PvE Opvragend Systeem FHIR Addendum

Medicatieproces

Datum:	11 april 2024
Status:	Definitief
Versie:	9.3
Classificatie:	Openbaar
Eigenaar:	VZVZ
Revisie:	01

Inhoudsopgave

1 Inleiding

Dit document bevat een addendum op het ‘PvE Medicatieproces – Opvragend Systeem’. De hierin opgenomen eisen zijn specifiek bedoeld voor XIS-leveranciers die met het FHIR-protocol berichten gaan uitwisselen.

Een aantal in dit addendum opgenomen eisen vervangen bestaande HL7v3 eisen. Daarnaast zijn er nog een aantal nieuwe eisen toegevoegd. Indien eisen zijn weggevallen, dan is dat ook opgenomen.

Vervangen eisen zijn gegroepeerd o.b.v. de ISO 25010. De nieuwe eisen zijn gegroepeerd per functionaliteit.

2 Vervangende eisen

2.1 Applicatiebeheer

2.1.1 Bevestigen applicatiekoppeling o.b.v. FHIR

Deze eis vervangt eis 'Bevestigen applicatiekoppeling' (GBX.APR.e4160).

Alias: GBX.APR.e4080.1

Details
Eis: Het XIS moet een applicatiekoppelingverificatie-bericht vanuit het LSP kunnen ontvangen. **Toelichting bij eis:** Op basis van het applicatiekoppelingverificatie-bericht wordt een zogenaamde 'ping' naar het op AORTA aangesloten systeem gestuurd. Als antwoord stuurt het systeem een 'pong' terug. Op deze manier kan in de keten worden gecontroleerd of een bronsysteem actief is. Het applicatiekoppelingverificatie-bericht is gespecificeerd in de 'AORTA on FHIR'-specificatie: https://aorta-on-fhir.scrollhelp.site/aorta-on-fhir-specificaties/Working-version/interfaces-resource-server#InterfacesResourceServer-AORTACapabilityStatementInterface

Vzvz_Moscow: Verplicht
Vzvz_Req_Verificatie: Acceptatietest
Vzvz_Req_Soort: Functional
Vzvz_Req_Type: Product

2.1.2 Wijzigen TKID applicatie o.b.v. FHIR

Deze eis vervangt eis 'Wijzigen TKID applicatie' (GBX.APR.e4060, GBX.APR.e4170.1).

Alias: GBX.APR.e4070.1

Details
Eis: Het XIS moet op basis van een 'TKID activatie'-bericht aangeven welke FHIR-interacties de applicatie kan versturen/verwerken. **Toelichting bij eis:** Door middel van het insturen van een TKID wordt er in het applicatieregister een koppeling gelegd tussen de applicatie die het 'TKID activatie'-bericht instuurt en de bijbehorende conformances. Door middel van deze koppeling wordt het voor de applicatie mogelijk om gebruik te kunnen maken van de verschillende interfaces met het LSP. De TKID-activatie wordt beschreven in de 'AORTA on FHIR'-publicatie: https://aorta-on-fhir.scrollhelp.site/aorta-on-fhir-specificaties/Working-version/interfaces-resource-broker-apr#InterfacesApplicatieregister-TKID-activatie

Vzvz_Moscow: Verplicht
Vzvz_Req_Verificatie: Acceptatietest
Vzvz_Req_Soort: Functional
Vzvz_Req_Type: Product

2.1.3 Verifiëren applicatiekoppeling

Eis Verifiëren applicatiekoppeling (GBX.APR.e4140) komt te vervallen. Deze functionaliteit wordt niet geboden binnen AORTA-on-FHIR.

2.2 Beveiligbaarheid

2.2.1 Toegangslog bijhouden (FHIR)

Deze eis vervangt eis 'Toegangslog bijhouden' (GBX.LOG.e4015.1).

Alias: GBX.LOG.e4016

Details
Eis: Het systeem moet alle binnenkomende en uitgaande berichten loggen in de toegangslog. Hierbij dienen onderstaande gegevens gelogd te worden, indien aanwezig in het bericht: 1. de identiteit van de patiënt/cliënt/burger (BSN) waar het bericht betrekking op heeft; 2. de identiteit van de organisatie waar het bericht vandaan komt of naar toe wordt gestuurd; 3. de functie en identiteit van de zorgverlener, medewerker of patiënt zoals opgenomen in het verstuurde en/of ontvangen bericht. De functie is de aorta-rolcode zoals opgenomen in het claim-element van het transactietoken. 4. de gebruikersinteractieID. Dit is een combinatie van HTTP-operatie, de URL inclusief de ontvangen zoekparameters en de contentVersion uit de AORTA-Version header; 5. het tijdstip en tijdzone (ten opzichte van UTC) van het moment dat het bericht ontvangen/verstuurd is; 6. de bericht-id van het ontvangen/verstuurde bericht. Dit is het messageID in de HTTP header; 7. het initiële bericht-id van het ontvangen/verstuurde bericht. Dit is het initialMessageID in de HTTP header; 8. de aan het bericht gekoppelde gegevensdienst. Dit is de waarde zoals opgenomen in de scope van het transactietoken; 9. een indicatie van eventueel opgetreden foutsituaties met betrekking tot het ontvangen en verzenden van de berichten. Hierbij dient de HTTP-foutcode, alle informatie in de eventueel aanwezige operationOutcome en de enventuele WWW-Authenticate HTTP response header gelogd te worden. **Toelichting bij eis:** Het doel van de logging is het inzichtelijk kunnen maken van de datastroom door de gehele keten. Het inzichtelijk maken van de loggegevens kan van belang zijn voor auditredenen of beheerwerkzaamheden zoals het oplossen van fouten in de keten. Deze eis is conform de vereisten zoals beschreven in de NEN7513.

Vzvz_Moscow: Verplicht
Vzvz_Req_Verificatie: Acceptatietest
Vzvz_Req_Soort: Functional
Vzvz_Req_Type: Product

2.3 Koppelbaarheid

2.3.1 Protocolstack voor berichtuitwisseling o.b.v. FHIR

Deze eis vervangt eis 'Protocolstack voor berichtuitwisseling' (GBX.CON.e4060.2).

Alias: GBX.CON.e4130.1

Details
Eis: Het GBx dient voor berichtuitwisseling met de ZIM de volgende protocolstack te gebruiken: • HL7 FHIR • JWT • HTTP v1.1/HTTP v2.0 • TLS v1.2/TLS 1.3 • TCP • IPv4 **Toelichting bij eis:** Het is niet toegestaan om een lagere protocolversie te hanteren dan die in deze protocolstack vermeld is.

Vzvz_Moscow: Verplicht
Vzvz_Req_Verificatie: Acceptatietest
Vzvz_Req_Soort: Functional
Vzvz_Req_Type: Product

3 Aanvullende eisen

3.1 Eisen m.b.t. Adressering

3.1.1 Adresseren ontvangende organisatie

Alias: GBX.ADR.e4010

Details
Eis: Een systeemgebruiker moet een organisatie kunnen selecteren waaraan hij een bericht wil versturen. Het moet voor een systeemgebruiker duidelijk zijn aan welke organisatie hij een bericht richt. Hiervoor dienen minimaal de volgende gegevens getoond te kunnen worden: • Organisatienaam; • Adresgegevens. **Toelichting bij eis:** Een systeemgebruiker moet door het systeem ondersteund worden in het kunnen zoeken en selecteren van een te adresseren organisatie. Om adresseringsfouten te voorkomen, is het niet toegestaan om adresgegevens door een systeemgebruiker zelf in te laten vullen. Condities: Indien er sprake is van een gerichte bevraging of verzending van patiëntgegevens.

Vzvz_Moscow: Conditioneel
Vzvz_Req_Verificatie: Acceptatietest
Vzvz_Req_Soort: Functional
Vzvz_Req_Type: Product

3.1.2 Verkrijgen URA te adresseren organisatie

Alias: GBX.ADR.e4020

Details
Eis: Het systeem dient een actuele URA van de te adresseren organisatie te verkrijgen via een betrouwbare bron. Hierbij dient een URA onweerlegbaar te zijn gekoppeld aan de functionele naam van de organisatie zoals vastgelegd bij het CIBG. **Toelichting bij eis:** Er moet voorkomen worden dat een kwaadwillende adresgegevens in die mate muteert, dat medische gegevens naar een andere organisatie dan de door de systeemgebruiker bedoelde organisatie kunnen worden gestuurd. Hiervoor dienen adresgegevens alleen door een daarvoor geautoriseerde bron te kunnen worden aangepast.

Een betrouwbare bron is een bron, waarin de CIBG-gegevens onweerlegbaar zijn vastgelegd en waarin die gegevens alleen gemuteerd kunnen worden door daarvoor geautoriseerde personen. Het ZORG-AB wordt gezien als een betrouwbare bron. Condities: Indien er sprake is van een gerichte bevraging of verzending van patiëntgegevens.

Vzvz_Moscow: Conditioneel
Vzvz_Req_Verificatie: Acceptatietest
Vzvz_Req_Soort: Functional
Vzvz_Req_Type: Product

3.1.3 Verkrijgen routeergegevens

Alias: GBX.ADR.e4030

Details
Eis: Routeergegevens kunnen worden bevraagd door middel van een bevraging gericht aan de Adresseringsserver. **Toelichting bij eis:** Het algoritme zoals geïmplementeerd in de Adresseringserver, ontlast een initiërende applicatie van het bepalen of een ontvangend systeem ook daadwerkelijk het te ontvangen bericht kan verwerken. De Adresseringserver bepaalt op basis van de in het applicatieregister (APR) geregistreerde conformances, of een ontvangend systeem het bericht kan verwerken of dat er mogelijk een transformatie door de berichtentransformatiedienst (BTD) mogelijk is. Aangezien conformances en eventuele berichttransformaties veranderlijk zijn, is het sterk aan te raden om gebruik te maken van de interface met de Adresseringserver. De interface met de Adresseringsservice is beschreven in de 'AORTA-on-FHIR'-publicatie: https://aorta-on-fhir.scrollhelp.site/aorta-on-fhir-specificaties/Working-version/interfaces-adressering-server Condities: Indien er sprake is van een gerichte bevraging of verzending van patiëntgegevens.

Vzvz_Moscow: Conditioneel
Vzvz_Req_Verificatie: Acceptatietest
Vzvz_Req_Soort: Functional
Vzvz_Req_Type: Product

3.2 Eisen m.b.t. Stelseltoken

3.2.1 Controleren Stelseltoken

Alias: GBX.STEL.e4010

Details
Eis: Wanneer een AORTA Stelseltoken wordt verkregen, dan dienen de volgende controles te worden uitgevoerd: • Of het token is uitgegeven door een vertrouwde partij; vertrouwde issuers van het AORTA Stelseltoken worden out-of-band aan betrokken partijen gecommuniceerd. • Of het certificaat, waarmee de handtekening is geplaatst, toebehoort aan de issuer van het AORTA Stelseltoken. • 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. **Toelichting bij eis:** De stelselnode is uitgewerkt in de 'AORTA on FHIR'-publicatie: https://aorta-on-fhir.scrollhelp.site/aorta-on-fhir-specificaties/Working-version/interfaces-aorta-stelselnode

Vzvz_Moscow: Verplicht
Vzvz_Req_Verificatie: Acceptatietest
Vzvz_Req_Soort: Functional
Vzvz_Req_Type: Product

3.2.2 Opvragen Stelseltoken

Alias: GBX.STEL.e4020

Details
Eis: Een XIS moet de mogelijkheid hebben om een Stelsteltoken op te vragen. Het Stelseltoken kan worden opgehaald op een aorta-base-URL die door VZVZ-beheer rechtstreeks, via een veilig kanaal, met aangesloten partijen wordt gecommuniceerd. De metadata uit een AORTA Stelseltoken mag voor een maximale duur van *max-age-aorta-stelseltoken* opgeslagen worden in de lokale cache. Indien de *max-age* is verlopen, dan dient de cache te worden geleegd. **Toelichting bij eis:** Het AORTA Stelseltoken bevat metadata m.b.t. de verschillende servers of componenten die binnen de AORTA infrastructuur vallen. Op basis van deze metadata kan een initiërend XIS de audience achterhalen van het AORTA Access Token. Een ontvangend XIS kan op basis van deze metadata controleren of de issuer van het AORTA Access Token inderdaad de te verwachten autorisatieserver is. Het AORTA Stelseltoken kan op de volgende wijze worden opgehaald: GET [aorta-base-URL]/metadata/v1

De stelselnode is uitgewerkt in de 'AORTA on FHIR'-publicatie: https://aorta-on-fhir.scrollhelp.site/aorta-on-fhir-specificaties/Working-version/interfaces-aorta-stelselnode.

Vzvz_Moscow: Verplicht
Vzvz_Req_Verificatie: Acceptatietest
Vzvz_Req_Soort: Functional
Vzvz_Req_Type: Product

3.2.3 Controleren issuer stelseltoken

Alias: GBX.BVL.e4130

Details
Eis: Bij ontvangst van een stelseltoken dient te worden gecontroleerd of: • het token is uitgegeven door een vertrouwde issuer van het AORTA stelseltoken; • het stelseltoken juist is ondertekend door een geldig certificaat dat toebehoort aan de vertrouwde issuer. **Toelichting bij eis:** Een vertrouwde issuer wordt door VZVZ aan de betrokken partijen gecommuniceerd. **Condities:** • Verplicht indien er geen controle wordt gedaan op de FQDN van de initiërende partij (GBX.BVL.e4140); Verplicht indien het stelseltoken wordt gebruikt.

Vzvz_Moscow: Conditioneel
Vzvz_Req_Verificatie: Acceptatietest
Vzvz_Req_Soort: Functional
Vzvz_Req_Type: Product

3.3 Eisen m.b.t. AORTA Access Token

3.3.1 Verkrijgen AORTA access token

Alias: GBX.AAT.e4020.2

Details
Eis: Het systeem dient vóór communicatie binnen de AORTA infrastructuur een AORTA access token te verkrijgen bij de AORTA Autorisatieserver voor zorgaanbieders. Afhankelijk van de wijze waarop geautoriseerd moet worden, worden de volgende tokens meegestuurd: • In het geval van VGU: 1. Transactietoken getekend met UZI-servercertificaat;

2. Mandaattoken;
3. Inschrijftoken (of in plaats daarvan een consenttoken indien er sprake is van een opvraag als gevolg van een notified pull);

- Zonder VGU:

1. Transactietoken getekend met authenticatiecertificaat van zorgverlenerspas;
2. Mandaattoken indien er sprake is van het versturen/opvragen onder mandaat;
3. Consenttoken indien er sprake is van een opvraag als gevolg van een notified pull.

Toelichting bij eis:

Het proces met betrekking tot het verkrijgen van AORTA access token staat beschreven in de 'AORTA on FHIR'-publicatie.

Vzvz_Moscow: Verplicht
Vzvz_Req_Verificatie: Acceptatietest
Vzvz_Req_Soort: Functional
Vzvz_Req_Type: Product

3.4 Configuratie

3.4.1 Configureren vertrouwde issuers/clients

Alias: GBX.CONF.e4010

Details
Eis: Door VZVZ verstrekte nieuwe gegevens met betrekking tot vertrouwde issuers en clients dienen binnen 24 uur geconfigureerd te worden. Het is mogelijk dat er meerdere instanties met dezelfde functionaliteit, maar met verschillende configuratiegegevens naast elkaar bestaan. Aanpassingen van configuratiegegevens dient te gebeuren door een daarvoor geautoriseerd persoon met een geldig tweefactormiddel. **Toelichting bij eis:** Om het zorgproces niet in gevaar te brengen is het noodzaak om medische gegevens beschikbaar te houden. Het is dan ook zaak om de configuratiegegevens actueel te houden om geen onterechte berichtafwijzingen te laten ontstaan. De verschillende componenten binnen AORTA zijn niet perse beperkt tot één instantie. Het is bijvoorbeeld mogelijk dat er meerdere autorisatieservers en VnC's zijn. Deze kunnen verschillende configuratiegegevens hebben en dienen ook als zodanig geconfigureerd te kunnen worden. Het aanpassen van configuratiegegevens door een kwaadwillende kan leiden tot een datalek(ken). Het is dan ook zaak om alleen geautoriseerde personen met een tweefactormiddel aanpassingen te kunnen laten doen.

Vzvz_Moscow: Verplicht
Vzvz_Req_Verificatie: Acceptatietest
Vzvz_Req_Soort: Functional

Vzvz_Req_Type: Product

3.5 Beveiliging

3.5.1 Toegang systeem met tweefactorauthenticatie

Alias: GBX.BVL.e4150

Details
Eis: Toegang tot medische gegevens en LSP-functionaliteit kan door een systeemgebruiker alleen verkregen worden door middel van het inloggen met tweefactorauthenticatie. **Toelichting bij eis:** Conform de NEN7510 (9.4.1 Beperking toegang tot informatie) moet een gebruiker voor toegang tot medische gegevens gebruik maken van een tweefactorauthenticatiemiddel. Hiervoor kan de UZI-pas worden gebruikt, maar ook andere tweefactorauthenicatiemiddelen zijn toegestaan.

Vzvz_Moscow: Verplicht
Vzvz_Req_Verificatie: Acceptatietest
Vzvz_Req_Soort: Functional
Vzvz_Req_Type: Product