contentVersion bevat de versie van de betreffende interactie die wordt gehanteerd in het request. Het attribuut acceptVersion bevat de versie of versies die door de resource broker mogen worden gehanteerd bij de verwerking van de interactie.

AOF.RB-I.RBL.200.v1

Bij iedere interactie worden in het HTTP-response, de volgende additionele custom HTTP headers meegezonden:

- AORTA-Version: contentVersion=<versienummer>

Het attribuut contentVersion bevat de daadwerkelijk gehanteerde versie.

AOF.RB-I.RBL.300.v1

Resource broker biedt een [FHIR-search interactie](#) op [AuditEvent](#) aan. Een resource client kan op de volgende wijze zoeken naar audit events:

```
GET [base]/AuditEvent{?[parameters]{&_format=[mime-type]}}
```

De waarde van de base-URL is gelijk aan:

- `https://<FQDN>{</path extension>}/fhir/<fhir-version>`

De waarde van <fhir-version> die wordt ondersteund is "R4".

Ondersteunde waarden voor `_format` zijn:

- de [mogelijke opties](#) die duiden op het [FHIR JSON formaat](#) of op het [FHIR XML formaat](#).

Ondersteunde parameters zijn:

- period

Let op! Het BSN van de patient waarnaar wordt gezocht, wordt meegegeven in het AORTA access_token, en dus niet in een query-parameter.

AOF.RB-I.RBL.400.v1

Resource broker levert AuditEvent instanties op die betrekking hebben op:

- inkomende berichten (A log) en de daarop geretourneerde responses (D log);
- uitgaand berichten (B log) en de daarop geretourneerde responses (C log);

A+D log entries zijn gecombineerd in één AuditEvent instance. Hetzelfde geldt voor B+C log entries.

AOF.RB-I.RBL.500.v1

FHIR profiel van AuditEvent:

| Attribuut | | Cardinaliteit | Opmerking |
|---|--------------------|---------------|---|
| Functioneel | Technisch | | |
| ID van rapporterende applicatie | source.observer | 1..1 | Referentie naar Device. Device.identificer bevat het app-id van de rapporterende Resource Broker component. |
| ID van initiërende organisatie en applicatie (source) | agent.type | 1..1 | Vaste waarde 110153 . |
| | agent.who | 1..1 | Referentie naar Device. Wanneer een entry betrekking heeft op een A+D log event, dan betreft dit een initiërend GBx-applicatie, en wordt ook een Organization instance meegegeven. Wanneer een entry betrekking heeft op een B+C log event, dan betreft dit de Resource Broker, en wordt geen Organization instance meegegeven. Device.identificer bevat het app-id van de verzendende applicatie. Device.owner bevat een referentie naar de hiervoor verantwoordelijke Organization. Organization.identificer bevat het organisatie-id van de verzendende organisatie, bijvoorbeeld de URA van de verzendende zorgaanbieder. |
| | agent.requestor | 1..1 | "true" |
| | agent.purposeOfUse | 0..1 | Mogelijk later gaan gebruiken voor noodsituaties. |
| ID van reagerende organisatie en applicatie (destination) | agent.type | 1..1 | Vaste waarde 110152 . |
| | agent.who | 1..1 | Referentie naar Device. Wanneer een entry betrekking heeft op een A+D log event, dan betreft dit de Resource Broker, en wordt geen Organization instance meegegeven. Wanneer een entry betrekking heeft op een B+C log event, dan betreft dit een reagerende GBx-applicatie, en wordt ook een Organization instance meegegeven. Device.identificer bevat het app-id van de ontvangende applicatie. Device.owner bevat een referentie naar de hiervoor verantwoordelijke Organization. Organization.identificer bevat het organisatie-id van de ontvangende organisatie, bijvoorbeeld de URA van de ontvangende zorgaanbieder. |
| | agent.requestor | 1..1 | "false" |
| interactie-id | type | 1..1 | "rest" voor RESTful FHIR interacties. "transmit" voor HL7v3 interacties. |
| | subtype | 0..* | "read", "create", "update", "search-type" etc. Slechts gevuld wanneer type gelijk is aan "rest". |
| | entity.type | 0..1 | Het FHIR resourcetype, waarop de FHIR-interactie betrekking had. Bijvoorbeeld "Observation" of "MedicationRequest". Slechts gevuld wanneer type gelijk is aan "rest". |

| | | | |
|---------------------------------|------------------------------|------|---|
| | entity.name | 1..1 | Het interactie-id van het request. Bijv. "search-type:Procedure:1.0" of "QUAF_IN990001NL01". Het interactie-id van de response kan hier desgewenst uit worden afgeleid. |
| gegevensdienst-id / contextcode | purposeOfEvent | 0..1 | Het type gegevens (data category) dat wordt uitgewisseld. Wordt gevuld met de contextCode (AORTA) of met een gegevensdienst-id (MedMij). system = "2.16.840.1.113883.2.4.3.111.15.1" of "???" Tom De Jong checkt bij Nictiz code = "<contextCode>" / "<gegevensdienst-id>" |
| patiënt | agent.type | 1..1 | Vaste waarde PAT. |
| | agent.who | 1..1 | Referentie naar Patient. Patient.identificer bevat het BSN van de persoon die onderwerp is van de persoonsgegevens in kwestie. |
| | agent.requestor | 1..1 | "false" wanneer de AuditEvent betrekking heeft op een interactie waarbij de patiënt zelf niet de opvrager was. "true" wanneer de AuditEvent betrekking heeft op een interactie waarbij de patiënt zelf wel de opvrager was. |
| datum en tijd van de activiteit | recorded | 1..1 | Datum/tijd van vastlegging in de log. |
| - | period | 1..1 | Periode tussen ontvangst request en retour response. |
| resultaat | outcome | 1..1 | Toegestane waarden zijn: <ul style="list-style-type: none"> • 0 - Success • 4 - Minor failure (statuscode 4xx geretourneerd) • 8 - Serious failure (statuscode 5xx geretourneerd) • 12 - Major failure (system died) |
| | outcomeDesc | 1..1 | Wordt gevuld met het volledige <i>result</i> veld uit de messageLog. Bevat dan de geretourneerde HTTP statuscode en eventuele gegenereerde foutcodes. |
| - | requestID (extension) | 1..1 | extension.url " http://www.aorta.nl/fhir/StructureDefinition/requestID " extension.valueString bevat het requestID dat wordt toegekend aan de betreffende A+D of B+C event (v3: gehele messageID van A of B log, fhir: deel van messageID van A of B log). |
| - | initialRequestID (extension) | 1..1 | extension.url " http://www.aorta.nl/fhir/StructureDefinition/initialRequestID " extension.valueString bevat het initialRequestID dat wordt toegekend aan de betreffende A+D en B+C event (v3: messageID van A log, fhir: deel van messageID van A log). Hiermee kunnen de instances aan elkaar worden gerelateerd. |

De FHIR-profielen van Device en die van Organization zijn beschreven op de pagina [AORTA FHIR-profielen](#).

Resource Broker MedMij-in

AS FHIR Resource Broker Interface

AOF.RB-I.ASF.100.v2

De AS FHIR Resource Broker Interface is nagenoeg gelijk aan de [AORTA FHIR Resource Interface](#), inclusief de gehanteerde HTTP-headers. Dit geldt zowel voor het generieke deel van de interface als voor de AORTA FHIR * interacties. In deze sectie worden daarom slechts de afwijkingen hierop beschreven.

M.b.t. de HTTP-headers die worden gebruikt geldt voor alle interacties de volgende uitzondering:

- In de Authorization header wordt een [MedMij access_token](#) meegestuurd
Authorization: Bearer <medmij_access_token>
- Tevens zal het, van DigiD ontvangen, authenticatietoken (Assertion), [base64url gecodeerd conform RFC 4648](#)) als volgt worden toegevoegd aan ieder request:
DigiD-Authenticatie: Bearer <DigiD SAML Assertion>

Een token dat wordt meegezonden is in sommige gevallen een XML SAMLv2 Assertion, en in andere situaties een JSON Web Token (JWT). Een JWT bestaat uit een aantal base64 strings, die aan elkaar zijn gekoppeld met punten. Omdat een base64url geëncodeerde SAMLv2 Assertion geen punten kan bevatten, is de ontvanger altijd in staat om het type token bepalen.

MedMij CapabilityStatement Interface

AOF.RB-I.MMC.100.v1

Resource broker biedt op zijn endpoint een [CapabilityStatement](#) aan. Een resource client kan het statement als volgt bij de resource broker opvragen:

```
GET [base]/metadata {?_format=[mime-type]}
```

De waarde van [base] is gelijk aan de in de MedMij ZAL geregistreerde ResourceEndpointUri.

Het gaat hier om een CapabilityStatement van het type "Instance", oftewel het bevat informatie over de daadwerkelijke installatie die benaderbaar is. Bovenstaande [capabilities interactie](#) is binnen FHIR verplicht voor FHIR servers.

Deze interface maakt deel uit van de resource interface, zoals gespecificeerd in het MedMij afsprakenstelsel. Op deze interface worden de additionele HTTP headers, zoals de Authorization header en de MedMij-Request-ID header, echter NIET toegepast.

MedMij FHIR Resource Broker Interface

Generiek

AOF.RB-I.MMF.100.v1

Resource broker biedt de resource interface, zoals gespecificeerd in het MedMij afsprakenstelsel. De resource broker biedt gedurende sommige perioden meerdere endpoints, d.w.z. één per actieve release van het MedMij afsprakenstelsel.



Verschil in resource interface tussen MedMij 1.2.0 en 1.3.0

Het MedMij afsprakenstelsel introduceert de HTTP header MedMij-Request-ID. Dit heeft tot gevolg dat deze header moet worden gecontroleerd (uitzondering indien afwezig) en ook moet worden gebruikt in de AORTA-ID header en in de logging van LSP+.

Ondersteunde MedMij gegevensdiensten

AOF.RB-I.OMG.100.v1

Resource broker ondersteunt de volgende MedMij gegevensdiensten:

| Gegevensdienstnaam | Gegevensdienst-ID | Technisch protocol tussen Resource Broker en Resource Server (xIS) | # inkomende interacties | # uitgaande interacties |
|--|-------------------|--|-------------------------|-------------------------|
| Verzamelen Documenten 3.0 | 51 | HL7-FHIR | 3 per document | |
| Delen Meetwaarden vitale functies 2.0 | 53 | HL7-FHIR, HL7v3 (via Transformatie Service) | 1 | |
| Verzamelen Meetwaarden vitale functies 2.0 | 52 | HL7-FHIR | 1 | |
| Verzamelen Basisgegevens zorg 3.0 | 48 | HL7-FHIR | 28 | |
| Verzamelen Basisgegevens GGZ 2.0 | 50 | HL7-FHIR | 19 | |
| Verzamelen verwijzingen naar vragenlijsten 2.0 | 59 | HL7-FHIR | 1 | |
| Delen antwoorden op vragenlijsten 2.0 | 60 | HL7-FHIR | 2 | |
| Verzamelen Afspraken 2.0 | 47 | HL7-FHIR, HL7v3 (via Transformatie Service) | 1 | |

De kolommen voor de aantallen interacties bevatten het maximum aantal interacties dat per persoon zal worden geïnitieerd om de gehele use case één maal te doorlopen.

RS-Logging Interface

AOF.RB-I.RSL.100.v2

Logbestanden die nodig zijn voor de managementrapportages kunnen, conform gemaakte afspraken in het DAP, middels een API, via HTTPS (TLS) door VZVZ-beheer worden opgehaald. Technisch formaat van de logbestanden is JSON.

De logging kan desgewenst worden opgesplitst in meerdere JSON-bestanden. Ieder JSON-bestand heeft wel altijd betrekking op interacties die plaats hebben gevonden conform één specifieke MedMij-release. Op deze manier kan in de rapportages een beeld worden gecreëerd van het gebruik van een bepaalde MedMij-release in de tijd.

AOF.RB-I.RSL.200.v1

De volgende loggegevens moeten beschikbaar worden gesteld:

| FHIR-v3 verkeer | FHIR-FHIR verkeer |
|---|--|
| <p>Ontvangen FHIR-requests en de bijbehorende geretourneerde FHIR-responses of error responses</p> <ul style="list-style-type: none"> • timestamp ontvangst • sessie-id • de jti claim van het ontvangen access token • ontvangen MedMij-Request-ID • gevraagd FHIR resourcetype • pseudo-BSN (zodanig dat ieder BSN voor eenzelfde zorgaanbieder altijd hetzelfde pseudo-BSN oplevert, maar dat hetzelfde BSN bij een andere zorgaanbieder tot een ander pseudo-BSN leidt) • timestamp retour • bij succes: grootte van de FHIR-response • error-codes (codes in OperationOutcomes) | <p>Ontvangen FHIR-requests en de bijbehorende geretourneerde FHIR-responses of error responses</p> <ul style="list-style-type: none"> • timestamp ontvangst • sessie-id • de jti claim van het ontvangen access token • ontvangen MedMij-Request-ID • gevraagd FHIR resourcetype • pseudo-BSN (zodanig dat ieder BSN voor eenzelfde zorgaanbieder altijd hetzelfde pseudo-BSN oplevert, maar dat hetzelfde BSN bij een andere zorgaanbieder tot een ander pseudo-BSN leidt) • timestamp retour • bij succes: grootte van de FHIR-response • geretourneerde WWW-Authenticate HTTP response header • geretourneerde codes in OperationOutcome(s) die de resource server zelf genereert |
| <p>Verzonden introspection requests en de bijbehorende ontvangen introspection responses of error responses</p> <ul style="list-style-type: none"> • timestamp verzending • sessie-id • de jti claim van het ontvangen access token • timestamp response • status token (actief of niet) • zorgaanbiedernaam • gegevensdienst-id's en bijbehorende gegevensdienstnamen • error-codes | <p>N.v.t.</p> |
| <p>N.v.t.</p> | <p>Verzonden ZAB requests en de bijbehorende ontvangen ZAB responses of error responses</p> <ul style="list-style-type: none"> • timestamp verzending • sessie-id • zorgaanbiedernaam • timestamp ontvangst response • ontvangen URA • alle ontvangen appID's • ontvangen error-codes |
| <p>N.v.t.</p> | <p>Verzonden token exchange requests en de bijbehorende ontvangen token exchange responses of error responses</p> <ul style="list-style-type: none"> • sessie-id • Inhoud van het verzonden request <ul style="list-style-type: none"> • timestamp • de jti claim van het subject_token (het van PGO Server ontvangen access_token) • subject_token_type • Inhoud van de ontvangen response <ul style="list-style-type: none"> • timestamp • de jti claim van het ontvangen access_token • token_type • Eventueel ontvangen error-codes |

| | |
|---|---|
| <p>Verzonden LSP-queries en de bijbehorende ontvangen LSP-responses of error responses, inclusief grootte van responses</p> <ul style="list-style-type: none"> • timestamp verzending • sessie-id • contextcode en appID's (LSP) • timestamp response • bij succes: grootte van de LSP-response • message_id (LSP) • error-codes - HL7 error-codes | N.v.t. |
| N.v.t. | <p>Verzonden FHIR-requests en de bijbehorende ontvangen FHIR-responses of error responses</p> <ul style="list-style-type: none"> • timestamp verzending • sessie-id • verzonden type FHIR-interactie (bijv. search-type of read) • verzonden Resource • verzonden zoekparameters • verzonden AORTA-Version request header • verzonden AORTA-ID request header • de jti claim van het verzonden access_token • timestamp response • bij succes: grootte van de LSP-response • ontvangen AORTA-Version response header • ontvangen AORTA-ID response header • eventueel ontvangen WWW-Authenticate HTTP response header • eventueel ontvangen OperationOutcome(s) |
| <p>HTTP- en processing errors</p> <ul style="list-style-type: none"> • sessie-id • ontvangen statuscode van introspectie bij Autorisatie Server • ontvangen statuscode van LSP • error bij XSLT-transformatie • geretourneerde statuscode | <p>HTTP- en processing errors</p> <ul style="list-style-type: none"> • sessie-id • ontvangen statuscode van ZAB • ontvangen HTTP statuscode van token exchange bij Autorisatie Server • ontvangen HTTP statuscode van LSP • geretourneerde HTTP statuscode |

Resource Broker ZA-in

AORTA FHIR Resource Broker Interface

AOF.RB-I.AFR.100.v3

De AORTA FHIR Resource Broker Interface is deels gelijk aan de [AORTA FHIR Resource Interface](#), inclusief de gehanteerde HTTP-headers. Dit geldt zowel voor het generieke deel van de interface als voor de AORTA FHIR * interacties. In deze sectie worden daarom slechts de afwijkingen hierop beschreven.

De waarde van de base-URL van de FHIR endpoints die de Resource Broker biedt t.b.v. de AORTA FHIR Resource Broker Interface ([base] dus), dient voor alle FHIR-interacties gelijk te zijn aan:

- `https://<FQDN>{</path extension>}/fhir/<fhir-version>`

De waarde van <fhir-version> is dan bijvoorbeeld "STU3", "R4" of "R5".

Resource Broker VnC

AOF.RB-I.VCI.50.v1

De waarde van de base-URL ([base]) van de FHIR endpoints die de Resource Broker VnC biedt , dient voor alle FHIR-interacties gelijk te zijn aan "https://<FQDN>{</path extension>}/fhir/<fhir-version>". De waarde van <fhir-version> is dan bijvoorbeeld "R4" of "R5".

Verzending & Consolidatie Interface

Generiek

AOF.RB-I.VCI.100.v3

De Verzending & Consolidatie Interface is nagenoeg gelijk aan de [AORTA FHIR Resource Interface](#). Dit geldt zowel voor het generieke deel van de interface als voor de AORTA FHIR * interacties. In deze sectie worden daarom slechts de afwijkingen hierop beschreven.

M.b.t. de HTTP headers die worden gebruikt gelden voor alle interacties de volgende extra headers:

- Conditionele request header: `DigiD-Authenticatie: Bearer <authenticatietoken>`

Een request die is gestuurd door een patiënt (via MedMij of een GBP) dient altijd een DigiD-Authenticatie header te bevatten.

Vooralsnog hoeven slechts JWT-based access_tokens, en SAML-based authenticatietokens te worden ondersteund.

Een token dat wordt meegezonden is in sommige gevallen een XML SAMLv2 Assertion, en in andere situaties een JSON Web Token (JWT). Een JWT bestaat uit een aantal base64 strings, die aan elkaar zijn gekoppeld met punten. Omdat een base64url geëncodeerde SAMLv2 Assertion geen punten kan bevatten, is de ontvanger altijd in staat om het type token bepalen.

Een SAML Assertion dient altijd base64url te worden gecodeerd conform [RFC 4648](#).

Resource Broker APR

Applicatie Register Interface

Generiek

AOF.RB-I.ARI.100.v2

Bij alle interacties die worden geboden door de applicatie register interface worden de volgende HTTP headers toegepast:

- Bij iedere interactie wordt in ieder HTTP-request, op de volgende wijze, een custom HTTP header meegezonden:
`AORTA-ID: initialRequestID=<UUID conform RFC4122>; requestID=<UUID conform RFC4122>`

Het initialRequestID attribuut bevat het ID van het allereerste request in de hele keten en dient te worden opgenomen in de logbestanden van alle partijen in de keten, zodat bij foutopsporing de verschillende logbestanden aan elkaar kunnen worden gerelateerd. Het requestID is voor iedere request message uniek. In requests wordt deze gegenereerd door de client. Ook het requestID dient te worden opgenomen in de verschillende logbestanden, zodat altijd duidelijk is op welk bericht een log entry van toepassing is.

TKID-activatie

AOF.RB-I.ARI.200.v1

Resource broker biedt een interactie aan, waarmee één of meerdere TKID's voor een xIS-instantie, op een aangegeven base endpointadres, kunnen worden geactiveerd.

Het technische formaat van een activate request is:

```
POST [base endpointadres]/activate
Content-Type: application/json; charset=utf-8
AORTA-ID: initialRequestID=<UUID conform RFC4122>; requestID=<UUID conform RFC4122>
AORTA-Version: contentVersion=<versienummer>; acceptVersion=<versienummer>

{
  "app-id": "<app-id>",
  "tkid": ["string", "string"]
}
```

| In Parameters: | | | |
|----------------|--------------|--------|---|
| Name | Cardinali ty | Type | Toelichting |
| app-id | 1..1 | string | Het app-id van de GBx-applicatie waarvoor de TKID('s) geactiveerd dienen te worden. Het betreft het app-id zonder aanduiding van een namingsysteem of root OID. |

| | | | |
|------|------|--------|---|
| tkid | 0..* | string | TKID die is toegekend tijdens AORTA acceptatie. |
|------|------|--------|---|

Het technische formaat van een activate response is:

```
200 OK
AORTA-Version: contentVersion=<versienummer>
```

Toelichting TKID

Middels een activatie van een TKID geeft de GBZ-beheerder aan dat het voor de xIS-instantie, die wordt aangeduid met het applicatieID, een bepaalde set van reeds verkregen acceptaties (nader aangeduid door een set van xIS-type kwalificaties ID's - TKID's) wil activeren. Als gevolg hiervan worden de AORTA systeemrollen, waarvoor het xIS-type blijkens de TKID's is geaccepteerd, in het APR gekoppeld aan de xIS-instantie (de Applicatie). Nadat deze actie is voltooid, kunnen de FHIR capabilities die deel uitmaken van deze AORTA systeemrollen, via de resource broker, bij het xIS worden aangesproken. **Bij een activatie wordt een eventueel eerder geregistreerde set van TKID's vervangen door de nieuwe set van TKID's.** Indien er een probleem is met één van de TKID's in een set, dan wordt de gehele transactie afgewezen en verandert er dus niets. Het is ook mogelijk om geen enkele tkid te activeren (door geen tkid attribueert op te nemen in de body van het request).

Bevragen Register

AOF.RB-I.ARI.300.v1

Het technische formaat van een *getApplication* request is:

```
POST [base endpointadres]/getApplication
Content-Type: application/json; charset=utf-8
AORTA-ID: initialRequestID=<UUID conform RFC4122>; requestID=<UUID conform RFC4122>
{
  "applicationId": ""
}
```

Input parameters:

| Name | Cardinality | Type | Toelichting |
|---------------|-------------|--------|--|
| applicationId | 1 | String | Formaat van een applID: "urn:oid:2.16.840.1.113883.2.4.6.6.<applicatie-id>". |

Het technische formaat van een *getApplication* response is:

```
200 OK
Content-Type: application/json; charset=utf-8
{
  "applicationId": "",
  "active": "",
  "address": "",
  "systemRoles": [""],
  "conformances": [{
    "interactionId": "",
    "send": "",
    "receive": ""
  }]
}
```

AOF.RB-I.ARI.400.v1

Het technische formaat van een *getApplications* request is:

```
POST [base endpointadres]/getApplications
Content-Type: application/json; charset=utf-8
AORTA-ID: initialRequestID=<UUID conform RFC4122>; requestID=<UUID conform RFC4122>
{
  "ura": ""
}
```

Input parameters:

| Name | Cardinality | Type | Toelichting |
|------|-------------|--------|---|
| ura | 1 | String | Formaat van een URA: "urn:oid:2.16.528.1.1007.3.3.<URA>". |

Het technische formaat van een *getApplications* response is:

```
200 OK
Content-Type: application/json; charset=utf-8
```

```
[{
  "applicationId": "",
  "active": "",
  "address": "",
  "systemRoles": [],
  "conformances": [{
    "interactionId": "",
    "send": "",
    "receive": ""
  }]
}]
```

Inhoud van een application object:

| Name | Cardinality | Type | Toelichting |
|----------------------------|-------------|-----------------------|---|
| applicationId | 1..1 | String | Waarde is "<appID van GBx-applicatie>" Formaat van een appID: "urn:oid:2.16.840.1.113883.2.4.6.6.<applicatie-id>". |
| active | 1.1 | String | Waarde "true" of "false". |
| address | 1..1 | String | FQDN waarop de GBx-applicatie kan worden bereikt. |
| systemRoles | 0..n | String | Codes van de ondersteunde systeemrollen |
| conformances | 0..n | Object met attributen | Informatie over de ondersteunde conformances |
| conformances.interactionId | 1..1 | String | Het interactie-id |
| conformances.send | 1..1 | String | Waarde "true" of "false". |
| conformances.receive | 1..1 | String | Waarde "true" of "false". |

Toetsen conformances

AOF.RB-I.ARI.500.v1

Resource broker biedt een interactie aan, waarmee kan worden bepaald of een bepaalde GBx-applicatie, gegevens conformances bevat.

Het technische formaat van een *hasConformance* request is:

```
POST [base endpointadres]/hasConformance
Content-Type: application/json; charset=utf-8
AORTA-ID: initialRequestID=<UUID conform RFC4122>; requestID=<UUID conform RFC4122>
{
  "applicationId": "",
  "interactionId": ["", ""]
}
```

Input parameters:

| Name | Cardinality | Type | Toelichting |
|---------------|-------------|--------|---|
| applicationId | 1..1 | string | Het app-id van de GBx-applicatie waarvoor de toets moet worden uitgevoerd. Het betreft het app-id zonder aanduiding van een namingsysteem of root OID. |
| interactionId | 1..n | String | Te toetsen interaction-id. Het versie-deel in het id attribuut wordt gespecificeerd conform semver , dus bijvoorbeeld "1.0.0" of "2.x". Resource Broker APR houdt bij het zoeken naar applicaties slechts rekening met het major nummer, omdat compatibiliteit hierdoor afdoende is geborgd. |

Het technisch formaat van een hasConformance response is:

```
200 OK
Content-Type: application/json; charset=utf-8

{
  "applicationId": "",
  "fqdn": "",
  "conformanceStatus": [{
    "interactionId": "",
    "status": ""
  }]
}
```

Output parameters:

| Name | Cardinality | Type | Toelichting |
|---------------------------------|-------------|-----------------------|---|
| applicationId | 1..1 | string | Het app-id van de GBx-applicatie waarvoor de toets moet worden uitgevoerd. Het betreft het app-id zonder aanduiding van een namingsystem of root OID. |
| fqdn | 1..1 | String | FQDN van de GBx-applicatie, die hoort bij het app-id. |
| conformanceStatus | 1..n | Object met attributen | Eén object voor ieder te toetsen interaction-id. |
| conformanceStatus.interactionId | 1..1 | String | Het getoetste interaction-id. Wordt gevuld met het ontvangen interactionId uit het request. |
| conformanceStatus.status | 1..1 | String | Informatie over of dit interactie-id al dan niet wordt ondersteund. Mogelijke waarden: <ul style="list-style-type: none"> • "Yes" • "No" |

Toetsen Mitz-status

AOF.RB-I.ARI.600.v1

Resource broker biedt een interactie aan, waarmee kan worden bepaald of een bepaalde GBx-applicatie gebruik maak van Mitz voor registratie en toetsing van patiënttoestemming.

Het technische formaat van een *isMitzClient* request is:

```
POST [base endpointadres]/isMitzClient
Content-Type: application/json; charset=utf-8
AORTA-ID: initialRequestID=<UUID conform RFC4122>; requestID=<UUID conform RFC4122>
{
  "applicationId": ""
}
```

Input parameters:

| Name | Cardinality | Type | Toelichting |
|---------------|-------------|--------|---|
| applicationId | 1..1 | string | Het app-id van de GBx-applicatie waarvoor de toets moet worden uitgevoerd. Het betreft het app-id zonder aanduiding van een namingsystem of root OID. |

Het technische formaat van een *isMitzClient* response is:

```
200 OK
Content-Type: application/json; charset=utf-8

{
  "status": ""
}
```

Output parameters:

| Name | Cardinality | Type | Toelichting |
|------|-------------|------|-------------|
|------|-------------|------|-------------|

| | | | |
|--------|------|--------|---|
| status | 1..1 | String | Informatie over of de GBx-applicatie gebruik maakt van Mitz. Mogelijke waarden: <ul style="list-style-type: none">• "Yes"• "No" |
|--------|------|--------|---|

Resource Server Interfaces - 0.7.x

- [HL7-FHIR Resource Server](#)
 - [Generiek voor alle FHIR resource server interfaces](#)
 - [AORTA CapabilityStatement Interface](#)
 - [AORTA FHIR Resource Interface](#)
 - [Generiek](#)
 - [AORTA FHIR read](#)
 - [AORTA FHIR search](#)
 - [AORTA FHIR create](#)
 - [AORTA FHIR update](#)
 - [AORTA FHIR batch/transaction](#)
 - [AORTA FHIR \\$is-allowed](#)
 - [Omgang met id, fullUrl en reference](#)
- [HL7-v3 Resource Server](#)
 - [AORTA v3-interface](#)

HL7-FHIR Resource Server

Generiek voor alle FHIR resource server interfaces

AOF.RS-I.GEN.100.v2

De volgende eisen gelden voor alle interfaces van de resource server:

1. De waarde van de base-URL van de FHIR endpoints die een resourceserver biedt ([base] dus), dient voor alle FHIR-interacties gelijk te zijn aan:
 - a. Indien <fhir-version> gelijk is aan STU3: <https://<FQDN>/fhir>, dus bijvoorbeeld "<http://myhost.customer.org/fhir>"
 - b. Indien <fhir-version> hoger dan STU3: <https://<FQDN>/fhir/<fhir-version>>, dus bijvoorbeeld "<http://myhost.customer.org/fhir/R4>"

De waarde van <fhir-version> is dan bijvoorbeeld "R4" of "R5".

AORTA CapabilityStatement Interface

AOF.RS-I.ACI.100.v1

Resource server biedt op zijn endpoint een [CapabilityStatement](#) aan. Een resource client kan het statement als volgt bij de resource server opvragen:

```
GET [base]/metadata {?_format=[mime-type]}
```

Het gaat hier om een CapabilityStatement van het type "Instance", oftewel het bevat informatie over de daadwerkelijke installatie die benaderbaar is. Bovenstaande [capabilities interactie](#) is binnen FHIR verplicht voor FHIR servers en dient binnen AORTA als een equivalent van de Ping-Pong interactie in HL7v3.

Op deze interface worden de additionele HTTP headers, die gelden voor de AORTA Resource Interface, NIET toegepast.

AORTA FHIR Resource Interface

Generiek

AOF.RS-I.FRI.100.v2

Via de AORTA Resource Interface kunnen verschillende services worden aangeroepen op een resource server. Deze services zijn in een use case formaat omschreven op de UC Resource Server pagina. Op deze pagina wordt voor iedere service verwezen naar de van toepassing zijnde implementatiehandleiding, zoals opgesteld en beheerd door Nictiz.

Ten opzichte van de Nictiz implementatiehandleidingen gelden voor alle interacties de volgende uitzonderingen:

- **Verplichte request header:** `Authorization: Bearer <AORTA_access_token>`

Een token dat wordt meegezonden is in sommige gevallen een XML SAMLv2 Assertion, en in andere situaties een JSON Web Token (JWT). Een JWT bestaat uit een aantal base64 strings, die aan elkaar zijn gekoppeld met punten. Omdat een base64url geëncodeerde SAMLv2 Assertion geen punten kan bevatten, is de ontvanger altijd in staat om het type token te bepalen.

Een SAML Assertion dient altijd base64url te worden gecodeerd conform [RFC 4648](#).

In het token, dat wordt ontvangen in een Authorization header, is informatie opgenomen over welke type inhoudelijk token het betreft en welke versie, dus bijvoorbeeld dat het gaat om een AORTA access_token.

AOF.RS-I.FRI.200.v2

- Bij iedere interactie wordt in ieder HTTP-request, op de volgende wijze, een custom HTTP header meegezonden:
AORTA-ID: initialRequestID=<UUID conform RFC4122>; requestID=<UUID conform RFC4122>
- Bij iedere interactie wordt in het HTTP-request op de volgende wijze een custom HTTP header meegezonden, met daarin de versie van de betreffende interactie die wordt gehanteerd in het request en de versie of versies die door de resource server mogen worden gehanteerd bij de verwerking van de interactie:
AORTA-Version: contentVersion=<versienummer>; acceptVersion=<versienummer>
- Bij iedere interactie wordt in de HTTP-response op de volgende wijze een custom HTTP header meegezonden met daarin de door resource server daadwerkelijk gehanteerde versie en, indien transformatie heeft plaatsgevonden, het ID van het transformatie algoritme waarmee de response tot stand is gekomen:
AORTA-Version: contentVersion=<versienummer>; transformationId=<ID van het gehanteerde transformatie algoritme>

AOF.RS-I.FRI.300.v1

Gebruik van de AORTA-ID header

Het initialRequestID attribuut bevat het ID van het allereerste request in de hele keten van resource client tot resource server. Voor interacties vanuit het MedMij netwerk bevat het initialRequestID attribuut de waarde van het MedMij-Request-ID dat werd ingestuurd door de PGO server. Het initialRequestID dient te worden opgenomen in de logbestanden van alle partijen in de keten (Resource Client, Resource Broker, Transformatie Server en Resource Server), zodat bij foutopsporing de verschillende logbestanden aan elkaar kunnen worden gerelateerd.

Het requestID is voor iedere request message uniek. In requests wordt deze gegenereerd door de client. Ook het requestID dient te worden opgenomen in de verschillende logbestanden, zodat altijd duidelijk is op welk bericht een log entry van toepassing is.

AOF.RS-I.FRI.400.v1

Gebruik van de AORTA-Version header

Wanneer een resource server een FHIR interactie ontvangt, dan kan het a.d.h.v. de syntax van het ontvangen request afleiden om welke interactie het gaat, bijvoorbeeld "een FHIR-search naar Observations", of "een FHIR-read van een Binary". Iedere interactie is voorzien van een versienummer. Voor versienummering wordt gebruik gemaakt van semantic versioning.

Het versienummer in de acceptVersion wordt gespecificeerd conform [semver](#), dus bijvoorbeeld "2.x" of "~1.2.3 || ^2.1.0". In de contentVersion dient het versienummer de exacte versie (naar keuze met of zonder patchnummer) te bevatten die is gehanteerd, dus zonder wildcards of ranges, bijvoorbeeld "2.2" of "2.3.2". De contentVersion geeft aan welke versie van de interactie daadwerkelijk is gehanteerd in de request of response. De acceptVersion geeft aan conform welke versie(s) de interactie mag worden verwerkt en beantwoord.

In het algemeen geldt dat een resource server een interactie dient te verwerken conform de hoogst aangegeven acceptVersion die het zelf op dat moment kan toepassen. In de MedMij use case zal de acceptVersion die wordt ingestuurd door Resource Broker MedMij-in in eerste instantie slechts één waarde bevatten.

AOF.RS-I.FRI.500.v1

Encoding van pipe symbolen

Wanneer zoekparameters van het type uri worden gebruikt, dan dienen eventuele "|" symbolen conform [RFC 3986](#) te worden geëncodeerd. De Resource Broker componenten encoderen "|" symbolen in FHIR interacties die zij verzenden. Resource Broker MedMij-in dient echter ook om te kunnen gaan met situaties waarbij een PGO Server een "|" symbool niet encodeert.

Zie ook de vraag die hierover is gesteld in [BITS](#).

AORTA FHIR read

AOF.RS-I.FRE.100.v1

De resource client initieert een [FHIR read interactie](#) bij de resource server en gebruikt hiervoor de HTTP GET Method op de volgende wijze:

```
GET [base]/[type]/[id]
```

Waarbij [type] het FHIR resourcetype aangeeft. Middels [id] wordt de juiste resource instance (op het betreffende FHIR endpoint) geïdentificeerd.

AORTA FHIR search

AOF.RS-I.FSE.100.v1

De resource client initieert een [FHIR search interactie](#) bij de resource server en gebruikt hiervoor de HTTP GET Method op de volgende wijze:

```
GET [base]/[type]{?[parameters]}
```

Waarbij [type] het FHIR resourcetype aangeeft. Middels [parameters] kan de zoekopdracht worden verfijnd.

AORTA FHIR create

AOF.RS-I.FCR.100.v1

De resource client initieert een [FHIR create interactie](#) bij de resource server en gebruikt hiervoor de HTTP POST Method op de volgende wijze:

```
POST [base]/[type]
```

Waarbij [type] het FHIR resourcetype aangeeft.

AOF.RS-I.FCR.200.v1

Wanneer de resource succesvol kan worden gecreëerd, dan retourneert de resource server ook de volgende location header:

- Location: [base]/[type]/[id]/_history/[vid]

Waarbij [id] en [vid] het [resource.id](#) en het versie id zijn van de zojuist gecreëerde resource instance.

AORTA FHIR update

AOF.RS-I.FUP.100.v1

De resource client initieert een [FHIR update interactie](#) bij de resource server en gebruikt hiervoor de HTTP PUT Method op de volgende wijze:

```
PUT [base]/[type]/[id]
```

Waarbij [type] het FHIR resourcetype aangeeft. Middels [id] wordt de juiste resource instance (op het betreffende FHIR endpoint) geïdentificeerd.

AORTA FHIR batch/transaction

AOF.RS-I.FBT.100.v1

De resource client initieert een [FHIR batch/transaction interactie](#) bij de resource server en gebruikt hiervoor de HTTP POST Method op de volgende wijze:

```
POST [base]
```

De inhoud van de POST is een FHIR Bundle van het type *batch of transaction*. Iedere Entry in de Bundle bevat een specifiek FHIR interactie die moet worden uitgevoerd.

Binnen AORTA kan een resource server afzonderlijk worden gekwalificeerd en geaccepteerd voor een AORTA FHIR batch interactie en voor een AORTA FHIR transaction interactie.

AOF.RS-I.FBT.200.v1

Ondersteunde FHIR interacties binnen een *batch* type Bundle:

- AORTA FHIR create.

AOF.RS-I.FBT.300.v1

Ondersteunde FHIR interacties binnen een *transaction* type Bundle:

- AORTA FHIR create;
- AORTA FHIR update.

Deze sets zullen in de loop van de tijd worden uitgebreid.

AOF.RS-I.FBT.400.v1

Interacties die zijn opgenomen in de Bundle dienen afzonderlijk te worden verwerkt conform de specificaties van de betreffende interactie. Daarnaast gelden de algemene FHIR verwerkingsregels voor *batch* en *transaction* type Bundles.

De HTTP-headers, zoals de `Authorization`, `AORTA-ID` en `AORTA-Version` headers gelden voor de gehele batch/transaction en zijn daarmee van toepassing op alle individuele interacties die zijn opgenomen in de Bundle.

AORTA FHIR \$is-allowed

AOF.RS-I.ISA.100.v2

De resource server ondersteunt op haar endpoint een custom FHIR operation, waarmee een resource client kan achterhalen of een zorgaanbieder:

- bepaalde gegevens, los van het feit of deze gegevens daadwerkelijk aanwezig zijn, beschikbaar stelt voor opvraag door een specifieke patiënt (middels een "verzamel-gegevensdienst"), danwel
- ontvankelijk is voor bepaalde gegevens die een specifieke patiënt haar wenst te sturen (middels een "delen-gegevensdienst"). Hierbij dienen tenminste de ontvankelijkheidscriteria te worden getoetst die zijn gespecificeerd in het MedMij afsprakenstelsel.

AOF.RS-I.ISA.200.v1

Een resource server dient een beschikbaarheids- of ontvankelijkheidsvraag te kunnen beantwoorden voor alle MedMij Verzamelen en Delen gegevensdiensten waarvoor het een rol vervult.

AOF.RS-I.ISA.300.v1

Een resource client kan de beschikbaarheid- of ontvankelijkheidsstatus als volgt ophalen:

```
GET [base]$is-allowed?scope=<scope aanduiding>
```

AOF.RS-I.ISA.400.v1

Het BSN van de betreffende patient is opgenomen in het `access_token`.

AOF.RS-I.ISA.500.v1

| In Parameters: | | | | |
|------------------------|---|------------------|---------------------------------|--|
| N a m e | C a r d i n a l i t y | T y p e | B i n d i n g | Toelichting |
| s c o p e | 1..1 | string | | De scope, waarvoor de status dient te worden bepaald. De parameter wordt gevuld met de string " <a href="http://fhir.nl/fhir/NamingSystem/medmij-scope <scope>">http://fhir.nl/fhir/NamingSystem/medmij-scope <scope> ". Voor de MedMij use case is de waarde van <scope> gelijk aan de scope van het MedMij Authorization Request, zoals gespecificeerd in het MedMij afsprakenstelsel. |
| Out Parameters: | | | | |
| N a m e | C a r d i n a l i t y | T y p e | B i n d i n g | Toelichting |
| re t u r n | 1..1 | OperationOutcome | | <p>Indien de operation succesvol kan worden verwerkt, dan worden een HTTP statuscode 200 en een OperationOutcome geretourneerd. Wanneer het aangegeven gebruik van één van de aangegeven scope-onderdelen bij deze zorgaanbieder is toegestaan, dan wordt de OperationOutcome als volgt gevuld:</p> <ul style="list-style-type: none"> • <i>issue.severity = information</i> • <i>issue.code = informational</i> • <i>issue.diagnostics = <de feitelijk scope die is toegestaan, eveneens voorzien van het namingsysteem "medmij-scope"></i> <p>Het retourneren van de feitelijk toegestane scope is nodig, omdat een scope meerdere onderdelen kan bevatten en deze mogelijk niet allemaal worden toegestaan.</p> <p>Wanneer géén van de aangegeven "verzamel-gegevensdiensten" bij deze zorgaanbieder is toegestaan, dan wordt de OperationOutcome als volgt gevuld:</p> <ul style="list-style-type: none"> • <i>issue.severity = information</i> • <i>issue.code = suppressed</i> <p>Wanneer géén van de aangegeven "delen-gegevensdiensten" bij deze zorgaanbieder is toegestaan, dan wordt de OperationOutcome als volgt gevuld:</p> <ul style="list-style-type: none"> • <i>issue.severity = information</i> • <i>issue.code = forbidden</i> <p>Indien de operation niet succesvol kan worden verwerkt, dan kan in sommige gevallen ook een OperationOutcome geretourneerd dienen te worden. De HTTP statuscode die wordt geretourneerd is dan echter niet gelijk aan 200.</p> <p>Een verzoek waarbij de scope bestaat uit een combinatie van (een) verzamel-gegevensdienst(en) en (een) delen-gegevensdienst(en) dient te worden beschouwd als een ongeldig verzoek.</p> |

 Voorbeeld \$is-allowed

HTTP request:

```
GET [base]$is-allowed?scope=http://fhir.nl/fhir/NamingSystem/medmij-scope|eenofanderezorgaanbieder~53 HTTP /1.1
```

XML-based HTTP response wanneer gebruik gegevensdienst is toegestaan:

200 OK

[andere headers]

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<OperationOutcome xmlns="http://hl7.org/fhir">
```

```
  <id value="0e855422-b8ef-4247-9443-f3747e78747e" />
```

```
  <issue>
```

```
    <severity value="information" />
```

```
    <code value="informational" />
```

```
    <diagnostics value="http://fhir.nl/fhir/NamingSystem/medmij-scope|eenofanderezorgaanbieder~53" />
```

```
  </issue>
```

```
</OperationOutcome>
```

XML-based HTTP response wanneer gebruik van een **delen**-gegevensdienst **niet** is toegestaan:

200 OK

[andere headers]

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<OperationOutcome xmlns="http://hl7.org/fhir">
```

```
  <id value="0e855422-b8ef-4247-9443-f3747e78747e" />
```

```
  <issue>
```

```
    <severity value="information" />
```

```
    <code value="forbidden" />
```

```
  </issue>
```

```
</OperationOutcome>
```

JSON-based HTTP response wanneer gebruik van een **verzamelen**-gegevensdienst **niet** is toegestaan:

200 OK

[andere headers]

```
{
  "resourceType": "OperationOutcome",
  "id": "0e855422-b8ef-4247-9443-f3747e78747e",
  "issue": [{
    "severity": "information",
    "code": "suppressed"
  }]
}
```

Omgang met id, fullUrl en reference

De MedMij informatiestandaard stelt:

- When a client performs a search on a server, all instances in the returned searchset Bundle SHOULD have the id field populated.
 - Omitting ids is strongly discouraged as it breaks the assumptions about RESTful behavior. However, a server that omits ids is still considered conformant when the conditions below are met:
 - The server does not natively support logical ids
 - And the use case doesn't require read / update / delete / patch support for any of the returned or referenced resources, as stated by the CapabilityStatement for the information standard.
 - And the server includes all referenced resources in the searchset Bundle (regardless of whether the client asked to do so).
- When a client reads, updates or otherwise addresses an existing resource on a server, the id element SHALL be populated in the request and response, and it SHALL match the id in the request URL.

AOF.RS-I.IFR.100.v1

AORTA eis m.b.t. vulling van resource.id

Een FHIR resource die door een bronsysteem wordt opgeleverd in een search kan zijn voorzien van een id attribuut, binnen FHIR ook wel aangeduid als een *logical id*. Dit is een technische sleutel die geacht wordt uniek te zijn en hetzelfde te blijven binnen een resource server, zodat duplicaten eenduidig kunnen worden herkend. Het id attribuut is verplicht wanneer de informatiestandaard voor een gegevensdienst één of meerdere interacties bevat (bijvoorbeeld een read- of een update-interactie) waarvoor het resource.id attribuut nodig is.

Wanneer een resource server Resource.id vult, dan dient deze te voldoen aan de eisen die FHIR stelt aan *logical id's*.

De informatiestandaard stelt verder dat:

- If an instance can be accessed on the server using RESTful operations, the id of that instance in the Bundle will be populated. The corresponding fullUrl in this case SHALL be the absolute URL to the instance on the server.
- Instances within the Bundle may use relative references to each other, like they are on the same server.
- When id-less instances need to be referenced from within a Bundle, there are two alternatives:
 - UUIDs can be used as single-use ids that will change each time the Bundle is generated. The fullUrl for the instance will be the UUID prefixed with urn:uuid:
 - OIDs can be used if the instance has an OID-based business identifier (i.e. the identifier field), like the UZI number of a healthcare provider. The fullUrl will be the OID prefixed with urn:oid:
 - Instances within the Bundle should use the prefixed version of the UUID/OID for referencing.

De FHIR core standaard stelt dat:

- The fullUrl element SHALL have a value except that: * fullUrl can be empty on a POST (although it does not need to when specifying a temporary id for reference in the bundle) * Results from operations might involve resources that are not identified.

Iedere entry in een FHIR Bundle die wordt opgeleverd of verstuurd dient te voldoen aan bovenstaande eisen.

AOF.RS-I.IFR.200.v1

Vulling van bundle.entry.fullUrl en transformatie van URL's

Een absolute fullUrl, die wijst naar de instance op de server, is slechts vereist wanneer een resource instance in de Bundle middels een FHIR-read, FHIR-update, FHIR-patch of een FHIR-delete moet kunnen worden benaderd. Een fullUrl in de bundle entry wordt in andere situaties gevuld met een single-use UUID, of met een OID.

Wanneer een Resource Server een FHIR Bundle retourneert met een absolute URL (fullUrl of reference), dan dient deze URL het volgende formaat te hebben:

- <base endpointadres van Reagerend xIS>/<type>/<id>

Resource Broker MedMij-in of Resource Broker ZA-in transformeert de URL in deze situaties naar volgende formaat:

- <base endpointadres van Resource Broker XX-in>/<appID>/<type>/<id>

Waarbij het <type> het geretourneerde resource type bevat, bijvoorbeeld "Observation" en <appID> het applicatie-id (zonder root OID) bevat van het bronsysteem.

Bovenstaande aanpassing van absolute URL's is nodig, zodat een Resource Client, indien van toepassing binnen een gegevensdienst, in staat is om, o.b.v. de URL in het zoekresultaat, een FHIR-read, FHIR-update, FHIR-patch of een FHIR-delete uit te voeren via de Resource Broker.

Voorbeeld van een Bundle

Een voorbeeld van een Bundle die het gebruik van id, fullUrl en reference illustreert is hieronder weergegeven.

```

<Bundle>
  ..
  <Entry>
    <fullUrl value="https://medmij-pgo.vzvz.nl/fhir/453782/Patient/4" />
    <Patient>
      <id value="4" />
      ..
    </Patient>
  </Entry>
  <Entry>
    <fullUrl value="urn:uuid:0e855422-b8ef-4247-9443-f3747e78747e" />
    <Patient>
      <!-- Onderstaande id mag op deze wijze worden gevuld, maar mag in deze situatie ook worden weggelaten -->
      <id value="0e855422-b8ef-4247-9443-f3747e78747e" />
      ..
    </Patient>
  </Entry>
  <Entry>
    <fullUrl value="https://medmij-pgo.vzvz.nl/fhir/453782/Observation/10" />
    <Observation>
      <id value="10" />
      <subject>
        <reference value="Patient/4" />
      </subject>
      ..
    </Observation>
  </Entry>
  <Entry>
    <fullUrl value="https://medmij-pgo.vzvz.nl/fhir/453782/Observation/11" />
    <Observation>
      <id value="11" />
      <subject>
        <reference value="urn:uuid:0e855422-b8ef-4247-9443-f3747e78747e" />
      </subject>
      ..
    </Observation>
  </Entry>
  <Entry>
    <fullUrl value="https://medmij-pgo.vzvz.nl/fhir/453782/Observation/12" />
    <Observation>

```

```
        <id value="12" />
        <subject>
            <reference value="https://medmij-pgo.vz.vz.nl/fhir/453782/Patient/5" />
        </subject>
        ..
    </Observation>
</Entry>
..
</Bundle>
```

HL7-v3 Resource Server

AORTA v3-interface

AOF.RS-I.AV3.100.v1

De interface specificaties zijn opgenomen in de HL7v3-Implementatiehandleidingen.

Transformatie Server Interfaces - 0.7.x

- [Overzicht transformaties](#)
- [TS Metadata Interface](#)
- [Transformatie Interface \(Generiek\)](#)
 - [Formaat van een transformatierequest](#)
 - [Formaat van een transformatieresponse](#)
 - [Generieke parameters](#)
- [Transformatie Interface \(transformatie tussen HL7-FHIR clients en HL7v3 servers\)](#)
 - [Produceren van een v3-request](#)
 - [Aanroep](#)
 - [Ondersteunde transformaties](#)
 - [Benodigde additionele parameters](#)
 - [Voorbeelden van transformaties](#)
 - [Produceren van een FHIR-response](#)
 - [Aanroep](#)
 - [Ondersteunde transformaties](#)
 - [Benodigde additionele parameters](#)
 - [Voorbeelden van transformaties](#)

De Transformatie Server bestaat uit een aantal endpoints. Ieder endpoint biedt een specifiek type transformatie. De interfaces hiervoor zijn beschreven op deze pagina.

Overzicht transformaties

AOF.TS-I.OTR.100.v2

De Transformatie Server biedt de volgende transformaties:

| Transformatie Algoritme ID | Input | | | Output | | |
|----------------------------|----------|---|---------------------------------|----------|---|----------------------------------|
| | Type | Protocol | Interactie-ID | Type | Protocol | Interactie-ID |
| 1 | request | application/fhir+xml, application/fhir+json | create:Observation:1.0: request | request | application/hl7-v3+xml | ZTSM_IN000004NL01 |
| 2 | response | application/hl7-v3+xml | MCCI_IN000002 | response | application/fhir+xml, application/fhir+json | create:Observation:1.0: response |
| | request | application/fhir+xml, application/fhir+json | create:Observation:1.0: request | | | |
| 3 | request | application/fhir+xml, application/fhir+json | search:Appointment:1.0: request | request | application/hl7-v3+xml | QUAF_IN990001NL01 |
| 4 | response | application/hl7-v3+xml | QUAF_IN990003NL01 | response | application/fhir+xml, application/fhir+json | search:Appointment:1.0: response |

TS Metadata Interface

AOF.TS-I.MDI.100.v2

De metadata van de transformatie server kan worden opgehaald via:

```
GET [base endpointadres]/metadata
```

De response bevat de volgende headers:

```
Cache-Control: must-revalidate, max-age=<max-age-ts-metadata>
Pragma: no-cache
```

Een client mag verkregen metadata conform de Cache-Control header directives, zoals [beschreven in RFC 7234](#), cachen.

De waarde van max-age-ts-metadata is configureerbaar in de transformatie server. Initiële waarde is 14400 seconden (4 uur).

De metadata wordt in JSON formaat geretourneerd en bestaat uit een array van algoritmes, die door de transformatie server worden ondersteund. Een algoritme object heeft het volgende formaat:

| Name | Cardinality | Type | Toelichting |
|------|-------------|------|-------------|
|------|-------------|------|-------------|

| | | | |
|-----------------------|------|--------|---|
| id | 1..1 | String | Uniek ID van het transformatie algoritme. |
| input | 1..n | | Vereiste input voor dit algoritme |
| input.type | 1..1 | String | Type van dit input bericht. Mogelijke waarden: "request", "response". |
| input.protocol | 1..n | String | Protocol van dit input bericht. Mogelijke waarden: "application/fhir+xml" of "application/fhir+json" of "application/hl7-v3+xml". |
| input.interaction-id | 1..1 | String | Interactie-id van dit input bericht. |
| output | 1..n | | Opgeleverde output bericht(en) door dit algoritme. |
| output.type | 1..1 | String | Type van dit output bericht. Mogelijke waarden: "request", "response". |
| output.protocol | 1..n | String | Protocol van dit output bericht. Mogelijke waarden: "application/fhir+xml" of "application/fhir+json" of "application/hl7-v3+xml". |
| output.interaction-id | 1..1 | String | Interactie-id van dit output bericht. |

Een voorbeeld metadata response is hieronder gegeven:

HTTP/1.1 200 OK

Content-Type: application/json

```
[
  {
    "id": "2",
    "input": [{
      "type": "response",
      "protocol": ["application/hl7-v3+xml"],
      "interaction-id": "MCCI_IN000002"
    },
    {
      "type": "request",
      "protocol": ["application/fhir+json", "application/fhir+xml"],
      "interaction-id": "create:Observation:1.0:request"
    }
  ],
  "output": [{
    "type": "response",
    "protocol": ["application/fhir+json", "application/fhir+xml"],
    "interaction-id": "create:Observation:1.0:response"
  }]
},
{
  "id": "4",
  "input": [{
    "type": "response",
    "protocol": ["application/hl7-v3+xml"],
    "interaction-id": "QUAF_IN990003NL01"
  }],
  "output": [{
    "type": "response",
    "protocol": ["application/fhir+json", "application/fhir+xml"],
    "interaction-id": "search-type:Appointment:1.0:response"
  }]
}
]
```

Transformatie Interface (Generiek)

Formaat van een transformatierequest

AOF.TS-I.FTR.100.v2

Middels één transformatierequest kan één (request of response) bericht worden getransformeerd.

Het generieke formaat is:

```
POST [base endpointadres]/to-xxx
Content-Type: application/json; charset=utf-8
AORTA-ID: initialRequestID=<UUID conform RFC4122>; requestID=<UUID conform RFC4122>

{
  meta: {
    format_in : "",
    protocol_in : "",
    protocol_out : "",
    transformation-id : ""
  },
  content_in : ""
}
```

Het initialRequestID attribuut bevat het ID van het allereerste request in de hele keten en dient te worden opgenomen in de logbestanden van alle partijen in de keten, zodat bij foutopsporing de verschillende logbestanden aan elkaar kunnen worden gerelateerd. Het requestID is voor iedere request message uniek. In requests wordt deze gegenereerd door de client. Ook het requestID dient te worden opgenomen in de verschillende logbestanden, zodat altijd duidelijk is op welk bericht een log entry van toepassing is.

Formaat van een transformatieresponse

AOF.TS-I.FOT.100.v2

Omdat een (request of response) bericht na transformatie uiteen kan vallen in meerdere berichten bevat een transformatieresponse een JSON array. Ieder object in deze array bestaat uit inhoud en metadata betreffende deze inhoud. Het generieke formaat is:

```
200 OK
Content-Type: application/json; charset=utf-8

[
  {
    meta: {
      format_out : "",
      protocol_out : "",
      transformation-id : "",
      interaction-id : ""
    },
    content_out : ""
  },
  {
    ..
  }
]
```

Generieke parameters

AOF.TS-I.TGP.100.v3

Input voor alle type transformaties is een JSON object met de volgende inhoud:

| Name | Cardinality | Type | Toelichting |
|------------------------|-------------|--|---|
| meta.format_in | 1..1 | Lege string of een string met waarde <i>escape of base64</i> | Gehanteerde encoding voor (orig_)content_in Wordt slechts gevuld wanneer de content een nadere aanduiding vereist bovenop de Content-Type aanduiding "application/json". |
| meta.protocol_in | 1..1 | String | Protocol van content_in (zie sectie Overzicht transformaties). |
| meta.protocol_out | 1..1 | | Gewenst protocol van het output bericht, of van de output berichten, (zie sectie Overzicht transformaties). |
| meta.transformation-id | 0..1 | String | Het ID van het te hanteren transformatie algoritme (zie sectie Overzicht transformaties). Indien deze niet wordt meegestuurd, dan probeert de transformatie server zelf, o.b.v. de wel meegezonden informatie, het juiste transformatie algoritme te bepalen. |
| content_in | 1..1 | String waarop de benodigde escaping is toegepast, of die base64 geëncodeerde data bevat. | De te vertalen content. |

AOF.TS-I.TGP.200.v2

Output van alle type transformaties is een set van JSON objecten met de volgende inhoud:

| Name | Cardinality | Type | Toelichting |
|------------------------|-------------|--------------------|--|
| meta.format_out | 1..1 | Zie meta.format_in | Gehanteerde encoding voor content_out |
| meta.protocol_out | 1..1 | String | Protocol van het output bericht (zie sectie Overzicht transformaties). |
| meta.transformation-id | 1..1 | String | Het ID van het gehanteerde transformatie algoritme (zie sectie Overzicht transformaties). |
| meta.interaction-id | 1..1 | String | Het interaction-id van het output bericht. |
| content_out | 1..1 | Zie content_in | De getransformeerde content. |

Transformatie Interface (transformatie tussen HL7-FHIR clients en HL7v3 servers)

Het kan hierbij gaan om transformatie van:

1. Een enkelvoudige FHIR-search naar een v3-bericht;
2. Een Bundle met FHIR-searches naar een set van v3-berichten;
3. Een enkelvoudige FHIR-create naar een v3-bericht;
4. Een Bundle met FHIR-creates naar één v3-bericht.
5. Een Bundle met FHIR-creates naar een set van v3-berichten.

De scope van deze versie van de transformatieservice is beperkt tot

- transformatie **van responses** behorende bij type 1;
- transformatie **van requests en responses** behorende bij type 4.

De scope is verder beperkt tot het HL7v3-bericht, inclusief de wrappers. De SOAP laag valt buiten de scope van de transformatieservice.

Produceren van een v3-request

Aanroep

AOF.TS-I.PV3.100.v1

POST [base endpointadres]/to-v3-request

Ondersteunde transformaties

AOF.TS-I.PV3.200.v1

Ondersteunde combinaties van meta.protocol_in en meta.protocol_out voor deze transformatie zijn:

| | |
|-----------------------------|------------------------------|
| protocol_in | protocol_out |
|-----------------------------|------------------------------|

| | |
|-----------------------|------------------------|
| application/fhir+xml | application/hl7-v3+xml |
| application/fhir+json | |

Deze transformatie is exclusief eventueel benodigde SOAP elementen of hiervoor benodigde HTTP-headers.

Benodigde additionele parameters

AOF.TS-I.PV3.300.v1

Additionele input parameters voor transformatie van requests zijn:

| Name | Cardinality | Type | Toelichting |
|-------------------------|-------------|--|---|
| meta.patient | 1..1 | String conform één van de volgende formaten <ul style="list-style-type: none"> "urn:oid:2.16.840.1.113883.2.4.6.3.<bsn>" "http://fhir.nl/fhir/NamingSystem/bsn <bsn>" | BSN van de patiënt die onderwerp is van het bericht. |
| meta.sender | 1..1 | String conform één van de volgende formaten <ul style="list-style-type: none"> "urn:oid:2.16.840.1.113883.2.4.6.6.<applicatie-id>" "http://fhir.nl/fhir/NamingSystem/aorta-app-id <applicatie-id>" | Applicatie-id van de initiërende applicatie |
| meta.receiver | 1..1 | Zie: sender type. | Applicatie-id van de ontvangende applicatie |
| meta.overseer.id | 1..1 | String conform één van de volgende formaten <ul style="list-style-type: none"> "urn:oid:2.16.840.1.113883.2.4.6.3.<bsn>" "http://fhir.nl/fhir/NamingSystem/bsn >" "urn:oid:2.16.528.1.1007.3.1.<uzi-nr-persoon>" "http://fhir.nl/fhir/NamingSystem/uzi-nr-pers <uzi-nr-persoon>" "urn:oid:2.16.528.1.1007.3.2.<uzi-nr-systeem op certificaat>" | ID van de verantwoordelijke persoon. |
| meta.overseer.role | 0..1 | String conform één van de volgende formaten <ul style="list-style-type: none"> "urn:oid:2.16.840.1.113883.2.4.3.11.8.<code>" "http://fhir.nl/fhir/NamingSystem/aorta-rolcode <code>" "urn:oid:2.16.840.1.113883.2.4.15.111.<code>" "http://fhir.nl/fhir/NamingSystem/uzi-rolcode <code>" | Rolcode van de verantwoordelijke persoon. Wordt niet gebruikt wanneer <code>user.id</code> een nummer bevat van een systeem. |
| meta.overseer.org.id | 1..1 | String conform één van de volgende formaten <ul style="list-style-type: none"> "urn:oid:2.16.528.1.1007.3.3.<ura>" "http://fhir.nl/fhir/NamingSystem/ura <ura>" | ID van de organisatie die de verantwoordelijke persoon vertegenwoordigt. Indien de verantwoordelijke persoon een patiënt is, dan wordt deze gevuld met het organisatie-id van VZVZ (root="2.16.840.1.113883.2.4.3.11.25" extension="00004005). |
| meta.overseer.org.name | 1..1 | String | Naam van de organisatie die de verantwoordelijke persoon vertegenwoordigt. Indien de verantwoordelijke persoon een patiënt is, dan wordt deze gevuld met "Vereniging van Zorgaanbieders voor Zorgcommunicatie". |
| meta.overseer.org.place | 0..1 | String | Vestiging locatie van de organisatie die de verantwoordelijke persoon vertegenwoordigt. Niet verplicht wanneer de verantwoordelijke persoon een patiënt is. |

| | | | |
|-----------------------|------|---|--|
| meta.author.id | 0..1 | Zie: overseer types | ID van de gebruiker. Verplicht indien de gebruiker afwijkt van de verantwoordelijke persoon. |
| meta.author.role | 0..1 | | Rolcode van de gebruiker. Verplicht indien de gebruiker afwijkt van de verantwoordelijke persoon. |
| meta.author.org.id | 0..1 | | ID van de organisatie die de gebruiker vertegenwoordigt. Verplicht indien de gebruiker afwijkt van de verantwoordelijke persoon. |
| meta.author.org.name | 0..1 | | Naam van de organisatie die de gebruiker vertegenwoordigt. Verplicht indien de gebruiker afwijkt van de verantwoordelijke persoon. |
| meta.author.org.place | 0..1 | | Vestiging locatie van de organisatie die de gebruiker vertegenwoordigt. Verplicht indien de gebruiker afwijkt van de verantwoordelijke persoon. |
| meta.method | 0..1 | String met waarde GET POST PUT DELETE | De gebruikte HTTP method. Verplicht wanneer het input bericht géén Bundle met een set van requests is. |
| meta.url | 0..1 | String | De gebruikte URL, inclusief eventuele (zoek)parameters. Verplicht wanneer het input bericht géén Bundle met een set van requests is. |

AOF.TS-I.PV3.400.v1

Additionele output parameters voor transformatie van requests zijn:

| Name | Cardinality | Type | Toelichting |
|--------------------|-------------|--------|---|
| meta.interactie-id | 1..1 | String | Het interactie-id van de geproduceerde HL7-v3 interactie. |

Voorbeelden van transformaties

Voorbeeld van een te transformeren FHIR-request:

```
POST [base]
AORTA-Transactie: SAML2-Bearer/JWT-Bearer <transactie_token>
DigiD-Authenticatie: SAML2-Bearer <DigiD SAML Assertion>
Content-Type: application/x-www-form-urlencoded
AORTA-ID: initialRequestID=<UUID conform RFC4122>; requestID=<UUID conform RFC4122>
AORTA-Version: contentVersion=<versienummer>; acceptVersion=<versienummer>
```

```
<Bundle xmlns="http://hl7.org/fhir">
  <id value="28943823489489"/>
  <type value="batch"/>
  <entry>
    <fullUrl value="urn:uuid:61ebe359-bfdc-4613-8bf2-c5e300945f0a"/>
    <resource>
      <Observation>
        ..
      </Observation>
    </resource>
    <request>
      <method value="POST"/>
      <url value="Observation"/>
    </request>
  </entry>
  <entry>
    ..
  </entry>
```

</Bundle>

Voorbeeld van een resulterend v3-request:

```
<?xml version="1.0" encoding="UTF-8"?>
<?xml-model href="../../../schematron/XXX.sch" type="application/xml" schematypens="http://purl.oclc.org/dsdl/schematron
"?>
.. SOAP wrapper ..
<INTERACTIE-ID xsi:schemaLocation="urn:hl7-org:v3 ../schemas/INTERACTIE-ID.xsd" xmlns:xsi="http://www.w3.org/2001
/XMLSchema-instance" xmlns="urn:hl7-org:v3">
  <!-- transmission wrapper -->
  <id root="2.16.840.1.113883.2.4.6.6.1.1" extension="4384723894787"/>
  <creationTime value=""/>
  <versionCode code="VERSIE"/>
  <interactionId root="2.16.840.1.113883.1.6" extension="INTERACTIE-ID"/>
  <profileId root="2.16.840.1.113883.2.4.3.11.1" extension="810"/>
  <processingCode code="P"/>
  <processingModeCode code="T"/>
  <acceptAckCode code="AL"/>
  <attentionLine>
    <keywordText code="PATID" codeSystem="2.16.840.1.113883.2.4.15.1">Patient.id</keywordText>
    <value root="2.16.840.1.113883.2.4.6.3" extension="100197243" xsi:type="II"/>
  </attentionLine>
  <receiver>
    <device determinerCode="INSTANCE" classCode="DEV">
      <id root="2.16.840.1.113883.2.4.6.6" extension="23434323"/>
    </device>
  </receiver>
  <sender>
    <device determinerCode="INSTANCE" classCode="DEV">
      <id root="2.16.840.1.113883.2.4.6.6" extension="1"/>
    </device>
  </sender>
  <ControlActProcess moodCode="EVN">
    <!-- control act wrapper -->
    <authorOrPerformer typeCode="AUT">
      <participant>
        <AssignedPerson>
          <id root="2.16.528.1.1007.3.1" extension="012345655"/>
          <code code="01.016" codeSystem="2.16.840.1.113883.2.4.15.111" displayName="
Internist"/>
          <Organization>
```

```

        <id root="2.16.528.1.1007.3.3" extension="02234567"/>
        <name>Bester</name>
    </Organization>
</AssignedPerson>
</participant>
</authorOrPerformer>
<overseer typeCode="RESP">
    <AssignedPerson>
        <id root="2.16.528.1.1007.3.1" extension="012345655"/>
        <code code="01.015" codeSystem="2.16.840.1.113883.2.4.15.111" displayName="Huisarts"/>
        <assignedPrincipalChoiceList>
            <assignedPerson>
                <name>Bester</name>
            </assignedPerson>
        </assignedPrincipalChoiceList>
        <Organization>
            <id root="2.16.528.1.1007.3.3" extension="02234567"/>
            <name>Jansen</name>
            <addr>
                <city>Amsterdam</city>
            </addr>
        </Organization>
    </AssignedPerson>
</overseer>
<subject>
    <!-- Payload -->
    <ClinicalDocument>
    ..
    </ClinicalDocument>
</subject>
</ControlActProcess>
</INTERACTIE-ID>

```

Produceren van een FHIR-response

Aanroep

AOF.TS-I.FRA.100.v1

POST [base endpointadres]/to-fhir-response

Ondersteunde transformaties

AOF.TS-I.FRT.100.v1

Ondersteunde combinaties van `meta.protocol_in` en `meta.protocol_out` voor deze transformatie zijn:

| protocol_in | protocol_out |
|------------------------|-----------------------|
| application/hl7-v3+xml | application/fhir+xml |
| | application/fhir+json |

Benodigde additionele parameters

AOF.TS-I.FAP.100.v2

Additionele input parameters voor transformatie van responses zijn:

| Name | Cardinality | Type | Toelichting |
|-----------------------|-------------|--------|---|
| orig_content_in | 0..1 | String | String waarop de benodigde escaping is toegepast, of die base64 geëncodeerde data bevat. |
| meta.interactie-id | 1..1 | String | Het interactie-id van de HL7-v3 interactie die de aanleiding was voor de te transformeren HL7v3-response. |
| meta.orig_protocol_in | 0..1 | String | Protocol van <code>orig_content_in</code> (zie sectie Overzicht transformaties). |

AOF.TS-I.FAP.200.v1

Additionele output parameters voor transformatie van responses zijn:

| Name | Cardinality | Type | Toelichting |
|----------------------|-------------|--------|--|
| meta.content-version | 1..1 | String | De <code>contentVersion</code> die moet worden gebruikt in de AORTA-Version HTTP header. |

Voorbeelden van transformaties

Voorbeeld van een te transformeren v3-response:

```
<?xml-model href="../../../schematron/XXX.sch" type="application/xml" schematypens="http://purl.oclc.org/dsdl/schematron"?>
.. SOAP wrapper ..
<INTERACTIE-ID xsi:schemaLocation="urn:hl7-org:v3 ../schemas/INTERACTIE-ID.xsd" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns="urn:hl7-org:v3">
  <id extension="235" root="2.16.528.1.1007.3.3.1234567.1"/>
  <creationTime value="20140704155629"/>
  <versionCode code="NICTIZED2005-Okt"/>
  <interactionId extension="INTERACTIE-ID" root="2.16.840.1.113883.1.6"/>
  <profileId extension="810" root="2.16.840.1.113883.2.4.3.11.1"/>
  <processingCode code="P"/>
  <processingModeCode code="T"/>
  <acceptAckCode code="NE"/>
  <acknowledgement typeCode="CA">
    <targetMessage>
      <id extension="4384723894787" root="2.16.840.1.113883.2.4.6.6.1.1"/>
    </targetMessage>
  </acknowledgement>
```

```

<receiver>
  <device determinerCode="INSTANCE" classCode="DEV">
    <id extension="1" root="2.16.840.1.113883.2.4.6.6"/>
  </device>
</receiver>
<sender>
  <device determinerCode="INSTANCE" classCode="DEV">
    <id extension="23434323" root="2.16.840.1.113883.2.4.6.6"/>
  </device>
</sender>
</INTERACTIE-ID>

```

Voorbeeld van een resulterende FHIR Bundle:

```

<Bundle xmlns="http://hl7.org/fhir">
  <id value="someidvalue123"/>
  <type value="batch-response"/>
  <entry>
    <fullUrl value="http://example.org/fhir/Patient/12423"/>
    <resource>
      <!-- whether to return the result resource depends on client preference -->
      <Observation>
        <id value="12423"/>
        ..
      </Observation>
    </resource>
    <response>
      <status value="201 Created"/>
      <location value="Observation/12423/_history/1"/>
      <etag value="W/&quot;l&quot;"/>
      <lastModified value="2014-08-18T01:43:33Z"/>
      <!-- Indien van toepassing -->
      <outcome>
        <OperationOutcome>
          ..
        </OperationOutcome>
      </outcome>
    </response>
  </entry>
  <entry>
    ..

```

</entry>

</Bundle>

Workflow Interfaces - 0.7.x

- [Taak Uitvoering Interface](#)
- [Taak Notificatie Interface](#)

Let op! Deze interfaces worden verwacht in AoF 0.8 , maar worden nog niet gebruikt in AoF 0.7.

Taak Uitvoering Interface

Deze interface wordt geboden door een Taak Uitvoerend Systeem. Initiatie van interacties vanuit een GBZ-applicatie (Resource Client) verloopt via Resource Broker ZA-in.

Via deze interface kunnen, door een Resource Client (Taak Aanvragend Systeem), een AORTA FHIR-create, een AORTA FHIR-read en een AORTA FHIR-update worden uitgevoerd m.b.t. een AORTA Task resource, op de wijze zoals beschreven in de *AORTA FHIR Resource Broker Interface*.

Resource Broker VnC stuurt geïnitieerde interacties vervolgens door naar het beoogde Taak Uitvoerend Systeem, waarbij de HTTP headers worden gehanteerd, conform de interface specificatie van het doelsysteem.

Taak Notificatie Interface

Deze interface wordt geboden door een Taak Aanvragend Systeem. Notificaties kunnen worden verzonden vanuit een GBZ-applicatie of vanuit een Resource Broker component (bijvoorbeeld RB ACT). Verzenden van notificaties vanuit een GBZ-applicatie (Resource Client) verloopt via Resource Broker ZA-in.

Resource Broker VnC stuurt geïnitieerde interacties vervolgens door naar het beoogde Taak Aanvragend Systeem, waarbij de HTTP headers worden gehanteerd, conform de interface specificatie van het doelsysteem.

Een notificatie kan als volgt worden afgeleverd:

```
POST <base>/notify-task/{<app-id>}/<task-system>/<task-code>/<task-id>
```

Waarbij:

- base gelijk is aan de FQDN van de server waarop een POST wordt uitgevoerd
- app-id, gelijk is aan het appID van de GBZ-applicatie die de notificatie uiteindelijk moet ontvangen (slechts aanwezig bij een POST op een tussenliggende component van de resource broker)
- task-system, gelijk is aan code.coding.system van deze Task
- task-code, gelijk is aan code.coding.code van deze Task
- task-id, gelijk is aan het [resource.id](#) van deze Task

Bij een notificatie wordt in het HTTP-request, op de volgende wijze, een custom HTTP header meegezonden:

- AORTA-ID: `initialRequestID=<UUID conform RFC4122>; requestID=<UUID conform RFC4122>`

Het HTTP POST request dat de notificatie draagt, kan optioneel ook een body bevatten met daarin de FHIR Task instance zelf, exclusief secondary resource instances waaraan het refereert (gelijk aan hoe een Task zou worden geretourneerd als gevolg van een FHIR-read). Wanneer een Taak Uitvoerend Systeem dit doet, dan is het voor dit systeem niet verplicht om ook een FHIR-read interactie m.b.t. deze Task te ondersteunen.

Use cases - 0.7.x

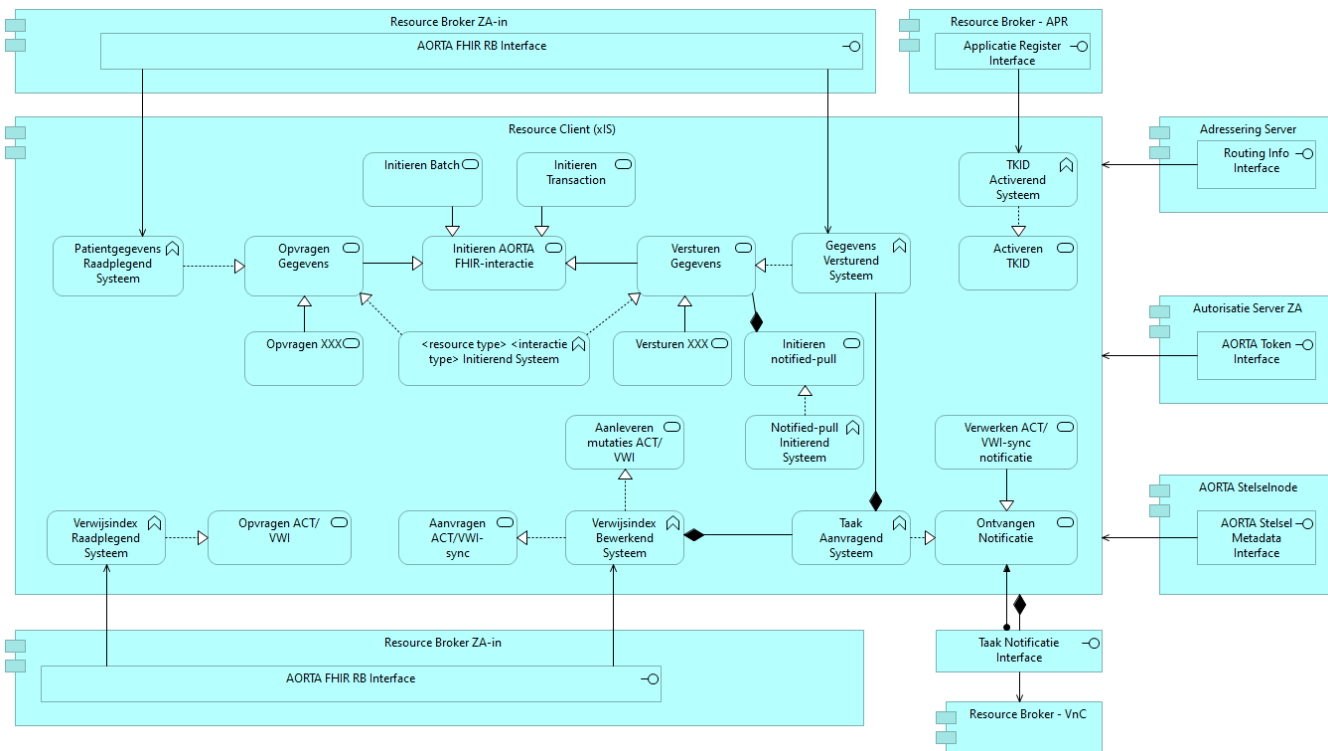
UC Resource Client - 0.7.x

- [Overzicht Resource Client](#)
- [Activeren TKID](#)
- [Initieren notified-pull](#)
- [Initieren AORTA FHIR-interactie](#)
- [UC extensions](#)
 - [Generieke UC extension: Opvragen gegevens](#)
 - [Generieke UC extension: Versturen gegevens](#)

Overzicht Resource Client

Een GBZ-applicatie kan zowel fungeren in de rol van Resource Server als in de rol van Resource Client. Een Resource Client initieert interacties. Een Resource Server reageert op interacties die worden geïnitieerd middels een interface. Een Resource Client biedt zelf geen in principe geen interfaces. Uitzondering hierop zijn callback interfaces, bijvoorbeeld t.b.v. notificaties.

Onderstaande figuur toont een overzicht van de interfaces, services en functies van de Resource Client.



Services zijn toegankelijk via interfaces en worden beschreven in de vorm van use cases. Responses die in een succes- of uitzonderingssituaties moeten worden geretourneerd zijn **voor iedere situatie beschreven**. De Resource Client maakt gebruik van een aantal interfaces, in het bijzonder van de AORTA FHIR RB Interface.

Een service wordt altijd vervuld middels één of meerdere applicatiefuncties (AORTA systeemrollen), bijvoorbeeld "Gegevens Versturend Systeem". Een Resource Client kan worden gekwalificeerd en geaccepteerd voor deze systeemrollen. Wanneer de ene systeemrol een andere vereist, dan is dit weergegeven middels een *composition* relatie.

Een aantal services maken gebruik van onderliggende services. Een dergelijk onderliggende service wordt dan beschreven in de vorm van een use case inclusion of als een use case extension.

Activeren TKID

Primaire actor: GBZ-beheerder

Secundaire actor: RB APR

Systeem: TKID Activerend Systeem

Pre-condities:

- Het systeem is aangesloten op de secundaire actor.
- De kwalificaties van de resource server zijn reeds geaccepteerd door VZVZ en zijn ook geregistreerd in de resource broker;
- De GBZ-beheerder beschikt over de juiste TKID's (ID's die zijn uitgereikt n.a.v. acceptatie van succesvol doorlopen kwalificaties) van alle te activeren AORTA systeemrollen.

Triggers:

- De primaire actor wil één of meerdere TKID's activeren.

Main flow:

1. De primaire actor kiest de optie om één of meerdere TKID's te activeren voor een bepaalde resource server.
2. Het systeem initieert de use case *Verwerken TKID-activatie* middels de *Applicatie Register Interface*.
 - a. Uitzondering 1: De interactie kon niet succesvol worden verwerkt
3. Het systeem ontvangt een response.

Postconditie bij succes:

- De verzonden TKID's zijn verwerkt door de resource broker, waardoor de resource server nu in de resource broker is gekoppeld aan de bijbehorende AORTA systeemrollen. Hiermee zijn tevens eventueel eerder doorlopen TKID activiteiten ongedaan gemaakt.

Post-condities bij falen:

- De bestaande koppelingen tussen AORTA systeemrollen met de resource server is ongewijzigd gebleven.

Uitzonderingen:

1. De interactie kon niet succesvol worden verwerkt
 - a. Het systeem ontvangt een toepasselijke foutcode (bijvoorbeeld niet geautoriseerd of ongeldig verzoek)

Initieren notified-pull

Primaire actor: Gebruiker OF Timer

Systeem: Notified-pull Initierend Systeem

Pre-condities:

- De resource client is aangesloten op de resource broker.

Triggers:

- De primaire actor wil een notified-pull initiëren.

Main flow:

1. Het systeem genereert een *AORTA consent_token*.
2. Het systeem creëert, t.b.v. de uitvoering van een notified-pull, een *AORTA Task*, middels de use case *Initieren AORTA-FHIR-interactie*.

Post-condities:

- De response is correct verwerkt in het systeem.

Use case extensions:

1. Initieren AORTA FHIR-interactie

Initieren AORTA FHIR-interactie

Primaire actor: Gebruiker OF Timer

Secundaire actor: RB ZA-in, Autorisatie Server ZA

Systeem: Patiëntgegevens Raadplegend Systeem OF Gegevens Versturend Systeem

Pre-condities:

- De resource client is aangesloten op de resource broker.

Triggers:

- De primaire actor wil gegevens opvragen of versturen.

Main flow:

1. Optioneel: het systeem initieert de use case *Bepaal route* middels de *Routing Info Interface*.
2. Het systeem initieert de use case *Uitgeven AORTA access_token* middels de *AORTA Token Interface*.
3. Het systeem initieert de use case *Verwerken AORTA FHIR-interactie* middels de *AORTA FHIR Resource Broker Interface*. Wanneer de scope meerdere interacties betreft, dan dient het systeem meerdere interacties te initiëren.
4. Het systeem logt het verzonden request, zoals beschreven in de "toelichting logging".
5. Het systeem ontvangt een response.
6. Het systeem logt de ontvangen response, zoals beschreven in de "toelichting logging".

Post-condities:

- De response is correct verwerkt in het systeem.

Use case extensions:

1. Opvragen gegevens
2. Versturen gegevens

Toelichting logging

Een resource client dient een log bij te houden van alle verzonden requests en van alle ontvangen responses. Een dergelijke log bevat, t.b.v. de traceerbaarheid van berichten in de keten tenminste de volgende attributen.

| Te loggen attribuut | Vulling in Request Log | Vulling in Response Log |
|---------------------|--|--|
| request-id | Uniek ID van het verzonden/ontvangen request. Wordt gevuld met het <code>requestID</code> dat werd verzonden in de <code>AORTA-ID</code> request header. | Uniek ID van het request waartoe de ontvangen response behoort. Wordt gevuld met het <code>requestID</code> dat werd verzonden in de <code>AORTA-ID</code> request header. |
| message-type | "request" | "response" |
| initial-message-id | Wordt gevuld met het <code>initialRequestID</code> dat werd verzonden in de <code>AORTA-ID</code> request header. | |
| sender_id | Het <code>appID</code> van de resource client die het request verstuurt. | Het <code>appID</code> van de resource server die de response retourneert. In dit geval dus het <code>appID</code> van de resource broker ZA-in component. |
| receiver_id | Het <code>appID</code> van de resource server die het request ontvangt. In dit geval dus het <code>appID</code> van de resource broker ZA-in component. | Het <code>appID</code> van de resource client die de response ontvangt. |

UC extensions

Generieke UC extension: Opvragen gegevens

Bij het opvragen van gegevens zijn ook de generieke, d.w.z. niet HL7v3-specifieke, eisen van toepassing die gelden voor een *Patiëntgegevens raadplegend systeem*, zoals gespecificeerd in het PvE Infrastructurele Systeemrollen.

Generieke UC extension: Versturen gegevens

Bij het versturen van gegevens zijn ook de generieke, d.w.z. niet HL7v3-specifieke, eisen van toepassing die gelden voor een *Gegevens versturend systeem*, zoals gespecificeerd in het PvE Infrastructurele Systeemrollen.

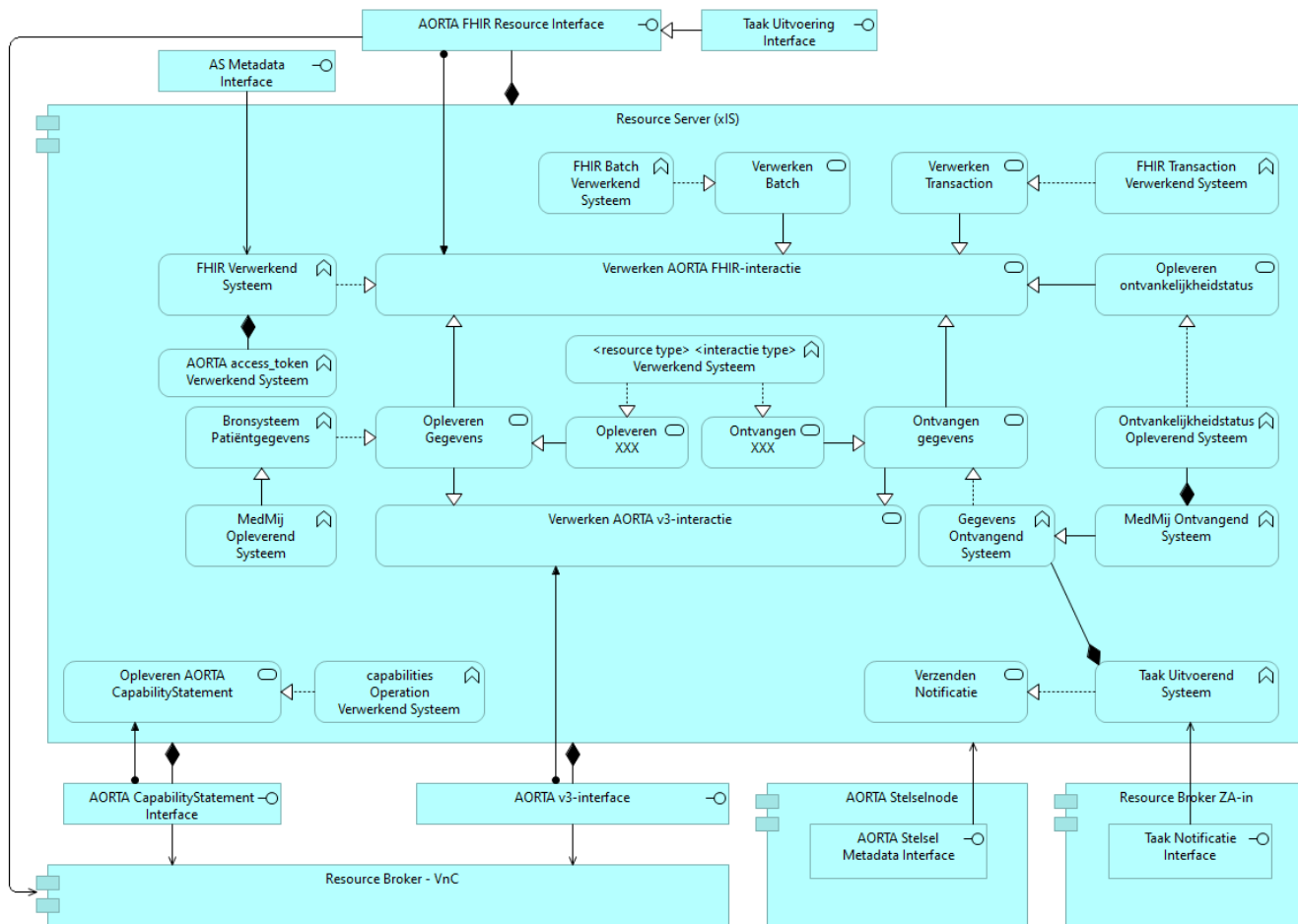
UC Resource Server - 0.7.x

- [Overzicht Resource Server](#)
- [HL7-FHIR Resource Server](#)
 - [Opleveren AORTA CapabilityStatement](#)
 - [Verwerken AORTA FHIR-interactie](#)
 - [UC extension: Opleveren ontvankelijkheidstatus](#)
 - [UC extension: Opleveren documenten](#)
- [HL7-v3 Resource Server](#)
 - [Verwerken AORTA v3-interactie](#)
- [Resource Server Algemeen](#)
 - [Generieke UC extension: Opleveren gegevens](#)
 - [Generieke UC extension: Ontvangen gegevens](#)

Overzicht Resource Server

Een GBZ-applicatie kan zowel fungeren in de rol van Resource Server als in de rol van Resource Client. Een Resource Server reageert op interacties die worden geïnitieerd middels een interface. Een Resource Server initieert zelf geen interacties.

Onderstaande figuur toont een overzicht van de interfaces, services en functies van de Resource Server.



De services zijn toegankelijk via een geboden interface en worden beschreven in de vorm van use cases. Responses die in een succes- of uitzonderingssituaties moeten worden geretourneerd zijn **voor iedere situatie beschreven**.

Een service wordt altijd vervuld middels één of meerdere applicatiefuncties (AORTA systeemrollen), bijvoorbeeld "FHIR Verwerkend Systeem". Een Resource Server kan worden gekwalificeerd en geaccepteerd voor deze systeemrollen. Wanneer de ene systeemrol een andere vereist, dan is dit weergegeven middels een *composition* relatie. Bijvoorbeeld: kwalificatie voor systeemrol "MedMij Ontvangend Systeem" vereist ook kwalificatie voor systeemrol "Ontvankelijkheidstatus Opleverend Systeem".

Een aantal services maken gebruik van onderliggende services. Een dergelijk onderliggende service wordt dan beschreven in de vorm van een use case inclusion of als een use case extension.

Verschillen tussen een HL7-FHIR Resource Server en een HL7v3 Resource Server zijn:

- Een HL7v3 Resource Server biedt een AORTA v3-interface i.p.v. een AORTA FHIR Resource Interface.
- Deze interface biedt toegang tot de generieke service "Verwerken AORTA v3-interactie".

HL7-FHIR Resource Server

Opleveren AORTA CapabilityStatement

Primaire actor: RB VnC

Systeem: capabilities Operation Verwerkend Systeem

Pre-condities:

- Het systeem is aangesloten op de secundaire actor.

Triggers:

- De resource broker wil de operationele status van de resource server toetsen.

Main flow:

1. Het systeem ontvangt een FHIR capabilities operation
 - a. Uitzondering 1: Ongeldig request
2. Het systeem retourneert een response.

Post-condities:

- Het systeem heeft een correcte response geretourneerd.

Uitzonderingen:

1. Ongeldig request
 - a. Het systeem genereert de vereiste foutresponse en keert terug naar de laatste stap van de main flow.

Verwerken AORTA FHIR-interactie

Primaire actor: RB VnC

Systeem: FHIR Verwerkend Systeem

Pre-condities:

- De vereiste TKID's voor deze resource server zijn geactiveerd in het Applicatie Register.

Triggers:

- De primaire actor initieert een FHIR-interactie.

Main flow:

1. Het systeem ontvangt een AORTA FHIR-interactie.
2. Het systeem controleert de geldigheid van het AORTA access_token, zoals omschreven in de [toelichting Controle en gebruik van het access_token](#).
 - a. Uitzondering 1: Het access_token kan niet worden gevalideerd of is ongeldig
3. Het systeem controleert de geldigheid van de AORTA-ID header.
 - a. Uitzondering 2: AORTA-ID header ontbreekt of is ongeldig
4. Het systeem controleert de geldigheid van de AORTA-Version header (**vooral nog mag slechts worden getoetst of de header aanwezig is, inhoudelijk wordt de header nog niet gebruikt**).
 - a. Uitzondering 2: AORTA-Version ontbreekt of is ongeldig
5. Afhankelijk van het type FHIR-interactie wordt nu de juiste generieke extension flow doorlopen, d.w.z. opleveren gegevens, ontvangen gegevens of opleveren ontvankelijkheidsstatus.
6. Het systeem retourneert een response.
7. Het systeem logt het ontvangen request en de geretourneerde response, zoals beschreven in de "toelichting logging".

Post-condities:

- Het systeem heeft een correcte response geretourneerd, zoals vereist voor de specifieke use case.

Uitzonderingen:

1. Het access_token kan niet worden gevalideerd of is ongeldig
 - a. Het systeem genereert de vereiste foutresponse en keert terug naar stap 6 van de main flow.
2. AORTA-ID header ontbreekt of is ongeldig

- a. Het systeem genereert de vereiste foutresponse en keert terug naar stap 6 van de main flow.
- 3. AORTA-Version ontbreekt of is ongeldig
 - a. Het systeem genereert de vereiste foutresponse en keert terug naar stap 6 van de main flow.

Use case extensions:

1. Opleveren gegevens
2. Ontvangen gegevens
3. Opleveren ontvankelijkheidsstatus

Controle en gebruik van het access_token

Om meta-informatie te kunnen meegeven bij een FHIR interactie en om het beveiligingsniveau te verhogen wordt bij iedere FHIR interactie een AORTA access_token meegestuurd. Een FHIR interactie die wordt ingestuurd door de Resource Broker en waar geen geldig access_token is bijgevoegd dient te worden geweigerd.

Het JWT-based access_token wordt op basis van RS256 (RSA Signature met SHA-256), digitaal ondertekend met de private key van de Autorisatie Server. De public key waarmee de digitale handtekening kan worden gecontroleerd wordt conform [RFC 7517](#), als een JWK beschikbaar gesteld.

De URL van waarop de JWK Set kan worden opgevraagd (jwks_uri) is opgenomen in de metadata van de autorisatieserver, die [via de AS Metadata Interface](#), kan worden opgehaald.

De iss van het token is opgenomen in het token zelf, maar wordt vanwege security redenen ook via het [AORTA Stelseltoken](#) bij de resource server aangemerkt als een vertrouwde issuer. De resource server mag geen tokens verwerken van niet-vertrouwde issuers. De resource server moet controleren dat de waarde van <iss> overeenkomt met de waarde van issuer in de ontvangen metadata.

Iedere JSON Web Key (JWK) in de set bevat een kid parameter. De juiste JWK in de JWK Set wordt gevonden o.b.v. de waarde van het kid attribuut in de header van de ontvangen JWT, en waarvan het kty attribuut gelijk is aan "RSA" en het use attribuut gelijk is aan "sig".

Het access_token wordt door de resource server gebruikt om vast te stellen of een binnenkomend verzoek mag worden behandeld en om de gegevensverwerking te loggen.

Uit te voeren controles m.b.t. het access_token:

1. Is het token uitgegeven door een voor mij vertrouwde partij (issuer, in dit geval door de Autorisatie Server MedMij of door de Autorisatie Server ZA), vertrouwde autorisatieservers zijn opgenomen in het [AORTA Stelseltoken](#).
2. Juistheid van de digitale handtekening (signature), inclusief de geldigheid van het certificaat waarmee de handtekening is geplaatst. Hierbij worden ook maatregelen genomen om [bedreiging 2.1 uit RFC 8725](#) tegen te gaan.
3. Wordt het token gebruikt door de partij (resource client) aan wie het is uitgegeven.
 - JWT-based access_token: via controle van de `client_id` claim in combinatie met de geauthentiseerde TLS-client. Het FQDN van de client (Resource Broker VnC) is opgenomen in het [AORTA Stelseltoken](#).
4. Mag het token door mij worden geconsumeerd.
 - JWT-based access_token: via controle van de `aud` claim
5. Is de geldigheidsduur van het token niet verstreken. Met betrekking tot het ingangstijdstip dient, wanneer problemen ontstaan door tijdsynchronisatie, een *gracetime* te kunnen worden gehanteerd. Deze bedraagt maximaal 15 seconden. Aanbevolen wordt om deze *gracetime* configureerbaar te maken.
6. Bij interactie door patiënt (te zien aan de role claim van het access_token):
 - JWT-based access_token: is de inhoud van de patient claim gelijk aan de inhoud van de sub claim.

Toelichting: omdat machtigingen/mandateringen nog niet worden ondersteund, mag de sub claim niet afwijken van de patient claim, en moet een token, wanneer dit wel het geval is, worden beschouwd als "invalid". De Autorisatieserver MedMij component zou een dergelijk token, binnen deze versie van de access_token definitie, nooit uitgeven.

7. Valt de interactie onder het type interacties waarvoor het access_token geldig is (scope). NB. de exacte scope van MedMij gegevensdiensten en van AORTA zorgtoepassingen wordt getoetst door de Resource Broker. De resource server kan volstaan met het toetsen van het SMART-on-FHIR deel van de scope. Een search op Observation vereist dan bijvoorbeeld dat patient/Observation.read deel uitmaakt van de scope. Bij ontvangst van een FHIR read interactie dient expliciet te worden getoetst of de gevraagde resource instance deel uitmaakt van het dossier van de patient die is aangegeven in het access_token.

NB. de scope van een access_token kan meerdere interacties omvatten, die ook na elkaar kunnen worden uitgevoerd. Een resource server moet het daarom toestaan wanneer eenzelfde access_token meerdere malen wordt gebruikt.

Toelichting logging

Een resource server dient een log bij te houden van alle ontvangen request en van alle retourneerde responses. Een dergelijke log bevat, t.b.v. de traceerbaarheid van berichten in de keten tenminste de volgende attributen.

| Te loggen attribuut | Vulling in Request Log | Vulling in Response Log |
|---------------------|--|---|
| request-id | Uniek ID van het verzonden/ontvangen request. Wordt gevuld met het <code>requestID</code> dat werd ontvangen in de <code>AORTA-ID</code> request header. | Uniek ID van het request waartoe de verzonden/ontvangen response behoort. Wordt gevuld met het <code>requestID</code> dat werd ontvangen /verzonden in de <code>AORTA-ID</code> request header. |
| message-type | "request" | "response" |
| initial-message-id | Gelijk aan het request-id, waarmee de keten van messages werd gestart. In de MedMij use case is dit het <code>MedMij-Request-ID</code> dat van PGO Server werd ontvangen door LSP+. Wordt gevuld met het <code>initialRequestID</code> dat werd ontvangen in de <code>AORTA-ID</code> request header. Het <code>initialRequestID</code> kan middels de log van de resource server van LSP+ worden teruggeleid naar het MedMij <code>access_token</code> dat werd gebruikt bij het resource request. A.d.h.v. het <code>access_token</code> kan vervolgens m.b.v. de log van de Autorisatieserver MedMij component worden achterhaald welk OAuth Authorization Request aan het <code>access_token</code> ten grondslag lag. | |
| sender_id | Het applID van de resource client die het request verstuurt of van de resource server die de response retourneert. | |
| receiver_id | Het applID van de resource server die het request ontvangt of van de resource client die de response ontvangt. | |

UC extension: Opleveren ontvankelijkheidstatus

Systeem: MedMij Ontvangend Systeem

Triggers:

- De resource server heeft een `$is-allowed` operation ontvangen

Main flow:

1. Het systeem genereert de te retourneren response.
2. Het systeem keert terug naar de main flow van de bovenliggende use case.

UC extension: Opleveren documenten

Systeem:

- DocumentManifest Search Verwerkend Systeem
- DocumentReference Search Verwerkend Systeem
- Binary Read Verwerkend Systeem

Triggers:

- De resource server heeft een FHIR-interactie ontvangen die deel uitmaakt van de gegevensdienst "Verzamelen documenten".

Main flow:

1. Het systeem zorgt ervoor dat slechts (referenties naar) documenten worden geretourneerd die behoren tot de set van ondersteunde mimetypes (zie toelichting "Ondersteunde mimetypes").
2. Het systeem zorgt ervoor dat wordt voldaan aan de toelichting "Vulling `content.attachment.url`".
3. Het systeem keert terug naar de bovenliggende use case.

Ondersteunde mimetypes

De informatiestandaard van MedMij perkt het aantal mogelijke op te leveren mimetypes in tot application/pdf (en specifiek tot PDF/A, waarbij minimaal PDF/A1b wordt vereist).

Omdat de Resource Broker mimetypes kan vertalen is het voor Resource Servers toegestaan om documenten op te leveren conform de volgende mimetypes (let op! nog niet mogelijk in AoF 0.5, 0.6 en 0.7):

1. application/pdf
2. application/msword
3. application/vnd.openxmlformats-officedocument.wordprocessingml.document
4. application/rtf
5. text/plain
6. text/html
7. image/jpeg
8. image/tiff

Nader onderzocht zal worden of ook de volgende mimetypes kunnen worden opgeleverd:

1. application/xml
2. image/bmp
3. image/png
4. text/xml

Vulling content.attachment.url

Wanneer een Resource Server een DocumentReference retourneert, dan dient `content.attachment.url` als volgt te worden gevuld:

- `<base endpointadres van resource server>/Binary/<id>`, of
- `Binary/<id>`

Resource Broker MedMij-in of Resource Broker ZA-in transformeert `content.attachment.url` voor oplevering naar het volgende formaat:

- `<base endpointadres van resource broker XX-in>/<appID>/Binary/<id>`

Waarbij `<appID>` het applicatie-id (zonder root OID) bevat van de Resource Server.

i Codering documenten

Binnen VIPP 5 bestaat correspondentie uit radiologieverslagen, specialistenbrieven, voortgangsbrieven en/of ontslagbrieven, opgesteld in de eigen organisatie. In onderstaande tabel zijn de bijbehorende, mogelijke, class en type coderingen opgenomen. De informatiestandaard stelt geen precieze eisen aan welke codes exact mogen worden toegepast.

| Type correspondentie | SNOMED class- en typecodes die door MedMij zijn doorgegeven aan VIPP 5 | Mogelijke SNOMED class- en typecodes uit de Waardelijsten waarnaar wordt verwezen vanuit het functioneel ontwerp van de informatiestandaard | Mogelijke LOINC class- en typecodes uit de Waardelijsten waarnaar wordt verwezen vanuit het technisch ontwerp van de informatiestandaard (de FHIR profielen) |
|----------------------|--|--|--|
| Radiologieverslag | class = 4201000179104 (Imaging reports) type = 722124004 (Radiology studies report) | diverse codes mogelijk, e.e.a. afhankelijk van het type onderzoek dat is uitgevoerd | class = 18726-0 (Radiology studies (set)) type = 73575-3 (Radiology Consult note), 68604-8 (Radiology Diagnostic study note) |
| Specialistenbrief | class = 371534008 (Summary reports) type = 371535009 (Transfer summary) | class = 9531000146107 (brief) type = 11061000146105 (polibrief), 11081000146102 (brief chirurgie) | class = 11488-4 (Consult Note), 11504-8 (Surgical operation note) type = diverse specifieke codes mogelijk |
| Voortgangsbrief | class = 371534008 (Summary reports) type = 371532007 (Progress report) | class = 9531000146107 (brief) type = 11061000146105 (polibrief), 11081000146102 (brief chirurgie), 11091000146100 (brief dagverpleging) | class = ?? type = 68607-1 (Progress letter), ook meer specifieke codes mogelijk |
| Ontslagbrief | class = 371534008 (Summary reports) type = 373942005 (Discharge summary) | class = 9531000146107 (brief) type = 11071000146104 (ontslagbrief) | class = 18842-5 (Discharge summary) type = 28574-2 (Discharge Note), ook meer specifieke codes mogelijk |

i Cardinaliteiten

Onderstaande tabel bevat een samenvatting van de gehanteerde cardinaliteiten in de informatiestandaard.

| DocumentManifest | | DocumentReference | | Document / Binary | |
|---|---|--|---|--|--------------------|
| Functioneel | FHIR | Functioneel | FHIR | Functioneel | FHIR |
| Identificatie (1..1) | masterIdentifier (1..1) | Identificatie (1..1) | masterIdentifier (1..1) | Identificatie (1..1) | id (1..1) |
| | identificier (1..*), mag gelijk zijn aan de masterIdentifier | | identificier (0..*) | | - |
| Status (1..1) | status (1..1) | Status (1..1) | status (1..1) | - | - |
| Type (1..1) >> SNOMED Waarde lijst typeCode | type (1..1) >> LOINC Document Type Valueset (preferred) | Type (1..1) >> SNOMED Waarde lijst typeCode | type (1..1) >> LOINC Document Type Valueset (preferred) | - | - |
| - | - | Klasse (0..1) >> SNOMED Waarde lijst classCode | class (0..1) >> LOINC Document Class Valueset (example) | - | - |
| Auteur (0..*) | author (0..1) | Auteur (1..*) - Verplicht indien aanwezig in bronsysteem | author (0..1) | - | - |
| - | subject (1..1) | - | subject (0..1) - Subject is desondanks wel verplicht bij kwalificatie | - | - |
| AanmaakDatum (1..1) | created (1..1) | IndexDatum (1..1) | indexed (1..1) | - | - |
| Bron (0..*) | source (1..1), is verplicht, FHIR profiel is op dit punt bepalend voor kwalificatie, gevuld met applicatie ID als een urn:oid | - | - | - | - |
| Inhoud. DocumentReferentie (1..*) | content.pReference (1..*) | - | - | - | - |
| - | - | Inhoud. Documentverwijzing (1..1) | content.attachment.url (1..1) | - | - |
| - | - | Inhoud. Documentformaat. mimeType (1..1) >> valueset | content.attachment.contentType (1..1) | ContentType. mimeType (1..1) >> valueset | contentType (1..1) |
| - | - | Inhoud. Documentformaat. formatCode (1..1) >> valueset | content.format (0..1) >> valueset (preferred) | ContentType. formatCode (1..1) >> valueset | - |
| - | - | - | - | Content (1..1) | content (1..1) |

HL7-v3 Resource Server

Verwerken AORTA v3-interactie

Primaire actor: RB VnC

Systeem: MedMij Opleverend Systeem of MedMij Ontvangend Systeem

Pre-condities:

- De vereiste TKID's voor deze resource server zijn geactiveerd in het Applicatie Register.

Triggers:

- De primaire actor initieert een v3-interactie.

Main flow:

1. Het systeem ontvangt een AORTA v3-interactie.
2. Afhankelijk van het HL7v3 interactie-id wordt nu de juiste generieke extension flow doorlopen, d.w.z. opleveren gegevens of ontvangen gegevens.
3. Het systeem retourneert een response.
4. Het systeem logt het ontvangen request en de geretourneerde response.

Post-condities:

- Het systeem heeft een correcte response geretourneerd, zoals vereist voor de specifieke use case.

Uitzonderingen:

1. Beschreven in reguliere AORTA PvE en Implementatiehandleidingen.

Use case extensions:

1. Opleveren gegevens
2. Ontvangen gegevens

Resource Server Algemeen

Generieke UC extension: Opleveren gegevens

Systeem: MedMij Opleverend Systeem

Triggers:

- De resource server heeft een FHIR-read of een FHIR-search interactie ontvangen, OF
- De resource server heeft een v3-interactie ontvangen, waarmee gegevens worden opgevraagd

Main flow:

1. Het systeem verifieert of de gevraagde gegevens mogen worden opgeleverd, zoals omschreven in de onderstaande "Toelichting beschikbaarheidsvoorwaarde".
 - a. Uitzondering 1: De gevraagde gegevens mogen niet worden opgeleverd.
2. Afhankelijk van de gegevensdienst waar de interactie deel van uitmaakt (FHIR-interactie), of van het interactie-id (v3-interactie)
 - a. wordt de ontvangen interactie nu verwerkt conform de gegevensdienst-specifieke implementatiehandleiding, zoals benoemd in de toelichting "Gegevensdienst-specifieke UC extensions en implementatiehandleidingen".
 - b. wordt (indien van toepassing) de juiste extension flow doorlopen, zoals aangegeven in de toelichting "Gegevensdienst-specifieke UC extensions en implementatiehandleidingen".
3. Het systeem zorgt ervoor dat bij eventueel op te leveren Patient resource instances de identifier is gevuld met het BSN van de betroffende persoon (zie "Toelichting vulling BSN bij opleveren van gegevens").
4. Het systeem keert terug naar de main flow van de bovenliggende use case.

Uitzonderingen:

1. De gevraagde gegevens mogen niet worden opgeleverd
 - a. Het systeem genereert de vereiste foutresponse (situatie "niet voldaan aan (MedMij) beschikbaarheidsvoorwaarde") en keert terug naar de laatste stap van de main flow van de bovenliggende use case.

Toelichting beschikbaarheidsvoorwaarde

In de programma's van eisen die gelden voor bronsystemen zijn een aantal eisen opgenomen die gaan over het al dan niet beschikbaar stellen van bepaalde gegevens voor opvragende partijen:

1. Patiëntgegevens mogen pas worden opgeleverd nadat het BSN van patiënt door de zorgaanbieder is geverifieerd.
2. Patiëntgegevens moeten na vastlegging, automatisch of op commando van een zorgverlener/medewerker, vrijgegeven kunnen worden. Vrijgegeven patiëntgegevens moeten ook weer kunnen worden afgeschermd. Vrijgeven en afschermen moet kunnen op dossierniveau. Vrijgeven en afschermen moet mogelijk zijn per individuele patiënt. Bij afschermen dient onderscheid gemaakt te kunnen worden tussen bevragingen door patiënten en bevragingen door zorgverleners/medewerkers.
3. Alvorens gegevens van een patiënt op te leveren, dient er gecontroleerd te worden of de patiënt hiervoor toestemming heeft verstrekt. Dit kan worden afgeleid van het access_token in combinatie met het AORTA vertrouwensmodel, of uit een lokaal, in het GBZ vastgelegde toestemming.
4. Indien de opvrager een patiënt is, dan dient de resource server (het GBZ) te controleren of een behandelrelatie bestaat (danwel heeft bestaan) tussen patiënt en zorgaanbieder, en of de leeftijd van de persoon van wie gegevens worden opgevraagd minimaal 16 jaar is.
5. Bij het al dan niet beschikbaar stellen van gegevens mag het systeem dat de patiënt gebruikt, en de organisatie dit systeem aanbiedt niet als een criterium worden gehanteerd.

Tevens moet de resource server borgen dat gegevens die worden opgeleverd daadwerkelijk betrekking hebben op de patiënt (BSN), zoals opgenomen in het AORTA access_token.

Indien de opvrager een patiënt, is dan geldt dat in de volgende situaties niet wordt voldaan aan de MedMij beschikbaarheidsvoorwaarde:

- Er bestaat geen behandelrelatie tussen zorgaanbieder en patiënt en een behandelrelatie heeft ook nooit bestaan.
- De leeftijd van de opvrager is niet toereikend.
- De gevraagde gegevens zijn afgeschermd of niet vrijgegeven.

Gegevensdienst-specifieke UC extensions en implementatiehandleidingen

De gegevensdienst-specifieke delen van deze use cases maken deel uit van de betreffende <resourcetype> <interactietype> Verwerkend systeemrollen, bijvoorbeeld *Observation Search Verwerkend Systeem* of *MedicationStatement Search Verwerkend Systeem*.

FHIR-interacties: de implementatiehandleiding die van toepassing is voor een specifieke gegevensdienst is opgenomen in onderstaande tabel.

| Gegevensdienstnaam | ID | Implementatiehandleiding | UC extension |
|--|----|---|----------------------|
| Verzamelen Documenten 3.0 | 51 | IH FHIR_PDFa_2020 | Opleveren Documenten |
| Delen Meetwaarden vitale functies 2.0 | 53 | IH FHIR_VitalSigns_2020 | - |
| Verzamelen Meetwaarden vitale functies 2.0 | 54 | | - |
| Verzamelen Basisgegevens zorg 3.0 | 48 | IH FHIR_BGZ_2017 | - |
| Verzamelen Basisgegevens GGZ 2.0 | 50 | IH FHIR_GGZ_2020 | - |
| Verzamelen verwijzingen naar vragenlijsten 2.0 | 59 | IH FHIR_Questionnaire_and_Questionnaire_Response_2020 | - |
| Delen antwoorden op vragenlijsten 2.0 | 60 | | - |
| Verzamelen Afspraken 2.0 | 47 | IH FHIR_eAfspraak_2020 | - |

HL7v3-interacties: de implementatiehandleiding die van toepassing is, is opgenomen in onderstaande tabel.

| Interactie-ID request | Interactie-ID response | Implementatiehandleiding | UC extension |
|-----------------------|------------------------|--|--------------|
| ZTQM_IN000004NL | MCCI_IN000002 | IH HL7v3 Delen Zelfmetingen | - |
| QUAF_IN990001NL01 | QUAF_IN990003NL01 | IH HL7v3 Verzamelen ContactAfspraken | - |

Toelichting vulling BSN bij opleveren van gegevens

Alle use cases waarin de resource server gegevens op dient te leveren zijn gebaseerd op de MedMij FHIR informatiestandaarden van Nictiz. Omdat het de bedoeling is dat gegevens (op termijn) zowel kunnen opgeleverd aan PGO Servers in MedMij als aan Initiërende GBZ'en binnen AORTA gelden een aantal specifieke AORTA aanvullingen op de informatiestandaarden.

Het [profiel voor nl-core-patient](#) bevat een attribuut Patient.identifier, waarin het BSN van een persoon kan worden opgenomen. De MedMij FHIR informatiestandaarden beschrijven echter dat geen BSN mag worden opgenomen in de Patient resource, omdat PGO Servers geen wettelijke grondslag hebben om deze te mogen verwerken.

Omdat voor uitwisseling tussen zorgaanbieders onderling het BSN juist wel verplicht is, is het gewenst dat de Patient.identifier daarom **wel wordt gevuld met het BSN** van de betreffende persoon. Resource Broker MedMij-in zal het BSN filteren voordat de gegevens worden geretourneerd aan een PGO Server.

Generieke UC extension: Ontvangen gegevens

Systeem: MedMij Ontvangend Systeem

Triggers:

- De resource server heeft een FHIR-create of een FHIR-update interactie ontvangen, OF
- De resource server heeft een v3-interactie ontvangen, waarmee gegevens worden gestuurd

Main flow:

1. Afhankelijk van de gegevensdienst waar de interactie deel van uitmaakt (FHIR-interactie), of van het interactie-id (v3-interactie)
 - a. wordt de ontvangen interactie nu verwerkt conform de gegevensdienst-specifieke implementatiehandleiding, zoals benoemd in de toelichting "Gegevensdienst-specifieke UC extensions en implementatiehandleidingen".
 - b. wordt (indien van toepassing) de juiste extension flow doorlopen, zoals aangegeven in de toelichting "Gegevensdienst-specifieke UC extensions en implementatiehandleidingen".
2. Het systeem verwerkt bij eventueel ontvangen Patient resource instances ook de identifier die is gevuld met het BSN van de betroffen persoon (zie "Toelichting vulling BSN bij ontvangen van gegevens").
 - a. Uitzondering 1: De ontvangen gegevens mogen niet worden verwerkt.
3. Het systeem keert terug naar de main flow van de bovenliggende use case.

Uitzonderingen:

1. De ontvangen gegevens mogen niet worden verwerkt
 - a. Het systeem genereert de vereiste foutresponse (situatie "client beschikt niet over de juiste autorisatie") en keert terug naar de laatste stap van de main flow van de bovenliggende use case.

Toelichting vulling BSN bij ontvangen van gegevens

Alle use cases waarin de resource server gegevens dient te ontvangen zijn gebaseerd op de MedMij FHIR informatiestandaarden van Nictiz. Omdat het de bedoeling is dat gegevens (op termijn) zowel kunnen worden ontvangen van PGO Servers in MedMij als van Initiërende GBZ'en binnen AORTA gelden een aantal specifieke AORTA aanvullingen op de informatiestandaarden.

Het [profiel voor nl-core-patient](#) bevat een attribuut Patient.identifier, waarin het BSN van een persoon kan worden opgenomen. De MedMij FHIR informatiestandaarden beschrijven echter dat geen BSN mag worden opgenomen in de Patient resource, omdat PGO Servers geen wettelijke grondslag hebben om deze te mogen verwerken.

Omdat voor uitwisseling tussen zorgaanbieders onderling het BSN juist wel verplicht is, zal de Patient.identifier daarom **wel worden gevuld met het BSN** van de betreffende persoon. Resource Broker MedMij-in zal het BSN toevoegen voordat de gegevens worden verzonden richting een resource server.

De resource server moet borgen dat gegevens die worden ontvangen en verwerkt daadwerkelijk betrekking hebben op de patiënt (BSN), zoals opgenomen in het AORTA access_token.

UC Workflow - 0.7.x

- UC Extensions
 - UC Extension: Opleveren Taak
- UC Templates
 - UC Template: Aanvragen Taak
 - UC Template: Opvragen Taak
 - UC Template: Bijwerken Taak
 - UC Template: Verwerken Aanvraag Taak
 - UC Template: Verwerken Taak Mutatie
 - UC Template: Verzenden Notificatie

Let op! Deze use cases worden verwacht in AoF 0.8 , maar worden nog niet gebruikt in AoF 0.7.

UC Extensions

UC Extension: Opleveren Taak

Main flow:

1. Het systeem zoekt de gevraagde taak op
 - a. Uitzondering 1: Taak niet gevonden
2. Het systeem keert terug naar de main flow van de bovenliggende use case.

Uitzonderingen:

1. Taak niet gevonden
 - a. Het systeem genereert de vereiste foutresponse (situatie: "resource-id niet bekend") en keert terug naar de main flow van de bovenliggende use case.

UC Templates

UC Template: Aanvragen Taak

Secundaire actor: Taak Uitvoerend Systeem

Systeem: Taak Aanvragend Systeem

Pre-condities:

- Het systeem is aangesloten op de secundaire actor.
- De primaire actor beschikt over de juiste kwalificaties om deze use case te mogen uitvoeren.

Main flow:

1. Het systeem initieert de use case *Verwerken Aanvraag Taak* middels de *Taak Uitvoering Interface*.
2. Het systeem ontvangt een response.
3. Het systeem keert terug naar de main flow van de bovenliggende use case.

Postconditie:

- Het request is verzonden en beantwoord.

UC Template: Opvragen Taak

Volgt later.

UC Template: Bijwerken Taak

Volgt later.

UC Template: Verwerken Aanvraag Taak

Let op: onderstaande beschrijving is slechts een template die kan worden gebruikt in de specificaties van de workflow voor concrete taken.

Primaire actor: Taak Aanvragend Systeem

Systeem: Taak Uitvoerend Systeem

Pre-condities:

- De primaire actor is aangesloten op het systeem;
- De benodigde kwalificaties van de primaire actor om deze functie te mogen gebruiken zijn reeds geregistreerd in het Applicatie Register.

Triggers:

- De primaire actor initieert een interactie waarmee een aanvraag voor een taak wordt ingediend

Main flow:

1. Het systeem ontvangt de interactie
2. Het systeem valideert de ontvangen interactie, zoals beschreven in de toelichting "Validatie van interacties m.b.t. XXX".
 - Uitzondering 1: Ongeldige interactie
3. Het systeem controleert of de primaire actor deze taak mag aanvragen.
 - Uitzondering 2: Primaire actor is niet geautoriseerd
4. Het systeem slaat de ontvangen aanvraag op.
5. ...
6. Het systeem retourneert een response.
7. Het systeem logt het ontvangen request en de geretourneerde response, zoals beschreven in de toelichting "Logging van interacties m.b.t. XXX".

Postconditie bij succes:

- De ontvangen aanvraag is opgeslagen in het systeem

Post-condities bij falen:

- De ontvangen aanvraag is niet opgeslagen in het systeem

Uitzonderingen:

1. Ongeldige interactie
 - a. Het systeem genereert de vereiste foutresponse (situatie "ongeldig verzoek") en keert terug naar stap 7 van de main flow.
2. Primaire actor is niet geautoriseerd
 - a. Het systeem genereert de vereiste foutresponse (situatie: "client beschikt niet over de juiste autorisatie") en keert terug naar stap 7 van de main flow.

UC Template: Verwerken Taak Mutatie

Volgt later.

UC Template: Verzenden Notificatie

Secundaire actor: Taak Aanvragend Systeem

Systeem: Taak Uitvoerend Systeem

Main flow:

1. Het systeem stuurt een notificatie naar het in de aanvraag aangegeven adres via de [Taak Notificatie Interface](#).
 - a. Uitzondering 2: Notificatie niet geslaagd
2. Het systeem logt de verzonden notificatie alsmede de relatie tussen de notificatie en de aanvraag.
3. Het systeem keert terug naar de main flow van de bovenliggende use case.

Postconditie bij succes:

- De notificatie is succesvol verzonden

Postconditie bij falen:

- De notificatie is niet succesvol verzonden

Uitzonderingen:

1. Notificatie niet geslaagd
 - a. **Wat wordt nu gedaan? Wordt een lijst van niet geslaagde notificaties bijgehouden?**