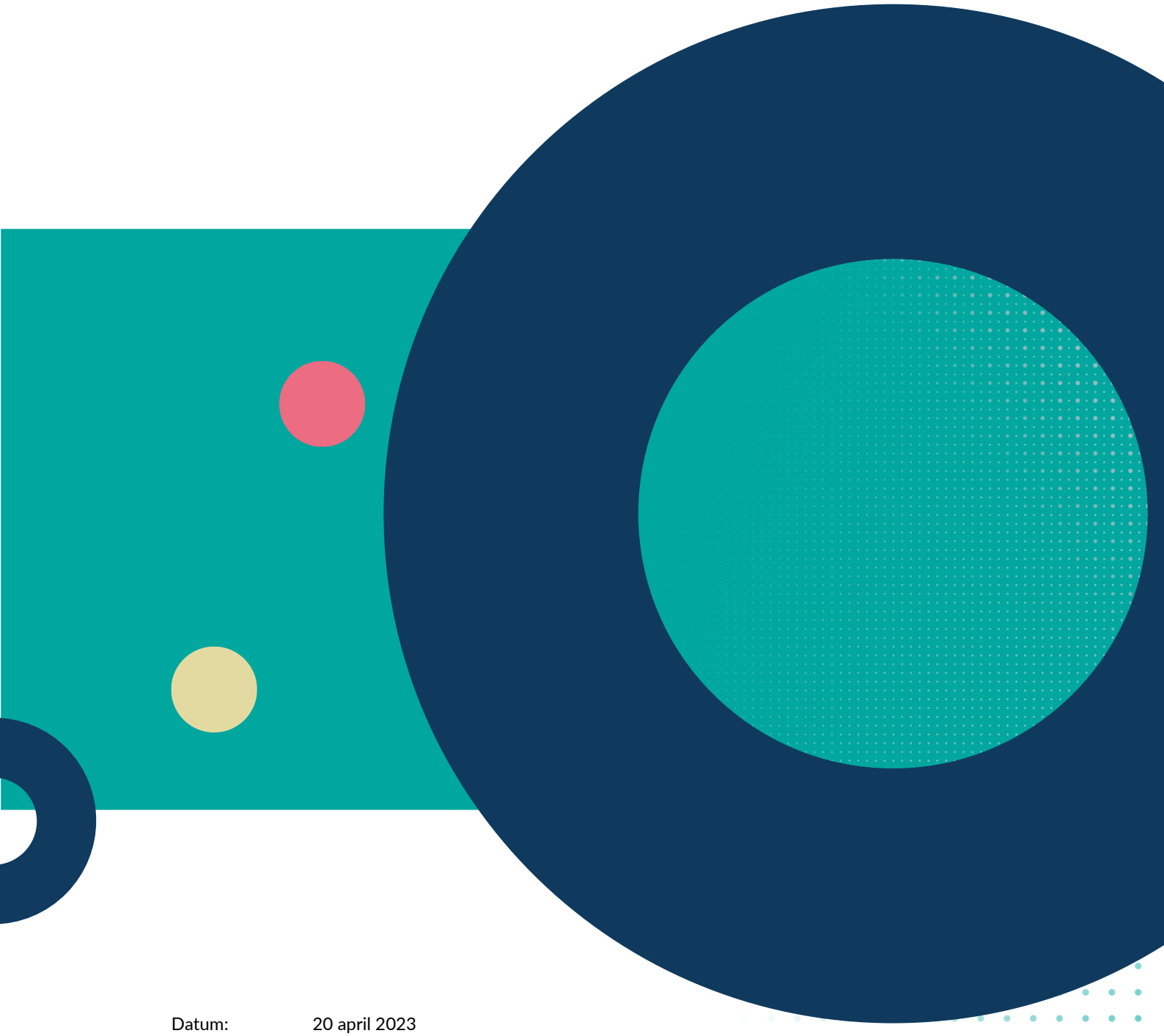
PvE Opvragend Systeem

Medicatieproces



Datum:	20 april 2023
Status:	Definitief
Versie:	9.3
Classificatie:	Openbaar
Eigenaar:	VZVZ
Revisie:	01

Inhoudsopgave

1 Inleiding

1.1 Inleiding

Dit programma van eisen gaat over de toepassing Medicatieproces. Dit Programma van Eisen(PvE) betreft een document waarin alle eisen zijn opgenomen waaraan een GBZ moet voldoen om aangesloten te worden op de AORTA-infrastructuur.

1.2 Doelgroep voor dit document

De doelgroep voor dit document bestaat uit diverse rollen aan de kant van de XIS-leverancier en de GBx beheerorganisatie. Het gaat hierbij om o.a. architecten, software ontwikkelaars, productmanagers, testers en systeembeheerders. Tevens is dit document bedoeld voor diverse rollen binnen VZVZ. Het gaat hierbij o.a. om architecten, productmanagers, testers, demandmanagers en ketenregie.

1.3 Doel en Scope

Het doel van dit document is om de eisen te beschrijven waaraan moet worden voldaan om een GBZ als Opvragend systeem t.b.v. Medicatieproces aan te sluiten op de AORTA-infrastructuur. De hierin opgenomen hoofdstukken gelden voor alle Opvragende systemen ongeacht het applicatieprofiel.

2 Generieke eisen

2.1 AORTA Eisen aan de Beheerorganisatie van een GBX

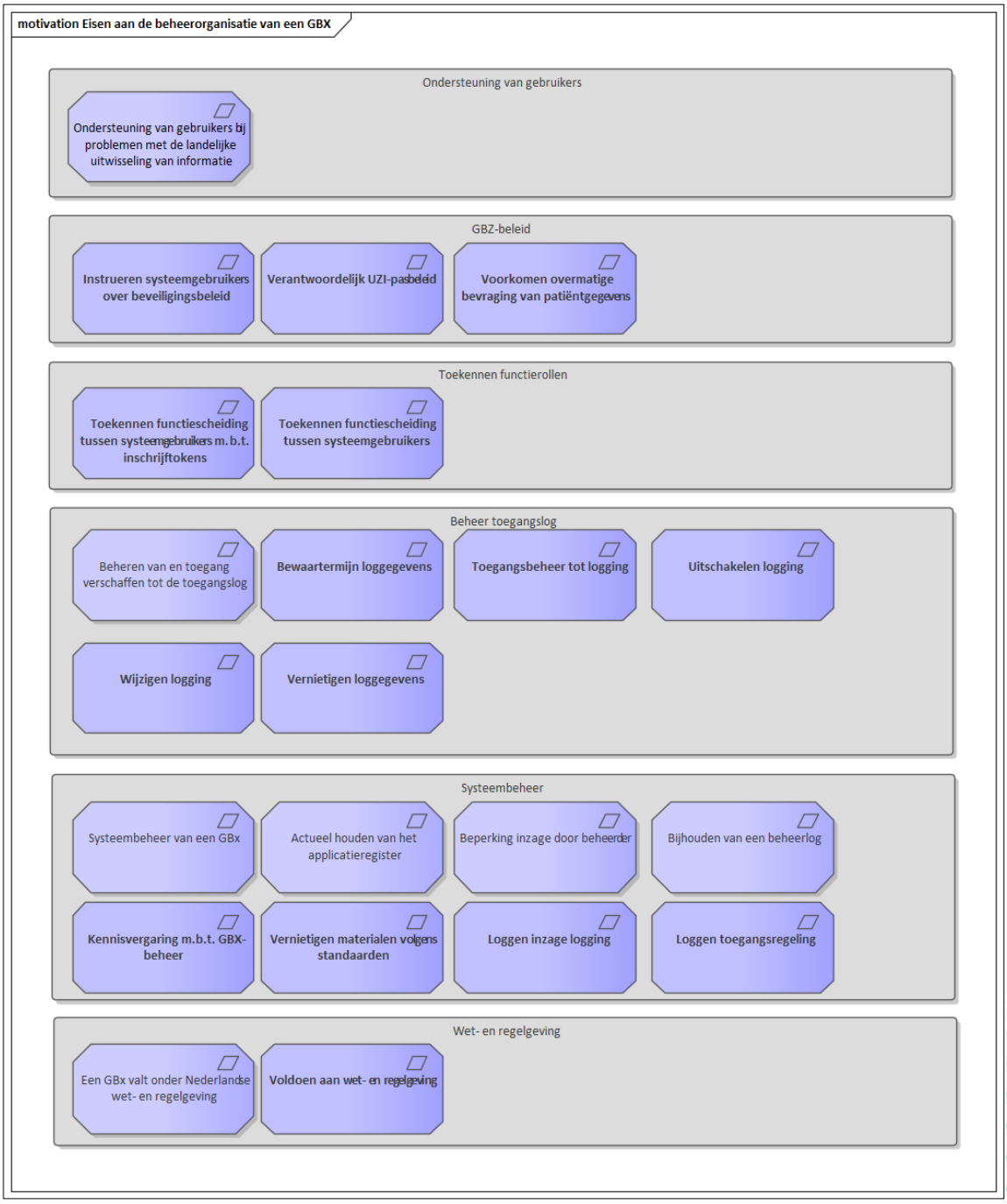


Figure 1 : Eisen aan de beheerorganisatie van een GBX

2.1.1 Wijzigen logging

Alias: AGE.LOG.e4060

Details
Eis: Gegevens in de log mogen niet wijzigbaar of verwijderbaar (alleen in het kader van eis **AGE.LOG.e4050**) zijn. Het niet kunnen wijzigen/verwijderen van loggegevens moet worden afgedwongen door technische maatregelen. **Toelichting** Conform NEN 7513:2018 Paragraaf 6.4.3

Vzvz_Moscow: n/a
Vzvz_Req_Verificatie: n/a
Vzvz_Req_Soort: n/a
Vzvz_Req_Type: n/a

2.1.2 Vernietigen loggegevens

Alias: AGE.LOG.e4050

Details
Eis: Loggegevens moeten bij het verstrijken van <*log_bewaartermijn*> automatisch worden verwijderd uit de actieve log en uit het archief. De logregels moeten op een zodanige wijze vernietigd worden dat de data niet te reconstrueren is. Dit betekent ook dat eventueel reservekopieen verwijderd/vernietigd/volledig overschreven zijn. **Toestemming** Conform NEN 7513:2018 paragraaf 8.5. Elke afsprakenstelsel/architectuur dient expliciet invulling te geven aan de waarde voor <*log_bewaartermijn*>. Indien deze waarde ontbreekt dan geldt de standaard waarde van 5 jaar.

Vzvz_Moscow: n/a
Vzvz_Req_Verificatie: n/a
Vzvz_Req_Soort: n/a
Vzvz_Req_Type: n/a

2.1.3 Uitschakelen logging

Alias: AGE.LOG.e4030

Details
Eis: Het loggen van de berichtuitwisseling in de toegangslog en het loggen van acties op de toegangslog mogen niet uitgeschakeld kunnen worden. **Toelichting bij eis:** Conform NEN 7513:2018 Paragraaf 6.4.2

Vzvz_Moscow: n/a
Vzvz_Req_Verificatie: n/a
Vzvz_Req_Soort: n/a

Vzvz_Req_Type: n/a

2.1.4 Toegangsbeheer tot logging

Alias: AGE.LOG.e4040

Details
Eis: Directe toegang tot loggegevens en tot zoekvragen moet alleen mogelijk zijn op basis van twee factor authenticatie en expliciete autorisatie. Alleen de rol toegangslogbeheerder kan geautoriseerd worden voor toegang tot loggegevens waarin echte patiëntgegevens voorkomen of kunnen worden afgeleid. **Toelichting** Conform NEN 7513:2018 Paragraaf 8.4

Vzvz_Moscow: n/a
Vzvz_Req_Verificatie: n/a
Vzvz_Req_Soort: n/a
Vzvz_Req_Type: n/a

2.1.5 Loggen toegangsregeling

Alias: AGE.LOG.e4070

Details
Eis: Elke wijziging in de toegangsregeling dient te worden gelogd. Hierbij moet onweerlegbaar kunnen worden vastgesteld welke persoon met welke rol welke specifieke aanpassing heeft doorgevoerd. **Toelichting** Conform NEN 7513:2018 Paragraaf 6.3

Vzvz_Moscow: n/a
Vzvz_Req_Verificatie: n/a
Vzvz_Req_Soort: n/a
Vzvz_Req_Type: n/a

2.1.6 Loggen inzage logging

Alias: AGE.LOG.e4020

Details
Eis: Rechtmatigheid. Elke inzage van de toegangslog dient gelogd te worden. Hierbij moet onweerlegbaar kunnen worden vastgesteld welke persoon met welke rol inzage heeft gehad in welke specifieke gegevens. **Toelichting** Deze eis is conform NEN 7513:2018.

Vzvz_Moscow: n/a
Vzvz_Req_Verificatie: Audit
Vzvz_Req_Soort: Functional
Vzvz_Req_Type: Product

2.1.7 Bewaartermijn loggegevens

Alias: AGE.LOG.e4010

Details
Eis: De bewaartermijn van de toegangsloggegevens is *<toegangslog_bewaartermijn>*. Voor de overige logs (technische logs) geldt een bewaartermijn van *<systeemlog_bewaartermijn>*. **Toelichting bij eis:** Voor de toegangslog (log met betrekking tot patiëntgegevens) geldt (mogelijk) een andere bewaartermijn dan voor de systeemlog. Conform NEN 7513:2018 paragraaf 8.5 kan een patiënt binnen een bepaalde tijdsperiode nog aanspraak maken op inzage in de loggegevens. Deze tijdsperiode kan voor de technische log echter onnodig lang zijn en daarmee onnodig veel opslagcapaciteit verbruiken. De waarden *<toegangslog_bewaartermijn>* en *<systeemlog_bewaartermijn>* kunnen per afsprakenstelsel/architectuur afgesproken worden. Indien deze waarden niet expliciet ingevuld worden door het afsprakenstelsel/architectuur, dan geldt voor beide de waarde 5 jaar.

Vzvz_Moscow: n/a
Vzvz_Req_Verificatie: Monitoring
Vzvz_Req_Soort: Non-Functional
Vzvz_Req_Type: Business

2.1.8 Voldoen aan wet- en regelgeving

Alias: GBX.ALG.e4010

Details
Eis: Een GBX dient te voldoen aan de NEN7510, NEN7512 en NEN7513 normen. **Toelichting bij eis:** • In de wet gebruik BSN in de zorg Artikel 2 Lid 4a is afgedwongen dat de gegevensverwerking, zoals bedoelt in de bijbehorende wet, aantoonbaar moet voldoen aan de NEN7510. • In de concept AMvB aanvullende bepalingen verwerking persoonsgegevens in de zorg wordt in artikel 5 gesteld dat de netwerkverbindingen (intern netwerk en GZN) moeten voldoen aan het bepaalde in NEN 7512 en in artikel 7 wordt gesteld dat de logging van zorgaanbieders moet voldoen aan het bepaalde in NEN 7513.

Vzvz_Moscow: Verplicht (Must)
Vzvz_Req_Verificatie: Eigenverklaring
Vzvz_Req_Soort: Non-Functional
Vzvz_Req_Type: Product

2.1.9 Vernietigen materialen volgens standaarden

Alias: GBX.SBH.e4070

Details
Eis: Om te voorkomen dat privacygevoelige of beveiliging gerelateerde gegevens achterblijven en in ongewenste handen vallen dienen niet (meer) gebruikte websites, apps, informatie of code te worden vernietigd volgens de standaard DoD 5220.22-M (E). Te vervangen fysieke opslagmedia dienen gecontroleerd vernietigd te worden volgens DIN 32757.

Toelichting bij eis:
Er is een proces nodig dat controleert of gegevens nog noodzakelijk zijn en te verwijderen gegevens voorgoed vernietigt.

Vzvz_Moscow: Verplicht (Must)
Vzvz_Req_Verificatie: Eigenverklaring
Vzvz_Req_Soort: Functional
Vzvz_Req_Type: Business

2.1.10 Een GBx valt onder Nederlandse wet- en regelgeving

Alias: GBX.CON.e4050.1

Details
Eis: De technische infrastructuur van het GBX dient zich in de Europese Unie te bevinden. De voertaal met de zorgaanbieder en de organisatie die het GBx beheert en exploiteert is Nederlands. Met betrekking tot de contracten tussen de zorgaanbieder en bovengenoemde moet de Nederlandse wet-en regelgeving van toepassing zijn. De zorgaanbieder en de organisatie's die het GBX beheert en exploiteert dient in Nederland gevestigd te zijn. In de contracten tussen de zorgaanbieder en bovengenoemde moet de Nederlandse wet- en regelgeving van toepassing zijn. **Toelichting bij eis:** Dit is nodig om er voor te zorgen dat de infrastructuur en dienstverlening volledig onder Nederlandse wet- en regelgeving valt. De exploitant dient waarborgen actief te hebben die voorkomen dat gegevens oneigenlijk gebruikt kunnen worden en te voldoen aan de privacy wetgeving.

Vzvz_Moscow: Verplicht (Must)
Vzvz_Req_Verificatie: Aansluittoets
Vzvz_Req_Soort: Non-Functional
Vzvz_Req_Type: Product

2.1.11 Kennisvergaring m.b.t. GBX-beheer

Alias: GBX.SBH.e4060

Details
Eis: De GBX-organisatie dient voordat zij een beheerorganisatie van een op de productie-omgeving van AORTA draaiend systeem wordt, ervoor te zorgen dat de binnen de GBX-organisatie aangewezen persoon met als rol GBX-beheerder de GBX-workshop van VZVZ heeft gevolgd. **Toelichting bij eis:** Uit de praktijk blijkt dat partijen de workshop nodig hebben om zich een goed beeld te vormen van de samenwerking tussen de eigen beheerorganisatie en de andere GZN-, GBZ- en LSP-beheerorganisaties in de keten. Daarbij biedt VZVZ in de productiefase verschillende vormen van ondersteunende dienstverlening en een escalatiepad op ketenniveau. Deze ketensamenwerking vergroot de efficiency en effectiviteit van inzet van resources, en voorkomt dat verstoringen onnodig lang duren.

Vzvz_Moscow: Verplicht
Vzvz_Req_Verificatie: Aansluittoets
Vzvz_Req_Soort: Non-Functional
Vzvz_Req_Type: Product

2.1.12 Bijhouden van een beheerlog

Alias: GBX.SBH.e4050

Details
Eis: Beheerhandelingen moeten worden vastgelegd in een beheerlog. De organisatie dient de opdrachtgever en toezichthouder inzage te geven in deze beheerlog. In het beheerlog wordt bijgehouden welke systeembeheerder de inhoud van welke berichten heeft ingezien. **Toelichting bij eis:** De beheerlog ondersteunt de controle op de juiste werking van systemen en de controle op het volgen van procedures.

Vzvz_Moscow: Verplicht (Must)
Vzvz_Req_Verificatie: Acceptatietest
Vzvz_Req_Soort: Non-Functional
Vzvz_Req_Type: Product

2.1.13 Beperking inzage door beheerder

Alias: GBX.SBH.e4040.3

Details
Eis: De systeembeheerder mag de inhoud van berichten slechts inzien indien dit noodzakelijk is voor het oplossen van problemen, is ingelogd met een tweefactorauthenticatiemiddel en uitsluitend op verzoek van een: • {GBZ} zorgverlener/medewerker; • {GBP} patiënt/klant, een leidinggevende of de Toezichthouder. **Toelichting bij eis:** Vanuit zijn ondersteunende rol kan het voor een servicedeskmedewerker ({GBP}, servicemanager ({GBP}) of een beheerder nodig zijn de inhoud van berichten in te zien, bijvoorbeeld om een mogelijk verschil in twee berichten die dezelfde inhoud zouden moeten hebben te onderzoeken. Mede vanwege deze eis is het nodig dat de beheerder expliciet door de organisatieverantwoordelijke is aangewezen.

Vzvz_Moscow: Verplicht (Must)
Vzvz_Req_Verificatie: Acceptatietest
Vzvz_Req_Soort: Non-Functional
Vzvz_Req_Type: Product

2.1.14 Actueel houden van het applicatieregister

Alias: GBX.SBH.e4030

Details
Eis:

GBX-beheer moet de beheerde GBX-applicatie(s) bij LSP-beheer aanmelden zodat deze in het applicatieregister kan worden opgenomen en zodat GBX-beheer de status ervan actueel kan houden in Supportal. **Toelichting bij eis:** Deze eis is nodig om te kunnen participeren in berichtuitwisselingen via AORTA. Het actueel houden van het applicatieregister is belangrijk voor een correcte afhandeling van berichten.

Vzvz_Moscow: Verplicht (Must)
Vzvz_Req_Verificatie: Documentverificatie
Vzvz_Req_Soort: Non-Functional
Vzvz_Req_Type: Product

2.1.15 Systeembeheer van een GBx

Alias: GBX.SBH.e4020 (voorheen GBX.SBH.e4020.2)

Details
Eis: De rol van systeembeheerder moet door de organisatie expliciet benoemd en belegd zijn. De systeembeheerder en diens vervanger(s) dienen met actuele telefoonnummers bekend te zijn bij de LSP-beheerder en de centrale AORTA servicedesk. Tenminste één beheerder dient altijd bereikbaar te zijn en in staat om de nodige beheertaken uit te voeren. De systeembeheerder dient verzoeken van het LSP met betrekking tot het configureren van het GBx en het activeren/deactiveren van op het LSP aangesloten systeem in te willigen. **Toelichting bij eis:** Deze eis zorgt ervoor dat een systeembeheerder altijd kan worden gewaarschuwd als er problemen zijn met een GBx, die ingrijpen van de systeembeheerder vergen.

Vzvz_Moscow: Verplicht (Must)
Vzvz_Req_Verificatie: Documentverificatie
Vzvz_Req_Soort: Non-Functional
Vzvz_Req_Type: Product

2.1.16 Beheren van en toegang verschaffen tot de toegangslog

Alias: GBX.SBH.e4010

Details
Eis: De organisatie moet een toegangslogbeheerder benoemen. De toegangslogbeheerder moet verzoeken van de toezichthouder om de lokale toegangslog te raadplegen inwilligen. **Toelichting bij eis:** Deze eis is nodig omdat de toezichthouder op AORTA voor het uitvoeren van haar bevoegdheden informatie nodig kan hebben over de gebeurtenissen waarbij het GBx met het LSP informatie heeft uitgewisseld. {GBx} Deze toegangslogbeheerder kan door alle zorgverleners worden gemandateerd om de toegangslog te raadplegen, om zo te voorkomen dat hij voor een verzoek tot raadplegen van de lokale toegangslog inzake een bepaalde patiënt/cliënt steeds de behandelende zorgverleners moet inschakelen.

{GBK} Deze toegangslogbeheerder kan worden gemandateerd om de toegangslog te raadplegen door de GBK-verantwoordelijke. {GBP} Deze Logbeheerder dient vóór de aansluiting aan het LSP te worden doorgegeven aan VZVZ.

Vzvz_Moscow: Verplicht (Must)
Vzvz_Req_Verificatie: Audit
Vzvz_Req_Soort: Non-Functional
Vzvz_Req_Type: Product

2.1.17 Toekennen functiescheiding tussen systeemgebruikers

Alias: GBX.FBH.e4025

Details
Eis: Het autorisatiebeleid binnen een organisatie moet rekening houden met het onderscheid tussen systeemgebruikers die gebruik mogen maken van LSP-functionaliteiten en systeemgebruikers die geen toegang tot deze functionaliteiten mogen hebben. De verantwoordelijke voor het toekennen van autorisaties binnen de organisatie dient in het systeem de juiste autorisaties toe te kennen aan de systeemgebruikers. **Toelichting:** GBZ-en zouden een additionele toegangscontrole moeten implementeren voor het initiëren van interacties met het LSP. Een medewerker met toegang tot het systeem van een GBZ zou niet automatisch ook toegang moeten hebben tot de functies om het LSP te bevragen.

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

2.1.18 Toekennen functiescheiding tussen systeemgebruikers m.b.t. inschrijftokens

Alias: GBX.FBH.e4020

Details
Eis: Er moet functiescheiding toegepast worden tussen systeemgebruikers die gerechtigd zijn om inschrijftokens op te stellen en gebruikers die het LSP kunnen bevragen. **Toelichting:** Deze eis moet de kans verlagen dat gegevens van een oneigenlijke patient worden bevraagd, doordat medewerkers niet zowel patiënten mogen inschrijven als betrokken zijn bij de medische processen. 1. 1. Met name bij zorgaanbieders van een grotere omvang zal dit goed toe te passen zijn en aansluiten bij de bestaande werkprocessen. De aanpassingen zijn vooral beleidsmatig en procedureel van aard. Het toepassen van deze maatregel is mogelijk al bestaande praktijk of kan anders wellicht met beperkte inspanning worden gerealiseerd. Voor kleine zorgaanbieders is dit mogelijk niet altijd haalbaar. **Condities:** Deze eis zal verplicht zijn voor grote zorgorganisaties. In overleg met VZVZ kan bepaald worden of deze eis verplicht zal zijn.

Vzvz_Moscow: Conditioneel
Vzvz_Req_Verificatie: Audit
Vzvz_Req_Soort: Non-Functional
Vzvz_Req_Type: Product

2.1.19 Voorkomen overmatige bevraging van patiëntgegevens

Alias: GBX.FBH.e4018

Details
Eis: Er mogen geen overmatige bevragingen van patiëntgegevens worden gedaan. In het geval van een bevraging door het systeem dient er een duidelijke trigger voor de bevraging te zijn. Indien een systeemgebruiker zelf een bevraging initiëert is het de verantwoordelijkheid van de systeemgebruiker om te bepalen of het gaat om een overmatige bevraging. **Toelichting:** Een overmatige bevraging van patiëntgegevens is een LSP-bevraging zonder een duidelijke noodzaak voor de betreffende patiënt. Het betreft hier bijvoorbeeld een bevraging zonder een duidelijke trigger, door een systeem, met als doel de lokale database aan te vullen met de meest recente patiëntinformatie (synchronisatie). Een duidelijke trigger kan bijvoorbeeld een afspraak zijn met de patiënt of een signaal als gevolg van een afgesloten abonnement.

Vzvz_Moscow: Verplicht
Vzvz_Req_Verificatie: Monitoring
Vzvz_Req_Soort: Non-Functional
Vzvz_Req_Type: Product

2.1.20 Verantwoordelijk UZI-pasbeleid

Alias: GBX.FBH.e4017

Details
Eis: Een organisatie moet zorgdragen dat er voldoende UZI-passen binnen een organisatie actief zijn. Het aantal benodigde UZI-passen is afhankelijk van de organisatiestructuur en de toepassing waarbinnen een UZI-pas wordt gebruikt. **Toelichting:** Zorgaanbieders waar veel zorgverleners werkzaam zijn mogen niet uit kostenoverwegingen besparen op UZI-passen en daarom bijvoorbeeld de mandatering in de gehele organisatie bij een of enkele specialisten leggen. Er dient goed afgewogen te worden wie verantwoordelijk is voor bepaalde interacties met het LSP. Verantwoordelijkheid wordt onder andere bepaald door de rol van de zorgverlener en het hebben van een (afgeleide) behandelrelatie met een patiënt.

Vzvz_Moscow: Verplicht
Vzvz_Req_Verificatie: Monitoring
Vzvz_Req_Soort: Non-Functional
Vzvz_Req_Type: Product

2.1.21 Instrueren systeemgebruikers over beveiligingsbeleid

Alias: GBX.FBH.e4015

Details
Eis:

Systeemgebruikers binnen een GBZ dienen op de hoogte te zijn van het beveiligingsbeleid en dienen het beveiligingsbeleid na te leven. In het beveiligingsbeleid dient in ieder geval aandacht te zijn voor:

- Het gebruik van de systemen en de toegang daartoe;
- Het gebruik van de UZI-pas (indien door het XIS gebruikt); Hierbij dient in ieder geval de verantwoordelijkheden met betrekking tot het bezit en het gebruik van de UZI-pas benoemd worden.
- Het concept van mandatering (indien door het XIS gebruikt); Hierbij dient in ieder geval aandacht besteed te worden aan de juiste fijnmazigheid waarop gemandateerd mag worden. De verantwoordelijkheid die wordt weergegeven in een mandaattoken moet bij de reële organisatiestructuur en werkwijze horen.

Het concept van inschrijftoken (indien door het XIS gebruikt).
Toelichting:
Een GBZ moet concreet beleid maken om het bewustzijn van het beveiligingsbeleid onder de medewerkers en zorgverleners te bevorderen en iedereen te wijzen op zijn verantwoordelijkheden.

Beleid om bewustzijn onder personeel te bewerkstelligen horen al standaard onderdeel te zijn van beveiligingsmaatregelen binnen een GBZ. Dit is voorgeschreven in NEN 7510, 7.2.2.

Vzvz_Moscow: Verplicht
Vzvz_Req_Verificatie: Monitoring
Vzvz_Req_Soort: Non-Functional
Vzvz_Req_Type: Product

2.1.22 Ondersteuning van gebruikers bij problemen met de landelijke uitwisseling van informatie

Alias: GBX.FBH.e4010

Details
Eis: De GBx-servicedesk dient gebruikers te ondersteunen bij GBx-, GZN- en LSP-gerelateerde problemen. De GBx-servicedesk dient: 1. Gebruikers een inschatting te geven van de verwachte oplostermijn; 2. Gebruikers regelmatig te informeren over de voortgang van de oplossing; 3. Tijdens kantooruren telefonisch bereikbaar te zijn voor gebruikers, GZN-leveranciers en het LSP-beheer; 4. Voor noodgevallen telefonisch bereikbaar te zijn voor gebruikers, de GZN en het LSP; 5. Incidenten en problemen te registreren en beheren; 6. een procedure geïmplementeerd te hebben voor het melden en afhandelen van incidenten en wijzigingsverzoeken conform het Dossier Afspraken en Procedures (AORTA DAP); 7. Nederlandstalig te zijn. **Toelichting bij eis:** Het doel van deze eis is om de landelijke elektronisch uitwisseling van gegevens door gebruikers te bevorderen, de diensten van AORTA te verbeteren en verstoringen te signaleren, voorkomen en verhelpen.

Vzvz_Moscow: Verplicht (Must)
Vzvz_Req_Verificatie: Aansluittoets
Vzvz_Req_Soort: Non-Functional
Vzvz_Req_Type: Product

2.2 AORTA Eisen Infrastructurele Systeemrollen

2.2.1 Abonnementenregister

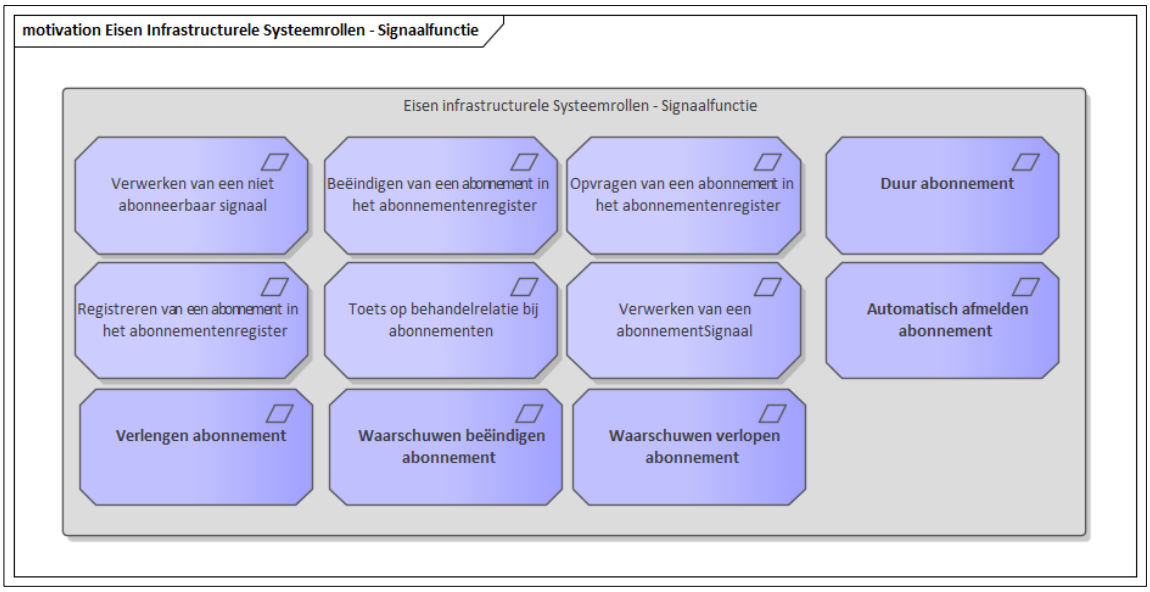


Figure 2 : Eisen Infrastructurele Systeemrollen - Signaalfunctie

2.2.1.1 *Waarschuwen verlopen abonnement*

Alias: GBX.SGL.e4080

Details
Eis: Een abonneehouder moet via een melding op de hoogte worden gebracht als een afgesloten abonnement binnen een tijdsbestek van <GBx_verlopen_abonnement> komt te verlopen. **Toelichting bij eis:** Er moet voorkomen worden dat door een verlopen abonnement het zorgproces in gedrang komt. Het is mogelijk om een abonneehouder de functionaliteit te bieden om een abonnement te verlengen. Met behulp van de conditionele abonnementberichten kan zonder gebruik van een UZI-pas het huidige abonnement verlengd worden. Voor de waarde <GBx_verlopen_abonnement> is geen expliciete waarde benoemd. Het is aan de XIS-leverancier om hier een waarde voor te kiezen dat past binnen het zorgproces van een zorgverlener.

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

2.2.1.2 *Waarschuwen beëindigen abonnement*

Alias: GBX.SGL.e4090

Details
Eis:

Een abonneehouder moet via een melding op de hoogte worden gebracht als een afgesloten abonnement door het systeem is beëindigd. **Toelichting bij eis:** Er moet voorkomen worden dat door het beëindigen van een abonnement het zorgproces in gedrang komt. Het is mogelijk om een abonneehouder de functionaliteit te bieden om een abonnement te verlengen. Met behulp van de conditionele abonnementberichten kan zonder gebruik van een UZI-pas het huidige abonnement verlengd worden. **Condities:** Deze eis is verplicht indien er gebruik wordt gemaakt van de abonnementsfunctionaliteit in de vorm van conditionele abonnementsberichten.

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

2.2.1.3 Verlengen abonnement

Alias: GBX.SGL.e4100

Details
Eis: Een abonnement dient door een abonneehouder of het systeem verlengd te kunnen worden. **Toelichting bij eis:** Om het zorgproces goed te laten werken is het van belang om een abonnement te kunnen verlengen. Verlengen kan gebeuren door een expliciete handeling van de gebruiker of automatisch door het systeem. Hoe de expliciete handeling geïmplementeerd dient te worden is aan de XIS-leverancier. Indien het systeem een abonnement verlengt, dient dit te gebeuren door middel van een conditioneel registratiebericht voor abonnementen. Een vereiste hierbij is dat er een behandelrelatie tussen de abonneehouder en de patiënt is vastgelegd.

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

2.2.1.4 Automatisch afmelden abonnement

Alias: GBX.SGL.e4060

Details
Eis: Een abonnement dient door het systeem afgemeld te worden indien de behandelrelatie met de patiënt of de einddatum van het abonnement is verlopen. **Toelichting bij eis:** Het afmelden van een abonnement door het systeem wordt gedaan door het versturen van een beëindigenAbonnement-bericht (QUQI_IN000003UV) zoals gespecificeerd in art-decor. Het bericht dient verstuurd te worden i.c.m. de benodigde tokens voor conditionele berichten. **Condities:**

Deze eis is verplicht indien er gebruik wordt gemaakt van de abonnementsfunctionaliteit in de vorm van conditionele abonnementsberichten.

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

2.2.1.5 Duur abonnement

Alias: GBX.SGL.e4070.1

Details
Eis: De duur van een abonnement mag maximaal 1,5 jaar bedragen. Een abonnement met een abonnementsduur van langer dan 1,5 jaar dient door het systeem geweigerd te worden. **Toelichting bij eis:** Om te voorkomen dat abonnementen onterecht voor lange duur in het LSP blijven bestaan zonder dat er nog een behandelrelatie is met de patiënt, is het noodzakelijk om een einddatum aan een abonnement te koppelen. Het is mogelijk om een bestaand abonnement te verlengen.

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

2.2.1.6 Verwerken van een abonnementSignaal

Alias: GBX.SGL.e4040.1

Details
Beginsituatie 1. Het systeem beschikt over de voor deze functie vereiste vertrouwensmiddelen, of 2. De patiënt/cliënt is lokaal ingelogd op vertrouwensniveau eIDAS-substantieel of hoger. **Trigger** Het systeem ontvangt een afleverenAbonnementSignaal bericht van de ZIM conform HL7v3 IH Sgl ABR. **Interacties** Het systeem verstuurd een bevestigingsbericht conform HL7v3 IH Sgl ABR. **Resultaat** Het bericht is verwerkt door: • Het signaal te presenteren aan de gebruiker en/of • Bij gebeurtenistype “wijziging gegevens” de gebruiker de mogelijkheid te bieden de gewijzigde gegevens gelijk op te vragen. • het signaal door het systeem te laten afhandelen **Uitzonderingen** Uitzonderingen zijn beschreven in Foutentabel. **Opties** - **Responsetijd** -

Betrouwbaarheid
Het abonnementSignaal wordt door de ZIM zim-signaal-aanbieden-STU keer aan de component STU aangeboden met zim-signaal-tijdsbestek tijd tussen het aanbieden.
Toelichting
Het bericht wordt verstuurd naar de applicatie. De organisatie moet zelf bepalen welke zorgverleners/medewerkers het signaal te zien krijgen. De zorgverlener die het abonnement geregistreerd heeft, wordt meegestuurd in het bericht. De gebeurtenis die heeft plaatsgevonden waar een abonnement op genomen is, wordt ook meegeleverd in het bericht.

Indien het bericht wordt verstuurd naar het portaal, dan moet het portaal het signaal na 5 minunten aan de patiënt versturen.

Het is mogelijk dat een portaal binnen de te versturen tijd meerdere signalen ontvangt van de ZIM. Een notificatie aan de patiënt dient voor de patiënt als trigger om zijn/haar loggegevens op te vragen. Het is dus voldoende om één notificatie te sturen naar een patiënt ondanks dat er mogelijk meer signalen zijn ontvangen door het portaal.

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

2.2.1.7 Toets op behandelrelatie bij abonnementen

Alias: GBX.SGL.e4035.2

Details
Eis: Een abonnement dient beëindigd te worden indien uit de inschrijving van de patiënt blijkt dat: • langer dan gbx-max-behandelrelatie-termijn geleden een behandelrelatie is vastgelegd volgens Bijhouden behandelrelatie en • er geen behandelrelatie meer blijkt uit de werkcontext en • de zorgverlener niet alsnog een behandelrelatie vastlegt volgens Bijhouden behandelrelatie. **Toelichting bij eis:** Bij het afsluiten en aanhouden van een abonnement gelden dezelfde autorisatie-eisen als in het geval van een bevraging. Dit betekent dus ook dat er een behandelrelatie met de patiënt dient te zijn op het moment van afsluiten van het abonnement en tijdens de looptijd van het abonnement.

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

2.2.1.8 Registreren van een abonnement in het abonnementenregister

Alias: GBX.SGL.e4010.1

Details
Beginsituatie 1. De gebruiker is lokaal ingelogd op vertrouwensniveau midden of hoger, of 2. De patiënt/cliënt is lokaal ingelogd op vertrouwensniveau eIDAS-substantieel of hoger.

3. De toekomstig abonneehouder heeft een behandelrelatie met de patiënt waar een abonnement voor afgesloten wordt.

Trigger

1. De gebruiker initieert de functie via het systeem;
2. Een systeemtrigger initieert de functie.

Interacties

1. Het systeem verzendt een registratieAbonnement bericht naar de ZIM conform HL7 IH Sgl ABR.
2. Het systeem ontvangt een antwoordRegistratieAbonnement conform HL7v3 IH Sgl ABR.

Resultaat

Het antwoordbericht is ontvangen en het resultaat van de interactie is kenbaar gemaakt aan de gebruiker

Uitzonderingen

Uitzonderingen zijn beschreven in Foutentabel en tabel LSP.ABR.t2065 in het Ontwerp Abonnementenregister.

Opties

Wanneer de gebruiker een GBZ-beheerder is dient er gebruik te worden gemaakt van fictieve BSN's.

Responsetijd

-

Betrouwbaarheid

Garantie geven dat gegevens in zendende en ontvangende systeem overeenstemmen

Toelichting

Er mag alleen door een zorgverlener een abonnement geregistreerd worden op wijziging van een gegevenssoort dat ingezien mag worden volgens het autorisatieprotocol. De abonneerbare gegevenssoorten zijn te vinden in paragraaf 4.1.1 van Ontwerp Abonnementenregister, evenals de logische attributen van het bericht. Een abonnement mag niet langer duren dan .

Het is mogelijk om gebruik te maken van conditionele abonnementsberichten. Hierbij dient er een mandaattoken van de verantwoordelijke zorgverlener meegestuurd te worden.

De abonneerbare abonnement-gebeurtenistypes zijn te vinden in paragraaf 4.1.1 van Ontwerp Abonnementenregister evenals de logische attributen van het bericht.
Het LSP patiëntenportaal moet de volgende abonnementen ondersteunen:

- Opgevraagde patiëntgegevens (gebeurtenistype LQD);
- Direct verstuurde patiëntgegevens (gebeurtenistype LSD);
- Wijzigingen in de VWI (gebeurtenistype WI);
- Afgenomen abonnement (gebeurtenistype WA).

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

2.2.1.9 Opvragen van een abonnement in het abonnementenregister

Alias: GBX.SGL.e4030

Details
Beginsituatie 1. De gebruiker is lokaal ingelogd op vertrouwensniveau midden of hoger, of 2. De patiënt/cliënt is lokaal ingelogd op vertrouwensniveau eIDAS-substantieel of hoger. **Trigger** De gebruiker initieert de functie via het systeem **Interacties** 1. Het systeem verzendt een opvragingAbonnement bericht naar de ZIM conform AORTA_Sgl_IH_Abonnementenregister_HL7.

2. Het systeem ontvangt een opleveringAbonnement bericht conform AORTA_Sgl_IH_Abonnementenregister_HL7.

Resultaat
De opgeleverde gegevens zijn door het systeem:
- Gepresenteerd aan de gebruiker of
- Gebruikt voor beëindiging van het abonnement

Uitzonderingen
Uitzonderingen zijn beschreven in [Foutentabel].
Opties
Wanneer de gebruiker een GBZ-beheerder is dient er gebruik te worden gemaakt van fictieve BSN's.
Het moet mogelijk zijn om de zender-organisatie-id te gebruiken als query-parameter (gelijk aan abonnement-organisatie-id) en daarnaast ten minste een van de volgende query parameters mee te geven:
- abonnement-id
- abonnement-applicatie-id
- abonnement-zorgverlener-id
- abonnement-gebeurtenis-type
- abonnement-gebeurtenis-object
- abonnement-gebeurtenis-subject

De definities van de parameters staan beschreven in Paragraaf 4.1.3 van Ontwerp Abonnementenregister.
Responsetijd
-
Betrouwbaarheid
-
Toelichting
Iedere zorgverlener van de organisatie die abonnementeigenaar is mag het abonnement opvragen. De oplevering van het aantal antwoorden wordt door de ZIM begrensd. Maximaal worden opgeleverd.

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

2.2.1.10 Beëindigen van een abonnement in het abonnementenregister

Alias: GBX.SGL.e4020.1

Details
Beginsituatie 1. De gebruiker is lokaal ingelogd op vertrouwensniveau midden of hoger, of 2. De patiënt/cliënt is lokaal ingelogd op vertrouwensniveau eIDAS-substantieel of hoger. **Trigger** De gebruiker initieert de functie via het systeem **Interacties** 1. Het systeem verzendt een opzeggingAbonnement bericht naar de ZIM conform AORTA_Sgl_IH_Abonnementenregister_HL7 2. Het systeem ontvangt een antwoordOpzeggingAbonnement conform AORTA_Sgl_IH_Abonnementenregister_HL7 **Resultaat** Het antwoordbericht is ontvangen en het resultaat van de interactie is kenbaar gemaakt aan de gebruiker **Uitzonderingen** Uitzonderingen zijn beschreven in [Foutentabel]. **Opties** Wanneer de gebruiker een GBZ-beheerder is dient er gebruik te worden gemaakt van fictieve BSN's. **Responsetijd** - **Betrouwbaarheid**

Garantie geven dat gegevens in zendende en ontvangende systeem overeenstemmen **Toelichting** Iedere zorgverlener die werkt onder de abonnee (organisatie) , mag het abonnement beëindigen. Het abonnement-id is noodzakelijk om een abonnement te beëindigen. Deze is te verkrijgen door middel van het opvragen van het abonnement. De logische attributen zijn te vinden in paragraaf 4.1.2 van Ontwerp Abonnementenregister. De XIS is verantwoordelijk voor het bijhouden van de einddatum van het abonnement. Zodra een abonnement niet meer actief is, dient de abonnementaanvrager hiervan op de hoogte te worden gebracht. Het is ook mogelijk om Verwerken van een niet abonneerbaar signaal te implementeren. ---------- Een patiënt/cliënt kan alleen zijn eigen abonnementen verwijderen. Hiervoor dient de patiënt/cliënt ingelogd te zijn op het portaal vanwaar hij het abonnement genomen heeft. Het abonnement-id is noodzakelijk om een abonnement te beëindigen. Deze is te verkrijgen door middel van het opvragen van het abonnement. Abonnementen van een patiënt dienen te worden verwijderd, zodra een patiënt zich uitschrijft bij een portaal.

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

2.2.1.11 Verwerken van een niet abonneerbaar signaal

Alias: GBX.SGL.e4050.1

Details
Beginsituatie Het systeem beschikt over de voor deze functie vereiste vertrouwensmiddelen. **Trigger** Het systeem ontvangt een afleverenNietabonneerbaarsignaal-bericht van de ZIM conform HL7v3 IH Sgl ABR. **Interacties** Het systeem verstuurd een bevestigingsbericht conform HL7v3 IH Sgl ABR. **Resultaat** Het bericht is verwerkt door: • Het signaal te presenteren aan de gebruiker en/of • Bij gebeurtenistype “abonnement verwijderd” de gebruiker de mogelijkheid te bieden het abonnement gelijk opnieuw af te sluiten. **Uitzonderingen** Uitzonderingen zijn beschreven in Foutentabel. **Opties** - **Responsetijd** - **Betrouwbaarheid** Het niet abonneerbaar signaal wordt door de ZIM keer aan de component STU aangeboden met tijd tussen het aanbieden. **Toelichting** Het bericht wordt verstuurd naar de applicatie. De organisatie moet zelf bepalen welke zorgverleners/medewerkers het signaal te zien krijgen. De logische attributen van dit bericht zijn te vinden in paragraaf 4.1.2. van Ontwerp gebeurtenisverwerking.

Van de volgende gebeurtenis wordt een niet abonneerbaar signaalverstuurd: • Gebeurtenis 'abonnement verwijderd' Een abonnement kan verwijderd worden door bezwaar van een patiënt of omdat het abonnement verlopen is.

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

2.2.2 Inschrijftoken beherend systeem

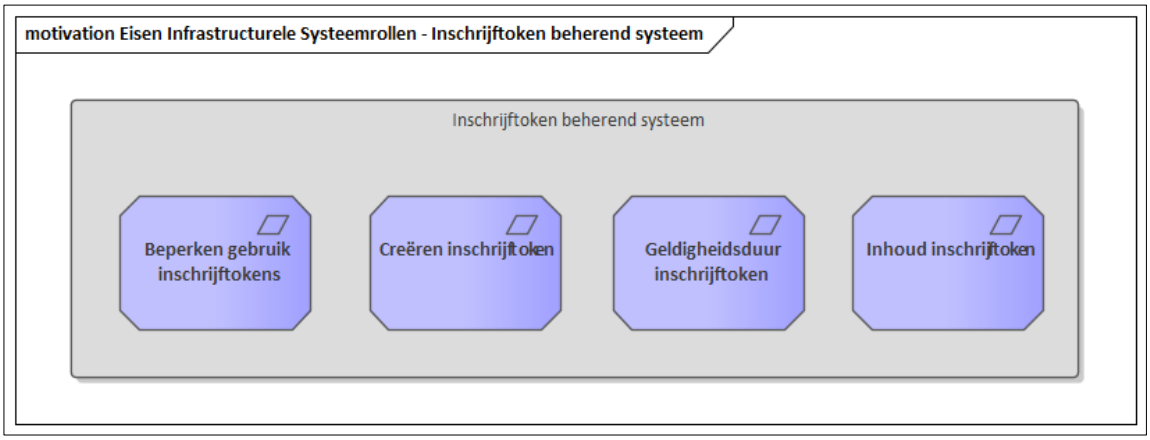


Figure 3 : Eisen Infrastructurele Systeemrollen - Inschrijftoken beherend systeem

2.2.2.1 Inhoud inschrijftoken

Alias: GBX.OPV.e4060.2

Details
Eis: In een inschrijftoken moeten de volgende gegevens opgenomen worden: 1. BSN van de specifieke patiënt; 2. UZI-nummer van de persoon die het inschrijftoken heeft aangemaakt; het UZI-nummer kan worden afgeleid uit het certificaat waarmee het token is ondertekend; 3. het abonneenummer (URA) van de zorgaanbieder waarbinnen het inschrijftoken geldig moet zijn; 4. Datum en tijdstip waarop inschrijftoken is aangemaakt; 5. Datum en tijdstip van registreren BSN; t.b.v. het werkproces mag dit ook het tijdstip van aanmaken van het inschrijftoken zijn; 6. Geldigheidsduur. **Toelichting:** De technische specificaties van het inschrijftoken zijn uitgewerkt in de [IH Inschrijftoken].

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

2.2.2.2 Geldigheidsduur inschrijftoken

Alias: GBX.OPV.e4100.1

Details
Eis: Een inschrijftoken heeft een maximale geldigheidsduur van 1,5 jaar. **Toelichting:** Een inschrijftoken kent een beperkte geldigheidsduur. Het is echter mogelijk om dezelfde informatie in het inschrijfttoken opnieuw te onderteken (zie eis GBX.OPV.e4050). De geldigheid van het UZI-certificaat waarmee het inschrijftoken is ondertekend heeft geen invloed op de geldigheid van het inschrijftoken. Een inschrijftoken heeft een maximale geldigheidsduur van 1,5 jaar.

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

2.2.2.3 Creëren inschrijftoken

Alias: GBX.OPV.e4050

Details
Eis: Alleen daarvoor geautoriseerde rol(len)/perso(o)n(en) moet(en) een inschrijftoken (conform eis GBX.OPV.e4060) kunnen creëeren en voor gebruik kunnen ondertekenen met het authenticatiecertificaat van de UZI-pas. Het authenticatiecertificaat waarmee het inschrijftoken wordt ondertekend moet geldig zijn op het moment van tekenen. **Toelichting:** Het inschrijftoken moet waarborgen dat een patiënt in behandeling is bij een zorgorganisatie en dat de bsn van een patiënt is gevalideerd bij het SBV-Z. Om het proces m.b.t. het aanmaken van inschrijftokens te controleren is het zaak om alleen geautoriseerde rollen en/of personen te autoriseren om een inschrijftoken aan te maken. Dit kunnen zorgverleners, zorgverlenerassistenten en/of baliemedewerkers zijn.

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

2.2.2.4 Beperken gebruik inschrijftokens

Alias: GBX.OPV.e4120

Details
Eis: Inschrijftokens mogen binnen de AORTA-omgeving alleen meegestuurd worden met die interacties zoals beschreven in de AORTA-documentatie. **Toelichting:**

Het LSP is niet voorbereid op het verwerken van een inschrijftoken indien dit niet expliciet is opgenomen in de AORTA-documentatie. Het LSP zal bij een onterecht meegestuurd inschrijftoken een foutmelding (XXXX) genereren.

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

2.2.3 Mandaatregistratie

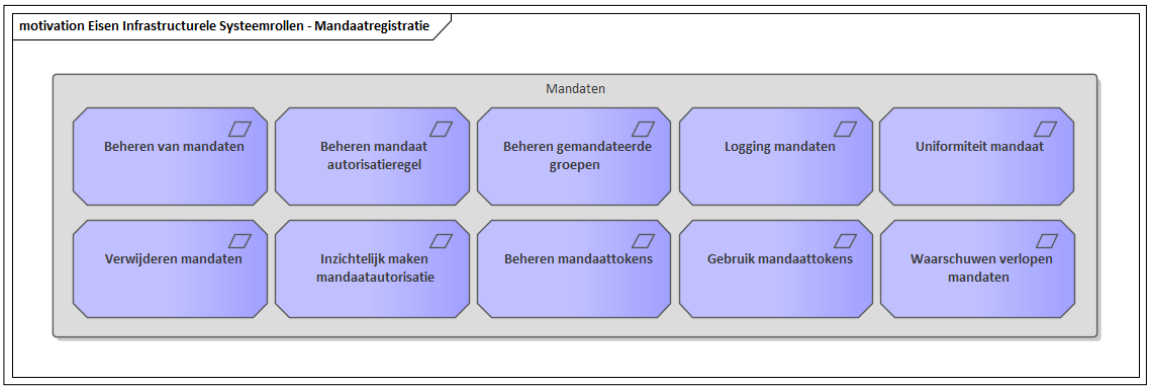


Figure 4 : Eisen Infrastructurele Systeemrollen - Mandaatregistratie

2.2.3.1 Uniformiteit mandaat

Alias: GBX.AUT.e4515

Details
Eis: Een mandaat dient te worden opgeslagen in de vorm van een mandaattoken zoals gespecificeerd in de https://public.vzvz.nl/display/A8/GBZ+AORTA_Auth_IH_Mandaattoken . **Toelichting bij eis:** Berichten die onder mandaat naar het LSP worden verstuurd, dienen te worden voorzien van een mandaattoken (zoals gespecifieerd in https://public.vzvz.nl/display/A8/GBZ+AORTA_Auth_IH_Mandaattoken). Het LSP krijgt dan altijd op een uniforme wijze het mandaat aangeleverd en kan deze vervolgens ook controleren.

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

2.2.3.2 Waarschuwen verlopen mandaten

Alias: GBX.AUT.e4522.1

Details

Eis:
Een mandaterende en de in de autorisatieregel opgenomen gemandateerde zorgverlener(s) moeten via een melding op de hoogte worden gebracht als respectievelijk zijn gegeven mandaat of zijn verkregen mandaat binnen een tijdsbestek van 1 maand komt te verlopen.

Toelichting bij eis:
Er moet voorkomen worden dat door een verlopen mandaat het zorgproces in gedrang komt.

Het kan voor komen dat een mandaterende niet in hetzelfde systeem werkt als een gemandateerde. Het is daarom van belang dat een gemandateerde ook op de hoogte wordt gesteld indien het mandaattoken bijna verlopen is.

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

2.2.3.3 Verwijderen mandaten

Alias: GBX.AUT.e4521.1

Details
Eis: Verlopen mandaten moeten in de volgende gevallen uit het systeem worden verwijderd: 1. De einddatum van het mandaat is verstreken; 2. De mandaterende zorgverlener is niet meer werkzaam bij de zorgaanbieder; 3. De mandaterende zorgverlener is niet meer werkzaam bij de zorgaanbieder in de rol zoals opgenomen is in het mandaat. **Toelichting bij eis:** Er moet voorkomen worden dat verlopen mandaten in het systeem achterblijven en mogelijk onterecht gebruikt worden. Indien een certificaat op de CRL is geplaatst, dan zal het mandaattoken vervangen moeten worden door een mandaattoken dat getekend is met een geldig certificaat. Afhankelijk van de reden waarom een certificaat op de CRL is geplaatst zal het mandaattoken meteen moeten worden verwijderd. In het geval de registratie is ingetrokken van een zorgverlener, dan zal deze ook niet meer werkzaam mogen zijn bij de zorgaanbieder onder de betreffende rol en zal het mandaattoken dus volgens de eis verwijderd moeten worden. Echter, als een zorgverlener zijn pas is kwijtgeraakt, dan zal niet direct het mandaattoken ingetrokken hoeven te worden. Het is mogelijk om het mandaattoken te laten bestaan, totdat de zorgverlener een nieuwe pas heeft ontvangen.

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

2.2.3.4 Logging mandaten

Alias: GBX.AUT.e4516

Details

Eis:
Met betrekking tot het mandaattoken dienen drie zaken gelogd te worden:

1. Mandaattoken; bij het aanmaken van een mandaattoken dienen de gegevens gelogd te worden zoals opgenomen in GBX.AUT.e4511.
2. Autorisatieregel; bij het aanmaken van een autorisatieregel dienen de gegevens gelogd te worden zoals opgenomen in GBX.AUT.e4514.
3. Groepen; bij elke wijziging aan een groep, dienen de gegevens gelogd te worden zoals opgenomen in GBX.AUT.e4515. In het geval een autorisatieregel geen gebruik maakt van groepen, dan hoeft deze uiteraard ook niet gelogd te worden.

In opdracht van VZVZ, van een toezichthouder of van een andere geautoriseerde belanghebbende moeten bovenstaande loggevens te allen tijden inzichtelijk gemaakt kunnen worden.

Toelichting bij eis:
Ten behoeve van een audit trail moet precies kunnen worden nagegaan of een mandaattoken terecht gebruikt is.
Het is mogelijk om de te loggen gegevens genoemd onder de punten a t/m c in één gecombineerde log op te nemen. Hierbij moet dan wel na elke aanpassing van een van de drie genoemde zaken opnieuw gelogd worden.

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

2.2.3.5 Gebruik mandaattokens

Alias: GBX.AUT.e4520

Details
Eis: Er moet voorkomen worden dat mandaattokens onderschept kunnen worden via onbeveiligde verbindingen binnen de interne GBx-infrastructuur. Hiervoor dient het token geëncrypt te worden met behulp van het publieke certificaat van de ZIM (https://public.vzvz.nl/display/A8/GBZ+AORTA_Auth_IH_Mandaattoken). **Toelichting bij eis:** Er moet voorkomen worden dat mandaattokens onderschept, gelezen en vervolgens misbruikt worden. Door middel van het encrypten van het token wordt het onmogelijk om misbruik te maken van het mandaat. Het geëncrypte token moet als zodanig tesamen met het bericht naar het LSP worden verzonden.

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

2.2.3.6 Beheren mandaattokens

Alias: GBX.AUT.e4519

Details
Eis: Mandaattokens dienen in een beveiligde container te worden opgeslagen. Een gebruiker krijgt door middel van een beveiligde verbinding alleen gebruik over die mandaattokens waarvoor het is geautoriseerd.

Toelichting bij eis: Er moet voorkomen worden dat mandaattokens onderschept, gelezen en vervolgens misbruikt worden. Door middel van implementatie van een beveiligde container krijgen medewerkers alleen gebruik over die mandaattokens waarvoor ze zijn geautoriseerd. De beveiligde container moet het onmogelijk maken om een mandaattoken te stelen.

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

2.2.3.7 Inzichtelijk maken mandaatautorisatie

Alias: GBX.AUT.e4517

Details
Eis: Het moet mogelijk zijn om een overzicht te genereren van de inhoud van een mandaat op een gegeven moment in de tijd. Hierbij moet in één overzicht inzichtelijk kunnen worden gemaakt welke zorgverleners er geautoriseerd waren om een specifiek mandaattoken te gebruiken. **Toelichting bij eis:** In opdracht van VZVZ, van een toezichthouder of van een andere geautoriseerde belanghebbende moet te allen tijden inzichtelijk gemaakt kunnen worden of een bepaalde zorgverlener gerechtigd was om gebruik te maken van een bepaald mandaattoken.

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

2.2.3.8 Beheren gemandateerde groepen

Alias: GBX.AUT.e4514

Details
Eis: In een autorisatieregel kunnen één of meerdere groepen van gemandateerden worden opgenomen. Een groep bestaat in ieder geval uit de volgende elementen: 1. Unieke identifier; dit kan een nummer of een groepsnaam zijn. 2. Lijst met gemandateerden; een lijst kan bestaan uit bijvoorbeeld UZI-nummer(s) of rollen/functies. Alleen op vertrouwensniveau midden is het mogelijk om de lijst met gemandateerden dynamisch uit te breiden. De identifier hoeft niet aangepast te worden bij uitbreiding van de lijst met gemandateerden. **Toelichting bij eis:** Door het gebruik van groepen in een autorisatieregel is het mogelijk om dynamisch rolcode's of UZI-nummers toe te voegen aan de lijst met gemandateerden. Mocht er gebruik worden gemaakt van een andere waarde dan UZI-nummer of rolcode, dan dient vanuit de logging ontegenzeggelijk te worden aangetoond welke UZI of rolcode er aan de waarde gekoppeld is.

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

2.2.3.9 Beheren mandaat autorisatieregel

Alias: GBX.AUT.e4513.1

Details
Eis: Een mandaat kan alleen afgegeven worden op basis van een autorisatieregel. Een autorisatieregel bepaalt of een bepaalde zorgverlener gebruik mag maken van een specifiek mandaat. De precieze invulling van een autorisatieregel is niet gespecificeerd. Dit is ter invulling van de zorginstelling. Een autorisatieregel moet in ieder geval wel de volgende attributen bevatten: 1. Lijst met werkcontext(en); De werkcontext(en) bepaalt de context(en) waarbinnen een mandaat geldig is. Dit kan bijvoorbeeld gekoppeld zijn aan een afdeling of een werkproces. 2. Lijst met gemandateerden; Dit kunnen UZI-nummer(s), lokale zorgverleneridentificaties of (lokaal gedefinieerde) rollen zijn. Er kan ook een groep(en) (GBX.AUT.e4514) worden opgenomen waar rolcodes of UZI-nummers aan gekoppeld zijn. Door het gebruik van groep(en) is het mogelijk om dynamisch rolcodes of UZI-nummers toe te voegen aan de lijst van gemandateerden. 3. Uniek identificatiekenmerk; Een autorisatieregel moet uniek gekenmerkt worden. Een uniek gekenmerkte autorisatieregel behorende bij een afgegeven mandaat mag niet veranderlijk zijn. **Toelichting bij eis:** Lokaal moet duidelijk en uniek geregistreerd zijn hoe er invulling is gegeven aan een autorisatieregel. Op verzoek (van bijvoorbeeld een toezichthouder) moet kunnen worden aangetoond dat een gemandateerde ten tijde van het versturen van een bericht onder mandaat, inderdaad gerechtigd was om gebruik te maken van het mandaattoken (GBX.AUT.e4517). Om een flexibel mandaat in te richten is het aan te raden om gebruik te maken van dynamische groepen in de autorisatieregel. Een groep wordt aangeduid door middel van een groepsnaam. De UZI-nummers die direct of indirect (door middel van de rolcode) gekoppeld worden aan een groepsnaam moeten op een veilige manier worden beheerd (eis GBX.AUT.e4514). Indien een lokale gebruikersidentificatie wordt gebruikt, dan kan het LSP alleen bevraagd worden via de conditionele query. Dit zal dan in een zorgtoepassing specifiek worden vereist. Een autorisatieregel mag niet aangepast worden. De attributen die zijn opgenomen in verwijzingen (zoals bijvoorbeeld bij de onder b. genoemde groepen) mogen wel worden aangepast. Autorisatieregels en de invulling met betrekking tot de werkcontext en de lijst met gemandateerden dienen in een beveiligde container te worden opgeslagen. Deze mogen alleen door een geautoriseerde medewerker worden ingezien en aangepast.

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

2.2.3.10 Beheren van mandaten

Alias: GBX.AUT.e4511

Details

Eis:
Een zorgverlener moet, wanneer hij lokaal is ingelogd op vertrouwensniveau midden, mandaten kunnen vastleggen, inzien en intrekken.
Gebruikers mogen uitsluitend mandaten vastleggen waarvoor zij mandaterende zijn.
Voor een mandaat worden tenminste de volgende gegevens vastgelegd:

1. de ingangsdatum van het mandaat;
2. de einddatum van het mandaat;
3. het UZI-nummer van de mandaterende zorgverlener;
4. de rolcode van de mandaterende zorgverlener;
5. het abonneenummer (URA) van de zorgaanbieder waarbinnen het mandaat geldig moet zijn;
6. de autorisatieregel (zie eis GBX.AUT.e4513) op basis waarvan een mandaat verkregen kan worden;
7. een unieke identifier.

Toelichting bij eis:
Met betrekking tot deze eis worden de volgende subeisen gedefinieerd:

- Het wijzigen van een mandaat is niet toegestaan. Het systeem dient in dat geval een nieuw mandaat aan te maken. Hierbij dient dus een nieuwe unieke identifier te worden opgenomen.
- De einddatum van het mandaat mag door een mandaatverlener leeg gelaten worden. In dat geval moet het systeem de vervaldatum van het handtekeningcertificaat opnemen als einddatum.
- De mandaatverlener mag geen einddatum invullen die na de geldigheidstermijn van zijn handtekeningcertificaat ligt. Het systeem dient dan een duidelijk foutmelding te genereren voor de gebruiker.
- De ingangsdatum van het mandaat mag in de toekomst liggen.
- Er kan alleen een mandaat worden afgesloten voor de eigen organisatie.
- Er dient een verwijzing naar een autorisatieregel te zijn opgenomen. Dit kan bijvoorbeeld door middel van een URI, die verwijst naar de daadwerkelijke inhoud van een autorisatieregel.
- Een autorisatieregel is niet uniek gekoppeld aan een mandaat. Het is dus mogelijk om naar dezelfde autorisatieregel te verwijzen in meerdere mandaten.

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

2.2.4 Mandaattoken beherend systeem

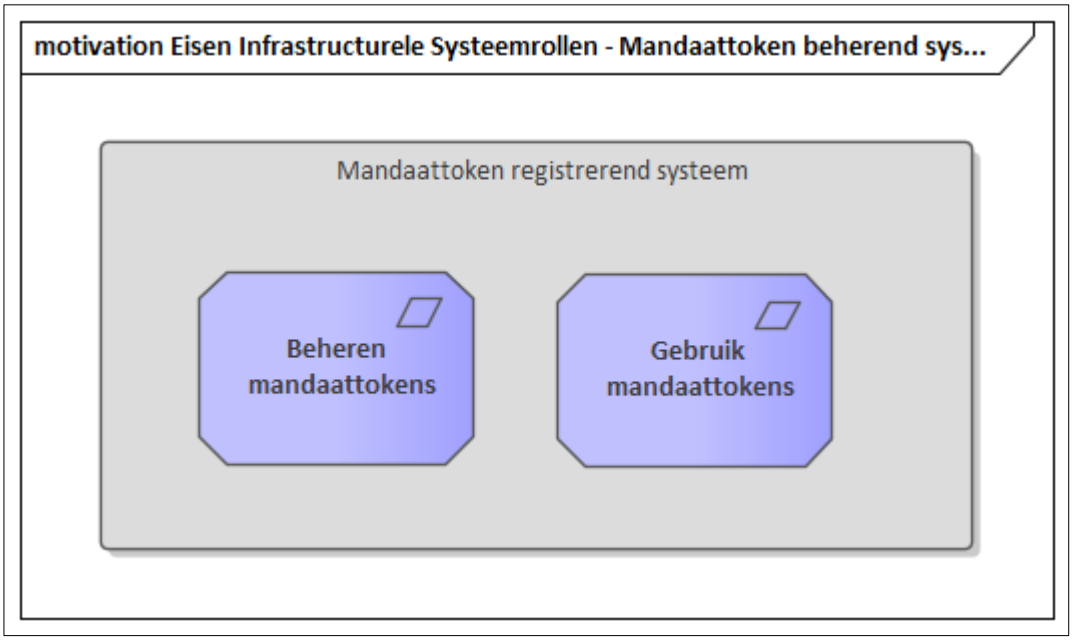


Figure 5 : Eisen Infrastructurele Systeemrollen - Mandaattoken beherend systeem

2.2.4.1 Gebruik mandaattokens

Alias: GBX.AUT.e4520

Details
Eis: Er moet voorkomen worden dat mandaattokens onderschept kunnen worden via onbeveiligde verbindingen binnen de interne GBx-infrastructuur. Hiervoor dient het token geëncrypt te worden met behulp van het publieke certificaat van de ZIM (https://public.vzvz.nl/display/A8/GBZ+AORTA_Auth_IH_Mandaattoken). **Toelichting bij eis:** Er moet voorkomen worden dat mandaattokens onderschept, gelezen en vervolgens misbruikt worden. Door middel van het encrypten van het token wordt het onmogelijk om misbruik te maken van het mandaat. Het geëncrypte token moet als zodanig tesamen met het bericht naar het LSP worden verzonden.

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

2.2.4.2 Beheren mandaattokens

Alias: GBX.AUT.e4519

Details
Eis: Mandaattokens dienen in een beveiligde container te worden opgeslagen. Een gebruiker krijgt door middel van een beveiligde verbinding alleen gebruik over die mandaattokens waarvoor het is geautoriseerd.

Toelichting bij eis: Er moet voorkomen worden dat mandaattokens onderschept, gelezen en vervolgens misbruikt worden. Door middel van implementatie van een beveiligde container krijgen medewerkers alleen gebruik over die mandaattokens waarvoor ze zijn geautoriseerd. De beveiligde container moet het onmogelijk maken om een mandaattoken te stelen.

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

2.2.5 Primaire interactie - opvragend systeem

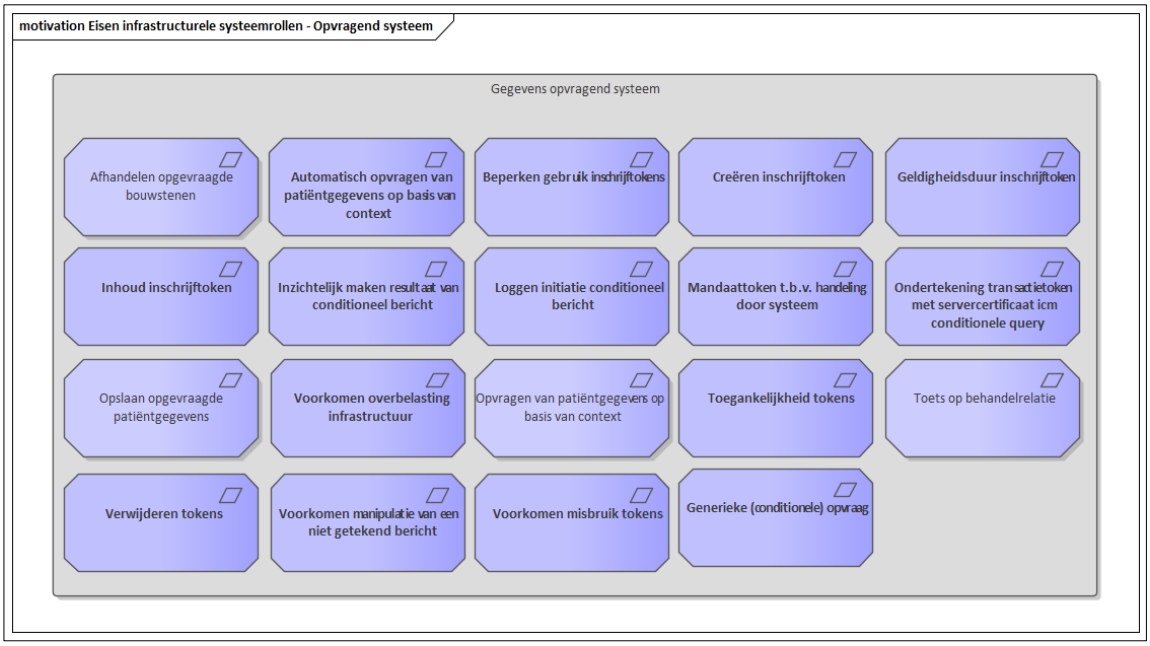


Figure 6 : Eisen infrastructurele systeemrollen - Opvragend systeem

2.2.5.1 *Voorkomen overbelasting infrastructuur*

Alias: GBX.OPV.e4130.1

Details
Eis: In het geval een conditioneel bericht wordt beantwoord met een foutmelding, dan heeft het systeem drie pogingen om het conditionele bericht nogmaals te versturen. Na drie pogingen mag het systeem het bericht niet nogmaals uitsturen en dient de GBZ-beheerder actie te ondernemen zoals is beschreven in de AORTA DAP. **Toelichting bij eis:** Er moet voorkomen worden dat de infrastructuur overbelast wordt door een conditioneel bericht. In het geval er een foutmelding optreedt, moet het niet mogelijk zijn dat het conditionele bericht onbeperkt vaak

wordt uitgestuurd totdat er een antwoord (geen foutmelding) terugkomt. De GBZ-beheerder wordt geacht om te onderzoeken wat de foutmelding is en hoe die volgens de AORTA DAP behandeld dient te worden.

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

2.2.5.2 Voorkomen misbruik tokens

Alias: GBX.OPV.e4170

Details
Eis: Inschrijf- en mandaattokens mogen alleen verstuurd worden over beveiligde verbindingen. **Toelichting:** Om te voorkomen dat (bepaalde) tokens worden afgevangen en misbruikt door een kwaadwillende moeten (bepaalde) tokens verstuurd worden over beveiligde verbindingen. Afhankelijk van de opslag- of creatielocatie van de tokens, kan dit impliceren dat een GBX ook intern gebruik dient te maken van beveiligde verbindingen.

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

2.2.5.3 Voorkomen manipulatie van een niet getekend bericht

Alias: GBX.OPV.e4180

Details
Eis: Berichten zonder een bijgaand transactietoken mogen binnen de interne GBZ-infrastructuur alleen verstuurd worden over beveiligde verbindingen. **Toelichting:** Om te voorkomen dat niet getekende berichten worden afgevangen en misbruikt door een kwaadwillende, moeten deze berichten verstuurd worden over beveiligde verbindingen. Hiermee kan gegarandeerd worden dat berichten tijdens de verzending niet worden aangepast.

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

2.2.5.4 Verwijderen tokens

Alias: GBX.OPV.e4110

Details
Eis: Indien de geldigheidsduur van een token is verlopen, dan dient deze automatisch te worden verwijderd.

Daarnaast moet het voor een gebruiker, die ingelogd is op vertrouwensniveau midden, mogelijk zijn om een token uit het systeem te verwijderen. **Toelichting:** Het verwijderen (en daarmee afwezig zijn) van een token leidt ertoe dat er geen automatische opvraag meer verstuurd mag worden t.b.v. het opvragen van patiëntgegevens van de in het token opgenomen patiëntID. Dit kan gevolgen hebben voor het werkproces van de gebruiker van het systeem. Het is dan ook aan te raden om de gebruiker(s) van het systeem (tijdig) op de hoogte te stellen van het verwijderen van een token. Hoe hier invulling aan te geven is aan de systeembouwer. Het gaat hierbij bijvoorbeeld om inschrijf- en consenttokens.

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

2.2.5.5 Toets op behandelrelatie

Alias: GBX.OPV.e4020.1

Details
Eis: Bij het opvragen van inhoudelijke patiëntgegevens verschaft het systeem de gebruiker slechts toegang indien de patiënt is ingeschreven volgens Verificatie van BSN in patiëntgegevens en 1. korter dan gbx-max-behandelrelatie-termijn geleden een behandelrelatie is vastgelegd volgens Bijhouden behandelrelatie of 2. een behandelrelatie blijkt uit de werkcontext of 3. de zorgverlener alsnog een behandelrelatie vastlegt volgens Bijhouden behandelrelatie.

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

2.2.5.6 Toegankelijkheid tokens

Alias: GBX.OPV.e4160.1

Details
Eis: Om misbruik van tokens door een kwaadwillende te bemoeilijken, moeten de tokens in een beveiligde omgeving worden opgeslagen. Toegang tot de tokens moet alleen mogelijk zijn voor geautoriseerde gebruikers. **Toelichting:** Er worden geen specifieke eisen gesteld aan de rollen die geautoriseerd zijn en aan de wijze van opslag van de tokens. Dit is afhankelijk van de lokale systeemimplementatie. De systeembouwer is verantwoordelijk voor een goede invulling van deze eis. Het gaat hierbij alleen om die tokens, die meerdere malen gebruikt kunnen worden, zoals inschrijf- en consenttokens.

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

2.2.5.7 *Opvragen van patiëntgegevens op basis van context*

Alias: GBX.OPV.e4015

Details
Beginsituatie 1. De gebruiker is lokaal ingelogd op vertrouwensniveau midden of hoger, en 2. er is voldaan aan eis Toets op behandelrelatie. **Trigger** De gebruiker initieert de functie via het systeem **Interacties** 1. Het systeem verzendt een opvragenPatiëntgegevensContext-bericht naar de ZIM. 2. Het systeem ontvangt een opleverenBouwsteeninstantiaties-bericht. **Resultaat** De opgeleverde gegevens zijn door het systeem: 1. gepresenteerd aan de gebruiker, of 2. verwerkt tot een beslissing die is gepresenteerd aan de gebruiker. **Uitzonderingen** Uitzonderingen zijn beschreven in de Foutentabel **Opties** Het opvragenPatiëntgegevensContext-bericht is een generiek opvraagbericht dat qua formaat voor elke zorgtoepassing gelijk is. In het bericht wordt een context meegegeven. De context in combinatie met de rolcode van de opvrager bepaalt uiteindelijk wat er daadwerkelijk opgeleverd gaat worden. Naast context kan de actualiteit en de gewenste responstijd uiterste-oplevertijd-gbz ingesteld worden. Het systeem moet altijd ten minste antwoorden in de eerst lagere bouwsteeninstantiatie-versie, t.o.v. de nieuwste versie, kunnen verwerken. **Responsetijd** GBZ-oplever-time-out is het tijdsinterval waarna een opvragend systeem geen oplevering meer van de ZIM hoeft te verwachten. **Toelichting** Op basis van de meegegeven context en rolcode in het opvragenPatiëntgegevensContext-bericht wordt door de ZIM bepaald welke bouwsteentypen opgevraagd moeten worden bij welke bronsystemen. De ZIM zal een gebundeld antwoord, opleverenBouwsteeninstantiaties-bericht, retourneren met daarin alle van de bronsysteem verkregen bouwsteeninstantiaties. Dit is een compleet ander concept dan het opvragen van patiëntgegevens zoals beschreven in eis Opvragen van patiëntgegevens,

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

2.2.5.8 *Opslaan opgevraagde patiëntgegevens*

Alias: GBX.OPV.e4030

Details
Eis: Wanneer patiëntgegevens, die conform Opvragen van patiëntgegevens zijn ontvangen, ongewijzigd in de eigen patiëntadministratie worden opgenomen dan moet worden vastgelegd dat het een kopie betreft. Hierbij moet de originele OID bij de gegevens opgeslagen worden.

Toelichting bij eis:
Gewoonlijk zullen patiëntgegevens die via het LSP worden opgevraagd niet in de eigen patiëntadministratie worden opgenomen. Het kan echter gewenst zijn om ontvangen patiëntgegevens als onderbouwing bij besluitvorming te bewaren.

In het verlengde hiervan kan de zorgverlener eigen aantekeningen toevoegen, of de ontvangen gegevens wijzigen. Gewijzigd overgenomen gegevens worden beschouwd als eigen dossiergegevens.

Om redundantie van informatie te voorkomen mogen als kopie aangemerkte patiëntgegevens niet bij de verwijsindex worden aangemeld en niet worden opgeleverd bij het verwerken van een opvraagverzoek.

Wanneer een gebruiker als kopie aangemerkte, lokale gegevens raadpleegt, is het raadzaam om aan te geven dat het een kopie betreft en dat de gegevens mogelijk zijn verouderd.

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

2.2.5.9 Ondertekening transactietoken met servercertificaat icm conditionele query

Alias: GBX.OPV.e4150.3

Details
Eis: Voor het gebruik van conditionele berichten moet er een transactietoken worden toegevoegd dat ondertekend is door het servercertificaat van het systeem waar vandaan het bericht verstuurd wordt. Het applicatieID van het betreffende systeem dient voor te komen in de autorisatieregel die is opgenomen in het mandaattoken. Dit mandaattoken dient in combinatie met het transactietoken, inschrijftoken en het conditionele bericht te worden verstuurd. **Toelichting bij eis:** Om een conditioneel bericht te kunnen versturen door een systeem, moet een zorgverlener het applicatieID('s) van een systeem kenmerken als systeem dat voor hem/haar een bericht mag versturen. Dit wordt vastgelegd in het mandaattoken. Om te kunnen garanderen dat een bericht door het betreffende systeem wordt verstuurd, is het nodig dat het systeem een transactietoken ondertekent en toevoegd bij het bericht.

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

2.2.5.10 Mandaattoken t.b.v. handeling door systeem

Alias: GBX.OPV.e4090.1

Details
Eis: Een bericht verstuurt door het systeem onder verantwoordelijkheid van een zorgverlener moet een getekend mandaattoken van de verantwoordelijke zorgverlener bevatten. Het mandaattoken moet een autorisatieregel bevatten (zie eis GBX.AUT.e4513) met minimaal de volgende invulling: • ApplicatieID('s) van systeem.

Toelichting bij eis: Een zorgverlener moet kunnen aangeven dat een systeem voor hem/haar automatisch een opvraag kan doen op basis van een specifieke trigger (zie GBX.OPV.e4040). Dit legt een zorgverlener vast in een mandaattoken. Het is mogelijk om hetzelfde mandaattoken te gebruiken om andere zorgverleners te mandateren.

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

2.2.5.11 Loggen initiatie conditioneel bericht

Alias: GBX.OPV.e4155.1

Details
Eis: De trigger die een conditioneel bericht initieert dient gelogd te worden. Hierbij dient de trigger gelinkt te kunnen worden aan een uitgaand conditioneel bericht. Indien het conditionele bericht geïnitieerd wordt door een systeemgebruiker, dan dient in ieder geval ook de gebruikersID (UZI-nummer of andere gebruikersID) gelogd te worden. **Toelichting bij eis:** In een audit of op verzoek van VZVZ moet duidelijk gemaakt kunnen worden wie of wat een conditioneel bericht getriggerd heeft. Hiervoor is het van belang dat de trigger gelogd wordt en gekoppeld kan worden aan een uitgaand conditioneel bericht. In het geval een systeemgebruiker het conditionele bericht triggert, dan dient de identificatie van de gebruiker ook gelogd te worden. Dit kan bijvoorbeeld een UZI-nummer zijn, maar mag ook een andere identifier zijn die getraceerd kan worden naar een uniek persoon.

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

2.2.5.12 Inzichtelijk maken resultaat van conditioneel bericht

Alias: GBX.OPV.e4045.1

Details
Eis: Het moet aan de gebruiker van het systeem inzichtelijk worden gemaakt wat het resultaat was van een conditioneel bericht**.** **Toelichting:** Met het in deze eis genoemde resultaat wordt bedoeld of er een conditioneel bericht is verstuurd en of deze succesvol is beantwoord. Met het in deze eis genoemde conditionele bericht wordt bedoeld: een bericht die ten behoeve van een gebruiker door het systeem is verstuurd. De definitie van gebruiker is afhankelijk van de trigger die gebruikt wordt om het conditionele bericht te initialiseren. Indien het openen van een dossier als trigger geldt, dan zal degene die het dossier opent op de hoogte gesteld moeten worden van het resultaat. Bij een automatische opvraag als gevolg van een binnenkomend abonnementsignaal, zal de verantwoordelijke zorgverlener (zoals opgenomen in het mandaattoken) op de hoogte gesteld moeten worden.

Het conditionele bericht creëert bij de gebruiker bepaalde verwachtingen. Indien het systeem niet kan voldoen aan die verwachtingen, dan dient dat inzichtelijk te worden gemaakt aan de gebruiker. De gebruikte triggers voor het conditionele bericht bepalen de wijze hoe de gebruiker in te lichten. Het is aan de systeembouwer om deze eis op een juiste manier te implementeren.

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

2.2.5.13 Inhoud inschrijftoken

Alias: GBX.OPV.e4060.2

Details
Eis: In een inschrijftoken moeten de volgende gegevens opgenomen worden: 1. BSN van de specifieke patiënt; 2. UZI-nummer van de persoon die het inschrijftoken heeft aangemaakt; het UZI-nummer kan worden afgeleid uit het certificaat waarmee het token is ondertekend; 3. het abonneenummer (URA) van de zorgaanbieder waarbinnen het inschrijftoken geldig moet zijn; 4. Datum en tijdstip waarop inschrijftoken is aangemaakt; 5. Datum en tijdstip van registreren BSN; t.b.v. het werkproces mag dit ook het tijdstip van aanmaken van het inschrijftoken zijn; 6. Geldigheidsduur. **Toelichting:** De technische specificaties van het inschrijftoken zijn uitgewerkt in de [IH Inschrijftoken].

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

2.2.5.14 Geldigheidsduur inschrijftoken

Alias: GBX.OPV.e4100.1

Details
Eis: Een inschrijftoken heeft een maximale geldigheidsduur van 1,5 jaar. **Toelichting:** Een inschrijftoken kent een beperkte geldigheidsduur. Het is echter mogelijk om dezelfde informatie in het inschrijfttoken opnieuw te onderteken (zie eis GBX.OPV.e4050). De geldigheid van het UZI-certificaat waarmee het inschrijftoken is ondertekend heeft geen invloed op de geldigheid van het inschrijftoken. Een inschrijftoken heeft een maximale geldigheidsduur van 1,5 jaar.

Vzvz_Moscow: Verplicht
Vzvz_Req_Verificatie: Acceptatietest
Vzvz_Req_Soort: Functional

Vzvz_Req_Type: Product

2.2.5.15 Creëren inschrijftoken

Alias: GBX.OPV.e4050

Details
Eis: Alleen daarvoor geautoriseerde rol(len)/perso(o)n(en) moet(en) een inschrijftoken (conform eis GBX.OPV.e4060) kunnen creëeren en voor gebruik kunnen ondertekenen met het authenticatiecertificaat van de UZI-pas. Het authenticatiecertificaat waarmee het inschrijftoken wordt ondertekend moet geldig zijn op het moment van tekenen. **Toelichting:** Het inschrijftoken moet waarborgen dat een patiënt in behandeling is bij een zorgorganisatie en dat de bsn van een patiënt is gevalideerd bij het SBV-Z. Om het proces m.b.t. het aanmaken van inschrijftokens te controleren is het zaak om alleen geautoriseerde rollen en/of personen te autoriseren om een inschrijftoken aan te maken. Dit kunnen zorgverleners, zorgverlenerassistenten en/of baliemedewerkers zijn.

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

2.2.5.16 Beperken gebruik inschrijftokens

Alias: GBX.OPV.e4120

Details
Eis: Inschrijftokens mogen binnen de AORTA-omgeving alleen meegestuurd worden met die interacties zoals beschreven in de AORTA-documentatie. **Toelichting:** Het LSP is niet voorbereid op het verwerken van een inschrijftoken indien dit niet expliciet is opgenomen in de AORTA-documentatie. Het LSP zal bij een onterecht meegestuurd inschrijftoken een foutmelding (XXXX) genereren.

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

2.2.5.17 Automatisch opvragen van patiëntgegevens op basis van context

Alias: GBX.OPV.e4040.1

Details
Beginsituatie: 1. Er is een behandelrelatie met de mandaterende zorgverlener geregistreerd voor de betreffende patiënt, en 2. Er is voldaan aan eis GBX.OPV.e4090, en 3. Er is voldaan aan eis GBX.OPV.e4050, en

4. Er is voldaan aan eis GBX.OPV.e4150.

Trigger:
Het systeem verstuurt een automatische opvraag als gevolg van bijvoorbeeld:

- een afspraak met de patiënt;
- het openen van een dossier van de patiënt;
- ontvangen van een bericht m.b.t. een specifieke patiënt;
- ontvangen van een signaal m.b.t. wijzigingen in patiëntgegevens van een specifieke patiënt;
- een handmatige trigger door een persoon.

Het is aan het XIS om verantwoord om te gaan met de triggers die een automatische opvraag kunnen veroorzaken.

Interacties:

1. Het systeem verzendt een opvragenPatiëntgegevensContext-bericht in combinatie met een inschrijftoken, mandaattoken en een transactietoken naar de ZIM.
2. Het systeem ontvangt een opleverenBouwsteeninstantiaties-bericht.

Resultaat:
De opgeleverde gegevens zijn door het systeem:

1. gepresenteerd aan de gebruiker, of
2. verwerkt tot een beslissing die is gepresenteerd aan de gebruiker, of
3. opgeslagen t.b.v. latere inzage door gebruiker.

Uitzonderingen:
Uitzonderingen zijn beschreven in de [Foutentabel]

Opties:
Het automatisch opvragen van patiëntgegevens is een wijze van opvragen die gebruikt kan worden naast het opvragen van patiëntgegevens op basis van context (GBX.OPV.e4015). Bij het implementeren van deze eis is ook GBX.OPV.e4015 verplicht.

Responsetijd:
GBZ-oplever-time-out is het tijdsinterval waarna een opvragend systeem geen oplevering meer van de ZIM hoeft te verwachten.

Betrouwbaarheid:
-

Toelichting bij eis:
Een automatische opvraag verschilt van een reguliere opvraag (GBX.OPV.e4015) m.b.t. de trigger en de daadwerkelijke bevrager van de patiëntgegevens. In het geval van een automatische opvraag doet het systeem een bevraging onder verantwoordelijkheid van een zorgverlener. Naast een waarborg van deze verantwoordelijkheid (in de vorm van een mandaattoken) dient ook een waarborg meegestuurd te worden dat een patiënt is ingeschreven bij de organisatie (inschrijftoken).

Het opvragen van patiëntgegevens dient gedaan te worden ten behoeve van een behandelende zorgverlener. Een automatische opvraag van patiëntgegevens moet door middel van het mandaattoken altijd gekoppeld zijn aan de behandelende zorgverlener die verantwoordelijk is voor de behandeling van de patiënt. Voor deze zorgverlener moet lokaal een behandelrelatie met de patiënt zijn vastgelegd.

Voor de werking m.b.t. het opvragenPatiëntgegevensContext-bericht zie eis GBX.OPV.e4010.

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

2.2.5.18 Afhandelen opgevraagde bouwstenen

Alias: GBX.OPV.e4017.1

Details
Eis:

Een XIS dat patiëntgegevens opvraagt op basis van een context, moet de aan de context gekoppelde bouwsteentypen kunnen verwerken. Hierbij dienen alle mogelijke bouwsteeninstantiaties verwerkt kunnen worden.
De te verwerken bouwsteentypen staan opgenomen in de implementatiehandleiding van de zorgtoepassing.

Toelichting bij eis:
Een zorgtoepassing bepaalt op basis van welke context(en) gegevens opgevraagd kunnen worden. Indien een context nog niet bestaat, dan bepaalt de zorgtoepassing ook welke bouwsteentypen er opgeleverd dienen te worden binnen de context en welke selectieparameters daarvoor kunnen gelden.
Er dienen gehele bouwsteentypen verwerkt te kunnen worden en niet alleen de specifieke bouwsteeninstantiaties behorende bij een zorgtoepassing, context of rolcode. Dit is van belang om er voor te zorgen dat een opvragend systeem voorbereid is op eventuele wijzigingen in de Selectie en Determinatieservice-tabellen.
Deze eis garandeert snellere doorlooptijden aan de kant van een XIS met betrekking tot de implementatie van nieuwe zorgtoepassingen en/of wijzigingen aan de Selectie en Determinatieservice.
Een XIS dient te kunnen omgaan met de situatie dat in een antwoordbericht bouwsteeninstantiaties voorkomen van een onverwacht, niet ondersteund bouwsteentype.
De implementatiehandleiding van een zorgtoepassing is opgenomen in Art-Decor (https://decor.nictiz.nl/pub/vzvz/). Hierin is voor elke systeemrol gespecifieerd welke interacties er ondersteund dienen te worden.

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

2.2.5.19 Generieke (conditionele) opvraag

Alias: GBX.BER.e3010

Details
Eis: Het systeem moet de generieke opvraag (GQZG_IN000001NL) kunnen versturen. Hierbij dient gebruik te worden gemaakt van de contextcode zoals opgenomen in de zorgtoepassing. **Toelichting bij eis:** Per zorgtoepassing zal er één of meerdere contextcodes worden gespecificeerd. Afhankelijk van de contextcode en de rolcode van de verantwoordelijk opvrager, zullen de juiste bevragingen naar de juiste bronsystemen uitgaan. De bevragingen naar de bronsystemen bepalen de uiteindelijke antwoorden die moeten kunnen worden verwerkt door het opvragende systeem. De specificatie van de generieke opvraag en de daarbij gebruikte parameters is opgenomen in de art-decorpublicatie van de zorgtoepassing.

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

2.2.6 Token beherend systeem

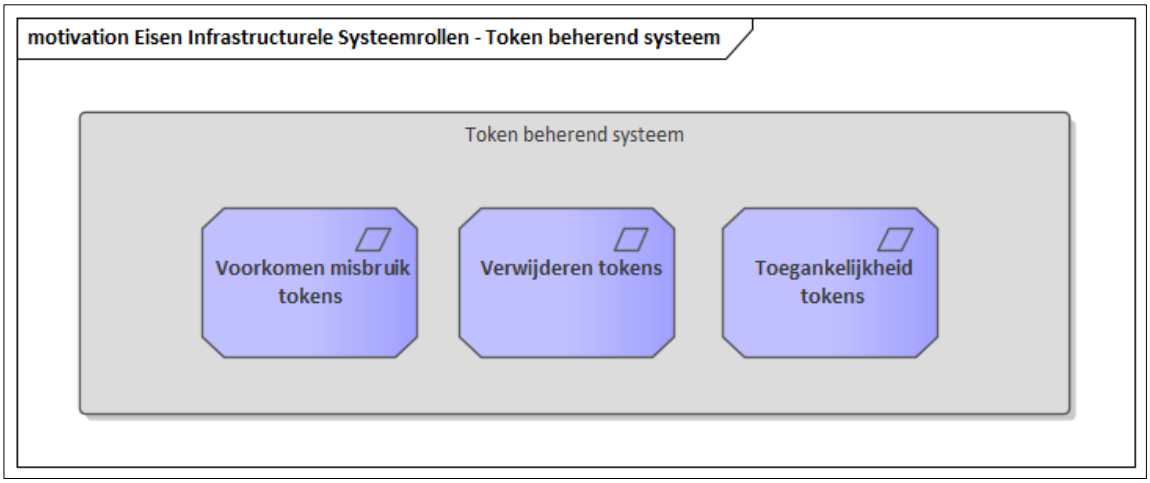


Figure 7 : Eisen Infrastructurele Systeemrollen - Token beherend systeem

2.2.6.1 Verwijderen tokens

Alias: GBX.OPV.e4110

Details
Eis: Indien de geldigheidsduur van een token is verlopen, dan dient deze automatisch te worden verwijderd. Daarnaast moet het voor een gebruiker, die ingelogd is op vertrouwensniveau midden, mogelijk zijn om een token uit het systeem te verwijderen. **Toelichting:** Het verwijderen (en daarmee afwezig zijn) van een token leidt ertoe dat er geen automatische opvraag meer verstuurd mag worden t.b.v. het opvragen van patiëntgegevens van de in het token opgenomen patiëntID. Dit kan gevolgen hebben voor het werkproces van de gebruiker van het systeem. Het is dan ook aan te raden om de gebruiker(s) van het systeem (tijdig) op de hoogte te stellen van het verwijderen van een token. Hoe hier invulling aan te geven is aan de systeembouwer. Het gaat hierbij bijvoorbeeld om inschrijf- en consenttokens.

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

2.2.6.2 Toegankelijkheid tokens

Alias: GBX.OPV.e4160.1

Details
Eis: Om misbruik van tokens door een kwaadwillende te bemoeilijken, moeten de tokens in een beveiligde omgeving worden opgeslagen. Toegang tot de tokens moet alleen mogelijk zijn voor geautoriseerde gebruikers. **Toelichting:**

Er worden geen specifieke eisen gesteld aan de rollen die geautoriseerd zijn en aan de wijze van opslag van de tokens. Dit is afhankelijk van de lokale systeemimplementatie. De systeembouwer is verantwoordelijk voor een goede invulling van deze eis. Het gaat hierbij alleen om die tokens, die meerdere malen gebruikt kunnen worden, zoals inschrijf- en consenttokens.

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

2.2.6.3 Voorkomen misbruik tokens

Alias: GBX.OPV.e4170

Details
Eis: Inschrijf- en mandaattokens mogen alleen verstuurd worden over beveiligde verbindingen. **Toelichting:** Om te voorkomen dat (bepaalde) tokens worden afgevangen en misbruikt door een kwaadwillende moeten (bepaalde) tokens verstuurd worden over beveiligde verbindingen. Afhankelijk van de opslag- of creatielocatie van de tokens, kan dit impliceren dat een GBX ook intern gebruik dient te maken van beveiligde verbindingen.

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

2.2.7 Zorgaanbiedersadresboek

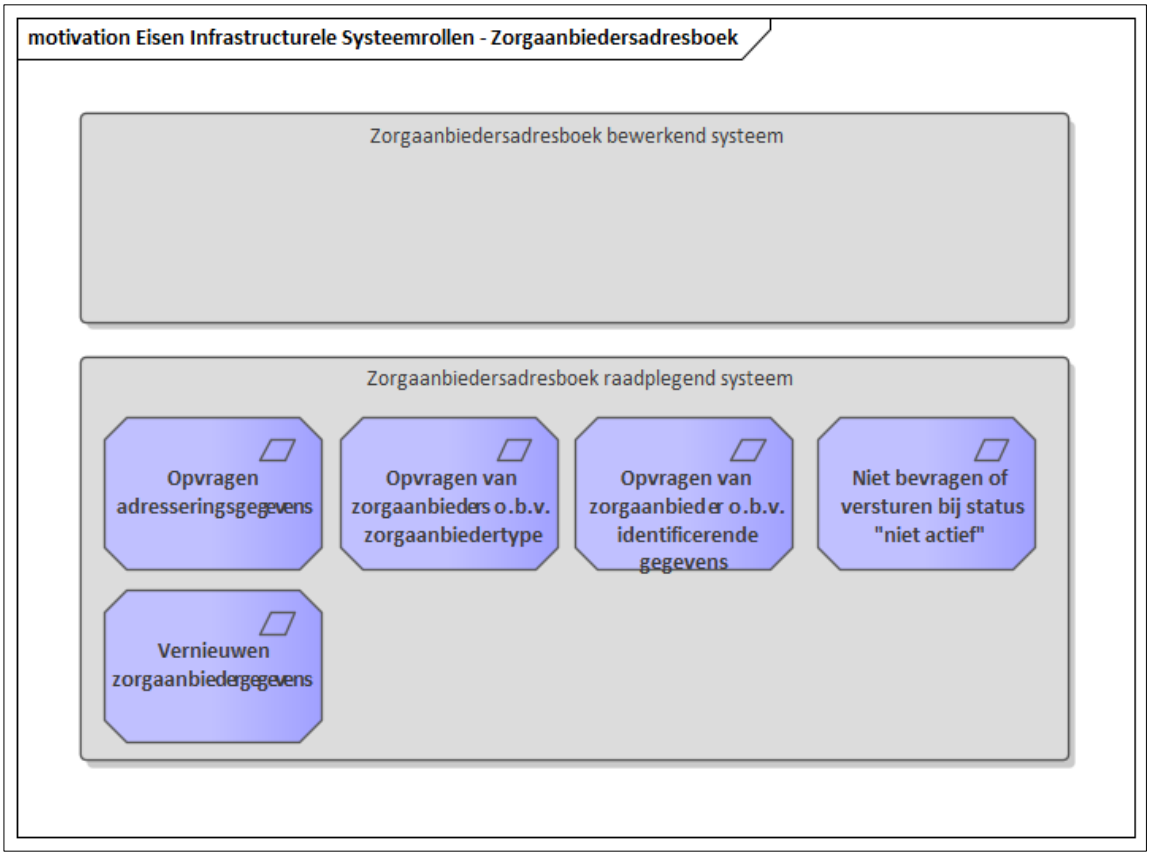


Figure 8 : Eisen Infrastructurele Systeemrollen - Zorgaanbiedersadresboek

2.2.7.1 Niet bevragen of versturen bij status "niet actief"

Alias: GBX.ZAB.e4050

Details
Eis: In het geval een applicatie van een opgevraagde zorgaanbieder niet de status 'actief' heeft, mag er geen bericht naar toe worden gestuurd. **Toelichting bij eis:** Het ZAB heeft een real time koppeling met het APR. Informatie met betrekking tot een applicatie zal dan ook altijd actueel zijn. In het geval, na een bevraging van het ZAB, blijkt dat een bepaalde applicatie niet de status actief heeft, dan mag er geen bericht aan het specifieke applicatieID worden verzonden. Hiermee worden onnodige foutmeldingen en onnodig verkeer voorkomen.

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

2.2.7.2 *Opvragen van zorgaanbieder o.b.v. identificerende gegevens*

Alias: GBX.ZAB.e4020.1

Details
Functie Opvragen van zorgaanbieders o.b.v. identificerende gegevens **Karakter** Conditioneel **Condities** In het geval er geen andere bron voor adressering aanwezig is, dan is deze eis verplicht. Een alternatieve bron dient actuele en onweerlegbare informatie te bevatten. **Beginsituatie** a. De gebruiker is lokaal ingelogd op vertrouwensniveau laag of hoger (trigger a), of b. Het systeem beschikt over de voor deze functie vereiste vertrouwensmiddelen (trigger b). **Trigger** a. De gebruiker initieert de functie via het systeem, of b. Het systeem initieert de functie automatisch. **Interacties** 1. Het systeem verzendt een REST-Request naar de ZAB. 2. Het systeem ontvangt een REST-Response van de ZAB. **Resultaat** De opgeleverde gegevens zijn door het systeem: a. gepresenteerd aan de gebruiker **Uitzonderingen** Uitzonderingen zijn beschreven in de Foutentabel. **Toelichting** Het moet mogelijk zijn om op basis van identificerende zorgaanbiedergegevens (in ieder geval o.b.v. de URA) de naam en NAW-gegevens van de betreffende Zorgaanbieder op te vragen. Alle specifieke zoekcriteria zijn opgenomen in de implementatiethandleiding van ZORG-AB (https://www.vzvz.nl/diensten/gemeenschappelijke-diensten/zorg-ab/releases).

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

2.2.7.3 *Opvragen van zorgaanbieders o.b.v. zorgaanbiedertype*

Alias: GBX.ZAB.e4015.1

Details
Functie Opvragen van zorgaanbieders o.b.v. zorgaanbiedertype **Karakter** Conditioneel **Condities**

In het geval er geen andere bron voor adressering aanwezig is, dan is deze eis verplicht. Een alternatieve bron dient actuele en onweerlegbare informatie te bevatten..

Beginsituatie
a. De gebruiker is lokaal ingelogd op vertrouwensniveau laag of hoger (trigger a), of
b. Het systeem beschikt over de voor deze functie vereiste vertrouwensmiddelen (trigger b).

Trigger
a. De gebruiker initieert de functie via het systeem, of
b. Het systeem initieert de functie automatisch.
Interacties
1. Het systeem verzendt een REST-Request naar de ZAB.
2. Het systeem ontvangt een REST-Response van de ZAB.

Resultaat
De opgeleverde gegevens zijn door het systeem:
a. gepresenteerd aan de gebruiker

Uitzonderingen
Uitzonderingen zijn beschreven in de Foutentabel.

Toelichting
Het moet mogelijk zijn om op basis van zorgaanbiedertype een lijst met alle zorgaanbieders van een bepaald type op te vragen. Het moet mogelijk zijn om hierbij bepaalde filterparameters toe te passen. Alle specifieke zoekcriteria zijn opgenomen in de implementatiehandleiding van ZORG-AB (https://www.vzvz.nl/diensten/gemeenschappelijke-diensten/zorg-ab/releases).

Het is mogelijk dat op basis van de zoekcriteria meerdere zorgaanbieders worden geretourneerd. Het aantal resultaten is beperkt tot de waarde zoals is opgenomen in de gebruikershandleiding van ZORG-AB (https://www.vzvz.nl/diensten/gemeenschappelijke-diensten/zorg-ab/releases).

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

2.2.7.4 Opvragen adresseringsgegevens

Alias: GBX.ZAB.e4010

Details
Functie Opvragen van technische adresseringsgegevens o.b.v. zorgaanbiedergegevens. **Karakter** Conditioneel **Condities** In het geval deze eis is opgenomen in een PvE is deze eis verplicht. **Beginsituatie** a. De gebruiker is lokaal ingelogd op vertrouwensniveau laag of hoger (trigger a), of b. Het systeem beschikt over de voor deze functie vereiste vertrouwensmiddelen (trigger b). **Trigger** a. De gebruiker initieert de functie via het systeem, of b. Het systeem initieert de functie automatisch.

Interacties
1. Het systeem verzendt een REST-Request naar de ZAB.
2. Het systeem ontvangt een REST-Response van de ZAB.

Resultaat
De opgeleverde gegevens zijn door het systeem:
a. verwerkt tot een beslissing (die is gepresenteerd aan de gebruiker).

Uitzonderingen
Uitzonderingen zijn beschreven in de Foutentabel.

Toelichting
Het moet mogelijk zijn om op basis van locatiegegevens en/of op basis van naamgeving van de zorgaanbieder technische adresseringsgevens op te vragen. Alle specifieke zoekcriteria zijn opgenomen in de implementatiehandleiding van ZORG-AB (https://www.vzvz.nl/diensten/gemeenschappelijke-diensten/zorg-ab/releases).

Het is mogelijk dat op basis van de zoekcriteria meerdere zorgaanbieders met hun (technische) identificeergegevens worden geretourneerd. Het aantal resultaten is beperkt tot het aantal zoals is opgenomen in de gebruikershandleiding van ZORG-AB (https://www.vzvz.nl/diensten/gemeenschappelijke-diensten/zorg-ab/releases).

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

2.2.7.5 Vernieuwen zorgaanbiedergegevens

Alias: GBX.ZAB.e4120

Details
Eis: Lokaal opgeslagen zorgaanbiedergegevens dienen actueel te zijn, voordat het gebruikt wordt ten behoeve van communicatie via de AORTA infrastructuur. **Toelichting bij eis:** Er moet voorkomen worden dat medische informatie naar een verkeerde en/of niet bestaande zorgaanbieder wordt verstuurd. Het is daarom van belang dat met name adresseringsgegevevens van de te adresseren zorgaanbieder actueel worden gehouden.

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

2.2.8 Applicatiebeheer

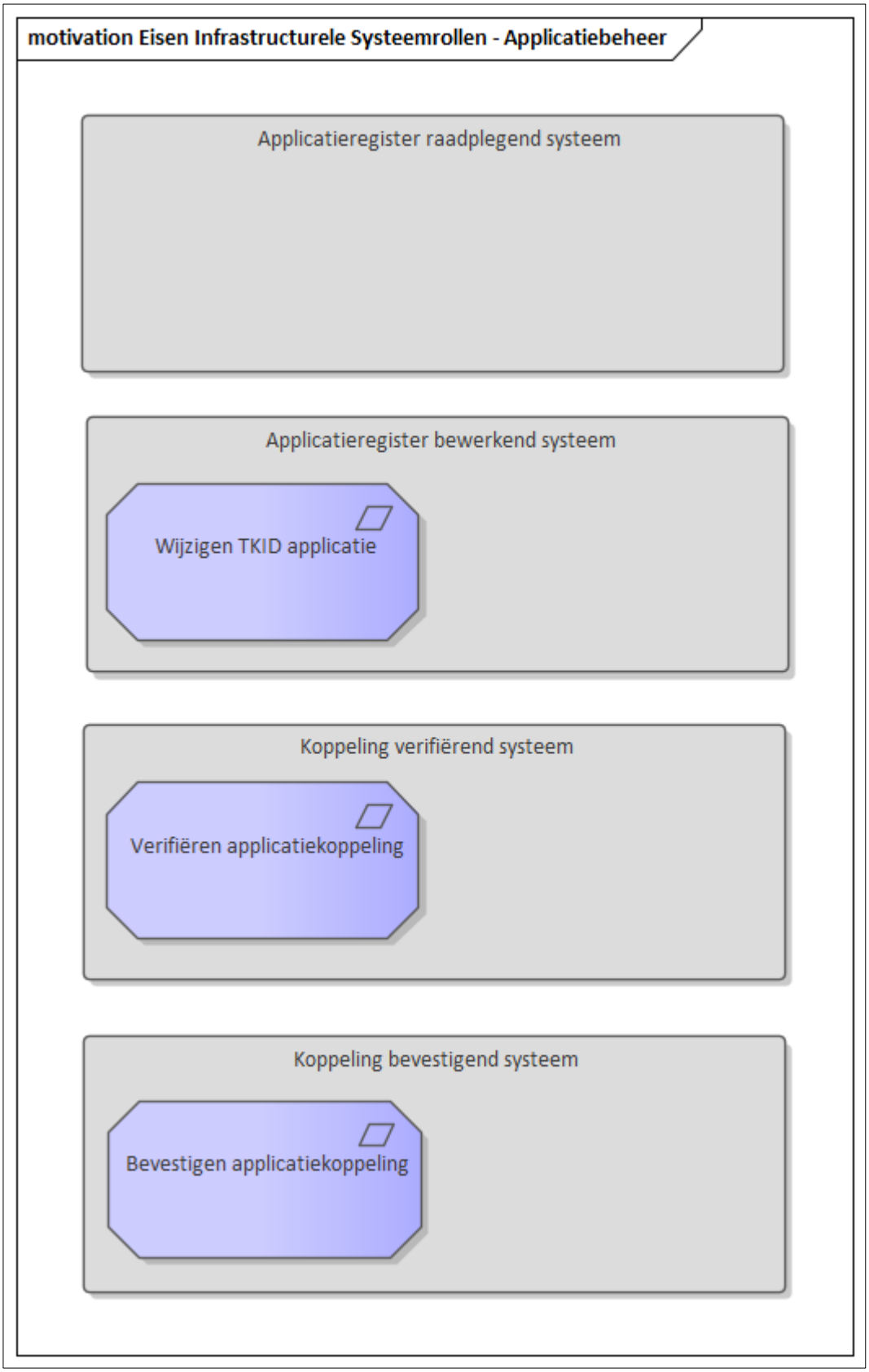

motivation Eisen Infrastructurele Systeemrollen - Applicatiebeheer
Applicatieregister raadplegend systeem
Applicatieregister bewerkend systeem
Wijzigen TKID applicatie
Koppeling verifiërend systeem
Verifiëren applicatiekoppeling
Koppeling bevestigend systeem
Bevestigen applicatiekoppeling

Figure 9 : Eisen Infrastructurele Systeemrollen - Applicatiebeheer

2.2.8.1 *Bevestigen applicatiekoppeling*

Alias: GBX.APR.e4160

Details
Beginsituatie Het systeem beschikt over de voor deze functie vereiste vertrouwensmiddelen. **Trigger** Het systeem ontvangt een verifiërenApplicatiekoppeling bericht conform IH AORTA. **Interacties** Het systeem stuurt een verifiërenApplicatiekoppelingAntwoord terug naar de verzender conform IH AORTA. **Resultaat** Het antwoordbericht is teruggestuurd naar de verzender. **Uitzonderingen** Uitzonderingen zijn beschreven in de Foutentabel. **Opties** Het bericht moet een authenticatietoken kunnen bevatten. **Responsetijd** - **Betrouwbaarheid** - **Toelichting** -

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

2.2.8.2 *Verifiëren applicatiekoppeling*

Alias: GBX.APR.e4140

Details
Beginsituatie De gebruiker is lokaal ingelogd op vertrouwensniveau laag of hoger. **Trigger** De gebruiker initieert de functie via het systeem. **Interacties** 1. Het systeem verzendt en verifiërenApplicatiekoppeling bericht naar de ZIM of een ander GBX conform IH APR. 2. Het systeem ontvangt een verifiërenApplicatiekoppelingAntwoord bericht conform IH APR. **Resultaat** De opgeleverde gegevens zijn door het systeem: • gepresenteerd aan de gebruiker, of • verwerkt tot een beslissing (die is gepresenteerd aan de gebruiker). **Uitzonderingen** Uitzonderingen zijn beschreven in de Foutentabel. **Opties** Het bericht moet een authenticatietoken kunnen bevatten. **Responsetijd** - **Betrouwbaarheid** Garantie geven dat versturen van gegevens niet zonder kennisgeving gestaakt wordt

Toelichting
-

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

2.2.8.3 Wijzigen TKID applicatie

Alias: GBX.APR.e4060, GBX.APR.e4170.1

Details
Beginsituatie De gebruiker is lokaal ingelogd op vertrouwensniveau laag of hoger. **Trigger** De gebruiker initieert de functie via het systeem. **Interacties** 1. Het systeem verzendt een *beherenTKID*-bericht naar de ZIM conform HL7v3 IH APR. 2. Het systeem ontvangt een ontvangstbevestiging conform HL7v3 IH APR. **Resultaat** Het LSP heeft de in het bericht opgenomen TKID's opgenomen in het applicatieregister. **Uitzonderingen** Uitzonderingen zijn beschreven in de Foutentabel. **Opties** - **Responsetijd** - **Betrouwbaarheid** - **Toelichting** De logische attributen van dit bericht zijn te vinden in het Ontwerp Applicatieregister. Vanuit het XIS-acceptatieproces wordt er een typekwalificatieID (TKID) gegenereerd. In overleg tussen de XIS-leverancier en het VZVZ-acceptatieteam wordt de granulariteit van een TKID bepaald. Het is mogelijk dat er voor een XIS-applicatie één of meerdere TKID's worden uitgegeven. Aan elk TKID zijn één of meerdere specifieke systeemrol(len) gekoppeld. Aan elk systeemrol zijn één of meerdere interactieID's gekoppeld. Een zorgaanbiederapplicatie (een bij de zorgaanbieder geïnstalleerde versie van een XIS-applicatie) kan meerdere TKID's ondersteunen. Zie het ONTW APR voor het gegevensmodel en een beschrijving m.b.t. TKID's. In het geval een zorgaanbiederapplicatie gebruik wil maken van de functionaliteit van een bepaalde systeemrol, dient de zorgaanbiederapplicatie aan de betreffende TKID (behorende bij de specifieke systeemrol(len)) gekoppeld te worden. Vanuit de applicatie dient met het 'beheren TKID'-bericht, het gewenste TKID ingestuurd te worden. Er mogen alleen TKID's ingestuurd worden, die door de afgenomen XIS-applicatiesoftware zijn verkregen naar aanleiding van een positieve acceptatie. De beheerder of het systeem van een bij een zorgaanbieder geïnstalleerde applicatie dient alleen die TKID's in te sturen waarvan alle systeemrollen ook daadwerkelijk door de geïnstalleerde applicatie ondersteund worden. Er kunnen meerdere TKID's in het bericht opgenomen worden. Zodra een TKID niet bekend is, wordt er een foutcode (INVALIDETKID) met bijbehorende foutmelding (zie Foutentabel) gegenereerd. De mogelijk overige correcte TKID's worden niet verwerkt in het applicatieregister. Alle TKID's dienen opnieuw ingestuurd te worden.

Bij elk door het LSP succesvol ontvangen ‘beheren TKID’-bericht, worden de bestaande TKID-koppelingen met de zorgaanbiederapplicatie verwijderd en worden er koppelingen gemaakt met de in het bericht opgenomen TKID’s. Hierbij geldt dat een bestaande status van reeds aanwezige systeemrollen (gekoppeld aan een TKID) niet wordt veranderd. Koppelingen die nog niet bekend waren binnen het applicatieregister krijgen direct de status ‘actief’.

In principe geldt dat er bij elk nieuw verkregen TKID, als gevolg van een acceptatie van een applicatiewijziging of –uitbreiding, er één of meerdere TKID’s opnieuw ingestuurd moeten worden. Denkbare situaties zijn:

- Installeren nieuwe functionaliteit;
  - Initiële installatie;
  - Nieuwe acceptatie van de XIS-applicatie.

Terugzetten oude functionaliteit (met een eerder verkregen TKID).

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

2.2.9 Patiëntadministratie

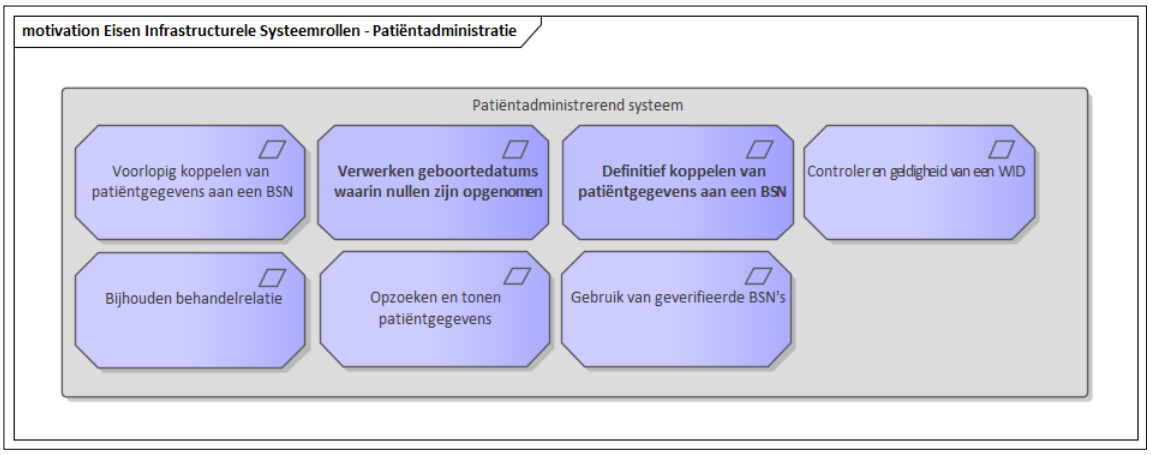


Figure 10 : Eisen Infrastructurele Systeemrollen - Patiëntadministratie

2.2.9.1 Gebruik van geverifieerde BSN's

Alias: GBX.IDA.e4060.1

Details
Eis: Het systeem moet aan Opzoeken en tonen patiënteninformatie, Voorlopig koppelen van patiëntgegevens aan een BSN, Controleren geldigheid van een WID, en Bijhouden behandelrelatie voldoen of (bij implementatie in een GBZ) een koppeling kunnen leggen met een derde systeem dat aan die eisen voldoet. Een systeem die gebruik maakt van een extern patiëntadministrerend systeem is verplicht om te controleren of een BSN daadwerkelijk aan alle AORTA eisen voldoet m.b.t. het BSN.

Toelichting bij eis:
Ieder GBZ moet over een patiëntadministratie beschikken, maar een XIS hoeft die niet per se in te bouwen. Het staat een GBZ vrij een eigen patiëntadministrerend systeem te kiezen dat voldoet aan de genoemde eisen. De systeemrol van Patiëntadministrerend systeem is daarmee niet verplicht voor XIS-typekwalificatie, maar een GBZ moet wel aantoonbaar over een dergelijk systeem beschikken en dit met het gebruikte XIS hebben gekoppeld om zodoende te kunnen garanderen dat er in de XIS-instantie met geverifieerde BSN's gewerkt wordt. Die gerefereerde eisen hoeven dan niet voor de XIS-typekwalificatie te worden ingebouwd.

Hoe de controle wordt gedaan op de geldigheid van een BSN is aan de XIS-applicatie. Het is denkbaar dat de XIS-applicatie het patiëntadministrerende systeem actief benaderd, maar het is ook mogelijk dat de XIS-applicatie de statussen van een BSN toegezonden krijgt. Er mogen in géén geval BSN's in een bericht worden opgenomen die niet voldoen aan de AORTA eisen.

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

2.2.9.2 Opzoeken en tonen patiëntgegevens

Alias: GBX.IDA.e4010.1

Details
Eis: Het systeem moet een gebruiker de mogelijkheid bieden een patiënt op te zoeken in de lokale patiëntadministratie van de zorgaanbieder, door het invoeren van identificerende gegevens, waarna wordt getoond: 1. of de patiënt/cliënt is gevonden, en zo ja 2. of het BSN wel/niet is opgevraagd of geverifieerd bij de SBV-Z 3. de datum en tijd van koppelen 4. de manier van vaststellen van de identiteit: * Controle van echtheid en geldigheidsdatum van WID en de gelijkenis van de in de WID genoemde identificerende gegevens * Vergewissen, • indien beschikbaar het UZI-nummer of anders een unieke identificatie van de gebruiker en het UZI-nummer van mandaterende zorgverlener indien van toepassing • in geval van WID-controle: aard en nummer van het WID. **Toelichting bij eis:** Deze eis voorkomt dat de SBV-Z telkens opnieuw wordt geraadpleegd.

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

2.2.9.3 Bijhouden behandelrelatie

Alias: GBX.IDA.e4050

Details
Eis: Het systeem moet een gebruiker de volgende mogelijkheden bieden in de lokale patiëntadministratie voor een patiënt/cliënt. De status van de behandelrelatie inzien, waarbij wordt getoond: 1. of een behandelrelatie bestaat, en zo ja met welke zorgverleners een behandelrelatie bestaat; 2. ten behoeve van welke zorgaanbieder (URA) de behandelrelatie wordt onderhouden. Een nieuwe behandelrelatie beginnen, waarbij wordt vastgelegd: 1. begindatum; 2. UZI-nummer van de zorgverlener; 3. de URA van de zorgaanbieder ten behoeve van wie de behandelrelatie onderhouden wordt. Een bestaande behandelrelatie beëindigen, waarbij wordt vastgelegd: 1. einddatum; 2. UZI-nummer van de zorgverlener. **Toelichting bij eis:** De zorgverlener onderhoudt de behandelrelatie hetzij ten behoeve van de zorgaanbieder waarvoor hij werkzaam is, hetzij als zorgaanbieder indien het een zelfstandig werkende beroepsbeoefenaar betreft. Een zorgverlener die de patiënt/cliënt niet ziet, bijvoorbeeld in een laboratorium, legt een behandelrelatie vast in de zin van een verklaring dat hij werkt in opdracht van een andere zorgverlener die een behandelrelatie met de patiënt/cliënt heeft.

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

2.2.9.4 Controleren geldigheid van een WID

Alias: GBX.IDA.e4040

Details
Eis: Het systeem moet voor een geselecteerde patiënt/cliënt de gebruiker de mogelijkheid bieden: 1. het 'in omloop mogen zijn' van het WID te controleren door raadplegen van de SBV-Z op basis van aard en nummer van het WID; 2. in de lokale patiëntenindex vast te leggen dat hij 'het in omloop mogen zijn' van het WID heeft gecontroleerd, onder vermelding van: * resultaat van de controle, * datum en tijd, * indien beschikbaar het UZI-nummer of anders een unieke identificatie van de gebruiker, * aard en nummer van het WID. • de onder 2. vastgelegde informatie op elk gewenst moment te raadplegen. **Toelichting bij eis:** Dit is belangrijk voor een zorgverlener/medewerker die in geval van twijfel over de echtheid of geldigheid van een WID wil nagaan of deze in omloop mag zijn. Hiertoe biedt de SBV-Z een dienst om te kunnen controleren of een bepaald WID in omloop is.

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

2.2.9.5 Definitief koppelen van patiëntgegevens aan een BSN

Alias: GBX.IDA.e4030

Details
Eis: Het systeem moet voor een geselecteerde patiënt/cliënt de gebruiker: • de mogelijkheid bieden gewaarschuwd te worden indien nog niet is vastgesteld dat het BSN hoort bij de patiënt/cliënt; • de mogelijkheid bieden in de lokale patiëntenindex vast te leggen dat hij heeft vastgesteld dat het betreffende BSN hoort bij de patiënt/cliënt, onder vermelding van: 1. de manier van vaststellen: i. Controle van echtheid en geldigheidsdatum van WID en de gelijkenis van de in de WID genoemde identificerende gegevens, ii. Vergewissen, 1. Datum en tijd van vaststellen, 2. indien beschikbaar het UZI-nummer of anders een unieke identificatie van de gebruiker, en het UZI-nummer van mandaterende zorgverlener indien van toepassing. 3. zorgaanbieder-id van de gebruiker; 4. in geval van WID-controle: aard en nummer van het WID. Daarmee is het BSN definitief gekoppeld. **Toelichting bij eis:** Dit is belangrijk voor een zorgaanbieder die (geautomatiseerd) wil vaststellen of is voldaan aan de eventuele wettelijke verplichting om de identiteit vast te stellen aan de hand van een WID. Merk op dat de toelichting op Wet gebruik burgerservicenummer in de zorg artikel 26 een grote verantwoordelijkheid legt bij de zorgaanbieder voor de afweging wel/niet WID controleren. Daarom is geautomatiseerde ondersteuning belangrijk. Manier van vaststellen: • Vaststellen identiteit; Bij inschrijving van een patiënt waar nog geen behandelrelatie mee is, is het verplicht de identiteit van de patiënt vast te stellen aan de hand van een Wettelijk Identificatie Document (WID): een paspoort, Nederlands rijbewijs, Nederlandse ID-kaart of Nederlands vreemdelingendocument. • WID-controle; Indien er wordt getwijfeld over de geldigheid van een identiteitsdocument, kan bij de Sectorale Berichten Voorziening in de Zorg (SBV-Z) een WID-controle worden uitgevoerd. Dit kan via een zorginformatiesysteem of via de website van SBV-Z. • Opvragen/verifiëren BSN; Hierna moet het BSN geverifiëerd worden en registreren worden dat deze verificatie heeft plaatsgevonden. Alle door VZVZ geaccepteerde zorginformatiesystemen ondersteunen deze mogelijkheid. Komt BSN van een patiënt via een andere zorgverlener? Dan hoeft het niet opnieuw geverifiëerd te worden. Ook als het nummer direct uit de BRP komt , kunt BSN-verificatie achterwege worden gelaten. Het systeem kan hierna overgaan tot het vrijgeven en aanmelden van de bij de patiënt/cliënt behorende gegevens.

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

2.2.9.6 *Voorlopig koppelen van patiëntgegevens aan een BSN*

Alias: GBX.IDA.e4020

Details
Eis: Het systeem moet een gebruiker de mogelijkheid bieden het door een burgerregister geretourneerde BSN te koppelen aan de identificerende gegevens in de lokale patiëntenindex waarbij bij het overgenomen BSN automatisch wordt vastgelegd: 1. de bron van het BSN; 2. datum en tijd van koppelen; 3. UZI-nummer of andere identificatie van de gebruiker. Er is dan sprake van een voorlopige koppeling tussen BSN en patiëntgegevens. **Toelichting bij eis:** Dit is nodig opdat een zorgverlener/medewerker kan voldoen aan de wettelijke verplichting van de zorgaanbieder om het BSN op te nemen in zijn administratie, zie Wbsn-z artikel 8.Voor het landelijk uitwisselen van medische patiëntgegevens moet de SBV-Z of de GBA / BRP zijn geraadpleegd.

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

2.2.9.7 *Verwerken geboortedatums waarin nullen zijn opgenomen*

Alias: GBX.IDA.e4015

Details
Eis: Een geboortedatum die teruggegeven wordt door de SBV-Z kan nullen bevatten (jjjjmm00, jjjj0000 of 00000000). Het XIS moet in staat zijn hiermee adequaat om te gaan zonder dat de applicatie vastloopt. **Toelichting bij eis:** Deze eis leidt tot de volgende aanvullende eisen: 1. Alle XISsen moeten naast de mogelijkheid om een BSN op te vragen of te verifiëren op basis van de Zoekpaden 1 en 2, ook de dienst opvragen van persoonsgegevens op basis van een ingevoerd BSN inbouwen. 2. Bij het overnemen van de gegevens uit de SBV-Z moet het voor de gebruiker mogelijk zijn om de geboortedatum aan te passen voor het opslaan, indien het systeem meldt dat de gegevens niet in de database kunnen worden opgeslagen. 3. Bij het aanpassen van de geboortedatum in een databasegeaccepteerde datum moet er een indicatie komen dat de geboortedatum handmatig is aangepast. (bijvoorbeeld andere kleur of een indicatie erbij). Nog mooier is de opgeleverde datum opslaan in een (apart) tekstveld. 4. De dienst 'opvragen persoonsgegevens op basis van BSN' moet kunnen worden uitgevoerd, ook als er al persoonsgegevens bekend zijn maar de verificatie mislukt is vanwege de geboortedatum. Hierbij kan er een dialoogvenster wordt getoond waarbij de gegevens van de SBV-Z worden vergeleken met die uit de database van de zorgverlener. Een aanpassing van de geboortedatum mag niet leiden tot 'het niet geverifieerd zijn van het BSN'. Dit geldt echter alleen tijdens de dialoog van vergelijken. Indien de geboortedatum buiten de dialoog om aangepast wordt, moet dit wel leiden tot het vervallen van de verificatie.

Vzvz_Moscow: Verplicht
Vzvz_Req_Verificatie: Acceptatietest

Vzvz_Req_Soort: Functional
Vzvz_Req_Type: Product

2.3 AORTA Eisen Kwaliteit Aangesloten Systemen

2.3.1 Betrouwbaarheid

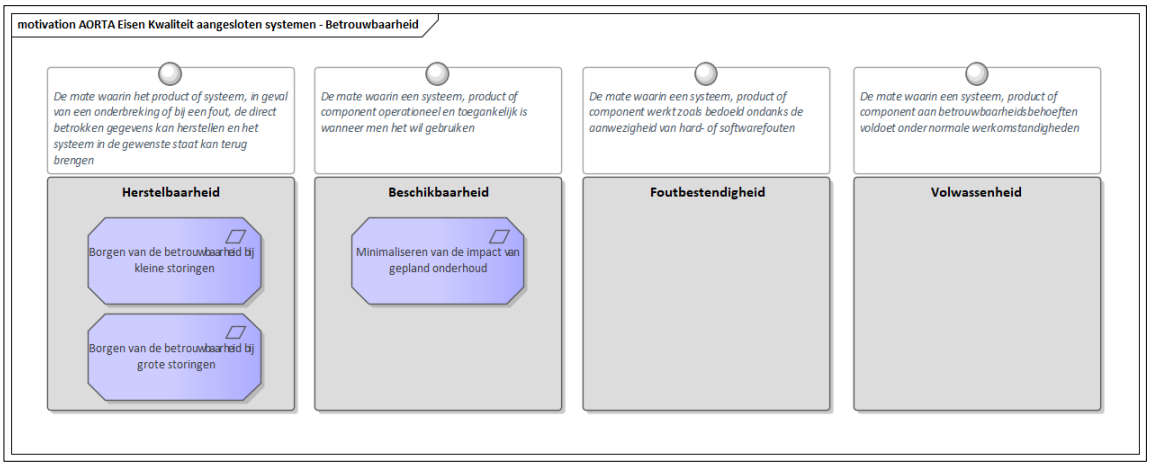


Figure 11 : AORTA Eisen Kwaliteit aangesloten systemen - Betrouwbaarheid

ISO 25010 definieert Betrouwbaarheid als: De mate waarin een systeem, product of component gespecificeerde functies uitvoert onder gespecificeerde condities gedurende een gespecificeerde hoeveelheid tijd.

2.3.1.1 Borgen van de betrouwbaarheid bij grote storingen

Alias: GBX.BET.e4020.1

Details
Eis: Grote storingen in een GBx mogen niet meer dan gemiddeld 2 keer per jaar voorkomen en dienen dan binnen 1 dag te zijn opgelost. **Toelichting bij eis:** De term 'grote storing' is niet SMART gedefineerd. Het kan vele soorten storingen betreffen. Het doel van deze eis is om te voorkomen dat een GBx na een ernstige storing zeer lang onbeschikbaar blijft. Onbeschikbaarheid zou bijvoorbeeld kunnen komen omdat er geen onderhoudscontract is en daardoor de hulp slechts langzaam op gang komt. Deze eis betekent voor de zorgaanbieder dat hij behalve professioneel beheer ook snel moet kunnen terugvallen op zijn XIS-leverancier, GZN en/of andere ICT-leveranciers. Zo moet bij ernstige storing, snel een leverancier beschikbaar zijn om het probleem te verhelpen. Wellicht kunnen zijn ICT-leveranciers hem een 24-uurs onderhoudscontract bieden. Indien de zorgaanbieder een ASP-leverancier heeft geselecteerd voor zijn XIS, zal hij dit wellicht geheel delegeren aan die ASP-leverancier.

Vzvz_Moscow: Verplicht (Must)
Vzvz_Req_Verificatie: Monitoring
Vzvz_Req_Soort: Non-Functional

Vzvz_Req_Type: Product

2.3.1.2 Borgen van de betrouwbaarheid bij kleine storingen

Alias: GBX.BET.e4010.1

Details
Eis: Kleine storingen in een GBx mogen niet meer dan gemiddeld 1 keer per maand voorkomen en dienen dan binnen 10 werkdagen te zijn opgelost. **Toelichting bij eis:** De term 'kleine storing' is niet SMART gedefinieerd. Het kan vele soorten storingen betreffen. Het doel van deze eis is om te voorkomen dat een GBZ te vaak uitvalt en na een eenvoudig te verhelpen storing meteen langere tijd onbeschikbaar blijft. Deze eis betekent voor de zorgaanbieder dat zijn ICT-voorzieningen professioneel moet (laten) beheren. Dit vergt periodieke controle met eventueel preventief onderhoud. Verder moet een onverhoopte storing meteen worden gesignaleerd, zodat een GBZ-beheerder snel beschikbaar kan zijn om het probleem te verhelpen. Wellicht kan zijn XIS-leverancier hem daarbij helpen. Indien de zorgaanbieder een ASP-leverancier heeft geselecteerd voor zijn XIS, zal hij dit wellicht geheel delegeren aan die ASP-leverancier. De afspraken en procedures zoals opgenomen in de AORTA DAP dienen hierbij gevolgd te worden.

Vzvz_Moscow: Verplicht (Must)
Vzvz_Req_Verificatie: Monitoring
Vzvz_Req_Soort: Functional
Vzvz_Req_Type: Product

2.3.1.3 Minimaliseren van de impact van gepland onderhoud

Alias: GBX.BES.e4020.2

Details
Eis: Gepland onderhoud van een GBX-applicatie mag niet meer dan twaalf keer per jaar voorkomen en dient niet langer dan een uur te duren. Gepland onderhoud wordt bij voorkeur uitgevoerd binnen aangetoonde daluren. De beheerders van de ZIM moeten twee weken van te voren worden ingelicht door de systeembeheerder. **Toelichting bij eis:** Deze eis is nodig om te voorkomen dat een GBx wegens onderhoud onnodig lang onbereikbaar is, ze betekent voor de organisatie dat onderhoud van de ICT-voorzieningen zoveel mogelijk wordt gepland en zodanig voorbereid dat het GBx slechts kort onbeschikbaar hoeft te zijn. **Implicaties:** Deze eis betekent voor de organisatie dat onderhoud van de ICT-voorzieningen zoveel mogelijk wordt gepland en zodanig voorbereid dat het GBX slechts kort onbeschikbaar hoeft te zijn.

Vzvz_Moscow: Verplicht (Must)
Vzvz_Req_Verificatie: Monitoring
Vzvz_Req_Soort: Non-Functional
Vzvz_Req_Type: Product

2.3.2 Beveiligbaarheid

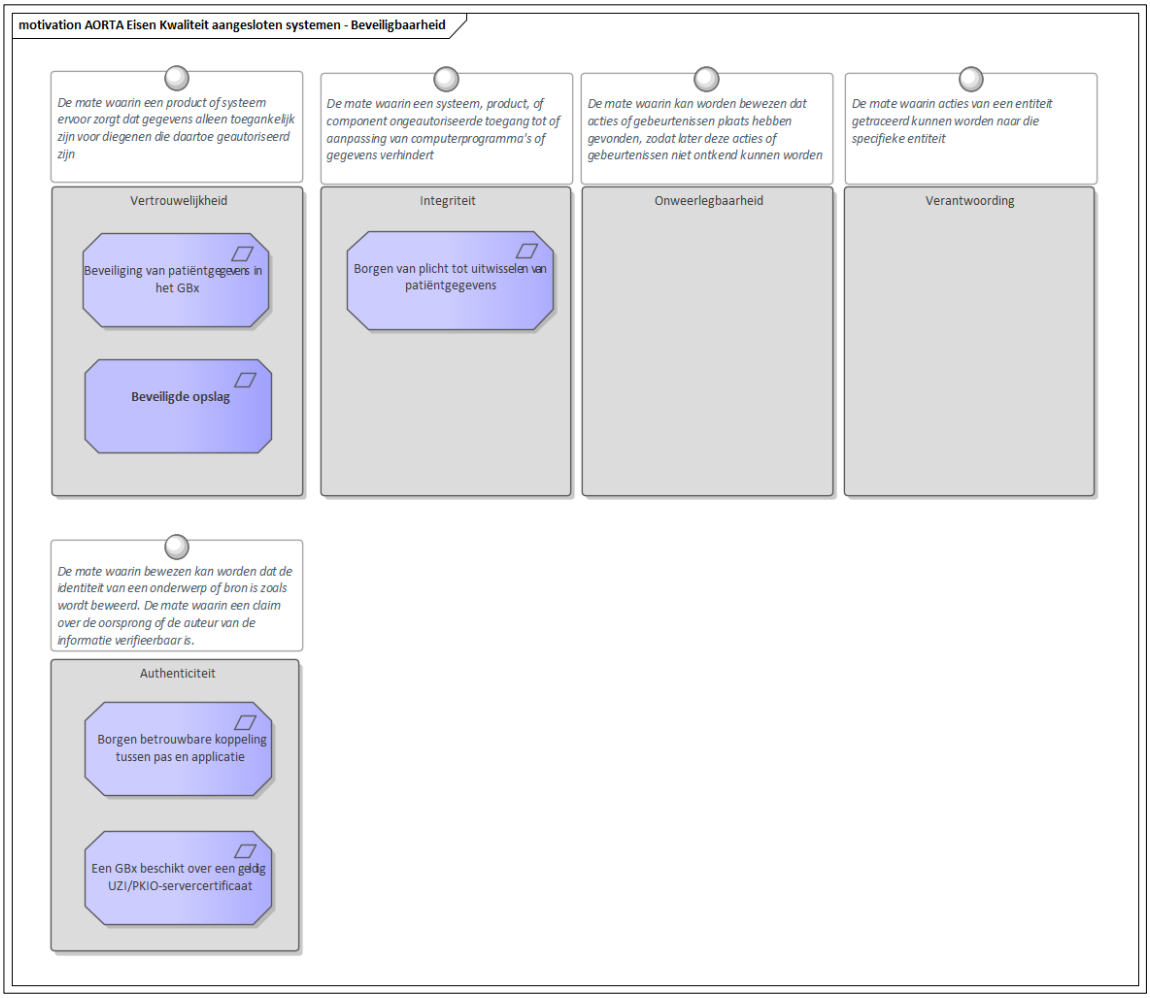


Figure 12 : AORTA Eisen Kwaliteit aangesloten systemen - Beveiligbaarheid

ISO 25010 definieert Beveiligbaarheid als: De mate waarin een product of systeem informatie en gegevens beschermt zodat personen, andere producten of systemen de juiste mate van gegevenstoegang hebben passend bij hun soort en niveau van autorisatie.

Dit schema toont de subcategorieën van Beveilgbaarheid volgens ISO 25010.

2.3.2.1 Beveiligde opslag

Alias: SYS.BVL.e4010.1

Details
Eis: Data die persoonsgegevens bevatten dienen versleuteld en beveiligd te worden opgeslagen. Het gaat hierbij om alle opgeslagen data (bv. logging en backups). **Toelichting bij eis:** In principe moet alle data met persoonsgegevens worden geëncrypted. Dit betreft o.a. gegevens die worden opgeslagen ten behoeve van een autorisatiesessie. Mocht hiervan met het oog op systeemprestaties van afgeweken worden, dan dient dit overlegt te worden met VZVZ.

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

2.3.2.2 Een GBx beschikt over een geldig UZI/PKIO-servercertificaat

Alias: GBX.BVL.e4080 (voorheen GBX.BVL.e4080.1)

Details
Eis: Een GBx dient een {GBx}UZI- of {GBK}{GBP}{GBO} PKIO-servercertificaat te hebben dat op naam staat van de opdrachtgever en is gecertificeerd door een Certificate Authority (CA) onder de root van de Staat der Nederlanden. **Toelichting bij eis:** Deze eis is nodig opdat de authenticiteit van het GBx en de exclusiviteit van getransporteerde gegevens door een Trusted Third Party (TTP) kan worden gewaarborgd.

Vzvz_Moscow: Verplicht (Must)
Vzvz_Req_Verificatie: Aansluittoets
Vzvz_Req_Soort: Functional
Vzvz_Req_Type: Product

2.3.2.3 Borgen van plicht tot uitwisselen van patiëntgegevens

Alias: GBX.BVL.e4070

Details
Eis: Als een GBx voor een systeemrol is aangesloten op de ZIM, moet dat GBx patiëntgegevens in het kader van die systeemrol ook daadwerkelijk uitwisselen onder de regie van de ZIM. **Toelichting bij eis:** Alle aan AORTA deelnemende partijen zijn gebaat bij een zo volledig mogelijk beeld van relevante patiëntgegevens, daarom is het van belang dat aangesloten partijen hun gegevens ook daadwerkelijk beschikbaar maken via AORTA.

Vzvz_Moscow: Verplicht (Must)
Vzvz_Req_Verificatie: Monitoring
Vzvz_Req_Soort: Functional
Vzvz_Req_Type: Product

2.3.2.4 Beveiliging van patiëntgegevens in het GBx

Alias: GBX.BVL.e4060

Details
Eis: Voor een GBx moet zijn gedefinieerd: 1. welke landelijke toepassingen en systeemrollen worden ondersteund en gebruikt; 2. hoe de grenzen van het GBx lopen door de ICT-voorzieningen van de organisatie; 3. hoe en wanneer patiëntgegevens die grenzen kunnen passeren;

4. hoe wordt gewaarborgd dat patiëntgegevens in de dossiers en postbussen niet kunnen lekken naar onbetrouwbare bestemmingen;
5. hoe wordt gewaarborgd dat patiëntgegevens uit onbetrouwbare bronnen niet kunnen terechtkomen in de dossiers en postbussen of de ZIM;
6. hoe wordt gewaarborgd dat anderen dan bevoegde gebruikers geen fysieke toegang tot (delen van) het GBx kunnen krijgen.

Toelichting bij eis:
Deze eis is nodig om te voorkomen dat patiëntgegevens, bijvoorbeeld via een andere applicatie, door willekeurige medewerkers kunnen worden benaderd terwijl de organisatie zijn GBx heeft beveiligd met firewalls, authenticatie- en vertrouwensmiddelen.

Vzvz_Moscow: Verplicht (Must)
Vzvz_Req_Verificatie: Documentverificatie
Vzvz_Req_Soort: Non-Functional
Vzvz_Req_Type: Product

2.3.2.5 Borgen betrouwbare koppeling tussen pas en applicatie

Alias: GBX.BVL.e4050.1

Details
Eis: Een GBx moet zodanig zijn ingericht dat: 1. passen met SHA-256-certificaten gelezen en gebruikt kunnen worden; 2. paslezers gekoppeld zijn aan werkplekken van gebruikers; 3. de PIN-code die ten behoeve van een authenticatiemiddel wordt ingetoetst op een werkplek, exclusief wordt aangeboden aan de gekoppelde paslezer, 4. {GBx} alle gegevens in berichten die ten behoeve van een gebruiker worden ontvangen exclusief aan die gebruiker worden gepresenteerd; 5. {GBK} alle gegevens in HL7-berichten die ten behoeve van een patiëntopdracht worden ontvangen exclusief gekoppeld worden aan de betreffende patiëntopdracht. 6. geborgd wordt dat: • {GBx} het in het bericht vermelde UZI-nummer en de rolcode van de auteur overeenkomen met de UZI-pashouder die het bericht heeft geïnitieerd; • {GBK} het in het bericht vermelde certificaatnummer en CA van de auteur overeenkomen met de PKIO-pashouder die het bericht heeft geïnitieerd; • {GBx} de auteur inderdaad is gemandateerd door de in het bericht vermelde (eind)verantwoordelijke, of dezelfde persoon is; • {GBx} de in het bericht vermelde URA van auteur, (eind)verantwoordelijke en zorginstelling aan elkaar gelijk zijn; • {GBK} de in het bericht vermelde instellingsindicatie van de auteur het klantenloket is; • {GBK} de instelling van de verantwoordelijke niet ingevuld is.

Vzvz_Moscow: Verplicht (Must)
Vzvz_Req_Verificatie: Audit
Vzvz_Req_Soort: Functional
Vzvz_Req_Type: Product

2.3.3 Prestatie-efficiëntie

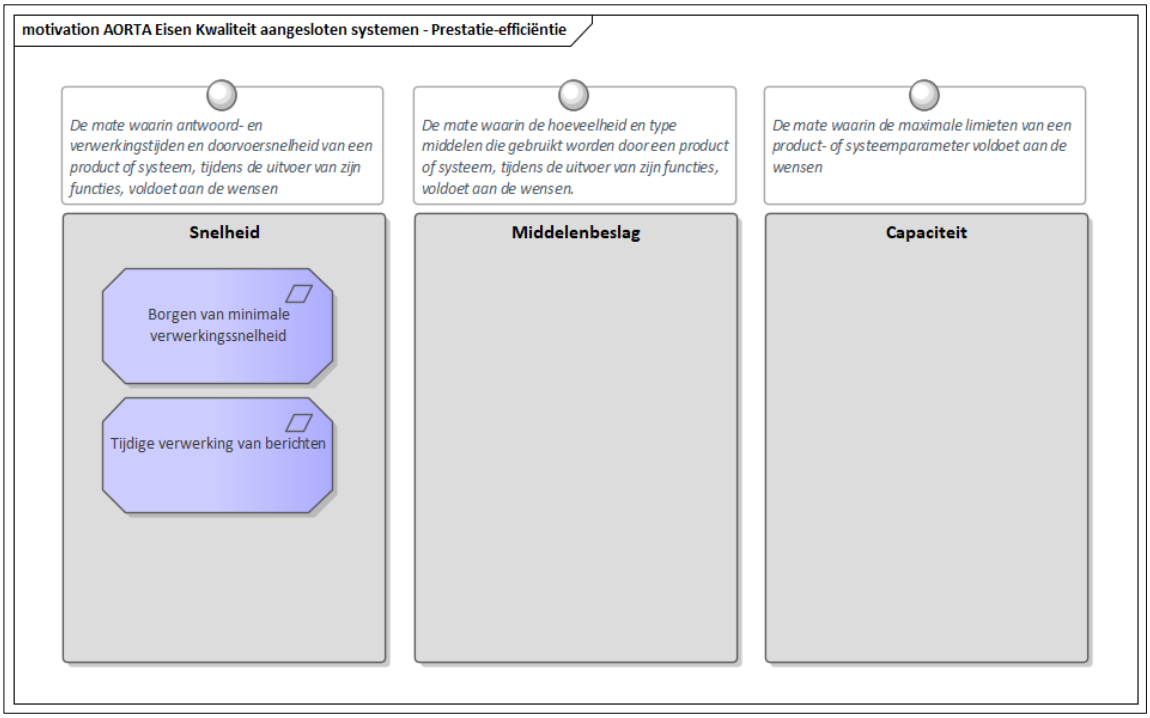


Figure 13 : AORTA Eisen Kwaliteit aangesloten systemen - Prestatie-efficiëntie

2.3.3.1 Tijdige verwerking van berichten

Alias: GBX.PST.e4015

Details
Eis: Een GBx dient voor gebruikersinteracties, na het commando van een gebruiker of een daaropvolgende ontvangst van een bericht van de ZIM, binnen 0,3 seconden het aangegeven resultaat te hebben bereikt. **Toelichting bij eis:** Deze eis is nodig om te voorkomen dat een zorgaanbieder bij zijn GZN of het LSP gaat klagen over te lange responstijden terwijl de oorzaak misschien ligt bij bijv. een eigen computer die in beslag wordt genomen door andere toepassingen of een lokaal netwerk met onvoldoende bandbreedte. Deze eis betekent voor de zorgaanbieder dat hij zijn XIS-applicatie moet installeren op ICT-voorzieningen met voldoende prestaties. Zonodig moeten bijv. de computers worden ingeregeld op de behoefte van deze XIS-applicatie, bijv. als ze ook worden gebruikt voor andere toepassingen. Wellicht kan zijn XIS-leverancier helpen bij het selecteren en inregelen van ICT-voorzieningen. Indien de zorgaanbieder een ASP-leverancier heeft geselecteerd voor zijn XIS, kan hij dit voor de centrale ICT-voorzieningen wellicht overlaten aan die ASP-leverancier, maar moeten de lokale werkplekken niet vergeten worden.

Vzvz_Moscow: Verplicht (Must)
Vzvz_Req_Verificatie: Monitoring
Vzvz_Req_Soort: Non-Functional
Vzvz_Req_Type: Product

2.3.3.2 Borgen van minimale verwerkingssnelheid

Alias: GBX.PST.e4010.1

Details
Eis: Een GBx dient minimaal de hieronder genoemde snelheden te halen voor de hieronder genoemde interactiemechanismen. **Interactiemechanisme Minimale verwerkingssnelheid** Sturen van gegevens 100 kb/sec Opvragen van gegevens 100 kb/sec Een GBx dient een zodanige capaciteit te hebben voor het beantwoorden en ontvangen van berichten van de ZIM dat het kan voldoen aan de gestelde verwerkingssnelheden. Indien dat als gevolg van een onverwacht hoge piekbelasting tijdelijk niet mogelijk is, dan prevaleren de eisen inzake beschikbaarheid boven de eisen inzake verwerkingssnelheid. **Toelichting bij eis:** Deze eis is nodig opdat een XIS-applicatie tijdig berichten van de ZIM kan verwerken/beantwoorden ten behoeve van andere zorgaanbieders, ook als de belasting zodanig hoog is, dat de volgende berichten binnenkomen terwijl de vorige nog niet verwerkt/beantwoord zijn. Deze eis betekent voor de organisatie dat de applicatie is geïnstalleerd op ICT-voorzieningen met voldoende capaciteit om een variabele belasting van berichten vanwege de ZIM te kunnen verwerken. Omdat de exacte belasting per GBx flink kan verschillen moet iedere organisatie zelf een inschatting maken van de benodigde capaciteit en ervoor zorgen dat het GBx die belasting aankan. De waarden van 100 kb/sec kunnen verschillen per gebruikte technologie. Voor de HL7v3-berichten gelden de waarde van 100 kb/sec. Met betrekking tot FHIR dienen deze waarden nog afgestemd te worden met de diverse leveranciers. Deze waarden dienen vastgesteld te worden na afloop van de PoC.

Vzvz_Moscow: Verplicht
Vzvz_Req_Verificatie: Monitoring
Vzvz_Req_Soort: Non-Functional
Vzvz_Req_Type: Product

2.3.4 Uitwisselbaarheid

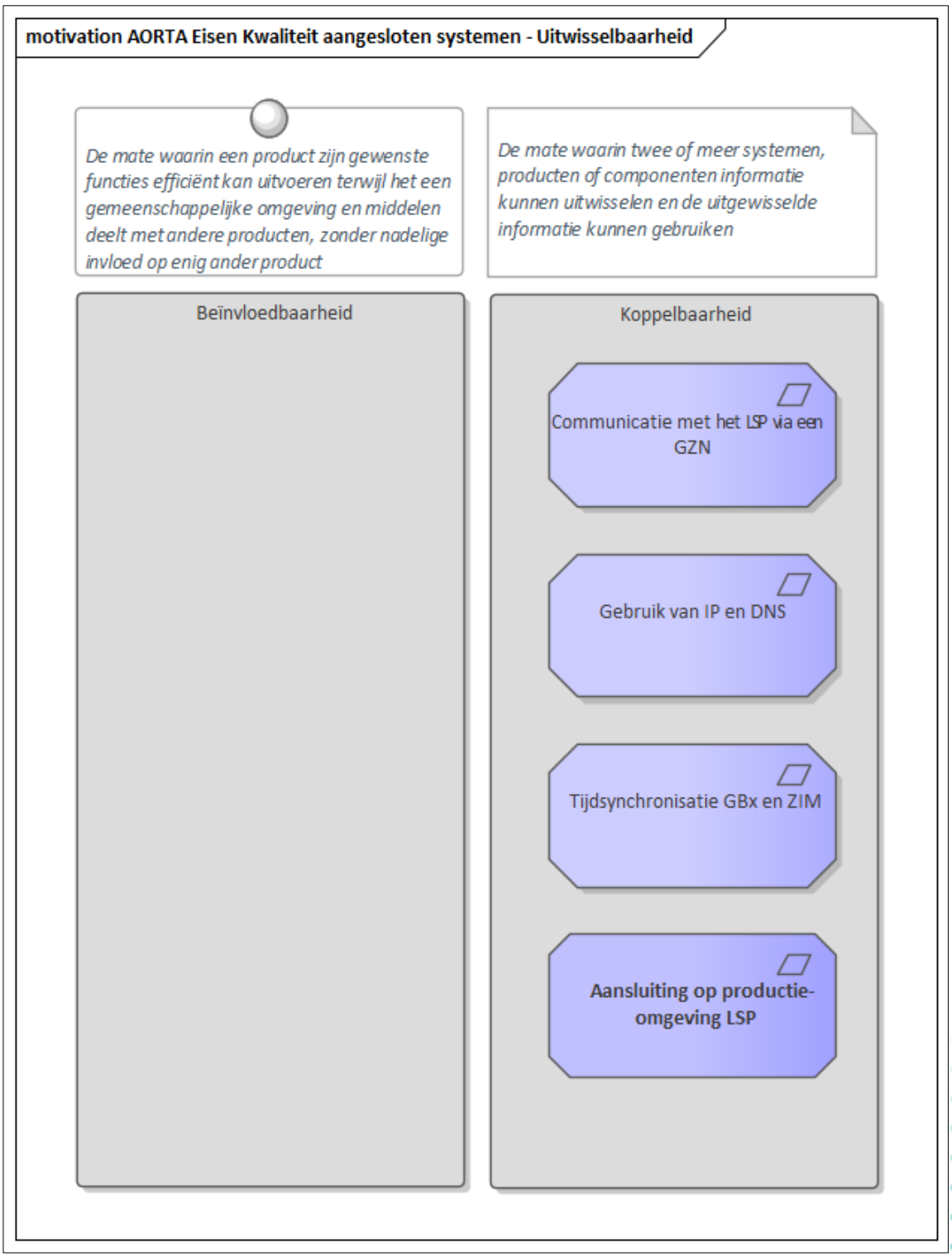


Figure 14 : AORTA Eisen Kwaliteit aangesloten systemen - Uitwisselbaarheid

ISO 25010 definieert Uitwisselbaarheid als: De mate waarin een product, systeem of component informatie uit kan wisselen met andere producten, systemen of componenten, en/of het de gewenste functies kan uitvoeren terwijl het dezelfde hard- of software-omgeving deelt.
Dit diagram toont de subcategorieën zoals gedefinieerd door ISO 25010.

2.3.4.1 Aansluiting op productie-omgeving LSP

Alias: GBX.CON.e4120

Details
Eis: GBZ-beheerder moet er namens de eigenaar van het GBZ op toezien dat uitsluitend productiesystemen gekoppeld worden aan de productie-omgeving van het LSP. Overtredingen van deze eis zullen gemeld worden aan de eigenaar van het GBZ. **Toelichting bij eis:** Vanwege mogelijke beveiligingsrisico's en kwaliteitgaranties in de keten mogen er alleen GBZ-en met een geaccepteerde XIS-applicatie aansluiten op de productie-omgeving van het LSP . Bij het niet naleven van bovenstaande eis behoudt VZVZ zich het recht voor op aanvullende sancties.

Vzvz_Moscow: Verplicht
Vzvz_Req_Verificatie: Monitoring
Vzvz_Req_Soort: Non-Functional
Vzvz_Req_Type: Product

2.3.4.2 Tijdsynchronisatie GBx en ZIM

Alias: GBX.CON.e4030.2

Details
Eis: Een GBx dient NTP te gebruiken voor tijdsynchronisatie met de ZIM. De tijdklok van een GBx mag niet meer dan een halve seconde afwijken van de tijdklok van de ZIM. **Toelichting bij eis:** Deze eis is nodig om te voorkomen dat de tijdklok van het GBx gaat afwijken van de tijdklok van de ZIM. Voor eenzelfde interactie tussen een GBx en de ZIM moeten beide systemen immers dezelfde tijdstempels loggen. Dit is belangrijk wanneer de toezichthouder of patiënt een geval van vermeend onrechtmatige uitwisseling van patiëntgegevens wil onderzoeken en daartoe zowel de lokale toegangslog van het GBx als de centrale toegangslog van het LSP wil raadplegen. Deze eis betekent voor de organisatie dat er binnen het GBx een NTP-client is geïnstalleerd en dat deze is afgestemd op de NTP-server van de ZIM. Ook is het mogelijk dat de GZN een gezamenlijke NTP-client beheert voor alle aangesloten zorgaanbieders en op een andere wijze klaarspeelt dat de tijdklok van hun GBx'en gelijk lopen met die van de ZIM. Deze eis betekent voor de organisatie dat het GBx periodiek moet synchroniseren tegen een NTP-server om synchroon te blijven met de ZIM.

Vzvz_Moscow: Verplicht (Must)
Vzvz_Req_Verificatie: Monitoring
Vzvz_Req_Soort: Non-Functional
Vzvz_Req_Type: Product

2.3.4.3 *Gebruik van IP en DNS*

Alias: GBX.CON.e4020, GBX.CON.e4020.1, GBX.CON.e4020.2

Details
Eis: Een GBx moet bereikbaar zijn voor de ZIM: 1. {GBx}{GBO} via het IP-adres dat is toegekend aan het GBx en dat is verkregen door DNS-vertaling van de hostnaam van dat GBx; 2. {GBK} via het IP-adres dat door het LSP is toegekend aan het GBK en dat is verkregen door DNS-vertaling van de hostnaam van dat GBK; 3. {GBP} via het IP-adres en de fully qualified domain name (FQDN) die door het LSP zijn toegekend aan het GBP en waarvoor het LSP de DNS-vertaling biedt. De ZIM moet bereikbaar zijn vanuit een GBx via het IP-adres van de operationele ZIM, dat is verkregen door DNS-vertaling van de hostnaam van de ZIM. Voor de DNS-vertaling geldt dat: 1. de hostnaam een maximale time-to-live (TTL) heeft voor verversing van de cache; 2. het IP-adres van de ZIM zich binnen een vooraf overeengekomen range bevindt die altijd gerouteerd moet worden naar de GZN; 3. een systeem vanuit de applicatie alleen benaderd mag worden op de FQDN. Vertaling naar IP-adres wordt door de DNS uitgevoerd. Een GBx mag de volgende IP-adressen niet intern gebruiken: 1. het IP-adres dat door het LSP is uitgegeven voor het GBx als geheel, 2. de IP-adressen die zijn gereserveerd voor de ZIM, 3. de IP-adressen uit het landelijke IP-nummerplan van het LSP. **Toelichting bij eis:** Deze eis is nodig om ervoor te zorgen dat FQDN en IP-adressen op een juiste wijze worden ingesteld. Deze eis is ook nodig voor het gebruik van een ZIM op twee operationele locaties en om IP-netwerkconflicten te voorkomen. Deze eis betekent voor de organisatie dat die voor zijn GBx/GBO een FQDN moet krijgen van zijn GZN en deze laten registreren bij het LSP of bij SIDN. De GZN zal daaraan een IP-adres toekennen. De organisatie moet het toegekende IP-adres tenslotte (laten) configureren in zijn netwerkapparatuur binnen zijn GBx. Deze eis betekent dat een applicatie een ZIM expliciet op naam benadert en dat systemen geconfigureerd moeten worden voor het gebruik van DNS. Door middel van DNS-resolving kan voor het GBx transparant gebruik gemaakt worden van de operationele ZIM op locatie 1 of locatie 2.

Vzvz_Moscow: Verplicht (Must)
Vzvz_Req_Verificatie: Aansluittoets
Vzvz_Req_Soort: Non-Functional
Vzvz_Req_Type: Product

2.3.4.4 *Communicatie met het LSP via een GZN*

Alias: GBX.CON.e4010, GBX.CON.e4010.1

Details
Eis: Een GBx dient via een DCN van een gekwalificeerde GZN te communiceren met het LSP. **Toelichting bij eis:** Organisaties kunnen bij VZVZ verifiëren of een netwerkaanbieder over een GZN-kwalificatie beschikt.

Vzvz_Moscow: Verplicht (Must)
Vzvz_Req_Verificatie: Aansluittoets
Vzvz_Req_Soort: Non-Functional
Vzvz_Req_Type: Product

2.4 AORTA Eisen Kwaliteit Applicatie

2.4.1 Beveiligbaarheid

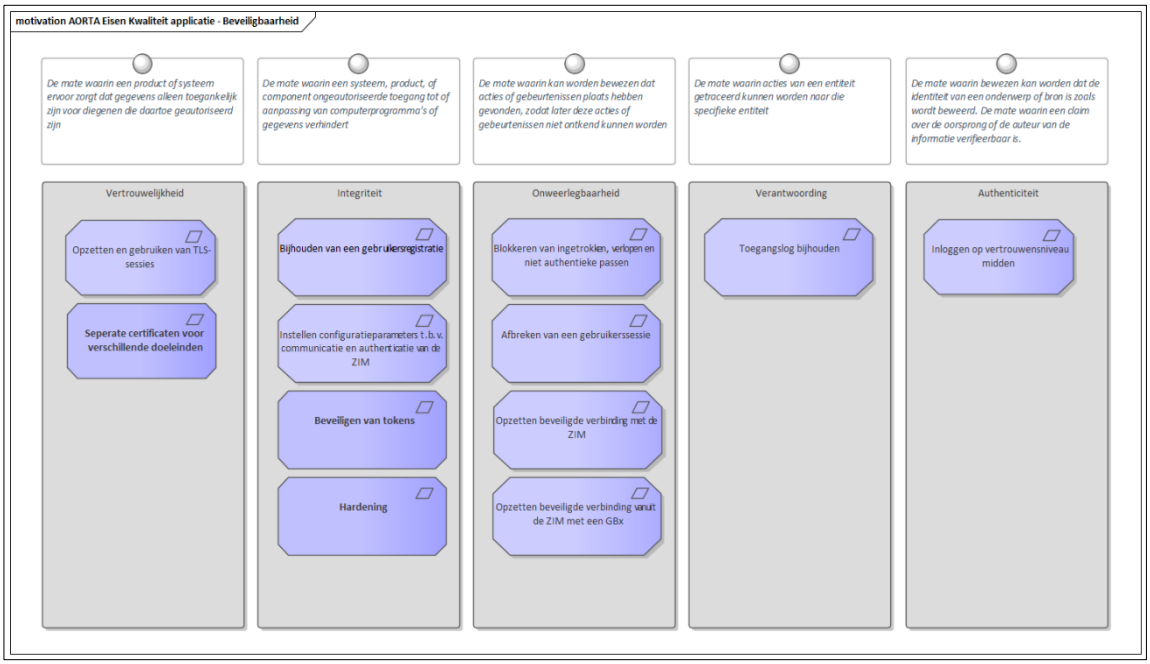


Figure 15 : AORTA Eisen Kwaliteit applicatie - Beveiligbaarheid

ISO 25010 definitieert Beveiligbaarheid als: De mate waarin een product of systeem informatie en gegevens beschermt zodat personen, andere producten of systemen de juiste mate van gegevenstoegang hebben passend bij hun soort en niveau van autorisatie.

2.4.1.1 Hardening

Alias: SYS.BVL.e4065

Details
Eis: Er dient hardening op de diverse systeemlagen te worden toegepast. Het gaat hierbij om hardening op het niveau van operating system, middleware en database. Alle systeemparameters dienen zodanig te zijn ingesteld dat met behoud van de gewenste functionaliteit een zo hoog mogelijk niveau van beveiliging bestaat. **Toelichting bij eis:** De intentie van deze eis is dat datgene wordt gedaan dat in de markt onder de gangbare maatregelen wordt gerekend op het gebied van hardening. Hierbij moet er uiteraard een afweging worden gemaakt tussen gebruiksvriendelijkheid en veiligheid.

Vzvz_Moscow: Verplicht
Vzvz_Req_Verificatie: Audit
Vzvz_Req_Soort: Non-Functional
Vzvz_Req_Type: Product

2.4.1.2 Opzetten beveiligde verbinding vanuit de ZIM met een GBx

Alias: GBX.CON.e4090.2

Details
Eis: Het GBx dient voor het landelijk uitwisselen van patiëntgegevens een TLS-sessie met de ZIM met de volgende kenmerken te accepteren: 1. tweezijdige authenticatie met behulp van het UZI-servercertificaat van het GBZ en het servercertificaat van de ZIM, 2. tijdelijke sleutels die elke 5 minuten ververst worden, 3. gebruikmakend van Cipher Suites die door het NCSC minimaal worden gekenmerkt als goed en tevens worden ondersteund door de ZIM.Voor encryptie moet altijd de sterkste vorm als eerste worden geprobeerd, 4. een maximale sessieduur van 8 uur, 5. een ten hoogste ongebruikte TLS-sessie van 15 minuten. **Toelichting bij eis:** Dit is nodig opdat de ZIM een voldoende hoog beveiligingsniveau kan afdwingen bij het opzetten van een TLS-sessie met een GBx. Dit betekent voor de zorgaanbieder dat hij of zijn XIS-leverancier de bovenstaande parameters moet instellen in de TLS-library in de betrokken XIS-applicatie(s) en/of de eventuele communicatieserver.

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

2.4.1.3 Seperate certificaten voor verschillende doeleinden

Alias: GBX.BVL.e4100.1

Details
Eis: Een GBZ dient voor transportbeveiliging een ander servercertificaat te gebruiken dan voor berichtauthenticatie. De verschillende certificaten horen daarbij in verschillende componenten ondergebracht te zijn in de architectuur van het XIS. **Toelichting bij eis:** Deze eis is conform NIST SP 800-57 norm; iedere XIS zou aparte sleutels moeten hanteren voor verschillende doeleinden. Deze eis impliceert dat een XIS een ander certificaat moet gebruiken voor TLS dan voor het ondertekenen van transactietokens. De applicaties van zorgaanbiedertype Ziekenhuis en Zelfstandig Behandelcentra (ZBC) dienen gebruik te maken van twee aparte servercertificaten zoals opgenomen in de eis. Alle overige zorgaanbiedertypes kunnen volstaan met applicaties waarbij gebruik wordt gemaakt van één servercertificaat. Indien door de

zorgaanbieder zelf gewenst (bijvoorbeeld uit netwerk technische praktische overwegingen) dan zijn twee aparte server certificaten uiteraard toegestaan. **Condities:** De verplichting voor het gebruik van een separaat certificaat is afhankelijk van de grootte van de zorgaanbiederorganisatie. Deze eis zal in overleg met VZVZ wel of niet toegepast dienen te worden.

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

2.4.1.4 Opzetten en gebruiken van TLS-sessies

Alias: GBX.CON.e4070.2

Details
Eis: Het GBx moet na het beschikbaar worden voor de ZIM: • verzoeken van de ZIM voor het opzetten van nieuwe TLS-sessies honoreren ten behoeve van berichtuitwisseling voor andere zorgaanbieders, • {GBx}{GBK}{GBO} voor gebruikers die landelijk patiëntgegevens willen uitwisselen, een of meer TLS-sessies met de ZIM (her)gebruiken voor berichtuitwisseling als gevolg van gebruikersfuncties. **Toelichting bij eis:** Deze eis is nodig opdat een GBx beveiligd kan communiceren met de ZIM volgens bewezen technologie op eigen initiatief en op initiatief van de ZIM.

Vzvz_Moscow: Verplicht (Must)
Vzvz_Req_Verificatie: Acceptatietest
Vzvz_Req_Soort: Functional
Vzvz_Req_Type: Product

2.4.1.5 Beveiligen van tokens

Alias: GBX.FBH.e4070.1

Details
Eis: Tokens moeten behandeld worden als medische gegevens (volgens de NEN7510). Binnen de organisatie moet er een speciale rol toegewezen (en geautoriseerd) worden om toegang te krijgen tot de diverse opgeslagen tokens (inschrijf- en mandaattoken). **Toelichting:** Ten behoeve van beheermaatregelen moet het mogelijk zijn om toegang te krijgen tot de beveiligde container waar de tokens zijn opgeslagen. Toegang tot deze tokens moet vanwege het voorkomen van misbruik van de tokens beperkt zijn tot daarvoor aangewezen rollen.

Vzvz_Moscow: Verplicht
Vzvz_Req_Verificatie: Audit
Vzvz_Req_Soort: Functional

Vzvz_Req_Type: Product

2.4.1.6 Instellen configuratieparameters t.b.v. communicatie en authenticatie van de ZIM

Alias: GBX.FBH.e4050.3

Details
Eis: De GBx-beheerder moet de volgende configuratieparameters in het GBx kunnen instellen: 1. URI en hostnaam van de ZIM, 2. applicatie-id van de eigen applicatie, 3. applicatie-id van het productieschakelpunt waarop kan worden aangesloten. **Toelichting bij eis:** Dit is nodig opdat een GBx deze parameters kan gebruiken bij de HTTP-communicatie met en authenticatie van de ZIM. De in het GBx ingestelde waarden komen overeen met de in het applicatieregister van de ZIM geregistreerde gegevens.

Vzvz_Moscow: Verplicht (Must)
Vzvz_Req_Verificatie: Acceptatietest
Vzvz_Req_Soort: Functional
Vzvz_Req_Type: Product

2.4.1.7 Bijhouden van een gebruikersregistratie

Alias: GBX.FBH.e4030

Details
Eis: Binnen het GBx dient te worden bijgehouden welke UZI-passen worden toegelaten voor gebruik. Deze gebruikersregistratie is uitsluitend toegankelijk voor gebruikers van de gastheerinstelling, na authenticatie op basis van een sterk authenticatiemiddel (2 factorauthenticatie bijvoorbeeld via een UZI-pas) van diezelfde gastheerinstelling. **Toelichting bij eis:** Dit is nodig om te voorkomen dat een willekeurig persoon de gebruikersregistratie kan aanpassen. Deze bevoegdheid komt bij een specifiek persoon te liggen. Dit betekent voor de zorgaanbieder dat hij moet zorgen dat de bovenstaande rol van autorisatiebeheerder door een van zijn medewerkers wordt ingevuld.

Vzvz_Moscow: Verplicht (Must)
Vzvz_Req_Verificatie: Acceptatietest
Vzvz_Req_Soort: Functional
Vzvz_Req_Type: Product

2.4.1.8 Opzetten beveiligde verbinding met de ZIM

Alias: GBX.CON.e4080.5

Details
Eis:

Het GBx dient voor het landelijk uitwisselen van patiëntgegevens een TLS-sessie met de ZIM met de volgende kenmerken op te zetten:

1. tweezijdige authenticatie met behulp van het servercertificaat van de ZIM en

* (indien tokenauthenticatie) het servercertificaat van het GBx voor vertrouwensniveau midden
* het servercertificaat van het GBx voor vertrouwensniveau laag {GBK} en midden

- tijdelijke sleutels die elke 5 minuten ververst worden door middel van TLS Secure Renegotiation;
- gebruikmakend van Cipher Suites die door het NCSC minimaal worden gekenmerkt als goed;
- gebruikmakend van de sterkste cipher suite die gedeeld wordt met de ZIM;
- gebruikmakend van de hoogste toegestane TLS-versie die door beide partijen wordt ondersteunt;
- een ongebruikte TLS-sessie van maximaal 15 minuten.

Toelichting bij eis:
Dit is nodig opdat een GBx een voldoende hoog beveiligingsniveau kan afdwingen bij het opzetten van een TLS-sessie met de ZIM.
Dit betekent voor de organisatie dat hij of zijn XIS-leverancier de bovenstaande parameters moet instellen in de TLS-library in de betrokken applicatie(s) en/of de eventuele communicatieserver. Het GBx is niet in staat te controleren of de ZIM daadwerkelijk het (server)certificaat van de GBx opvraagt, maar mag er impliciet van uitgaan dat dit gebeurt en dat de ZIM het certificaat ook controleert. Hiermee wordt tweezijdige authenticatie bewerkstelligd.

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

2.4.1.9 Toegangslog bijhouden

Alias: GBX.LOG.e4015.1

Details
Eis: Het systeem moet de volgende berichtuitwisselingen loggen: 1. Ontvangen opvraagberichten en de daarop verzonden antwoorden; 2. Verzonden opvraagberichten en daarop verkregen antwoorden; 3. Verzonden opdrachtberichten en kennisgevingberichten. De log bevat per berichtuitwisseling tenminste: 1. de identiteit van de patiënt/cliënt (BSN) 2. identiteit van de opvragende/versturende en bestemde organisatie 3. de functie en identiteit van de opvragende of versturende zorgverlener of medewerker of patiënt. 4. type van de uitgevoerde gebruikersinteractie 5. het tijdstip en tijdzone (ten opzichte van UTC) van de gebruikersinteractie 6. de bericht-id van het ontvangen (opvraag- of bevestig-) bericht 7. de bericht-id van het verzonden (oplever- of opdracht-) bericht 8. de gegevenssoorten of contextcodes van de verzonden en ontvangen patiëntstukken; 9. een indicatie van eventueel opgetreden foutsituaties met betrekking tot het ontvangen en verzenden van de berichten. **Toelichting bij eis:** Dit is nodig opdat aan de hand van de berichtuitwisseling precies achterhaald kan worden:

- {GBx}{GBO}wat voor soort patiëntstukken wanneer zijn opgevraagd door welke zorgverlener/medewerker van welke andere zorgaanbieder;
- {GBK} wat voor soort opvragingen, opdrachten en kennisgevingen wanneer zijn verzonden resp. ontvangen door welke klantenloketmedewerker;
- wat voor soort patiëntstukken wanneer zijn toegestuurd aan welke andere zorgaanbieder of ZIM;
- welke inhoud die patiëntstukken precies hadden;
- wat voor soort patiëntstukken wanneer zijn opgevraagd door welke patiënt vanuit welke organisatie.

Dit betekent voor de zorgaanbieder dat hij of zijn XIS-leverancier deze berichtenlogfunctie moet inbouwen in de betrokken XIS-applicatie(s) of de eventuele communicatieserver.

Vzvz_Moscow: Verplicht (Must)
Vzvz_Req_Verificatie: Acceptatietest
Vzvz_Req_Soort: Functional
Vzvz_Req_Type: Product

2.4.1.10 Afbreken van een gebruikerssessie

Alias: GBX.IDA.e4090.1

Details
Eis: Het systeem moet een gebruikerssessie voor het landelijk uitwisselen van patiëntgegevens op vertrouwensniveau laag of midden afsluiten: 1. op commando van de gebruiker (zoals een muisklik of toetsencombinatie); 2. door uitnemen van het vertrouwensmiddel door de zorgverlener/medewerker; 3. wanneer de applicatie gedurende maximaal 60 minuten niet is gebruikt. Deze tijd dient instelbaar te zijn in het syteem, maar mag niet de 60 minuten overschrijden; 4. wanneer de sessie gedurende 1 uur open staat; 5. IP-adres van gebruiker gedurende een sessie wijzigt. **Toelichting bij eis:** Dit is nodig opdat een gebruiker zelf zijn gebruikerssessie kan uitloggen met de zekerheid dat niemand anders zijn sessie kan voortzetten en vervolgens zijn bevoegdheden kan misbruiken. Daarnaast is deze eis nodig om te tegen te gaan dat een in onbruik geraakte sessie door een onbevoegde kan worden misbruikt.

Vzvz_Moscow: Verplicht (Must)
Vzvz_Req_Verificatie: Acceptatietest
Vzvz_Req_Soort: Functional
Vzvz_Req_Type: Product

2.4.1.11 Blokkeren van ingetrokken, verlopen en niet authentieke passen

Alias: GBX.IDA.e4085.2

Details
Eis: Het GBx dient het starten van een gebruikersessie op vertrouwensniveau midden te weigeren indien: 1. de geldigheidstermijn van het transactietoken is verlopen of nog niet is aangevangen; 2. het transactietoken niet correct is ondertekend; 3. het certificaat, waarmee het transactietoken is getekend, op een geldige lijst staat van ingetrokken certificaten (CRL) van het UZI-register; 4. het transactietoken is geweigerd door het LSP.

Toelichting bij eis:
Deze eis is conform de regels van PKI Overheid. Er moet voorkomen worden dat een GBZ toegang geeft als gevolg van een ongeldige UZI-pas.

Alleen een gebruiker die een UZI-pas heeft en de pincode weet, kan een geldig transactietoken genereren.

Vzvz_Moscow: Verplicht (Must)
Vzvz_Req_Verificatie: Acceptatietest
Vzvz_Req_Soort: Functional
Vzvz_Req_Type: Product

2.4.1.12 Inloggen op vertrouwensniveau midden

Alias: GBX.IDA.e4080.3

Details

Eis:
Het systeem moet een gebruiker de mogelijkheid bieden een gebruikerssessie op vertrouwensniveau midden te starten door:

1. {GBx}{GBK}het invoeren van zijn vertrouwensmiddel op de werkplek en het invoeren van de bijbehorende toegangscode;
2. {GBP} zich op niveau DigiD-midden te authenticeren.

{GBx} Een GBx dient hierbij een UZI-pas toe te laten indien:

1. de UZI-pas is vastgelegd in de gebruikerstabel (zie ook eis GBX.FBH.e4030);
2. het passen betreft die zijn uitgegeven onder de op dat moment geldende certificaatboom of –bomen. (SHA-256).

Hierbij dient de applicatie te controleren of het certificaat op de pas niet op de CRL staat.

{GBK} Een GBK dient hierbij een PKIO-pas toe te laten indien de betreffende medewerker geautoriseerd is voor toegang tot de GBK-applicatie en te weigeren in de overige gevallen.

Toelichting bij eis:
Dit is nodig opdat gebruikers in staat worden gesteld tot het landelijk uitwisselen van gegevens op vertrouwensniveau midden.

VZVZ levert gratis generiek tooling in de vorm van Zorg-ID om de implementatie van het authenticeren met de UZI-pas te ondersteunen.

Vzvz_Moscow: Verplicht (Must)
Vzvz_Req_Verificatie: Audit
Vzvz_Req_Soort: Functional
Vzvz_Req_Type: Product

2.4.2 Uitwisselbaarheid

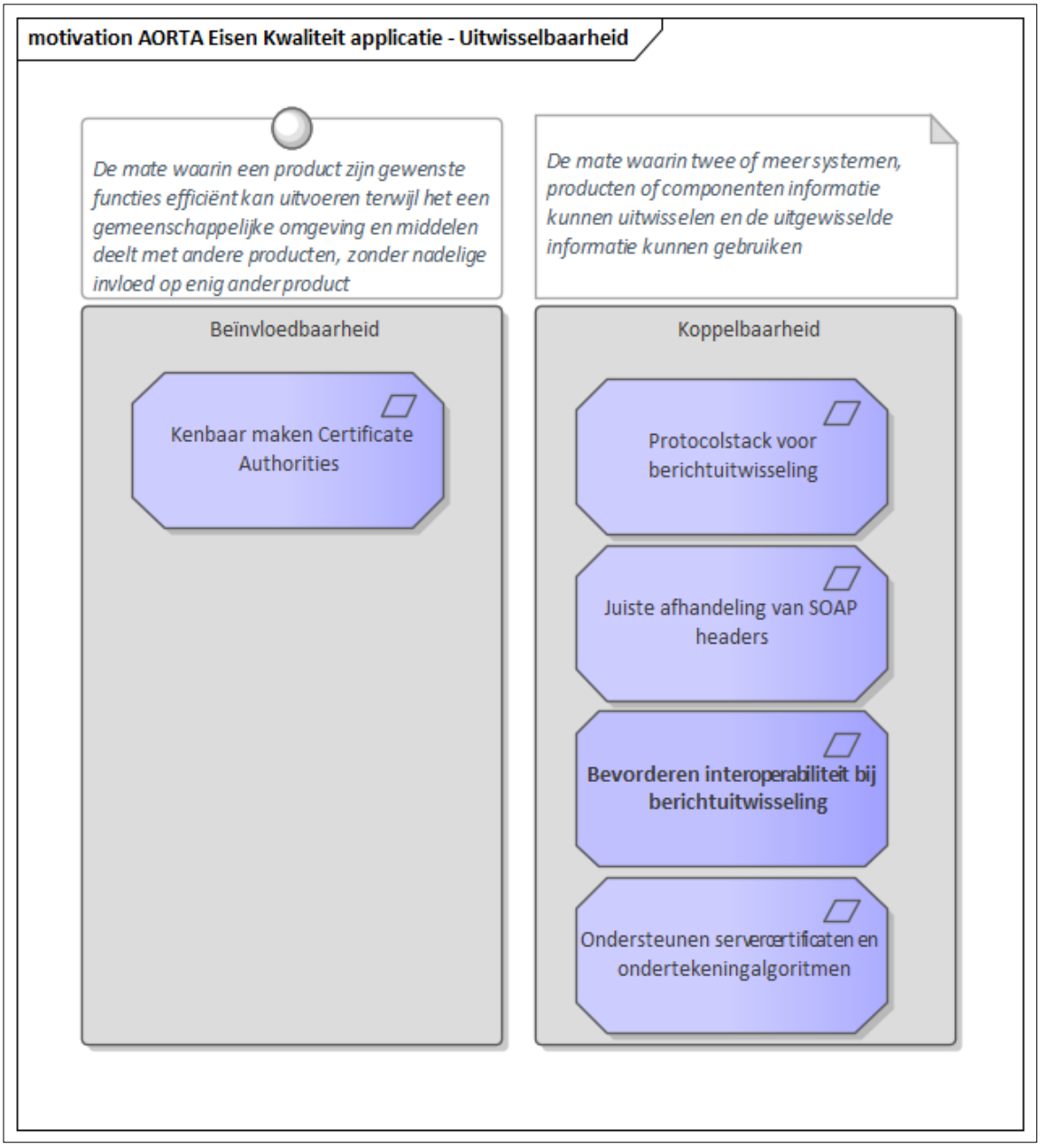


Figure 16 : AORTA Eisen Kwaliteit applicatie - Uitwisselbaarheid

ISO 25010 definieert Uitwisselbaarheid als: De mate waarin een product, systeem of component informatie uit kan wisselen met andere producten, systemen of componenten, en/of het de gewenste functies kan uitvoeren terwijl het dezelfde hard- of software-omgeving deelt.

2.4.2.1 Kenbaar maken Certificate Authorities

Alias: GBX.CON.e4100

Details
Eis:

Het GBx dient alleen de keten van Certificate Authorities (CA's) van het GBX-certificaat kenbaar te maken aan de ZIM in het “certificate request” bericht van de TLS-handshake, waaronder ook het stamcertificaat (Root CA) van de keten. **Toelichting bij eis:** Dit is nodig opdat een GBx beperkt kenbaar maakt welke CA's het vertrouwt. Dit betekent voor de zorgaanbieder dat hij of zijn XIS-leverancier selectief om moeten gaan met het aantal CA's waarmee de betrokken XIS-applicatie(s) en/of de eventuele communicatieserver worden opgezet.

Vzvz_Moscow: Verplicht (Must)
Vzvz_Req_Verificatie: Aansluittoets
Vzvz_Req_Soort: Functional
Vzvz_Req_Type: Product

2.4.2.2 Ondersteunen servercertificaten en ondertekeningalgoritmen

Alias: GBX.CON.e4110.2

Details
Eis: Het GBx dient UZI/PKIo-servercertificaten van de (verschillende) generatie(s) te ondersteunen zoals beschikbaar wordt gesteld door het UZI-Register. Er moet gebruik worden gemaakt van het SHA-256 ondertekeningsalgoritme. **Toelichting bij eis:** Het UZI-register geeft UZI-servercertificaten uit onder één of meerdere certificaatbomen. In het geval er onder diverse certificaatbomen UZI-servercertificaten wordt uitgegeven, is het zaak om alle servercertificaten uitgegeven onder de diverse certificaatbomen te kunnen ondersteunen. Een GBX-communicatieserver dient te zijn ingericht op het ondertekeningalgoritme SHA-256.

Vzvz_Moscow: Verplicht (Must)
Vzvz_Req_Verificatie: Monitoring
Vzvz_Req_Soort: Functional
Vzvz_Req_Type: Product

2.4.2.3 Bevorderen interoperabiliteit bij berichtuitwisseling

Alias: GBX.CON.e4066

Details
Eis: Het GBX volgt voor berichtuitwisseling als bedoeld in eis GBX.CON.e4060 de WS-I Basic Profile 1.0 specificaties.

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

2.4.2.4 *Juiste afhandeling van SOAP headers*

Alias: GBX.CON.e4065

Details
Eis: Het GBx volgt voor de afhandeling van SOAP-headers in berichten de aanwijzingen zoals beschreven in implementatiehandleiding Berichttransport. **Toelichting bij eis:** Het gaat hierbij onder andere om het op de juiste wijze in acht nemen van SOAP-headerattributen 'mustUnderstand' and 'actor'.

Vzvz_Moscow: Verplicht (Must)
Vzvz_Req_Verificatie: Acceptatietest
Vzvz_Req_Soort: Functional
Vzvz_Req_Type: Product

2.4.2.5 *Protocolstack voor berichtuitwisseling*

Alias: GBX.CON.e4060.2

Details
Eis: Het GBx dient voor berichtuitwisseling met de ZIM de volgende protocolstack te gebruiken: • HL7v3 • SOAP v1.1 • SAML 2.0 • HTTP v1.1 • TLS v1.2/TLS v1.3 • TCP • IPv4 **Toelichting bij eis:** Het is niet toegestaan om een lagere protocolversie te hanteren dan die in deze protocolstack vermeld is, zoals bv SSLv2 en SSLv3. Voor de versie van TLS geldt dat de beveiligingsrichtlijnen van NCSC worden gevolgd indien redelijkerwijs mogelijk. Alle deelnemers dienen minimaal TLS 1.2 te ondersteunen, tenzij het ook mogelijk is om TLS 1.3 te ondersteunen. Bij de TLS-handshake dient de hoogste toegestane TLS-versie gekozen te worden die beide partijen ondersteunen. Het GBX volgt voor berichtuitwisseling de WS-I Basic Profile 1.0 specificaties.

Vzvz_Moscow: Verplicht (Must)
Vzvz_Req_Verificatie: Aansluittoets
Vzvz_Req_Soort: Functional
Vzvz_Req_Type: Product

2.5 Eisen XIS-leverancier

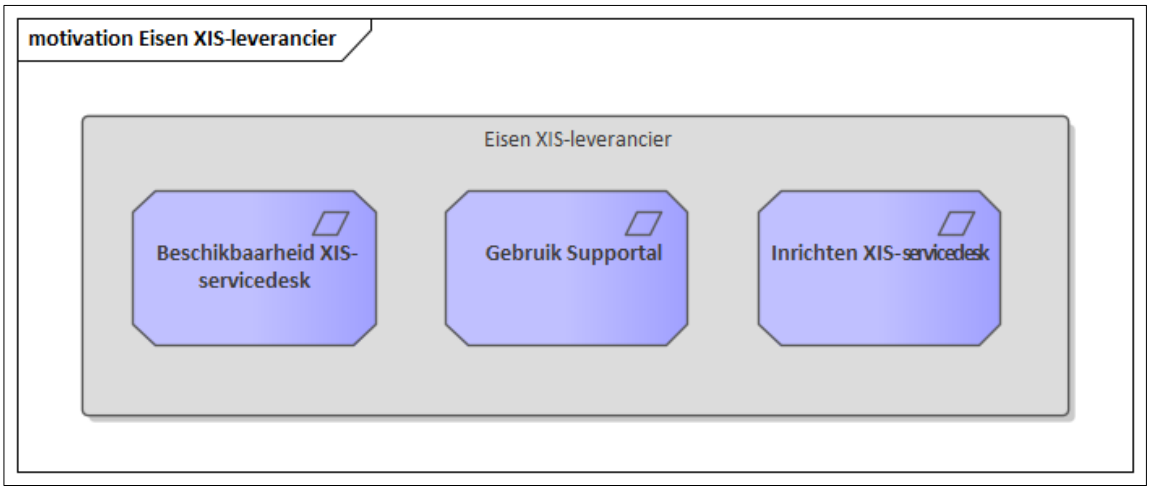


Figure 17 : Eisen XIS-leverancier

2.5.1 Inrichten XIS-servicedesk

Alias: XIS.SVD.e4030.2

Details
Eis: De XIS-leverancier moet een 'XIS-servicedesk' inrichten die als aanspreekpunt fungeert voor problemen m.b.t. het XIS, ketentestbevindingen en opvolging van werkplanafspraken. De XIS-servicedesk moet onderdeel uitmaken van het ketenbeheerproces. **Toelichting bij eis:** Via de GBZ-Servicedesks is niet altijd een goede voortgang te boeken met betrekking tot het oplossen van XIS gerelateerde problemen. Het ontbreken van voortgang wordt met name veroorzaakt doordat de GBZ-beheerder geen invloed heeft op de planning bij de leveranciers en doordat het precieze probleem en de ernst van het probleem niet altijd duidelijk doorkomen bij de XIS-leverancier. Daarnaast ontbreekt het de GBZ-beheerder in sommige gevallen aan de technische kennis, die nodig is om bepaalde problemen te detecteren en/of te benoemen. De XIS-servicedesk moet de GBZ-beheerder ondersteunen bij het oplossen van eventuele technische bevindingen van het XIS. Daarnaast moet het XIS-servicedesk benaderbaar zijn voor VZVZ om bepaalde problemen en oplossingstijden te bespreken en de voortgang te bewaken. Het doel is om tot betere kwaliteit van de software te komen en om problemen in de keten effectiever op te lossen. Naast bovenstaande wordt de XIS-servicedesk benaderd voor de opvolging van ketentestbevindingen en de opvolging van de werkplanafspraken. Er dient in ieder geval een telefoonnummer en een emailadres bekend te zijn van de XIS-servicedesk.

Vzvz_Moscow: Verplicht
Vzvz_Req_Verificatie: Monitoring
Vzvz_Req_Soort: Non-Functional
Vzvz_Req_Type: Business

2.5.2 Gebruik Supportal

Alias: XIS.SVD.e4020

Details
Eis: De XIS-leverancier moet voor in gebruik name van een applicatie in productie, het XIS-aanspreekpunt en contactgegevens beschikbaar gesteld hebben via Supportal. **Toelichting bij eis:** Om een goed beheerproces te kunnen implementeren is het van belang dat de verantwoordelijke aanspreekpunten vindbaar en benaderbaar zijn. Het huidige ketenbeheerproces maakt voor communicatie binnen de keten gebruik van Supportal. Het is van belang dat ook het XIS-aanspreekpunt vindbaar is in Supportal.

Vzvz_Moscow: Verplicht
Vzvz_Req_Verificatie: Monitoring
Vzvz_Req_Soort: Non-Functional
Vzvz_Req_Type: Business

2.5.3 Beschikbaarheid XIS-servicedesk

Alias: XIS.SVD.e4010.1

Details
Eis: Een ingericht XIS-Servicedesk moet tijdens kantoortijden beschikbaar zijn voor vragen vanuit VZVZ, GBZ-beheerders van eigen klanten en XIS-servicedesks van andere XIS-leveranciers. **Toelichting bij eis:** Voor de oplostijden en de precieze beschikbaarheid van het XIS-servicedesk wordt verwezen naar de in de toekomst op te stellen DAP.

Vzvz_Moscow: Verplicht
Vzvz_Req_Verificatie: Monitoring
Vzvz_Req_Soort: Non-Functional
Vzvz_Req_Type: Business

2.6 Generieke eisen aan een XIS

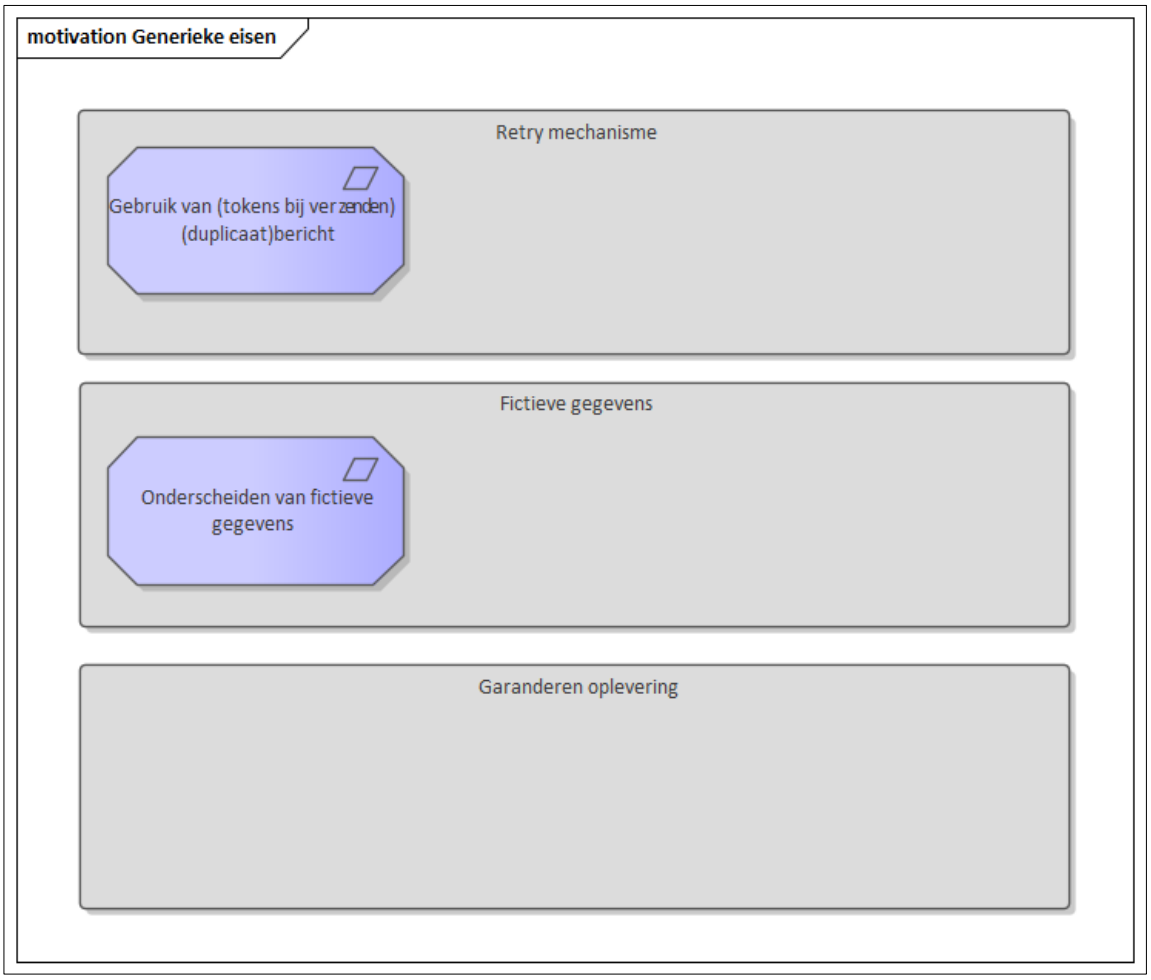


Figure 18 : Generieke eisen

2.6.1 Gebruik van (tokens bij verzenden) (duplicaat)bericht

Alias: GBX.BTW.e4010

Details
Eis: Ieder initiërend systeem: 1. moet bij tokenauthenticatie ieder nieuw bericht voorzien van een nieuw authenticatietoken; 2. moet ieder duplicaatbericht identiek maken aan het originele bericht (inclusief alle identificerende gegevens); 3. kan bij tokenauthenticatie ieder duplicaatbericht ook voorzien van een identiek authenticatietoken; 4. mag een antwoord 'token reeds gebruikt' niet als succes interpreteren. **Toelichting bij eis:** Deze eis is onder andere nodig om: • eventuele retry-mechanismen correct te laten werken; • de opdrachtnemende applicatie (waaronder de ZIM) in staat te stellen duplicaatdetectie te doen.

Duplicaatdetectie dient onder andere om zeker te stellen dat een opdracht maximaal één keer wordt uitgevoerd. Voor raadplegingen hoeft geen duplicaatdetectie uitgevoerd te worden door de ontvanger. Bij raadplegingen maakt het voor het resultaat dan ook niet uit of duplicaten of nieuwe opvragingen gebruikt worden. Bij het versturen van een duplicaatbericht is het mogelijk om een duplicaat-authenticatietoken mee te sturen. Het is echter ook mogelijk om een nieuw authenticatietoken te maken.

Vzvz_Moscow: Verplicht (Must)
Vzvz_Req_Verificatie: Monitoring
Vzvz_Req_Soort: Functional
Vzvz_Req_Type: Product

2.6.2 Onderscheiden van fictieve gegevens

Alias: GBX.BVL.e4090

Details
Eis: Het systeem moet fictieve gegevens opvallend onderscheidend presenteren aan gebruikers. **Toelichting bij eis:** Deze eis dient om onjuist gebruik van fictieve gegevens te voorkomen.

Vzvz_Moscow: Verplicht (Must)
Vzvz_Req_Verificatie: Acceptatietest
Vzvz_Req_Soort: Functional
Vzvz_Req_Type: Product

3 Eisen voor specifieke zorgtoepassingssysteemrollen

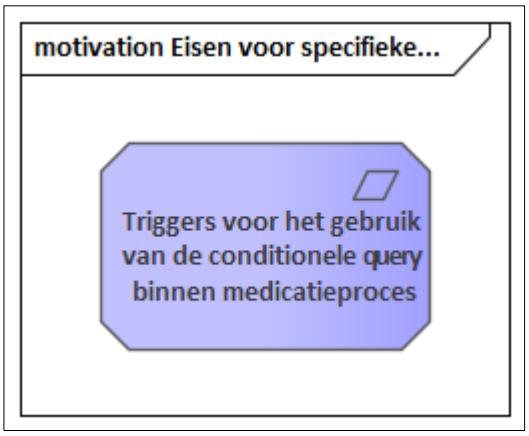


Figure 19 : Eisen voor specifieke zorgtoepassingssysteemrollen

3.1 Triggers voor het gebruik van de conditionele query binnen medicatieproces

Alias:

Details
Eis: Alleen bij de volgende triggers mag de conditionele query worden gebruikt binnen medicatieproces: - Openen van het dossier - Vastleggen van een afspraak - Ontvangen voorstel medicatieafspraak/verstrekkingsverzoek - Ontvangst afhandeling voorschrift - Vastleggen ontslag **Toelichting bij eis:** Binnen Preventie en Populatiemanagement mogen alleen gegevens van dezelfde organisatie worden opgevraagd aangezien er niet met een UZI pas wordt geauthenticeerd bij de opvraag. **Condities:** Deze eis is verplicht.

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