



Huisartswaarneemgegevens - Waarnemend Huisartssysteem

Datum:	14-10-2020
Status:	Definitief
Versie:	6.13
Classificatie:	Openbaar
Eigenaar:	VZVZ
Revisie:	1

Beste Lezer,

Binnen VZVZ zijn wij druk bezig met het verbeteren van onze publicaties. Voor u ligt een vernieuwd Programma van Eisen. Het volgende is veranderd:

Opmaak eisen

De eisen worden nu niet meer in een tabelvorm weergegeven. Daarnaast wordt de naam van de eis weergegeven en daarna de identificatiecode.

Onder de eis vindt u een aantal attributen behorende bij de eis:

Vz vz_Moscow: beschrijft of de eis verplicht, optioneel of conditioneel

Vz vz_Req_Soort: beschrijft of de eis functioneel en non-functioneel is.

Vz vz_Req_Type: beschrijft het type eis, en of het een product-, user- en business eis is.

Vz vz_Req_Verificatie: beschrijft de manier waarop de eis getest moet worden.

Vz vz_INI: het ini-nummer betreft het issuereferentienummer. Naar aanleiding van dit nummer kan via de releasenotes achterhaald worden waar de aanpassing van de eis betrekking op heeft. Ook kan aan de hand van dit nummer meer informatie opgevraagd worden bij VZVZ.

Schema kwaliteitskenmerken ISO-25010

De kwaliteitseisen in dit document zijn onderverdeeld in de kwaliteitscategorieën van de ISO-norm 25010. Elke paragraaf start met een overzicht (schema) van alle eisen die vallen onder die paragraaf. De niet-functionele (software-)eisen zijn kwaliteitseisen waaraan een systeem moet voldoen. De ISO-norm 25010 beschrijft de kwaliteitskenmerken van de software. Het model voor productkwaliteit onderscheidt hierin acht hoofdcategorieën:

1. **Functionele geschiktheid** (Functional suitability). De mate waarin een softwareproduct of computersysteem functies levert die voldoen aan de uitgesproken en veronderstelde behoeften, bij gebruik onder gespecificeerde condities.
2. **Prestatie-efficiëntie** (Performance efficiency). De prestaties in verhouding tot de hoeveelheid middelen die gebruikt worden onder genoemde condities.
3. **Uitwisselbaarheid** (Compatibility). 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.
4. **Bruikbaarheid** (Usability). De mate waarin een product of systeem gebruikt kan worden door gespecificeerde gebruikers om effectief, efficiënt en naar tevredenheid gespecificeerde doelen te bereiken in een gespecificeerde gebruiksccontext.
5. **Betrouwbaarheid** (Reliability). De mate waarin een systeem, product of component gespecificeerde functies uitvoert onder gespecificeerde condities gedurende een gespecificeerde hoeveelheid tijd.
6. **Beveiligbaarheid** (Security). 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.
7. **Onderhoudbaarheid** (Maintainability). De mate waarin een product of systeem effectief en efficiënt gewijzigd kan worden door de aangewezen beheerders.
8. **Overdraagbaarheid** (Portability). De mate waarin een systeem, product of component effectief en efficiënt overgezet kan worden van één hardware, software of andere operationele of gebruiksomgeving naar een andere.

Als er geen eis staat bij een categorie, dan betekent het dat wij geen eis hebben aangemaakt voor die categorie.

Inhoudsopgave

Inhoudsopgave.....	3
1. Inleiding.....	4
1.1 Doelgroep voor dit document	4
1.2 Doel en scope.....	4
1.3 Documenthistorie.....	4
2. AORTA Eisen Infrastructurele Systeemrollen	5
2.1. Eisen Infrastructurele Systeemrollen - Mandaatregistratie	5
2.2. Eisen infrastructurele systeemrollen - Opvragend systeem	10
2.3. Eisen infrastructurele systeemrollen - Primaire interacties - versturend systeem.....	23
2.4. Eisen Infrastructurele Systeemrollen - Applicatiebeheer.....	26
2.5. Generieke eisen.....	31
2.6. Eisen Infrastructurele Systeemrollen - Patiëntadministratie	34
2.7. Eisen Infrastructurele Systeemrollen - Verwijsindex	40
2.8. Eisen Infrastructurele Systeemrollen - Zorgaanbiedersadresboek	46
3. AORTA Eisen Kwaliteit Aangesloten Systemen	52
3.1. AORTA Eisen Kwaliteit aangesloten systemen - Prestatie-efficiëntie	52
3.2. AORTA Eisen Kwaliteit aangesloten systemen - Betrouwbaarheid.....	53
3.3. AORTA Eisen Kwaliteit aangesloten systemen - Beveiligbaarheid.....	56
3.4. AORTA Eisen Kwaliteit aangesloten systemen - Uitwisselbaarheid	59
4. AORTA Eisen Kwaliteit Applicatie	62
4.1. AORTA Eisen Kwaliteit applicatie - Beveiligbaarheid	62
4.2. AORTA Eisen Kwaliteit applicatie - Uitwisselbaarheid	69
5. AORTA Eisen Organisatie van een GBX	72
5.1. Eisen aan de beheerorganisatie van een GBX	72

1. Inleiding

Dit document beschrijft de eisen waaraan softwaresystemen moeten voldoen om als XIS gekwalificeerd te kunnen worden voor aansluiting op het LSP als 'Waarnemend huisartssysteem'.

1.1 Doelgroep voor dit document

De primaire doelgroepen van dit document zijn: Productmanagers, architecten, ontwerpers, ontwikkelaars en testers van XIS-leveranciers en VZVZ.

1.2 Doel en scope

De functionele eisen die worden beschreven in dit document worden gebruikt bij de kwalificatie van XIS-en die willen aansluiten op het LSP als 'waarnemend huisartssysteem'. De eisen zijn gebaseerd op AORTA v8.2.0.0.

1.3 Documenthistorie

Versie	Revisie	Datum	Omschrijving
6.13	1	14-10-2020	Geheel herziene versie met nieuwe layout en inhoudelijk nieuwe opzet, met minder doorverwijzingen naar andere programma's van eisen. Door deze trendbreuk is het aangeven van wijzigingen met vorige versies niet meer mogelijk en evenmin zinvol. Voor eventuele aanpassingen wordt vooralsnog verwezen naar de AORTA release notes v8.2.0.0.

2. AORTA Eisen Infrastructurele Systemrollen

2.1. Eisen Infrastructurele Systemrollen - Mandaatregistratie



GBX.AUT.e4514 - Beheren gemandateerde groepen

Eis:

In een autorisatieregels 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 gemandateerde(n); een lijst kan bestaan uit bijvoorbeeld UZI-nummer(s) of rollen/functies.

Alleen op vertrouwensniveau midden is het mogelijk om de lijst met gemandateerde(n) dynamisch uit te breiden. De identifier hoeft niet aangepast te worden bij uitbreiding van de lijst met gemandateerde(n).

Toelichting bij eis:

Door het gebruik van groepen in een autorisatieregels is het mogelijk om dynamisch rolcode's of UZI-nummers toe te voegen aan de lijst met gemandateerde(n).

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.

Identificatiecode	GBX.AUT.e4514
Vzvv_Moscow	Verplicht
Vzvv_Req_Soort	Functional
Vzvv_Req_Verificatie	Acceptatietest

GBX.AUT.e4513 - Beheren mandaat autorisatieregels

Eis:

Een mandaat kan alleen afgegeven worden op basis van een autorisatieregels. Een autorisatieregels 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 gemandateerde(n); Dit kunnen UZI-nummer(s) 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](#)).

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.

Identificatiecode	GBX.AUT.e4513
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Functional
Vz vz_Req_Verificatie	Acceptatietest

GBX.AUT.e4519 - Beheren mandaattokens

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.

Identificatiecode	GBX.AUT.e4519
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Functional
Vz vz_Req_Verificatie	Monitoring

GBX.AUT.e4511 - Beheren van mandaten

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.

Identificatiecode	GBX.AUT.e4511
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Functional
Vz vz_Req_Verificatie	Acceptatietest

GBX.AUT.e4520 - Gebruik mandaattokens

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 ([IH Berichtauthenticatie 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.

Identificatiecode	GBX.AUT.e4520
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Functional
Vz vz_Req_Verificatie	Acceptatietest

GBX.AUT.e4517 - Inzichtelijk maken mandaatautorisatie

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.

Identificatiecode	GBX.AUT.e4517
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Functional
Vz vz_Req_Verificatie	Acceptatietest

GBX.AUT.e4516 - Logging mandaten

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. Autorisatieregels; bij het aanmaken van een autorisatieregels 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 autorisatieregels 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 loggegevens 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.

Identificatiecode	GBX.AUT.e4516
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Functional
Vz vz_Req_Verificatie	Acceptatietest

GBX.AUT.e4515 - Uniformiteit mandaat

Eis:

Een mandaat dient te worden opgeslagen in de vorm van een mandaattoken zoals gespecificeerd in de [IH berichtauthenticatie mandaattoken].

Toelichting bij eis:

Berichten die onder mandaat naar het LSP worden verstuurd, dienen te worden voorzien van een mandaattoken (zoals gespecificeerd in [IH berichtauthenticatie mandaattoken]). Het LSP krijgt dan altijd op een uniforme wijze het mandaat aangeleverd en kan deze vervolgens ook controleren.

Identificatiecode	GBX.AUT.e4515
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Functional
Vz vz_Req_Verificatie	Acceptatietest

GBX.AUT.e4521.1 - Verwijderen mandaten

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.

Identificatiecode	GBX.AUT.e4521.1
Vz vz_INI	INI-9312
Vz vz_Moscow	Conditioneel
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product

GBX.AUT.e4522.1 - Waarschuwen verlopen mandaten**Eis:**

Een mandaterende en de in de autorisatieregels 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 <GBx_verlopen_mandaat> 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.

Identificatiecode	GBX.AUT.e4522.1
Vz vz_INI	INI-9229
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Acceptatietest

2.2. Eisen infrastructurele systeemrollen - Opvragend systeem

GBX.OPV.e4190 - Voorkomen van foutmeldingen en onverwachts gedrag van een applicatie

Eis:

Waardes in velden die conform het XSD-schema zijn, maar niet kunnen worden verwerkt door het ontvangende systeem moeten kunnen worden genegeerd door de ontvangende applicatie.

Toelichting:

Om succesvol bouwstenen te kunnen uitwisselen moet er een versiebeheer mechanisme worden toegepast. Dit versiebeheer mechanisme verplicht opvragende systemen velden die zij niet kunnen verwerken, maar die wel volgens het schema zijn toegestaan te kunnen negeren. Hierdoor zijn systemen voorbereid op wijzigingen die in de toekomst doorgevoerd kunnen worden.

Identificatiecode	GBX.OPV.e4190
Vz vz_Moscow	Verplicht
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Acceptatietest

GBX.OPV.e4017 - Afhandelen opgevraagde bouwstenen

Eis:

Een XIS dat patiëntgegevens opvraagt op basis van contexten, moet van de aan die contexten gerelateerde bouwsteentypen alle mogelijke bouwsteeninstantiaties kunnen verwerken

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.

Identificatiecode	GBX.OPV.e4017
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Acceptatietest

GBX.OPV.e4040.1 - Automatisch opvragen van patiëntgegevens op basis van context

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.

Identificatiecode	GBX.OPV.e4040.1
Vz vz_INI	INI-9271
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Acceptatietest
Vz vz_Req_Vertrouwensniveau	Laag

GBX.OPV.e4120 - Beperken gebruik inschrijftokens

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.

Identificatiecode	GBX.OPV.e4120
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Monitoring

GBX.OPV.e4050 - Creëren inschrijftoken

Eis:

Alleen daarvoor geautoriseerde rol(len)/perso(o)n(en) moet(en) een inschrijftoken (conform eis GBX.OPV.e4060) kunnen creëren 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, zorgverlenersassistenten en/of baliemedewerkers zijn.

Identificatiecode	GBX.OPV.e4050
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Acceptatietest

GBX.OPV.e4100.1 - Geldigheidsduur inschrijftoken**Eis:**

Een inschrijftoken heeft een maximale geldigheidsduur van *<max_geldigheidsduur_inschrijftoken>*.

Toelichting:

Een inschrijftoken kent een beperkte geldigheidsduur. Het is echter mogelijk om dezelfde informatie in het inschrijftoken opnieuw te ondertekenen (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.

De *<max_geldigheidsduur_inschrijftoken>* wordt gesteld op 1.5 jaar.

Identificatiecode	GBX.OPV.e4100.1
Vz vz_INI	INI-9104
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Acceptatietest

GBX.OPV.e4060.2 - Inhoud inschrijftoken**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].

Identificatiecode	GBX.OPV.e4060.2
Vz vz_INI	INI-9104
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Acceptatietest

GBX.OPV.e4045.1 - Inzichtelijk maken resultaat van conditioneel bericht**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.

Identificatiecode	GBX.OPV.e4045.1
Vz vz_INI	INI-9313
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Acceptatietest

GBX.OPV.e4155.1 - Loggen initiatie conditioneel bericht**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.

Identificatiecode	GBX.OPV.e4155.1
Vzvvz_INI	INI-9313
Vzvvz_Moscow	Verplicht
Vzvvz_Req_Soort	Functional
Vzvvz_Req_Type	Product
Vzvvz_Req_Verificatie	Acceptatietest

GBX.OPV.e4090.1 - Mandaattoken t.b.v. handeling door systeem

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.

Identificatiecode	GBX.OPV.e4090.1
Vzvvz_INI	INI-9271
Vzvvz_Moscow	Verplicht
Vzvvz_Req_Soort	Functional
Vzvvz_Req_Type	Product
Vzvvz_Req_Verificatie	Acceptatietest

GBX.OPV.e4150.2 - Ondertekening transactietoken met servercertificaat

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.

Identificatiecode	GBX.OPV.e4150.2
-------------------	-----------------

Vz vz_INI	INI-9271,INI-9313
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Acceptatietest

GBX.OPV.e4030 - Opslaan opgevraagde patiëntgegevens

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 verwijzindex 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.

Identificatiecode	GBX.OPV.e4030
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Acceptatietest

GBX.OPV.e4010.1 - Opvragen van patiëntgegevens

Beginsituatie

- De gebruiker is lokaal ingelogd op vertrouwensniveau midden of hoger, en
- Er is voldaan aan eis [Toets op behandelrelatie](#).

Trigger

- De gebruiker initieert de functie via het systeem

Interacties

- Het systeem verzendt een opvragenPatiëntgegevens-bericht naar de ZIM, zoals beschreven in de eisen aan de concrete systeemrol.
- Het systeem ontvangt een opleverenPatiëntgegevens-bericht, zoals beschreven in de eisen aan de concrete systeemrol.

Resultaat

De opgeleverde gegevens zijn door het systeem:

- a. gepresenteerd aan de gebruiker, of
- b. verwerkt tot een beslissing die is gepresenteerd aan de gebruiker.

Uitzonderingen

Uitzonderingen zijn beschreven in de [Foutentabel](#).

Opties

Bij het samenstellen van het opvragenPatiëntgegevens-bericht moeten de query-parameters meegegeven kunnen worden, zoals beschreven in het PvE voor de concrete systeemrol. Ook kan men de gewenste responstijd instellen [uiterste-oplevertijd-gbz](#), wanneer iemand een volledig medicatiedossier wil opvragen zou de responstijd verhoogd kunnen worden.

Wanneer het systeem een opvraagbericht in de nieuwste versie stuurt, moet het systeem antwoorden in de eerst lagere versie ook kunnen verwerken.

Responsetijd

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

Toelichting

Wanneer het systeem een opvraagbericht in de nieuwste versie stuurt, worden systemen die deze versie nog niet ondersteunen door de ZIM bevroegd in de eerst lagere versie.

Wanneer het systeem een opvraagbericht in de eerst lagere versie dan de nieuwste stuurt, hoeft slechts rekening te worden gehouden met antwoorden in deze eerst lagere versie.

Het systeem kan desgewenst voorafgaand aan een opvraagbericht opvragen wat de hoogste gemeenschappelijke versie van dat opvraagbericht is via een 'opvragen Interactieve versie' bericht (zie: applicatieregister raadplegend systeem), zodat het vervolgens het opvraagbericht naar de ZIM kan sturen in die gemeenschappelijk ondersteunde versie.

Identificatiecode	GBX.OPV.e4010.1
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Functional
Vz vz_Req_Verificatie	Acceptatietest

GBX.OPV.e4015 - Opvragen van patiëntgegevens op basis van context

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](#).

Identificatiecode	GBX.OPV.e4015
Vzvz_Moscow	Verplicht
Vzvz_Req_Soort	Functional
Vzvz_Req_Type	Product
Vzvz_Req_Verificatie	Acceptatietest
Vzvz_Req_Vertrouwensniveau	Midden

GBX.OPV.e4160 - Toegankelijkheid inschrijftokens

Eis:

Om misbruik van inschrijftokens door een kwaadwillende te bemoeilijken, moeten de inschrijftokens in een beveiligde omgeving worden opgeslagen. Toegang tot de inschrijftokens 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 inschrijftokens. Dit is afhankelijk van de lokale systeemimplementatie. De systeembouwer is verantwoordelijk voor een goede invulling van deze eis.

Identificatiecode	GBX.OPV.e4160
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Audit

GBX.OPV.e4020 - Toets op behandelrelatie

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](#).

Identificatiecode	GBX.OPV.e4020
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Acceptatietest

GBX.OPV.e4080 - Verkrijgen berichtID van antwoord n.a.v. BSN-controle

Eis:

Ten behoeve van het inschrijftoken dient er een uniek berichtID van het antwoordbericht op een SBV-Z 'verifiëren BSN'-vraag te worden verkregen. De 'verifiëren BSN'-vraag moet worden verstuurd via een aansluiting op de SBV-Z. Voor de 'verifiëren BSN'-vraag kunnen de volgende zoekpaden ([SBV-Z]) gebruikt worden:

- Zoekpad 1;
- Zoekpad 2.

Van het 'verifiëren BSN'-antwoord dient minimaal de volgende elementen gelogd te worden:

- Het berichtID;
- Meldingsoort;

Oorspronkelijke vraag.

Toelichting:

Voor gebruik op het LSP is het verplicht om via een technische koppeling met het SBV-Z een 'verifiëren BSN'-controle uit te voeren en het resultaat op te nemen in het inschrijftoken. Voor andere toepassingen dan AORTA kan het mogelijk zijn om deze controle achterwege te laten.

Identificatiecode	GBX.OPV.e4080
Vz vz_INI	INI-9137
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Acceptatietest

GBX.OPV.e4070 - Verkrijgen berichtID van antwoord n.a.v. WID-controle**Eis:**

Ten behoeve van het inschrijftoken dient er een uniek berichtID van het antwoordbericht op een SBV-Z 'WID controle'-vraag te worden verkregen. De 'WID controle'-vraag moet worden verstuurd via een aansluiting op de SBV-Z. Voor de 'WID controle'-vraag dienen er drie gegevens ingevoerd te worden:

- Het BSN van de patiënt;
- Het type van het identiteitsbewijs;
- Het nummer van het identiteitsbewijs.

Van het 'WID controle'-antwoord dient minimaal de volgende elementen gelogd te worden:

- Het berichtID;
- Meldingsoort;

Oorspronkelijke vraag.

Toelichting:

Voor gebruik op het LSP is het verplicht om via een technische koppeling met het SBV-Z een WID-controle uit te voeren en het resultaat op te nemen in het inschrijftoken. Voor andere toepassingen dan AORTA kan het mogelijk zijn om deze controle achterwege te laten.

Identificatiecode	GBX.OPV.e4070
Vz vz_INI	INI-9137
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Acceptatietest

GBX.OPV.e4110 - Verwijderen inschrijftokens**Eis:**

Indien de geldigheidsduur van een inschrijftoken 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 inschrijftoken uit het systeem te verwijderen.

Toelichting:

Het verwijderen (en daarmee afwezig zijn) van een inschrijftoken leidt ertoe dat er geen automatische opvraag meer verstuurd mag worden t.b.v. het opvragen van patiëntgegevens van de in het inschrijftoken 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 inschrijftoken. Hoe hier invulling aan te geven is aan de systeembouwer.

Identificatiecode	GBX.OPV.e4110
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Acceptatietest

GBX.OPV.e4180 - Voorkomen manipulatie van een niet getekend bericht**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.

Identificatiecode	GBX.OPV.e4180
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Audit

GBX.OPV.e4170 - Voorkomen misbruik tokens**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.

Identificatiecode	GBX.OPV.e4170
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Audit

GBX.OPV.e4130.1 - Voorkomen overbelasting infrastructuur**Eis:**

In het geval een conditioneel bericht wordt beantwoord met een foutmelding, dan heeft het systeem `<automatische_retry_conditioneel_bericht>` pogingen om het conditionele bericht nogmaals te versturen.

Na <automatische_retry_conditioneel_bericht> pogingen mag het systeem het bericht niet nogmaals uitsenden en dient de GBZ-beheerder actie te ondernemen zoals is beschreven in de [AORTA DAP].

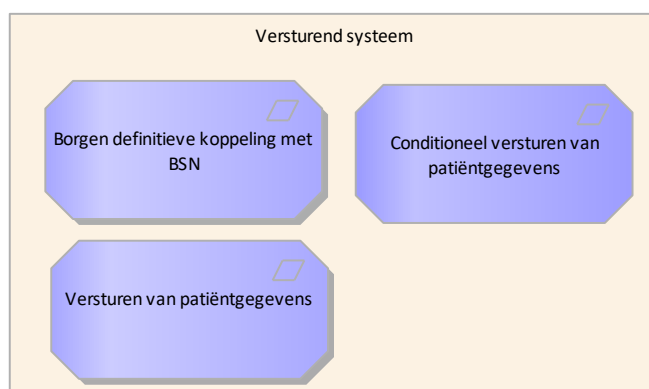
Toelichting bij eis:

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.

Voor het <automatische_retry_conditioneel_bericht> geldt een waarde van 3.

Identificatiecode	GBX.OPV.e4130.1
Vzvv_INI	INI-9313
Vzvv_Moscow	Verplicht
Vzvv_Req_Soort	Functional
Vzvv_Req_Type	Product
Vzvv_Req_Verificatie	Acceptatietest

2.3. Eisen infrastructuurle systeemrollen - Primaire interacties - versturend systeem



GBX.STU.e4020 - Borgen definitieve koppeling met BSN

Eis:

Het systeem mag alleen patiëntgegevens versturen indien voor die patiëntgegevens sprake is van een definitieve koppeling met het BSN.

Toelichting bij eis:

Deze eis zorgt ervoor dat een gebruiker conform Wbsn-z artikel 9 alleen patiëntgegevens kan versturen nadat de vereiste BSN-verificatie en eventueel benodigde WID-controle is gedaan.

Identificatiecode	GBX.STU.e4020
Vzvv_Moscow	Verplicht
Vzvv_Req_Soort	Functional
Vzvv_Req_Type	Product

GBX.STU.e4015 - Conditioneel versturen van patiëntgegevens**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 bericht als gevolg van bijvoorbeeld:

- het afsluiten van een dossier van de patiënt;
- een handmatige trigger door een persoon.

Het is aan het XIS om verantwoord om te gaan met de triggers die een automatisch bericht kunnen laten versturen.

Interacties:

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

Resultaat:

De bevestiging is ontvangen en het resultaat van de interactie is kenbaar gemaakt aan de gebruiker.

Uitzonderingen:

Uitzonderingen zijn beschreven in de [Foutentabel]

Opties:

Het conditioneel versturen van patiëntgegevens is een wijze van versturen die gebruikt kan worden naast het versturen van patiëntgegevens zoals beschreven in GBX.STU.e4010. Bij het implementeren van deze eis is ook GBX.STU.e4010 verplicht.

Responsetijd:

-

Betrouwbaarheid:

-

Toelichting bij eis:

Een conditioneel verstuurbericht verschilt van een regulier verstuurbericht (GBX.STU.e4010) m.b.t. de trigger en de daadwerkelijke verstuurder van de patiëntgegevens. In het geval van een conditioneel verstuurbericht verzendt het systeem een bericht 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 versturen van patiëntgegevens dient gedaan te worden ten behoeve van een behandelende zorgverlener. Het conditioneel versturen 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 versturenPatiëntgegevens-bericht zie eis GBX.STU.e4010.

Identificatiecode	GBX.STU.e4015
Vz vz_INI	INI-9313
Vz vz_req_Moscow	Optioneel
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Acceptatietest

GBX.STU.e4010 - Versturen van patiëntgegevens

Conditie

-

Beginsituatie

De gebruiker is lokaal ingelogd op vertrouwensniveau midden of hoger.

Trigger

De gebruiker initieert de functie via het systeem.

Interacties

1. Het systeem verzendt een versturenPatiëntgegevens-bericht naar de ZIM, zoals beschreven in de eisen aan de concrete systeemrol.
2. Het systeem ontvangt een bevestiging conform [AORTA Wrp IH Berichtwrappers HL7](#).

Resultaat

De bevestiging is ontvangen en het resultaat van de interactie is kenbaar gemaakt aan de gebruiker.

Uitzonderingen

Uitzonderingen zijn beschreven in de Foutentabel.

Opties

Het systeem moet de mogelijkheid bieden om:

- De afzender van een ander bericht als bestemming te gebruiken.
- Handmatig een bestemming in te voeren.

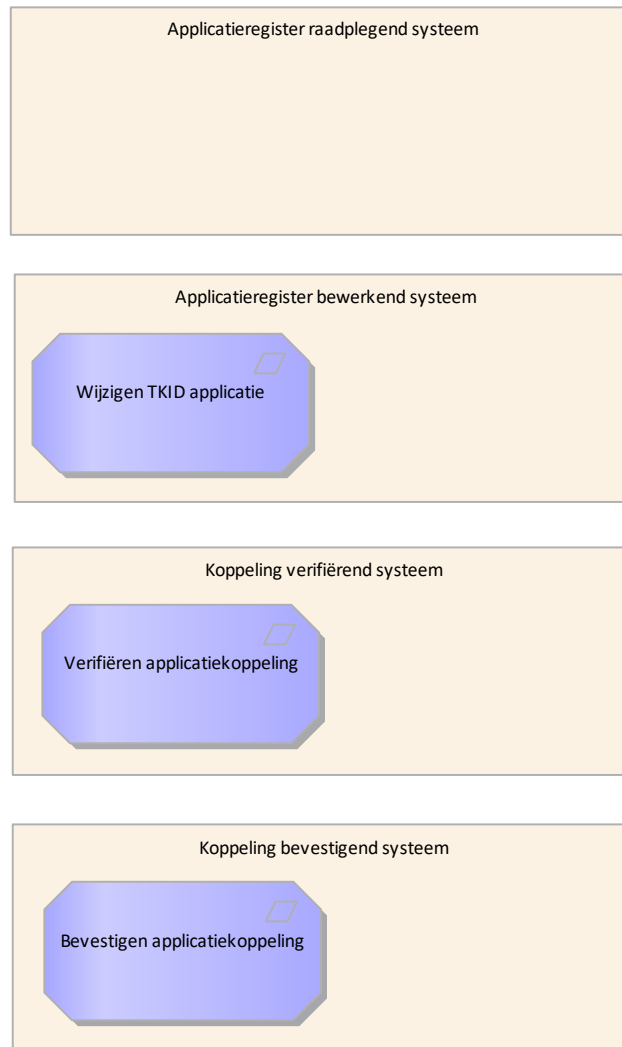
Het systeem moet berichten versturen in een versie die het ontvangende systeem ondersteunt.

Toelichting

De berichtversie die wordt ondersteund door het ontvangende systeem kan worden opgevraagd bij het applicatieregister (zie: applicatieregister raadplegend systeem: opvragen Interactieversie).

Identificatiecode	GBX.STU.e4010
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Acceptatietest
Vz vz_Req_Vertrouwensniveau	Midden

2.4. Eisen Infrastructurele Systeemrollen - Applicatiebeheer



GBX.APR.e4160 - Bevestigen applicatiekoppeling

Beginsituatie

Het systeem beschikt over de voor deze functie vereiste vertrouwensmiddelen.

Trigger

Het systeem ontvangt een verifiërenApplicatiekoppeling bericht conform [HL7v3 IH APR](#).

Interacties

Het systeem stuurt een verifiërenApplicatiekoppelingAntwoord terug naar de verzender conform [HL7v3 IH APR](#).

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

-

Identificatiecode	GBX.APR.e4160
Vzvv_Moscow	Verplicht
Vzvv_Req_Soort	Functional
Vzvv_Req_Type	Product
Vzvv_Req_Verificatie	Acceptatietest

GBX.APR.e4140 - Verifiëren applicatiekoppeling

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 verifiërenApplicatiekoppeling bericht naar de ZIM of een ander GBX conform [HL7v3 IH APR](#).
2. Het systeem ontvangt een verifiërenApplicatiekoppelingAntwoord bericht conform [HL7v3 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

-

Identificatiecode	GBX.APR.e4140
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Acceptatietest
Vz vz_Req_Vertrouwensniveau	Laag

GBX.APR.e4060, GBX.APR.e4170.1 - Wijzigen TKID applicatie

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'.

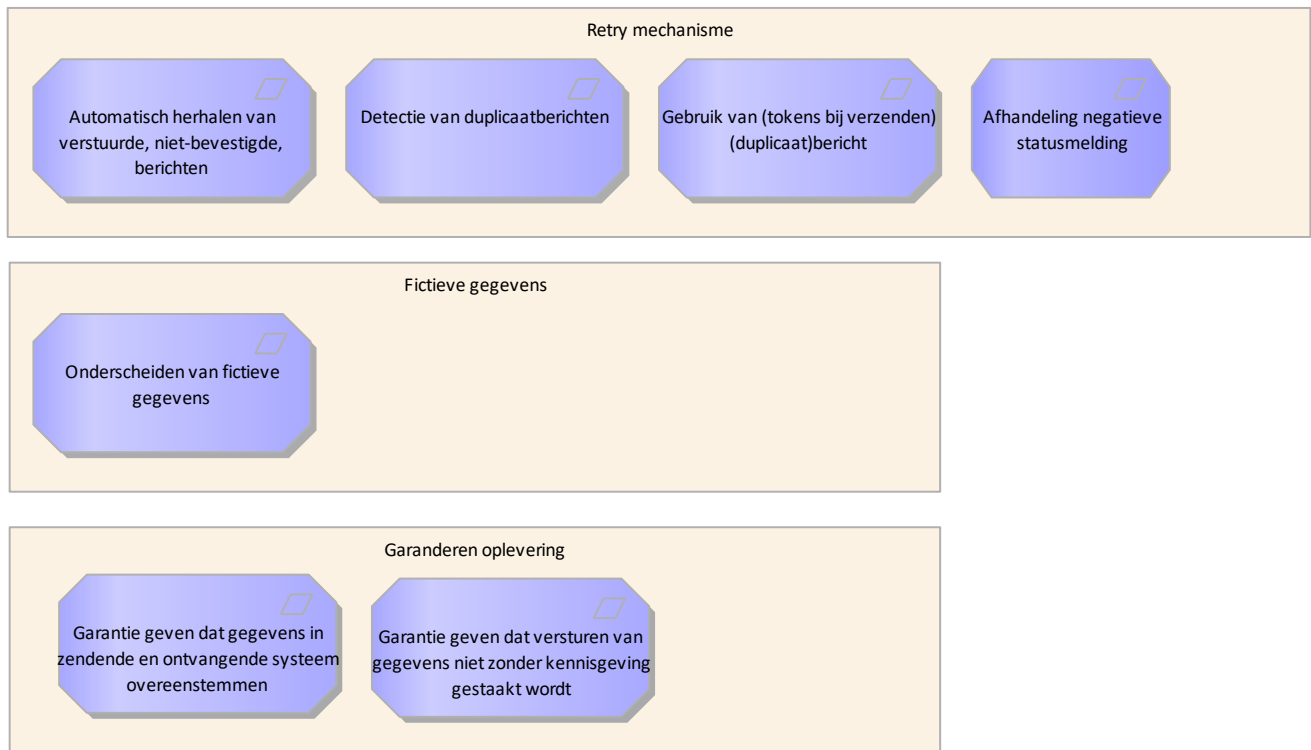
In principe geldt dat er bij elk nieuw verkregen TKID, als gevolg van een acceptatie van een applicatiewijziging of –uitbreiding, er één of meerdere TKID's opnieuw ingestuurd moeten worden. Denkbare situaties zijn:

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

Terugzetten oude functionaliteit (met een eerder verkregen TKID).

Identificatiecode	GBX.APR.e4060, GBX.APR.e4170.1
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Acceptatietest
Vz vz_Req_Vertrouwensniveau	Laag

2.5. Generieke eisen



GBX.TOE.e4708 - Afhandeling negatieve statusmelding

Bij een negatieve statusmelding van Mitz hoeft het systeem geen automatisch herhaalde pogingen uit te voeren.

Identificatiecode	GBX.TOE.e4708
Vz vz_Req_Verificatie	Acceptatietest

GBX.BTW.e4050 - Automatisch herhalen van verstuurde, niet-bevestigde, berichten

Eis:

Voor gegevens versturende systemen geldt het volgende:

1. Het systeem mag tot een maximum van [[gbx-opdracht-retry](#)] aantal pogingen doen met een duplicaatbericht in een tijdspanne van [[gbx-min-timeout](#)] tot [[gbx-max-timeout](#)].
2. Wanneer het systeem na bovenstaande poging(en) geen afdoende antwoord heeft ontvangen, mag het een nieuwe poging uitvoeren met een nieuw bericht, waarin dezelfde inhoud en dus ook hetzelfde patiëntstuk-id is opgenomen. Dit wordt beschouwd als een nieuwe transactie, waarbij dus ook punt 1 weer geldig is.
3. Wanneer op een nieuwe poging tot toevoegen van gegevens, als bedoeld in punt 2 een antwoord 'bestaat al' wordt ontvangen, mag het systeem dit als succes interpreteren. Immers, de unieke patiëntstuk-id's garanderen dat het om de

juiste gegevens gaat.

4. Wanneer op een nieuwe poging tot verwijderen van gegevens, als bedoeld in punt 2, een antwoord 'bestaat niet' wordt ontvangen, mag het systeem dat als succes interpreteren.
5. Op een nieuwe poging tot wijzigen van gegevens, als bedoeld in punt 2, mag alleen een antwoord dat expliciet 'succes' aanduidt als succes geïnterpreteerd worden.
6. Een nieuwe poging als bedoeld in punt 2 mag ook uitgevoerd worden direct na de eerste poging, het is dus niet verplicht om eerst een nieuwe poging uit te voeren met een duplicaatbericht.

Toelichting bij eis:

Een retry-mechanisme dient om de gebruiker niet te vermoeien met foutmeldingen in geval van een incidentele communicatiestoring.

Wanneer de ZIM bij tokenauthenticatie een bericht verwerkt, wordt het authenticatietoken gecontroleerd en kan dit token niet nogmaals gebruikt worden. Een nieuwe poging met een duplicaatbericht is bij tokenauthenticatie dan ook alleen zinvol wanneer het originele bericht niet bij de ZIM is aangekomen.

De ZIM initieert zelf geen retries naar ontvangende systemen. Iedere poging van het versturend systeem resulteert in maximaal één poging van de ZIM per ontvangend systeem.

Identificatiecode	GBX.BTW.e4050
Vz vz_Moscow	Optioneel
Vz vz_Req_Soort	Functional
Vz vz_Req_Verificatie	Acceptatietest

GBX.BTW.e4030 - Detectie van duplicaatberichten

Eis:

Een reagerend systeem moet na het ontvangen van een bericht, anders dan een raadpleging, aan de hand van het patiëntstuk-id bepalen of het om een nieuw of om een reeds verwerkt bericht gaat. Een reeds verwerkt bericht moet worden beantwoord met een fout.

Toelichting bij eis:

Voor interacties die idempotent zijn (deze kunnen zonder neveneffecten meerdere malen uitgevoerd worden) is duplicaatdetectie niet nodig. Voor niet-idempotente interacties is dit wel nodig.

Deze eis dient om te voorkomen dat opdrachten onterecht meerdere malen worden uitgevoerd.

Identificatiecode	GBX.BTW.e4030
Vz vz_Moscow	Conditioneel
Vz vz_Req_Soort	Functional
Vz vz_Req_Verificatie	Acceptatietest

GBX.BTW.e4070 - Garantie geven dat gegevens in zendende en ontvangende systeem overeenstemmen

Eis:

Voor gegevens versturende systemen geldt het volgende:

1. [Gebruik van \(tokens bij verzenden\) \(duplicaat\)bericht](#) is verplicht.

2. Bij falende communicatie, eventueel na herhaalde pogingen als bedoeld in [Automatisch herhalen van verstuurde, niet-bevestigde, berichten](#), mag niet gestopt worden, maar dienen deze stappen herhaald te worden tot er een uitkomst is die als succes geïnterpreteerd mag worden. Dat mag na tussenkomst van een gebruiker of systeembeheerder.

Toelichting bij eis:

Deze eis voorkomt dat een bericht vergeten wordt wanneer het niet succesvol verstuurd kan worden.

Deze eis kan bijvoorbeeld worden geïmplementeerd door:

- gebruikers bij de eerstvolgende keer inloggen te informeren over niet bevestigde berichten;
- gebruikers de mogelijkheid te bieden een lijst met niet bevestigde berichten te bekijken.

In geval van bijvoorbeeld aanmelden gegevens moet er uiteindelijk succes geboekt worden, anders raakt de verwijzindex corrupt.

Identificatiecode	GBX.BTW.e4070
Vz vz_Moscow	Conditioneel
Vz vz_Req_Soort	Functional
Vz vz_Req_Verificatie	Acceptatietest

GBX.BTW.e4080 - Garantie geven dat versturen van gegevens niet zonder kennisgeving gestaakt wordt

Eis:

Voor gegevens versturende systemen geldt het volgende:

1. [Gebruik van \(tokens bij verzenden\) \(duplicaat\)bericht](#) is verplicht.
2. Bij falende communicatie, eventueel na herhaalde pogingen als bedoeld in [Automatisch herhalen van verstuurde, niet-bevestigde, berichten](#), mag wel gestopt worden, maar moet de gebruiker gewaarschuwd worden dat de communicatie niet gelukt is.

Toelichting bij eis:

Bijvoorbeeld bij falen van verzenden van een voorschrift kan de voorschrijver besluiten terug te grijpen op een papieren recept. Opnieuw blijven proberen is dan niet altijd nodig (mits de verwijzindex correct is) noch zinvol.

Identificatiecode	GBX.BTW.e4080
Vz vz_Moscow	Conditioneel
Vz vz_Req_Soort	Functional
Vz vz_Req_Verificatie	Acceptatietest

GBX.BTW.e4010 - Gebruik van (tokens bij verzenden) (duplicaat)bericht

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.

Identificatiecode	GBX.BTW.e4010
Vz vz_Moscow	Verplicht (Must)
Vz vz_Req_Soort	Functional
Vz vz_Req_Verificatie	Monitoring

GBX.BVL.e4090 - Onderscheiden van fictieve gegevens

Eis:

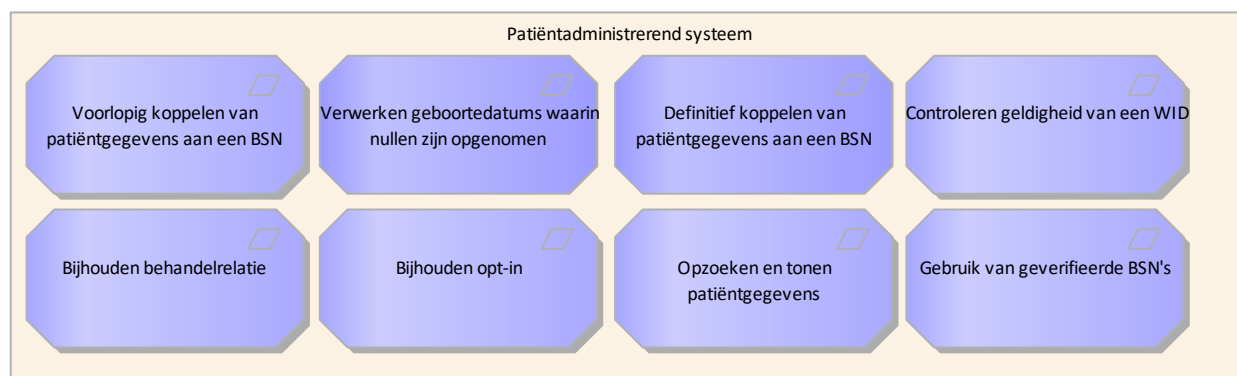
Het systeem moet fictieve gegevens opvallend onderscheidend presenteren aan gebruikers.

Toelichting bij eis:

Deze eis dient om onjuist gebruik van fictieve gegevens te voorkomen.

Identificatiecode	GBX.BVL.e4090
Vz vz_Moscow	Verplicht (Must)
Vz vz_Req_Soort	Functional
Vz vz_Req_Verificatie	Demo

2.6. Eisen Infrastructurele Systeemrollen - Patiëntadministratie



GBX.IDA.e4050 - Bijhouden behandelrelatie

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.

Identificatiecode	GBX.IDA.e4050
Vzvv_Moscow	Optioneel
Vzvv_Req_Soort	Functional
Vzvv_Req_Type	Product
Vzvv_Req_Verificatie	Acceptatietest

GBX.IDA.e4100.1 - Bijhouden opt-in

Eis:

Het systeem moet in de lokale patiëntadministratie een zogenaamde opt-in-registratie bijhouden waarin voor iedere patiënt/cliënt wordt geregistreerd of de patiënt/cliënt wel of niet akkoord is met het beschikbaar stellen van zijn medische gegevens aan andere zorgaanbieders die bij de behandeling van de patiënt betrokken zijn. Deze opt-in-registratie moet de mogelijkheid bieden aan de gebruiker om per patiënt te registreren:

1. of de patiënt gevraagd is om akkoord te gaan met het beschikbaar stellen van zijn medische gegevens aan andere zorgaanbieders (opt-in);
2. of de patiënt naar aanleiding van deze vraag akkoord is gegaan;
3. de datum waarop de patiënt akkoord is gegaan;

4. de einddatum van de geldigheid van de opt-in;
5. een unieke identificatie van de set van voorwaarden waarmee de patiënt heeft ingestemd.

Toelichting bij eis:

De geldigheid van de opt-in kan onbeperkt zijn.

De unieke identificatie genoemd onder 5) moet een verwijzing zijn naar de juiste toestemmingsfolder van VZVZ met de juiste uitgavedatum.

Eis vervalt na migratie naar Mitz

Identificatiecode	GBX.IDA.e4100.1
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Acceptatietest

GBX.IDA.e4040 - Controleren geldigheid van een WID

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.
3. 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.

Identificatiecode	GBX.IDA.e4040
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Acceptatietest

GBX.IDA.e4030 - Definitief koppelen van patiëntgegevens aan een BSN

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 gelijkheid van de in de WID genoemde identificerende gegevens,
 - ii. Vergewissen,
 1. Datum en tijd van vaststellen,
 2. indien beschikbaar het UZI-nummer of anderszins een unieke identificatie van de gebruiker, en het UZI-nummer van de 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 [Bbsn-z] 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 geverifieerd 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 geverifieerd 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.

Identificatiecode	GBX.IDA.e4030
Vzvv_Moscow	Optioneel
Vzvv_Req_Soort	Functional
Vzvv_Req_Type	Product
Vzvv_Req_Verificatie	Acceptatietest

GBX.IDA.e4060.1 - Gebruik van geverifieerde BSN's

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.

Identificatiecode	GBX.IDA.e4060.1
Vz vz_INI	INI-9140
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Functional
Vz vz_Req_Verificatie	Acceptatietest

GBX.IDA.e4010.1 - Opzoeken en tonen patiëntgegevens

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,
5. indien beschikbaar het UZI-nummer of anders een unieke identificatie van de gebruiker en het UZI-nummer van mandaterende zorgverlener indien van toepassing
6. 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.

Identificatiecode	GBX.IDA.e4010.1
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product

GBX.IDA.e4015 - Verwerken geboortedatums waarin nullen zijn opgenomen**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 worden 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.

Identificatiecode	GBX.IDA.e4015
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Acceptatietest

GBX.IDA.e4020 - Voorlopig koppelen van patiëntgegevens aan een BSN**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.

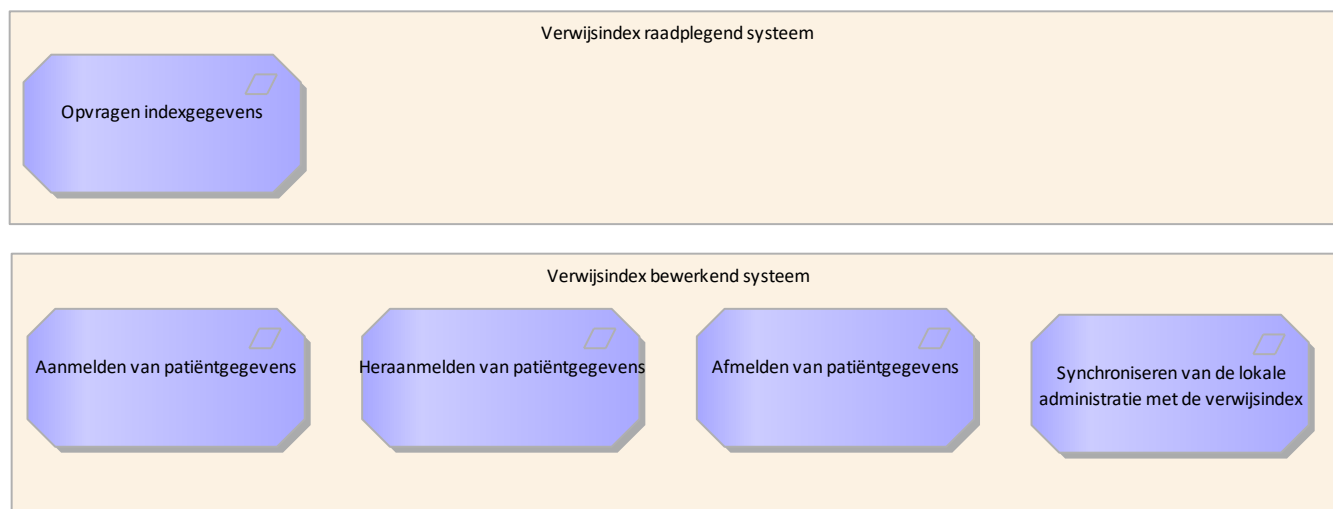
Toelichting bij eis:

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.

Identificatiecode	GBX.IDA.e4020
Vzvv_Moscow	Verplicht
Vzvv_Req_Soort	Functional
Vzvv_Req_Type	Product
Vzvv_Req_Verificatie	Acceptatietest

2.7. Eisen Infrastructurele Systemrollen - Verwijsindex



GBX.VWI.e4010.3 - Aanmelden van patiëntgegevens

Beginsituatie

1. De gebruiker is lokaal ingelogd op vertrouwensniveau laag of hoger.
2. Voor de onderhavige patiënt is opt-in geregistreerd.

Trigger

1. De gebruiker initieert de functie via het systeem, of
2. Het systeem initieert de functie automatisch n.a.v. het vrijgeven van patiëntgegevens.

Interacties

1. Het systeem verzendt een publicerenGegevens bericht naar de ZIM conform [HL7v3 IH VWI](#).
2. Het systeem ontvangt een bevestiging conform [HL7v3 IH VWI](#).

Resultaat

- De verwijzing is opgenomen in de verwijsindex, er is een bevestigingsbericht ontvangen door het systeem en er wordt een melding getoond aan de gebruiker (trigger 1).
- De verwijzing is opgenomen in de verwijsindex en er is een bevestigingsbericht ontvangen door het systeem (trigger 2).

Uitzonderingen

Uitzonderingen zijn beschreven in de [Foutentabel](#).

Opties

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

Responsetijd

-

Betrouwbaarheid

[Garantie geven dat gegevens in zendende en ontvangende systeem overeenstemmen](#)

Toelichting

Indien gegevens automatisch worden aangemeld, dan moet dit gebeuren op basis van een door de gebruiker vastgelegde systeeminstelling.

Identificatiecode	GBX.VWI.e4010.3
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Acceptatietest
Vz vz_Req_Vertrouwensniveau	Laag

GBX.VWI.e4030.2 - Afmelden van patiëntgegevens

Beginsituatie

De gebruiker is lokaal ingelogd op vertrouwensniveau laag of hoger.

Trigger

1. De gebruiker initieert de functie via het systeem, of
2. Het systeem initieert de functie automatisch indien er geen vrijgegeven patiëntstukken meer zijn aangemeld onder het betreffende categorie-id, of
3. Het systeem initieert de functie automatisch wanneer voor een patiënt opt-out geregistreerd wordt, indien voor deze zelfde patiënt eerder opt-in geregistreerd was en op basis hiervan gegevens waren aangemeld.

Interacties

1. Het systeem verzendt een afmeldenGegevens bericht naar de ZIM conform [HL7v3 IH VWI](#).
2. Het systeem ontvangt een bevestiging conform [HL7v3 IH VWI](#).

Resultaat

- De verwijzing is afgemeld in de verwijzindex, er is een bevestigingsbericht ontvangen door het systeem en er wordt een

melding getoond aan de gebruiker (trigger 1).

- De verwijzing is afgemeld in de verwijzindex en er is een bevestigingsbericht ontvangen door het systeem (trigger 2 en 3).

Uitzonderingen

Uitzonderingen zijn beschreven in de [Foutentabel](#).

Opties

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

Responsetijd

-

Betrouwbaarheid

[Garantie geven dat gegevens in zendende en ontvangende systeem overeenstemmen](#)

Toelichting

Afmelden van gegevens is nodig om ervoor te zorgen dat de ZIM het systeem niet langer zal vragen naar deze gegevens.

Het systeem moet aan de gebruiker een faciliteit bieden om bij het systeem aan te geven dat het een afmelding moet doen voor alle patiënten waarvoor geen opt-in is verkregen.

Identificatiecode	GBX.VWI.e4030.2
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Acceptatietest
Vz vz_Req_Vertrouwensniveau	Laag

GBX.VWI.e4020.3 - Heraanmelden van patiëntgegevens

Beginsituatie

- De gebruiker is lokaal ingelogd op vertrouwensniveau laag of hoger.
- Er zijn gegevens beschikbaar gekomen om heraan te melden.
- Voor de onderhavige patiënt is opt-in geregistreerd.

Trigger

1. De gebruiker initieert de functie via het systeem, of
2. Het systeem initieert de functie automatisch n.a.v. het vrijgeven nieuwe gegevens of het afschermen, bijwerken van bestaande patiëntgegevens.

Interacties

1. Het systeem verzendt een publicerenGegevens bericht naar de ZIM conform [HL7v3 IH VWI](#).
2. Het systeem ontvangt een bevestiging conform [HL7v3 IH VWI](#).

Resultaat

1. De verwijzing is opgenomen in de verwijfsindex, er is een bevestigingsbericht ontvangen door het systeem en er wordt een melding getoond aan de gebruiker (trigger 1).
2. De verwijzing is opgenomen in de verwijfsindex en er is een bevestigingsbericht ontvangen door het systeem (trigger 2).

Uitzonderingen

Uitzonderingen zijn beschreven in de [Foutentabel](#).

Opties

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

Responsetijd

-

Betrouwbaarheid

[Garantie geven dat gegevens in zendende en ontvangende systeem overeenstemmen](#)

Toelichting

Elke keer als de gebruiker nieuwe gegevens heeft toegevoegd, moet dit worden heraangemeld bij de VWI. Dit is nodig om ervoor te zorgen dat de verwijzingen in de VWI actueel blijven.

Als het LSP, bij een poging tot heraanmelden, aan een GBZ terugmeldt dat de categorie niet bestaat in de verwijfsindex, dan probeert het GBZ automatisch alle vrijgegeven patiëntstukken in die categorie aan te melden.

Het heraanmelden dient te gebeuren binnen 15 minuten, nadat er nieuwe patiëntstukken zijn vrijgegeven.

Identificatiecode	GBX.VWI.e4020.3
Vzvz_Moscow	Verplicht
Vzvz_Req_Soort	Functional
Vzvz_Req_Type	Product
Vzvz_Req_Verificatie	Acceptatietest
Vzvz_Req_Vertrouwensniveau	Laag

GBX.VWI.e4510.1 - Opvragen indexgegevens

Beginsituatie

1. De gebruiker is lokaal ingelogd op vertrouwensniveau laag 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 opvragenIndexgegevens-bericht naar de ZIM conform [HL7v3 IH VWI](#).
2. Het systeem ontvangt een opleverenIndexgegevens-bericht conform [HL7v3 IH VWI](#).

Resultaat

De opgeleverde gegevens zijn door het systeem:

- gepresenteerd aan de gebruiker, of
- verwerkt tot een beslissing (die is gepresenteerd aan de gebruiker), of
- verwerkt door het systeem.

Uitzonderingen

Uitzonderingen zijn beschreven in de [Foutentabel](#).

Opties

-

Responsetijd

-

Betrouwbaarheid

-

Toelichting

Deze eis is nodig voor een gebruiker die wil weten welke (soorten van) patiëntgegevens landelijk beschikbaar zijn voor een bepaalde patiënt. Indien gegevens van het initiërende systeem voldoet aan de opvraag, dan wordt deze ook opgeleverd.

Het systeem mag de gebruiker bij het opvragen van de indexgegevens slechts toegang verschaffen indien:

- de zorgverlener zelf patiëntgegevens heeft aangemeld bij de verwijzindex en de behandelrelatie niet is beëindigd, zie [Bijhouden behandelrelatie](#) , of
- de patiënt/cliënt is ingeschreven volgens [Opzoeken en tonen patiënteninformatie](#) , en:

1. een behandelrelatie is vastgelegd volgens [Bijhouden behandelrelatie](#) , of
2. een behandelrelatie blijkt uit de werkcontext, of
3. de zorgverlener alsnog uitdrukkelijk volgens [Bijhouden behandelrelatie](#) een behandelrelatie en toestemming vastlegt,

In andere gevallen moet het GBZ een foutmelding geven.

Een andere toepassing is dat een gebruiker kan controleren of dat wat er verwacht wordt in de VWI te staan, hetzelfde is als wat er daadwerkelijk in de VWI staat. Op basis hiervan zou men een synchronisatieslag uit kunnen (laten) voeren. Het opvragen van eigen gegevens kan op vertrouwensniveau laag gebeuren. Voor het opvragen van indexgegevens m.b.t. andere bronnen dient een opvragenindexgegevens-bericht op vertrouwensniveau midden te worden verstuurd.

Identificatiecode	GBX.VWI.e4510.1
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Acceptatietest
Vz vz_Req_Vertrouwensniveau	Laag

GBX.SYNC.e4010.1 - Synchroniseren van de lokale administratie met de verwijzindex

Beginsituatie

Er zijn:

- in de lokale GBZ-administratie patiëntstukken gekenmerkt als aangemeld op het LSP, of
- op het LSP patiëntstukken gekenmerkt als aangemeld door het GBZ.

Trigger

1. De GBZ-beheerder initieert de functie via het systeem, of
2. Het systeem initieert de functie automatisch n.a.v. het periodieke synchronisatiemoment.

Interacties

1. Het systeem wisselt een vergelijkingsbestand met de lokale administratie van patiëntstukken (zie [Ontwerp VWI](#) en [HL7v3 IH VWI](#)) uit met het LSP via asynchrone bestandsuitwisseling (zie [Ontwerp en IH ABU](#)).
2. Het LSP voert de vergelijking uit van de lokale administratie met hetgeen geregistreerd is in de Verwijsindex waarbij gevonden verschillen in een resultaatbestand worden gezet.
3. Het LSP wisselt het resultaatbestand (zie [Ontwerp VWI](#) en [HL7v3 IH VWI](#)) uit met het systeem via asynchrone bestandsuitwisseling (zie [Ontwerp en IH ABU](#)).
4. Het systeem wordt geacht bij ieder gevonden verschil uit het resultaat bestand de volgende actie te ondernemen:
 1. In geval van een teveel aangemelde verwijzing; Het systeem stuurt een *afmeldenVerwijzing*-bericht naar de ZIM conform [HL7v3 IH VWI](#) voor het betreffende patiëntstuk.
 2. In geval van het ontbreken van een verwijzing of het niet bijgewerkt zijn van een verwijzing; Het systeem stuurt een *publicerenGegevens*-bericht naar de ZIM conform [HL7v3 IH VWI](#) voor het betreffende patiëntstuk.
1. Bij het uitvoeren van deze acties dient er rekening gehouden te worden met een al of niet gegeven toestemming van de patiënt.

Resultaat

De inhoud van de lokale administratie komt overeen met de inhoud van de administratie van de verwijzingen in de Verwijsindex.

Uitzonderingen

Uitzonderingen zijn beschreven in de [Foutentabel](#).

Responsetijd

-

Betrouwbaarheid

-

Toelichting

Het systeem moet indien er aanleiding toe is of in

opdracht van de LSP-beheerder de lokale administratie synchroniseren met de Verwijsindex.

Het is van belang om de inhoud van de Verwijsindex zuiver te houden en daarmee eventuele fouten te voorkomen.

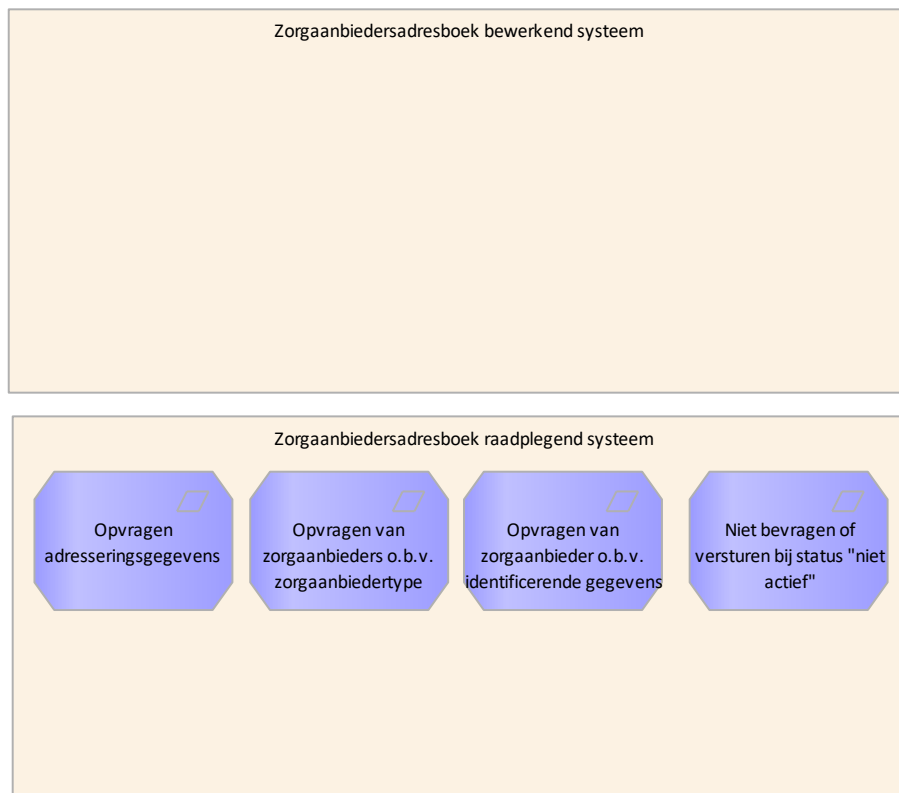
Het publiceren van indexgegevens op vertrouwensniveau laag maakt het mogelijk om een geautomatiseerd synchronisatieproces uit te voeren tussen de GBZ-administratie en de Verwijsindex. Een GBZ dient door het sturen van een BestandAanmakenGereed-bericht de synchronisatie functie te starten. Daarna worden de stappen zoals besproken in het ontwerp gevolgd.

Uiteindelijk wordt er door het GBZ een bestand met verschillen ontvangen. Al deze opgeleverde verschillen dienen door het GBZ verwerkt te worden door verwijzingen aan te maken, bij te werken of te verwijderen. Dit kan door het versturen van een publicerenGegevens bericht respectievelijk afmeldenGegevens-bericht.

Als aan de hand van veelvuldig geconstateerde foutmeldingen geconcludeerd kan worden dat de VWI mogelijk niet synchroon loopt met de lokale GBZ-administratie, dan moet het mogelijk zijn om het synchronisatieproces uit te voeren in opdracht van een LSP-beheerder.

Identificatiecode	GBX.SYNC.e4010.1
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Acceptatietest
Vz vz_Req_Vertrouwensniveau	Laag

2.8. Eisen Infrastructurele Systeemrollen - Zorgaanbiedersadresboek



GBX.ZAB.e4050 - Niet bevragen of versturen bij status "niet actief"

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 applicatielD worden verzonden. Hiermee worden onnodige foutmeldingen en onnodig verkeer voorkomen.

Identificatiecode	GBX.ZAB.e4050
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Acceptatietest

GBX.ZAB.e4010 - Opvragen adresseringsgegevens

Functie

Opvragen van technische adresseringsgegevens o.b.v. zorgaanbiedergegevens.

Karakter

Conditioneel

Conditie

In het geval deze eis is opgenomen in een PvE <Zorgtoepassing> 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 adresseringsgegevens op te vragen. Alle specifieke zoekcriteria zijn opgenomen in de [IH ZAB].

Het is mogelijk dat op basis van de zoekcriteria meerdere zorgaanbieders met hun (technische) identificeergegevens worden geretourneerd. Het aantal resultaten is beperkt tot <ZAB_Max_Zorgaanbiederaantal>.

Identificatiecode	GBX.ZAB.e4010
Vz vz_Moscow	Conditioneel
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Acceptatietest
Vz vz_Req_Vertrouwensniveau	Laag

GBX.ZAB.e4020 - Opvragen van zorgaanbieder o.b.v. identificerende gegevens

Functie

Opvragen van zorgaanbieders o.b.v. identificerende gegevens

Karakter

Conditioneel

Conditie

In het geval deze eis is opgenomen in een PvE <Zorgtoepassing> 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. gepresenteerd aan de gebruiker

Uitzonderingen

Uitzonderingen zijn beschreven in de Foutentabel.

Toelichting

Het moet mogelijk zijn om op basis van identificerende zorgaanbidergegevens (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 [IH ZAB].

Identificatiecode	GBX.ZAB.e4020
Vz vz_Moscow	Conditioneel
Vz vz_Req_Soort	Functional

Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Acceptatietest
Vz vz_Req_Vertrouwensniveau	Laag

GBX.ZAB.e4015 - Opvragen van zorgaanbieders o.b.v. zorgaanbiedertype

Functie

Opvragen van zorgaanbieders o.b.v. zorgaanbiedertype

Karakter

Conditioneel

Conditie

In het geval deze eis is opgenomen in een PvE <Zorgtoepassing> 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. 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 [IH ZAB].

Het is mogelijk dat op basis van de zoekcriteria meerdere zorgaanbieders worden geretourneerd. Het aantal resultaten is beperkt tot <ZAB_Max_Zorgaanbiederaantal>.

Identificatiecode	GBX.ZAB.e4015
Vzvv_Moscow	Conditioneel
Vzvv_Req_Soort	Functional
Vzvv_Req_Type	Product
Vzvv_Req_Verificatie	Acceptatietest

3. AORTA Eisen Kwaliteit Aangesloten Systemen

3.1. AORTA Eisen Kwaliteit aangesloten systemen - Prestatie-efficiëntie



GBX.PST.e4010 - Borgen van minimale verwerkingssnelheid

Eis:

Een GBx dient minimaal de hieronder genoemde snelheden te halen voor het verwerken van de gerelateerde HL7v3-berichten.

Interactiemechanisme Minimale verwerkingssnelheid

Sturen van gegevens <GBx-verwerkingssnelheid-sturen>

Opvragen van gegevens <GBx-verwerkingssnelheid-opvragen>

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.

Identificatiecode	GBX.PST.e4010
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Non-Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Monitoring

GBX.PST.e4015 - Tijdige verwerking van berichten

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:

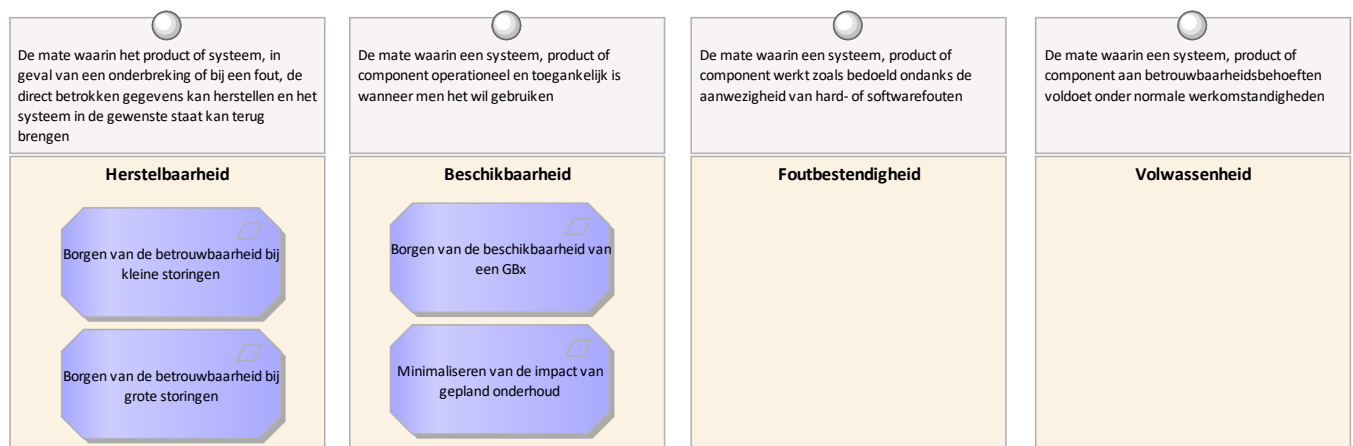
Deze eis is nodig om te voorkomen dat een zorgaanbieder bij zijn GZN of het LSP gaat klagen over te lange responstijden terwijl de oorzaak misschien ligt bij bijv. een eigen computer die in beslag wordt genomen door andere toepassingen of een lokaal netwerk met onvoldoende bandbreedte.

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.

Identificatiecode	GBX.PST.e4015
Vz vz_Moscow	Verplicht (Must)
Vz vz_Req_Soort	Non-Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Audit

3.2. 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.



GBX.BES.e4010, GBX.BES.e4010.1 - Borgen van de beschikbaarheid van een GBx

Eis:

Met uitzondering van gepland onderhoud dient een GBx-applicatie te allen tijde beschikbaar te zijn voor het afhandelen van berichten.

{GBZ} {GBP} De totale beschikbaarheid is minimaal 99,5%.

{GBK} De totale beschikbaarheid is minimaal 90,0%.

{GBO} De beschikbaarheid van het systeem is afhankelijk van procedurele afspraken tussen de uitwisselende partijen.

Toelichting bij eis:

Deze eis is nodig om te voorkomen dat een organisatie, die patiëntgegevens beschikbaar stelt of bereikbaar moet zijn om patiëntgegevens te ontvangen, de voor deze zaken benodigde systemen aan het eind van de werkdag uitschakelt. Deze eis betekent dat deze ICT-voorzieningen nagenoeg continu operationeel moeten zijn. De beschikbaarheid wordt als een voortschrijdend gemiddelde berekend. Omdat het GBK signaleringen kan ontvangen, is de eis verplicht voor GBK.

Implicaties:

Deze eis betekent dat deze ICT-voorzieningen nagenoeg continu operationeel moeten zijn. De beschikbaarheid wordt als een voortschrijdend gemiddelde berekend.

Identificatiecode	GBX.BES.e4010, GBX.BES.e4010.1
Vz vz_Moscow	Verplicht (Must)
Vz vz_Req_Soort	Non-Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Monitoring

GBX.BET.e4020.1 - Borgen van de betrouwbaarheid bij grote storingen

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 gedefinieerd. 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.

Identificatiecode	GBX.BET.e4020.1
Vz vz_INI	INI-8416
Vz vz_Moscow	Verplicht (Must)
Vz vz_Req_Soort	Non-Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Monitoring

GBX.BET.e4010.1 - Borgen van de betrouwbaarheid bij kleine storingen

Eis:

Kleine storingen in een GBx mogen niet meer dan gemiddeld <aan tal_kleine_storingen> keer per maand voorkomen en dienen dan binnen <oplostijd_kleine_storingen> 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.

Voor de waarden <aan tal_kleine_storingen> en <oplostijd_kleine_storingen> moeten de waardes gehanteerd worden zoals zijn opgenomen in de [AORTA DAP]. Deze eis dient als kapstokeis. Het is mogelijk dat de tekst en variabele namen in de [AORTA DAP] afwijken van deze eis.

Identificatiecode	GBX.BET.e4010.1
Vz vz_INI	INI-8416
Vz vz_Moscow	Verplicht (Must)
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Monitoring

GBX.BES.e4020, GBX.BES.e4020.1 - Minimaliseren van de impact van gepland onderhoud

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 GBZ 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 GBZ slechts kort onbeschikbaar hoeft te zijn. Omdat het GBK signaleringen kan ontvangen, is de eis verplicht voor GBK.

Implicaties:

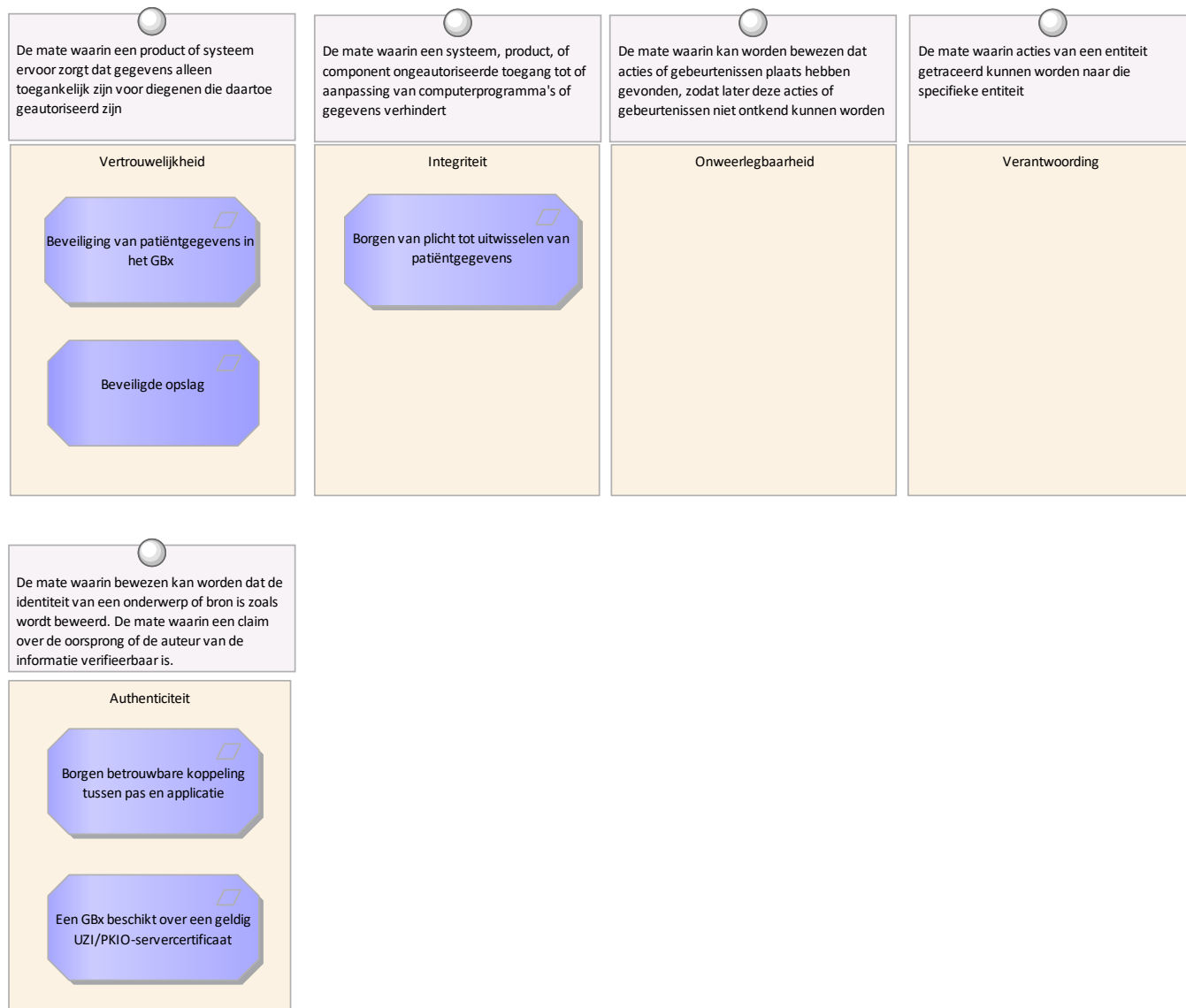
Deze eis betekent voor de organisatie dat onderhoud van de ICT-voorzieningen zoveel mogelijk wordt gepland en zodanig voorbereid dat het GBX slechts kort onbeschikbaar hoeft te zijn.

Identificatiecode	GBX.BES.e4020, GBX.BES.e4020.1
Vz vz_Moscow	Verplicht (Must)
Vz vz_Req_Soort	Non-Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Monitoring

3.3. 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 Beveiligbaarheid volgens ISO 25010.



SYS.BVL.e4010 - Beveiligde opslag

Eis:

Data die persoonsgegevens bevatten dienen geëncrypted 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

behoefte van een autorisatiesessie. Mocht hiervan met het oog op systeemprestaties van afgeweken worden, dan dient dit overlegt te worden met de DVZA-opdrachtgever.

Identificatiecode	SYS.BVL.e4010
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Audit

GBX.BVL.e4060 - Beveiliging van patiëntgegevens in het GBx

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.

Identificatiecode	GBX.BVL.e4060
Vz vz_Moscow	Verplicht (Must)
Vz vz_Req_Soort	Non-Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Documentverificatie

GBX.BVL.e4050.1 - Borgen betrouwbare koppeling tussen pas en applicatie

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.

Identificatiecode	GBX.BVL.e4050.1
Vz vz_Moscow	Verplicht (Must)
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Audit

GBX.BVL.e4070 - Borgen van plicht tot uitwisselen van patiëntgegevens

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.

Identificatiecode	GBX.BVL.e4070
Vz vz_Moscow	Verplicht (Must)
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Monitoring

GBX.BVL.e4080 (voorheen GBX.BVL.e4080.1) - Een GBx beschikt over een geldig UZI/PKIO-servercertificaat

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:

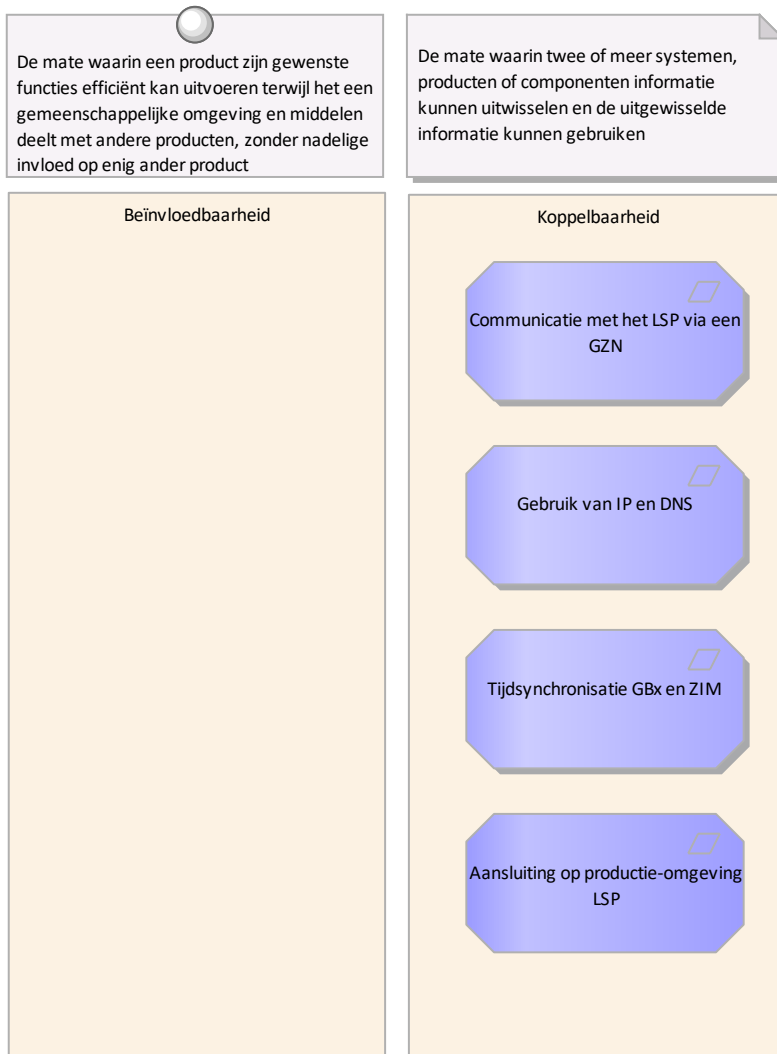
Deze eis is nodig opdat de authenticiteit van het GBx en de exclusiviteit van getransporteerde gegevens door een Trusted Third Party (TTP) kan worden gewaarborgd.

Identificatiecode	GBX.BVL.e4080 (voorheen GBX.BVL.e4080.1)
Vz vz_Moscow	Verplicht (Must)
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Aansluittoets

3.4. 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.



GBX.CON.e4120 - Aansluiting op productie-omgeving LSP

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.

Identificatiecode	GBX.CON.e4120
Vz vz_INI	INI-6499
Vz vz_Req_Soort	Non-Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Monitoring

GBX.CON.e4010, GBX.CON.e4010.1 - Communicatie met het LSP via een GZN

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.

Identificatiecode	GBX.CON.e4010, GBX.CON.e4010.1
Vz vz_Moscow	Verplicht (Must)
Vz vz_Req_Soort	Non-Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Aansluittoets

GBX.CON.e4020, GBX.CON.e4020.1, GBX.CON.e4020.2 - Gebruik van IP en DNS

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/GB0 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.

Identificatiecode	GBX.CON.e4020, GBX.CON.e4020.1, GBX.CON.e4020.2
Vz vz_Moscow	Verplicht (Must)
Vz vz_Req_Soort	Non-Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Aansluittoets

GBX.CON.e4030, GBX.CON.e4030.1 - Tijdsynchronisatie GBx en ZIM

Eis:

Een GBx dient NTP te gebruiken voor tijdsynchronisatie met de ZIM. De tijd klok van een GBx mag niet meer dan een halve seconde afwijken van de tijd klok van de ZIM.

Toelichting bij eis:

Deze eis is nodig om te voorkomen dat de tijd klok van het GBx gaat afwijken van de tijd klok 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.

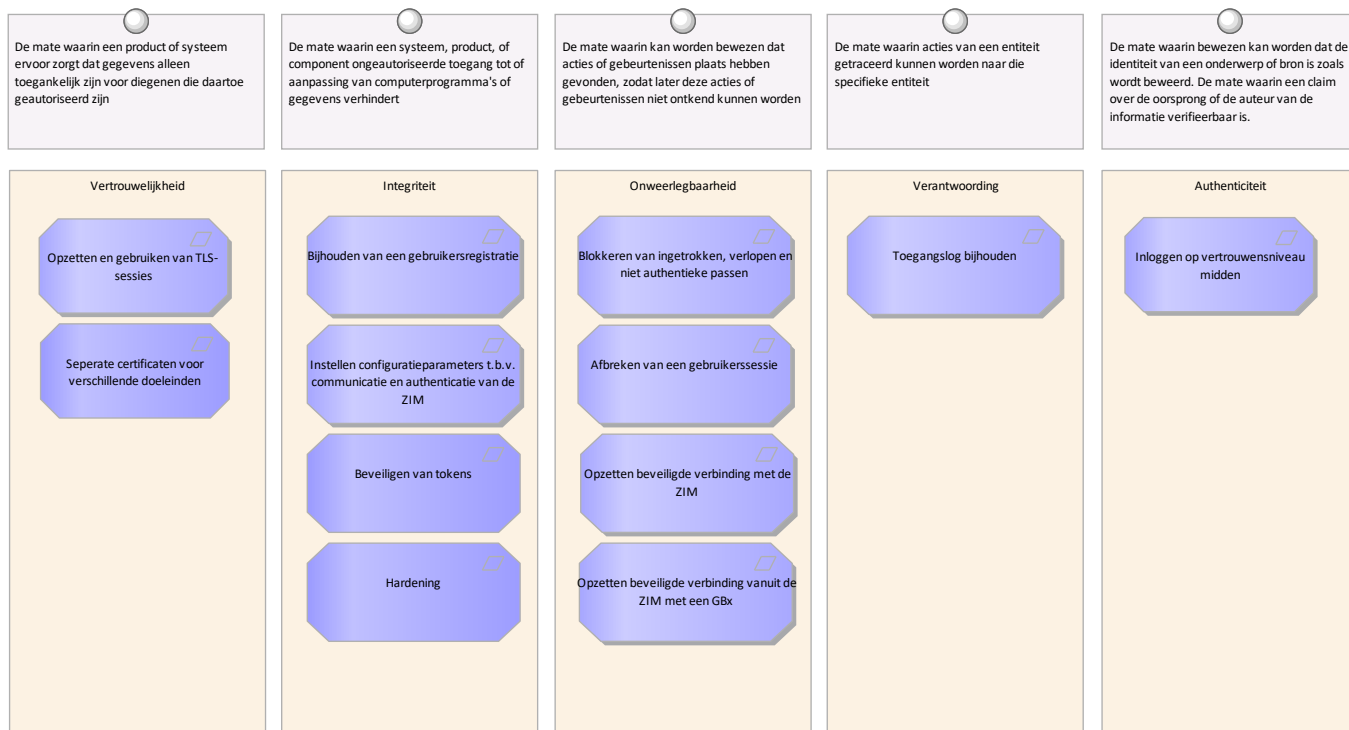
Deze eis betekent voor de organisatie dat er binnen het GBx een NTP-client is geïnstalleerd en dat deze is afgestemd op de NTP-server van de ZIM. Ook is het mogelijk dat de GZN een gezamenlijke NTP-client beheert voor alle aangesloten zorgaanbieders en op een andere wijze klaarspeelt dat de tijd klok van hun GBx'en gelijk lopen met die van de ZIM. Deze eis betekent voor de organisatie dat het GBx periodiek moet synchroniseren met de ZIM.

Identificatiecode	GBX.CON.e4030, GBX.CON.e4030.1
Vz vz_Moscow	Verplicht (Must)
Vz vz_Req_Soort	Non-Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Monitoring

4. AORTA Eisen Kwaliteit Applicatie

4.1. 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.



GBX.IDA.e4090 - Afbreken van een gebruikerssessie

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 [gebruiker-max-applicatie-onbruik](#) niet is gebruikt;
4. wanneer de sessie gedurende *<gebruiker-max-sessie-duur>* open staat.
5. IP-adres van gebruiker gedurende een sessie wijzigt.

De parameter [gebruiker-max-applicatie-onbruik](#) is binnen de applicatie instelbaar, naar redelijkheid en risico, en heeft een maximale waarde van 60 minuten.

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.

Identificatiecode	GBX.IDA.e4090
Vz vz_Moscow	Verplicht (Must)
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Acceptatietest

GBX.FBH.e4070.1 - Beveiligen van tokens

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.

Identificatiecode	GBX.FBH.e4070.1
Vz vz_INI	INI-9282
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Audit

GBX.FBH.e4030 - Bijhouden van een gebruikersregistratie

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.

Identificatiecode	GBX.FBH.e4030
Vz vz_Moscow	Verplicht (Must)
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Acceptatietest

GBX.IDA.e4085.2 - Blokkeren van ingetrokken, verlopen en niet authentieke passen

Eis:

Het GBx dient het starten van een gebruikerssessie 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.

Identificatiecode	GBX.IDA.e4085.2
Vz vz_Moscow	Verplicht (Must)
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Acceptatietest

SYS.BVL.e4065 - Hardening

Eis:

Er dient hardening op de diverse systeemplagen te worden toegepast. Het gaat hierbij om hardening op het niveau van operating system, middleware en database.

Alle systeemparemeters 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.

Identificatiecode	SYS.BVL.e4065
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Non-Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Audit

GBX.IDA.e4080.3 - Inloggen op vertrouwensniveau midden

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.

Identificatiecode	GBX.IDA.e4080.3
Vz vz_Moscow	Verplicht (Must)
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Audit

GBX.FBH.e4050.2 - Instellen configuratieparameters t.b.v. communicatie en authenticatie van de ZIM

Eis:

De GBx-beheerder moet de volgende configuratieparameters in het GBx kunnen instellen:

1. URI en hostnaam van de ZIM,
2. applicatie-id,
3. applicatie-id van het operationele schakelpunt 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.

Identificatiecode	GBX.FBH.e4050.2
Vz vz_Moscow	Verplicht (Must)
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Acceptatietest

GBX.CON.e4080.3 - Opzetten beveiligde verbinding met de ZIM

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
2. tijdelijke sleutels die elke [applicatie-max-sleutel-duur](#) ververs worden door middel van TLS Secure Renegotiation;
3. gebruikmakend van Cipher Suites die door het NCSC minimaal worden gekenmerkt als voldoende;
4. gebruikmakend van de sterkste cipher suite die gedeeld wordt met de ZIM;
5. een ten hoogste ongebruikte TLS-sessie van [applicatie-max-sessie-onbruik](#).

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.

Identificatiecode	GBX.CON.e4080.3
Vz vz_Moscow	Conditioneel.
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Acceptatietest

GBX.CON.e4090.2 - Opzetten beveiligde verbinding vanuit de ZIM met een GBx

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 [systeem-max-sleutel-duur](#) ververs worden,
3. gebruikmakend van Cipher Suites die door het NCSC minimaal worden gekenmerkt als voldoende(goed dus altijd ook) en tevens worden ondersteund door de ZIM.Voor encryptie moet altijd de sterkste vorm als eerste worden geprobeerd,
4. een maximale sessieduur van [systeem-max-sessie-duur](#),
5. een ten hoogste ongebruikte TLS-sessie van [systeem-max-sessie-onbruik](#).

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.

Identificatiecode	GBX.CON.e4090.2
Vz vz_INI	INI-8598
Vz vz_Moscow	Conditioneel.
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Acceptatietest

GBX.CON.e4070.2 - Opzetten en gebruiken van TLS-sessies

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.

Identificatiecode	GBX.CON.e4070.2
Vz vz_Moscow	Verplicht (Must)
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Acceptatietest

GBX.BVL.e4100.1 - Seperate certificaten voor verschillende doeleinden

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 (ref. [4]); 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.

Conditie:

De verplichting voor het gebruik van een sepeeraat certificaat is afhankelijk van de grootte van de zorgaanbiederorganisatie.

Deze eis zal in overleg met VZVZ wel of niet toegepast dienen te worden.

Identificatiecode	GBX.BVL.e4100.1
Vzvz_INI	INI-9103
Vzvz_Moscow	Conditioneel
Vzvz_Req_Soort	Functional
Vzvz_Req_Type	Product
Vzvz_Req_Verificatie	Audit

GBX.LOG.e4015.1 - Toegangslog bijhouden

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:

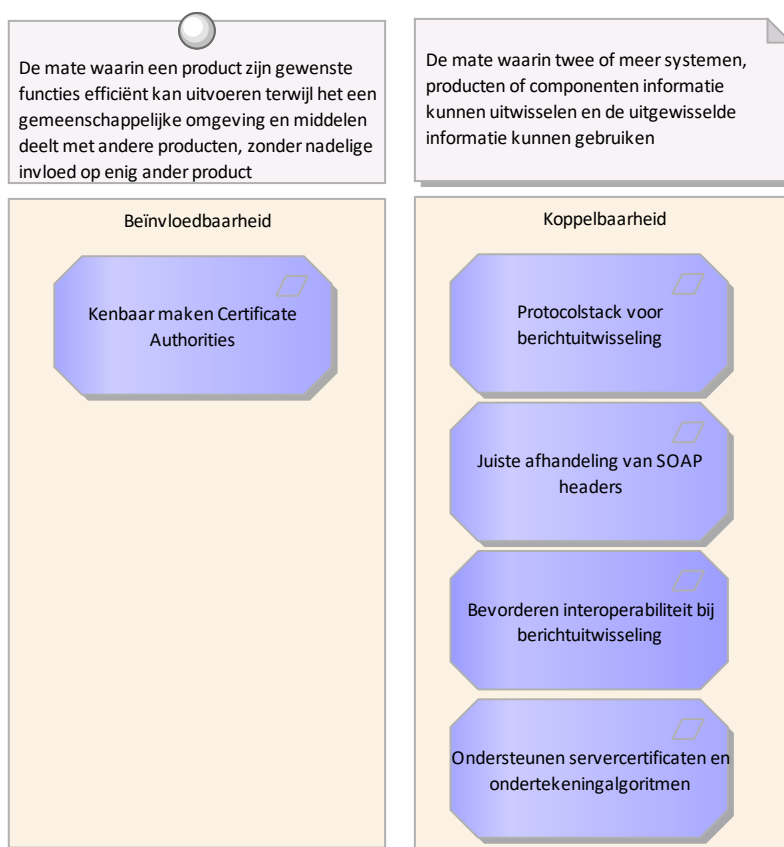
- {GBx}{GBO} wat voor soort patiëntstukken wanneer zijn opgevraagd door welke zorgverlener/medewerker van welke andere zorgaanbieder;
- {GBK} wat voor soort opvragingen, opdrachten en kennisgevingen wanneer zijn verzonden resp. ontvangen door welke klantenloketmedewerker;
- wat voor soort patiëntstukken 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.

Identificatiecode	GBX.LOG.e4015.1
Vzvv_INI	INI-9201 INI-9106
Vzvv_Moscow	Verplicht (Must)
Vzvv_Req_Soort	Functional
Vzvv_Req_Type	Product
Vzvv_Req_Verificatie	Acceptatietest

4.2. 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.



GBX.CON.e4066 - Bevorderen interoperabiliteit bij berichtuitwisseling

Eis:

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

Identificatiecode	GBX.CON.e4066
Vzvv_Moscow	Verplicht
Vzvv_Req_Soort	Functional
Vzvv_Req_Type	Product
Vzvv_Req_Verificatie	Acceptatietest

GBX.CON.e4065 - Juiste afhandeling van SOAP headers

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'.

Identificatiecode	GBX.CON.e4065
Vz vz_Moscow	Verplicht (Must)
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Acceptatietest

GBX.CON.e4100 - Kenbaar maken Certificate Authorities

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.

Identificatiecode	GBX.CON.e4100
Vz vz_Moscow	Verplicht (Must)
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Acceptatietest

GBX.CON.e4110.2 - Ondersteunen servercertificaten en ondertekeningalgoritmen

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 ondertekeningalgoritme.

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.

Identificatiecode	GBX.CON.e4110.2
Vz vz_Moscow	Verplicht (Must)
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Monitoring

GBX.CON.e4060.1 (voorheen GBX.CON.e4060.2, GBZ.AE.CON.e01,GBZ.AE.CON.e04, GBP.AE.CON.e01) - Protocolstack voor berichtuitwisseling

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
- TCP
- IPv4

Toelichting bij eis:

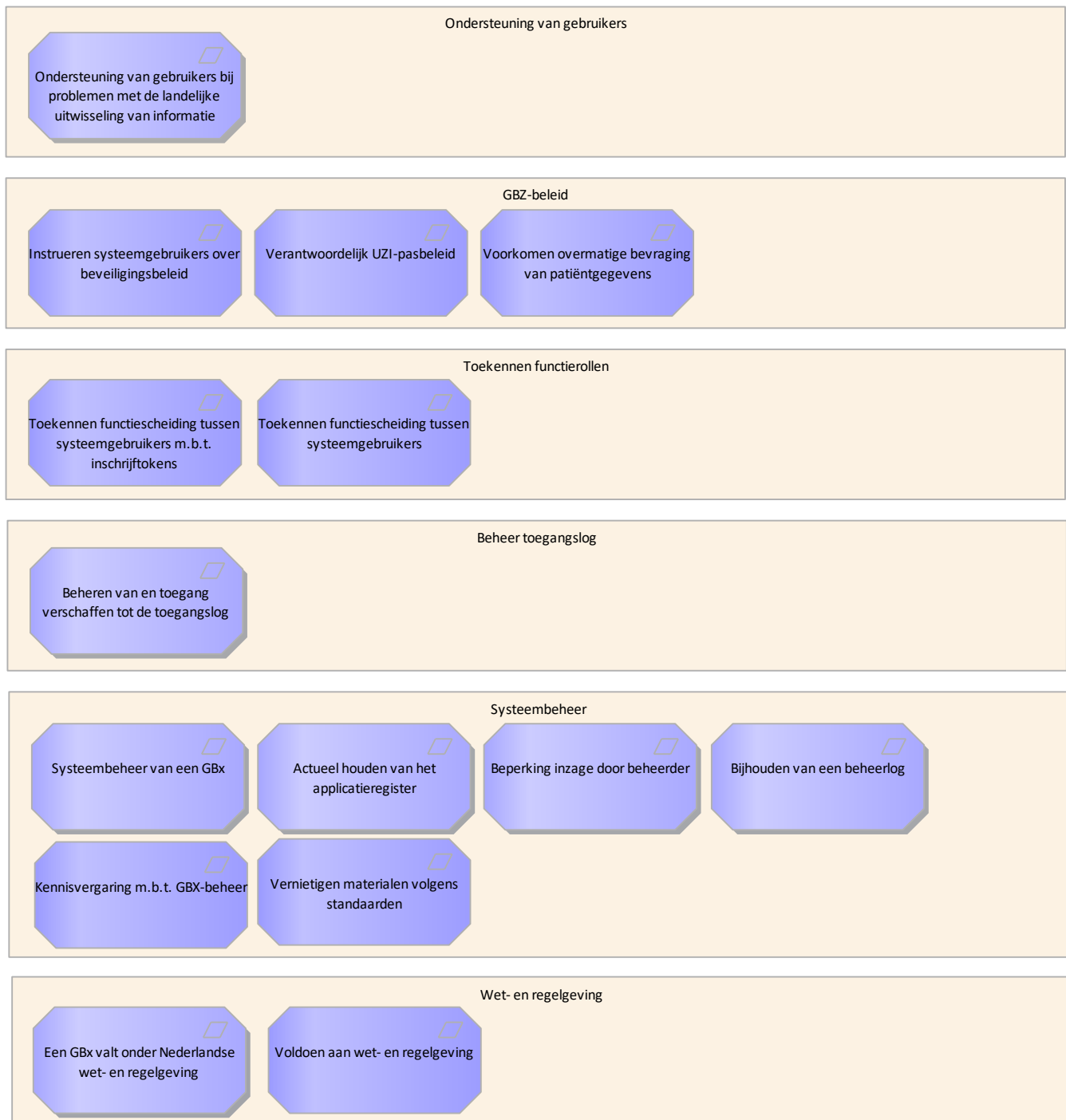
Het is niet toegestaan om een lagere protocolversie te hanteren dan die in deze protocolstack vermeld is, zoals bv SSLv2 en SSLv3.

Het GBX volgt voor berichtuitwisseling de WS-I Basic Profile 1.0 specificaties.

Identificatiecode	GBX.CON.e4060.1 (voorheen GBX.CON.e4060.2, GBZ.AE.CON.e01,GBZ.AE.CON.e04, GBP.AE.CON.e01)
Vz vz_Moscow	Verplicht (Must)
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Aansluittoets

5. AORTA Eisen Organisatie van een GBX

5.1. Eisen aan de beheerorganisatie van een GBX



GBX.SBH.e4030 (voorheen GBX.SBH.e4030.1) - Actueel houden van het applicatieregister

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.

Identificatiecode	GBX.SBH.e4030 (voorheen GBX.SBH.e4030.1)
Vz vz_Moscow	Verplicht (Must)
Vz vz_Req_Soort	Non-Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Documentverificatie

GBX.SBH.e4010 (voorheen GBX.SBH.e4010.1) - Beheren van en toegang verschaffen tot de toegangslog

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.

Identificatiecode	GBX.SBH.e4010 (voorheen GBX.SBH.e4010.1)
Vz vz_Moscow	Verplicht (Must)
Vz vz_Req_Soort	Non-Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Audit

GBX.SBH.e4040.3 - Beperking inzage door beheerder

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.

Identificatiecode	GBX.SBH.e4040.3
Vz vz_INI	INI-8412
Vz vz_Moscow	Verplicht (Must)
Vz vz_Req_Soort	Non-Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Documentverificatie

GBX.SBH.e4050 - Bijhouden van een beheerlog

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.

Identificatiecode	GBX.SBH.e4050
Vz vz_Moscow	Verplicht (Must)
Vz vz_Req_Soort	Non-Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Audit

GBX.CON.e4050.1 (voorheen GBX.ALG.e4010, GBX.CON.e4050.2) - Een GBx valt onder Nederlandse wet- en regelgeving

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.

Identificatiecode	GBX.CON.e4050.1 (voorheen GBX.ALG.e4010, GBX.CON.e4050.2)
Vz vz_Moscow	Verplicht (Must)
Vz vz_Req_Soort	Non-Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Aansluittoets

GBX.FBH.e4015 - Instrueren systeemgebruikers over beveiligingsbeleid

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.

Identificatiecode	GBX.FBH.e4015
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Non-Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Monitoring

GBX.SBH.e4060 - Kennisvergaring m.b.t. GBX-beheer

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.

Identificatiecode	GBX.SBH.e4060
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Non-Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Aansluittoets

GBX.FBH.e4010 (voorheen GBX.FBH.e4010.1, GBX.FBH.e4010.3, GBX.FBH.e4000, GBP.FBH.e4010) - Ondersteuning van gebruikers bij problemen met de landelijke uitwisseling van informatie

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.

Identificatiecode	GBX.FBH.e4010 (voorheen GBX.FBH.e4010.1, GBX.FBH.e4010.3, GBX.FBH.e4000, GBP.FBH.e4010)
Vz vz_Moscow	Verplicht (Must)
Vz vz_Req_Soort	Non-Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Documentverificatie

GBX.SBH.e4020 (voorheen GBX.SBH.e4020.2) - Systeembeheer van een GBx

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.

Identificatiecode	GBX.SBH.e4020 (voorheen GBX.SBH.e4020.2)
Vz vz_Moscow	Verplicht (Must)
Vz vz_Req_Soort	Non-Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Documentverificatie

GBX.FBH.e4025 - Toekennen functiescheiding tussen systeemgebruikers

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.

Identificatiecode	GBX.FBH.e4025
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Non-Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Audit

GBX.FBH.e4020 - Toekennen functiescheiding tussen systeemgebruikers m.b.t. inschrijftokens

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 bevroegd, doordat medewerkers niet zowel patiënten mogen inschrijven als betrokken zijn bij de medische processen.

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.

Conditie:

Deze eis zal verplicht zijn voor grote zorgorganisaties. In overleg met VZVZ kan bepaald worden of deze eis verplicht zal zijn.

Identificatiecode	GBX.FBH.e4020
Vz vz_Moscow	Conditioneel
Vz vz_Req_Soort	Non-Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Audit

GBX.FBH.e4017 - Verantwoordelijk UZI-pasbeleid

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.

Identificatiecode	GBX.FBH.e4017
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Non-Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Monitoring

GBX.SBH.e4070 - Vernietigen materialen volgens standaarden

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.

Identificatiecode	GBX.SBH.e4070
Vz vz_Moscow	Verplicht (Must)
Vz vz_Req_Soort	Functional
Vz vz_Req_Type	Business
Vz vz_Req_Verificatie	Eigenverklaring
Vz vz_Sleutel	GBX.SBH.e4070

GBX.ALG.e4010 - Voldoen aan wet- en regelgeving

Eis:

Een GBX dient te voldoen aan de NEN751x 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.

Identificatiecode	GBX.ALG.e4010
Vz vz_Moscow	Verplicht (Must)
Vz vz_Req_Soort	Non-Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Eigenverklaring

GBX.FBH.e4018 - Voorkomen overmatige bevraging van patiëntgegevens

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 initieert 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.

Identificatiecode	GBX.FBH.e4018
Vz vz_Moscow	Verplicht
Vz vz_Req_Soort	Non-Functional
Vz vz_Req_Type	Product
Vz vz_Req_Verificatie	Monitoring