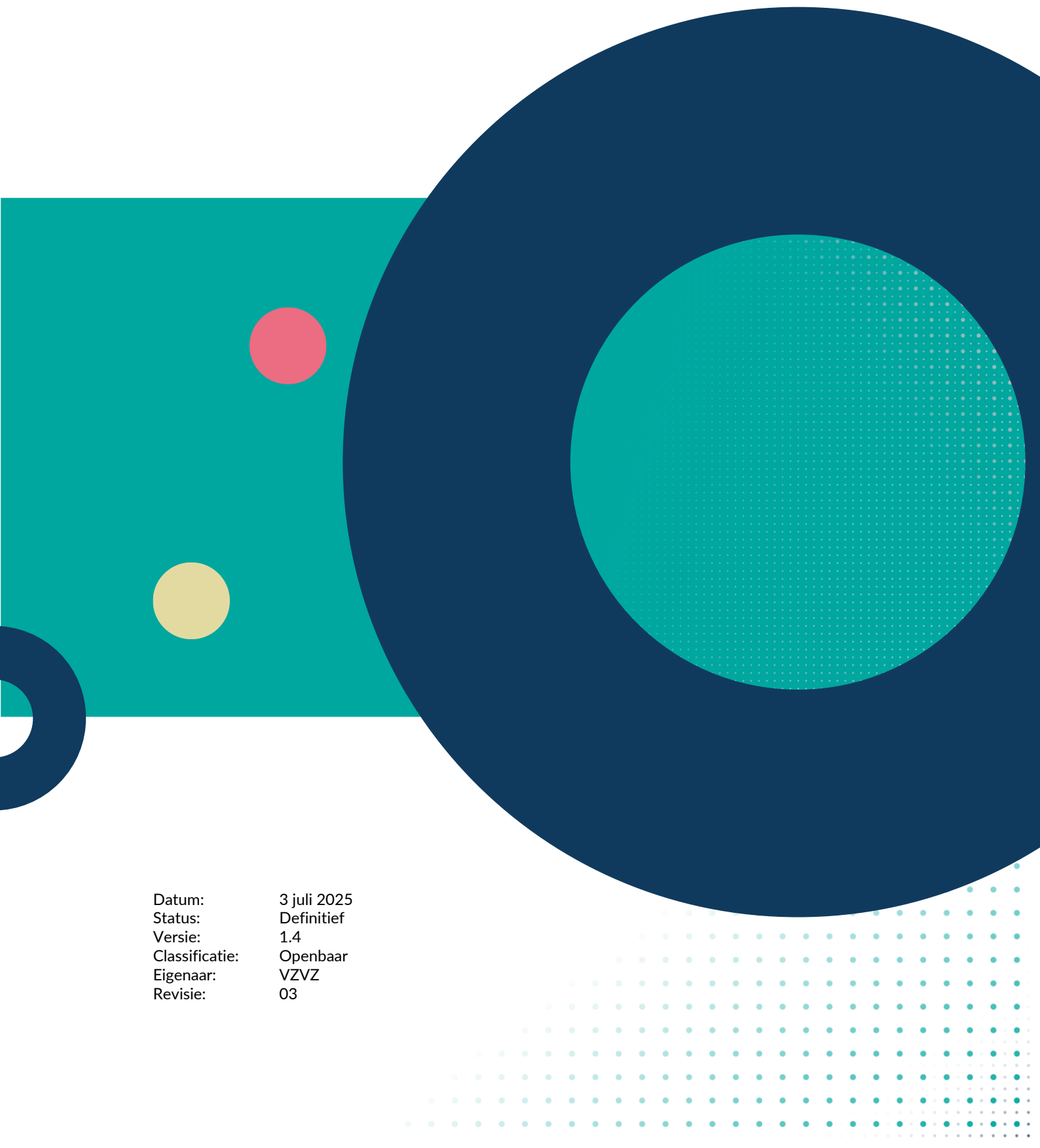




PvE HAPIS

Acute Zorg

Datum: 3 juli 2025
Status: Definitief
Versie: 1.4
Classificatie: Openbaar
Eigenaar: VZVZ
Revisie: 03



Documenthistorie

Datum	Status	Versie	Omschrijving
2 november 2023	Definitief	1.3	Initiële document
14 februari 2025	Definitief	1.4	Verwijderd: Systeemrollen - Infrastructuur - Gegevens opvragend systeem GBX.AUT.e4520 GBX.AUT.e4515 GBX.IDA.e4015 GBX.FBH.e4090 GBX.FBH.e4018 GBX.BVL.e4050.1 Toegevoegd: Primaire interactie - ontvangend systeem Token beherend systeem GBX.OPV.e4170 GBX.ADR.e4010.1 GBX.ADR.e4020 GBX.FBH.e4070.2 GBX.BVL.e4100.1 AZ.BER.e4050 AZ.BER.e4040 GBX.BVL.e4090 Aangepast: GBX.ALG.e4010.1 GBX.SBH.e4070.1 GBX.CON.e4050.2 GBX.SBH.e4050.1 GBX.SBH.e4020.1 GBX.SBH.e4010.1 GBX.IDA.e4010.2 GBX.IDA.e4050.1 GBX.IDA.e4040.1 GBX.IDA.e4030.2 GBX.IDA.e4015.1 SYS.BVL.e4010.2 GBX.CON.e4090.3 GBX.FBH.e4030.1 GBX.CON.e4080.6 GBX.IDA.e4080.5 XIS.SVD.e4010.2 GBX.FBH.e4070.2 GBX.IDA.e4085.4 GBX.AUT.e4521.3 GBX.AUT.e4516.2 GBX.AUT.e4514.3 GBX.AUT.e4513.3 GBX.AUT.e4511.2 GBX.OPV.e4110.1
2 juni 2025	Definitief	1.4 revisie 02	Verwijderd: GBX.STU.e4020 GBX.OPV.e4210

			Toegevoegd: GBX.AZ.e4060 GBX.OPV.e4212 Gewijzigd: GBX.AUT.e4517.1 GBX.AUT.e4521.4 GBX.IDA.e4030.3 GBX.IDA.e4015.2 GBX.IDA.e4020.1 GBX.OPV.e4110.2 GBX.CON.e4120.1 GBX.CON.e4010.2 GBX.BVL.e4100.2 GBX.CON.e4070.3 GBX.CON.e4060.3 AGE.LOG.e4060.1 GBX.SBH.e4040.4 AGE.LOG.e4070.1 GBX.APR.e4160.1 GBX.APR.e4140.1 GBX.AUT.e4516.3 GBX.AUT.e4511.3 GBX.OPV.e4160.2 GBX.AUT.e4514.4 GBX.ADR.e4020.1 GBX.STU.e4510.1 GBX.BES.e4010.1 SYS.BVL.e4010.3 GBX.BVL.e4070.1 GBX.CON.e4050.3 GBX.SBH.e4020.2 GBX.BVL.e4090.1
03 juli 2025	Definitief	1.4 revisie 3	Toegevoegd: AZ.BER.e4045

Inhoudsopgave

Documenthistorie	2
1 Inleiding.....	6
1.1 Inleiding	6
1.2 Doelgroep voor dit document.....	6
1.3 Doel en Scope	6
1.4 Verwijzingen.....	6
2 Generieke eisen.....	7
2.1 AORTA Eisen Infrastructurele systeemrollen	7
2.1.1 Systeemrollen - Infrastructuur - Applicatiebeheer	7
2.1.2 Systeemrollen - Infrastructuur - Gegevens versturend systeem	10
2.1.3 Primaire interactie - ontvangend systeem.....	13
2.1.4 Mandaatregistratie	16
2.1.5 Mandaattoken beherend systeem	20
2.1.6 Patiëntadministratie.....	21
2.1.7 Token beherend systeem.....	25
2.2 AORTA Eisen Kwaliteit Aangesloten Systemen.....	27
2.2.1 Betrouwbaarheid	27
2.2.2 Beveiligbaarheid	29
2.2.3 Prestatie-efficiëntie.....	31
2.2.4 Uitwisselbaarheid	34
2.3 AORTA Eisen Kwaliteit Applicatie	37
2.3.1 Beveiligbaarheid	37
2.3.2 Uitwisselbaarheid	43
2.4 AORTA Eisen aan de Beheerorganisatie van een GBX.....	46
2.4.1 Wijzigen logging.....	46
2.4.2 Vernietigen loggegevens.....	47
2.4.3 Uitschakelen logging.....	47
2.4.4 Toegangsbeheer tot logging.....	47
2.4.5 Loggen toegangsregeling	48
2.4.6 Loggen inzage logging	48
2.4.7 Bewaartermijn loggegevens	48
2.4.8 Voldoen aan wet- en regelgeving	49
2.4.9 Vernietigen materialen volgens standaarden	49
2.4.10 Een GBx valt onder Nederlandse wet- en regelgeving.....	49
2.4.11 Kennisvergaring m.b.t. GBX-beheer	50
2.4.12 Bijhouden van een beheerlog	50

2.4.13	Beperking inzage door beheerder.....	50
2.4.14	Actueel houden van het applicatieregister.....	51
2.4.15	Systeembeheer van een GBx.....	51
2.4.16	Beheren van en toegang verschaffen tot de toegangslog	51
2.4.17	Toekennen functiescheiding tussen systeemgebruikers.....	52
2.4.18	Verantwoordelijk UZI-pasbeleid.....	52
2.4.19	Instrueren systeemgebruikers over beveiligingsbeleid.....	53
2.4.20	Ondersteuning van gebruikers bij problemen met de landelijke uitwisseling van informatie	53
2.5	Generieke eisen aan een XIS.....	54
2.5.1	Onderscheiden van fictieve gegevens	54
2.6	Eisen XIS-leverancier	55
2.6.1	Inrichten XIS-servicedesk	55
2.6.2	Gebruik Supportal	55
2.6.3	Beschikbaarheid XIS-servicedesk.....	56

1 Inleiding

1.1 Inleiding

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

1.2 Doelgroep voor dit document

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

1.3 Doel en Scope

Het doel van dit document is om de eisen te beschrijven waaraan moet worden voldaan om een GBZ als HAPIS t.b.v. Acute zorg aan te sluiten op de AORTA-infrastructuur. Het gaat hierbij specifiek om de Spoedmelding (bericht 21), Triageverwijzing (bericht 20) en de Bevestiging MKA HAP (bericht 22).

1.4 Verwijzingen

In het document komen verschillende verwijzingen voor.

Verwijzingen naar eisen worden gekenmerkt door de identificatie van de eis zonder versienummer (bijvoorbeeld GBX.XXX.e4010 kan verwijzen naar GBX.XXX.4010.2).

De volgende documentverwijzingen zijn opgenomen:

- IH AORTA: <https://decor.nictiz.nl/pub/vzvv/aorta-vzvv-html-20241011T125847/index.html>
- Foutentabel: <https://aorta.scrollhelp.site/aorta-8.4.0/current/bestandenlijst>
- ZORG-AB specificaties: <https://www.vzvv.nl/diensten/gemeenschappelijke-diensten/zorg-ab/releases>
- AORTA-publicatieversie: <https://aorta.public.vzvv.nl/aorta-8.4.0>
- Verschillende documenten m.b.t. AORTA: [Bestandenlijst](#)

2 Generieke eisen

2.1 AORTA Eisen Infrastructurele systeemrollen

2.1.1 Systeemrollen - Infrastructuur - Applicatiebeheer

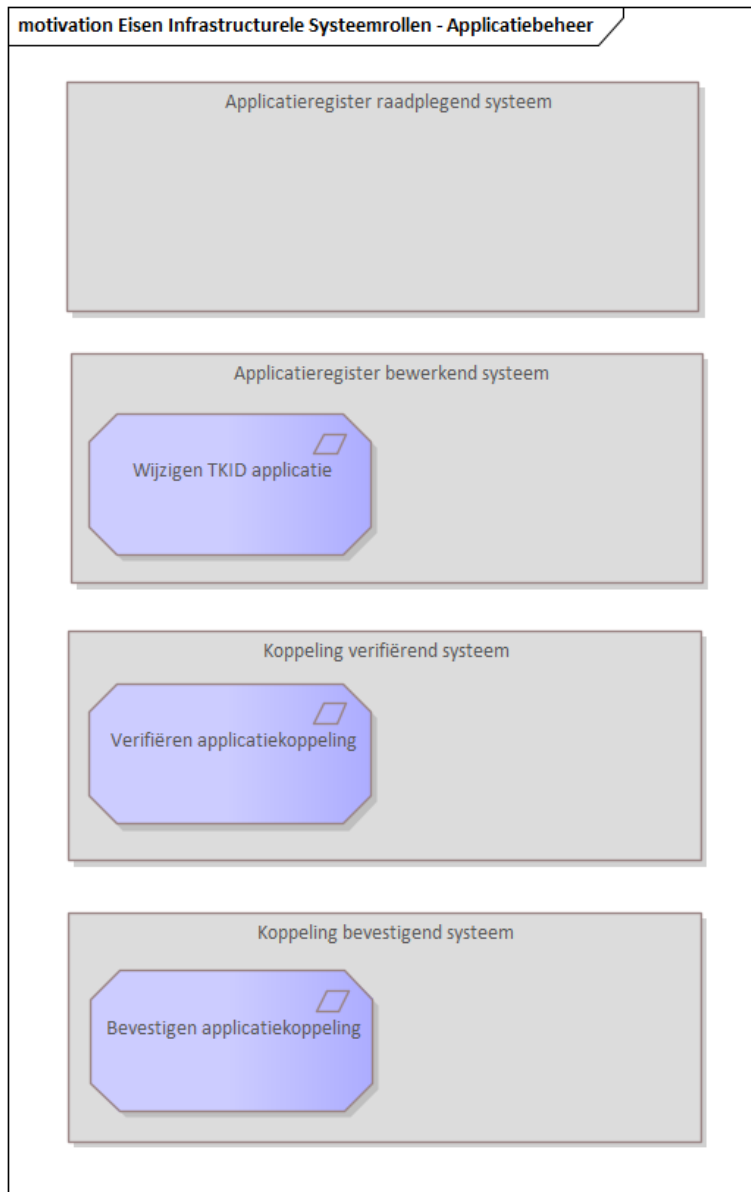


Figure 1 : Eisen Infrastructurele Systeemrollen - Applicatiebeheer

2.1.1.1 Bevestigen applicatiekoppeling

Alias: GBX.APR.e4160.1

Details
Beginsituatie Het systeem beschikt over de voor deze functie vereiste vertrouwensmiddelen.

Trigger Het systeem ontvangt een verifiëren applicatiekoppeling bericht conform IH AORTA.
Interacties Het systeem stuurt een verifiëren applicatiekoppeling antwoord terug naar de verzender conform IH AORTA.
Resultaat Het antwoordbericht is teruggestuurd naar de verzender.
Uitzonderingen Uitzonderingen zijn beschreven in de Foutentabel.
Opties -
Responsetijd Het verifiëren applicatiekoppeling antwoord dient verstuurd te worden binnen 60 seconden na ontvangst van een verifiëren applicatiekoppeling bericht.
Betrouwbaarheid -
Toelichting -

Vzvv_Moscow: Verplicht
Vzvv_Req_Verificatie: Acceptatietest
Vzvv_Req_Soort: Functional
Vzvv_Req_Type: Product

2.1.1.2 Verifiëren applicatiekoppeling

Alias: GBX.APR.e4140.1

Details
Beginsituatie De gebruiker is lokaal ingelogd op vertrouwensniveau laag of hoger.
Trigger De gebruiker initieert de functie via het systeem.
Interacties 1. Het systeem verzendt een verifiëren applicatiekoppeling bericht naar de ZIM of een ander GBX conform IH AORTA. 2. Het systeem ontvangt een verifiëren applicatiekoppeling antwoord conform IH AORTA.
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 -
Responsetijd -

Betrouwbaarheid

-

Toelichting

-

Vz vz_Moscow: Verplicht

Vz vz_Req_Verificatie: Acceptatietest

Vz vz_Req_Soort: Functional

Vz vz_Req_Type: Product

2.1.1.3 Wijzigen TKID applicatie

Alias: GBX.APR.e4060.1

Details

Beginsituatie

De gebruiker is lokaal ingelogd op vertrouwensniveau laag of hoger.

Trigger

De gebruiker initieert de functie via het systeem.

Interacties

- Het systeem verzendt een beherenTKID-bericht naar de ZIM conform IH AORTA.
- Het systeem ontvangt een ontvangstbevestiging conform IH AORTA.

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 Ontwerp Applicatieregister 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 beherenTKID-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.

Alle voor de gewenste XIS-functionaliteit benodigde TKID's moeten 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. De fout dient hersteld te worden en de TKID's dienen opnieuw ingestuurd te worden.

Voor een ontvangen beherenTKID-bericht (met daarin correcte TKID's), 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 in het bericht opgenomen TKID) niet wordt veranderd. Koppelingen die nog niet bekend waren binnen het applicatieregister krijgen direct de status 'actief'. Koppelingen die bekend zijn in het applicatieregister maar niet meer door de in het bericht opgenomen TKIDs worden vereist, worden verwijderd

Denkbare situaties voor het insturen van TKID's zijn:

- Installeren nieuwe functionaliteit m.b.t. het uitwisselen van informatie via de AORTA-infrastructuur;
- Initiële installatie;
- Nieuwe acceptatie van de XIS-applicatie;
- Terugzetten oude functionaliteit (met een eerder verkregen TKID).

Vz vz_Moscow: Verplicht

Vz vz_Req_Verificatie: Acceptatietest

Vz vz_Req_Soort: Functional

Vz vz_Req_Type: Product

2.1.2 Systeemrollen - Infrastructuur - Gegevens versturend systeem

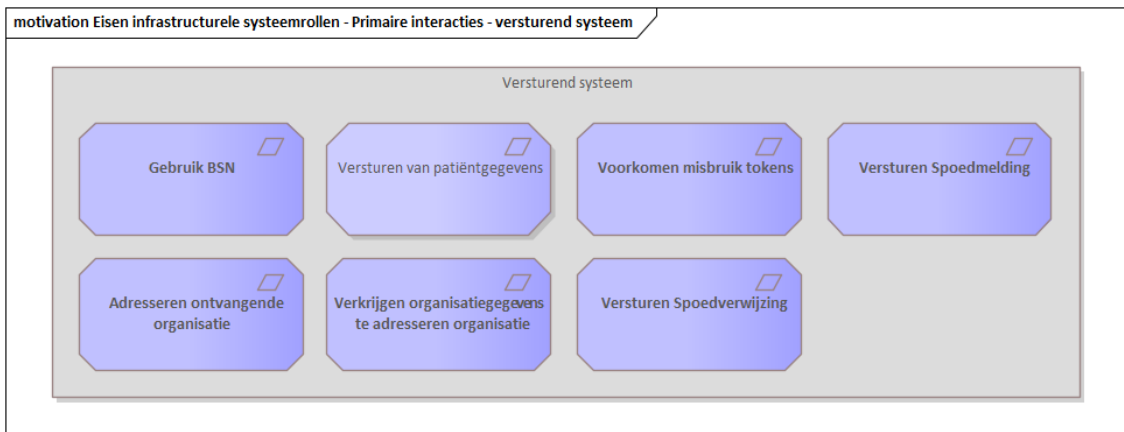


Figure 2 : Eisen infrastructurale systeemrollen - Primaire interacties - versturend systeem

2.1.2.1 Voorkomen misbruik tokens

Alias: GBX.OPV.e4170

Details
Eis: Inschrijf- en mandaattokens mogen alleen verstuurd worden over beveiligde verbindingen.
Toelichting:

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

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

2.1.2.2 *Versturen van patiëntgegevens*

Alias: GBX.STU.e4010

Details
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).

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

2.1.2.3 *Gebruik BSN*

Alias: GBX.AZ.e4060

Details
Eis:

Het systeem mag alleen een BSN opnemen in het bericht, indien er sprake is van een bij de SBV-Z gevalideerd BSN.

Toelichting bij eis:

De specificatie van het Spoedmelding-bericht en de daarbij gebruikte parameters zijn opgenomen in de Art-Decor publicatie van Acute Zorg.

Vz vz_Moscow: Verplicht

Vz vz_Req_Verificatie: Acceptatietest

Vz vz_Req_Soort: Functional

Vz vz_Req_Type: Product

2.1.2.4 Versturen Spoedmelding

Alias: AZ.BER.e4040

Details

Eis:

Het systeem moet het Spoedmelding-bericht (ZTAZ_IN000002NL01) kunnen versturen.

Toelichting bij eis:

De specificatie van het Spoedmelding-bericht en de daarbij gebruikte parameters zijn opgenomen in de Art-Decor publicatie van Acute Zorg.

Vz vz_Moscow: Verplicht

Vz vz_Req_Verificatie: Acceptatietest

Vz vz_Req_Soort: Functional

Vz vz_Req_Type: Product

2.1.2.5 Versturen Spoedverwijzing

Alias: AZ.BER.e4045

Details

Eis:

Het systeem moet het spoedverwijzing-bericht (ZTAZ_IN000001NL01) kunnen versturen.

Toelichting bij eis:

De specificatie van het spoedverwijzing-bericht en de daarbij gebruikte parameters zijn opgenomen in de Art-Decor publicatie van Acute Zorg.

Vz vz_Moscow: Verplicht

Vz vz_Req_Verificatie: Acceptatietest

Vz vz_Req_Soort: Functional

Vz vz_Req_Type: Product

2.1.2.6 Adresseren ontvangende organisatie

Alias: GBX.ADR.e4010.1

Details

Eis:

Een systeemgebruiker moet een organisatie kunnen selecteren waaraan hij een bericht wil versturen. Het moet voor een systeemgebruiker duidelijk zijn aan welke organisatie hij een bericht richt. Hiervoor dienen minimaal de volgende gegevens getoond te kunnen worden:

- Organisatienaam;
- Fysieke Adresgegevens van de organisatie.

Toelichting bij eis:

Een systeemgebruiker moet door het systeem ondersteund worden in het kunnen zoeken en selecteren van een te adresseren organisatie. Om adresseringsfouten te voorkomen, is het niet toegestaan om adresgegevens door een systeemgebruiker zelf in te laten vullen.

Vz vz_Moscow: Verplicht
Vz vz_Req_Verificatie: Acceptatietest
Vz vz_Req_Soort: Functional
Vz vz_Req_Type: Product

2.1.2.7 Verkrijgen organisatiegegevens te adresseren organisatie

Alias: GBX.ADR.e4020.1

Details
Eis: Het systeem dient actuele organisatiegegevens van de te adresseren organisatie te verkrijgen via een betrouwbare bron. Hierbij dienen de organisatiegegevens onweerlegbaar te zijn gekoppeld aan de gegevens zoals vastgelegd bij het CIBG. Toelichting bij eis: Er moet voorkomen worden dat een kwaadwillende adresgegevens in die mate muteert, dat medische gegevens naar een andere organisatie dan de door de systeemgebruiker bedoelde organisatie kunnen worden gestuurd. Hiervoor dienen adresgegevens alleen door een daarvoor geautoriseerde bron te kunnen worden aangepast. Een betrouwbare bron is een bron, waarin de CIBG-gegevens onweerlegbaar zijn vastgelegd en waarin die gegevens alleen gemuteerd kunnen worden door daarvoor geautoriseerde personen. Het ZORG-AB wordt gezien als een betrouwbare bron.

Vz vz_Moscow: Verplicht
Vz vz_Req_Verificatie: Acceptatietest
Vz vz_Req_Soort: Functional
Vz vz_Req_Type: Product

2.1.3 Primaire interactie - ontvangend systeem

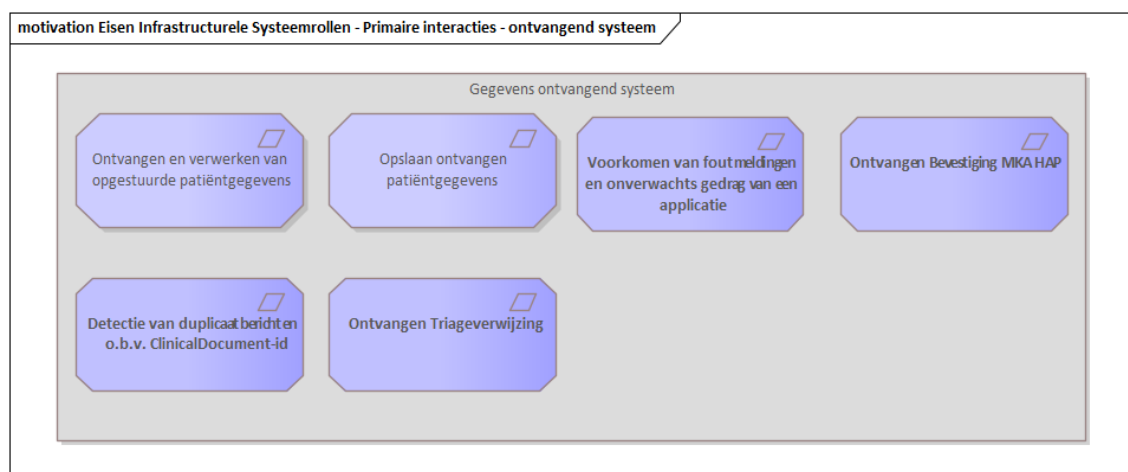


Figure 3 : Eisen Infrastructurele Systeemrollen - Primaire interacties - ontvangend systeem

2.1.3.1 Voorkomen van foutmeldingen en onverwachts gedrag van een applicatie

Alias: GBX.OPV.e4190.1

Details

Eis:

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

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.

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

2.1.3.2 Opslaan ontvangen patiëntgegevens

Alias: GBX.STU.e4520

Details

Eis:

Wanneer patiëntgegevens, die conform GBX.STU.e4510 zijn ontvangen, ongewijzigd in de eigen patiëntadministratie worden opgenomen en de patiëntgegevens niet ontvangen zijn in het kader van een dossieroverdracht, dan moet worden vastgelegd dat het een kopie betreft.

Toelichting bij eis:

Gewoonlijk zullen patiëntgegevens die via het LSP worden ontvangen in de eigen patiëntadministratie worden opgenomen. Wanneer dit automatisch gebeurt is het raadzaam om de geadresseerde gebruiker van de verwerkte berichten op de hoogte te stellen.

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

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

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

2.1.3.3 Ontvangen en verwerken van opgestuurde patiëntgegevens

Alias: GBX.STU.e4510.1

Details

Conditie

-

Beginsituatie

Het systeem beschikt over de voor deze functie vereiste vertrouwensmiddelen.

Trigger

Het systeem ontvangt een versturenPatiëntgegevens-bericht

Interacties

Het systeem stuurt een bevestiging naar de afzender conform IH AORTA.

Resultaat

De ontvangen patiëntgegevens zijn verwerkt.

Uitzonderingen

Uitzonderingen zijn beschreven in de Foutentabel.

Opties

Een systeem dat berichten in de nieuwste versie ondersteunt, dient ook berichten in de eerst lagere versie te ondersteunen.

Responsetijd

Het systeem dient in staat te zijn <gbx-verwerkingssnelheid> kilobytes aan berichtinhoud per seconde te verwerken.

Betrouwbaarheid

-

Toelichting

Indien het verplicht is voor het ontvangen bericht om het patient-id in de transmissionwrapper te vermelden, dan dient dat gelijk te zijn aan het patient-id in de inhoud van het bericht. Indien dit niet het geval is, moet een foutmelding worden teruggestuurd en moet de verwerking worden afgebroken.

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

2.1.3.4 Ontvangen Triageverwijzing

Alias: AZ.BER.e4050

Details

Eis:

Het systeem moet Triageverwijzing (ZTAZ_IN000003NL01) kunnen verwerken en na ontvangst een Accept Acknowledgement (MCCI_IN000002) terugsturen.

Toelichting bij eis:

Triageverwijzing wordt verstuurd vanuit een MKA aan een HAP. De HAP dient de Triageverwijzing in zijn systeem te kunnen verwerken. Na ontvangst van de Triageverwijzing dient de HAP een accept acknowledgement terug te sturen.

De specificatie van de Triageverwijzing is opgenomen in de Art-Decor publicatie van Acute Zorg.

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

2.1.3.5 Ontvangen Bevestiging MKA HAP

Alias: AZ.BER.e4040

Details

Eis:

Het systeem moet Bevestiging MKA HAP (ZTAZ_IN000007NL01) kunnen verwerken en na ontvangst een Accept Acknowledgement (MCCI_IN000002) terugsturen.

Toelichting bij eis:

Bevestiging MKA HAP wordt verstuurd vanuit een MKA aan een HAP. De HAP dient de Bevestiging MKA HAP in zijn systeem te kunnen verwerken. Na ontvangst van de Bevestiging MKA HAP dient de HAP een accept acknowledgement terug te sturen.

De specificatie van de Bevestiging MKA HAP is opgenomen in de Art-Decor publicatie van Acute Zorg.

Vzvv_Moscow: Verplicht
Vzvv_Req_Verificatie: Acceptatietest
Vzvv_Req_Soort: Functional
Vzvv_Req_Type: Product

2.1.3.6 Detectie van duplicaatberichten o.b.v. ClinicalDocument-id

Alias: GBX.OPV.e4212

Details
Eis: Duplicaatdetectie dient plaats te vinden op basis van het ClinicalDocument-id in het bericht. Toelichting bij eis: Er dient duplicaatdetectie te worden uitgevoerd bij het verwerken van de verstuurbedichten. Hierbij dient te worden gecontroleerd of het ClinicalDocument in het bericht, al eerder is verstuurd. De duplicaatdetectie dient op basis van het ClinicalDocument-id plaats te vinden.

Vzvv_Moscow: Verplicht
Vzvv_Req_Verificatie: Acceptatietest
Vzvv_Req_Soort: Functional
Vzvv_Req_Type: Product

2.1.4 Mandaatregistratie

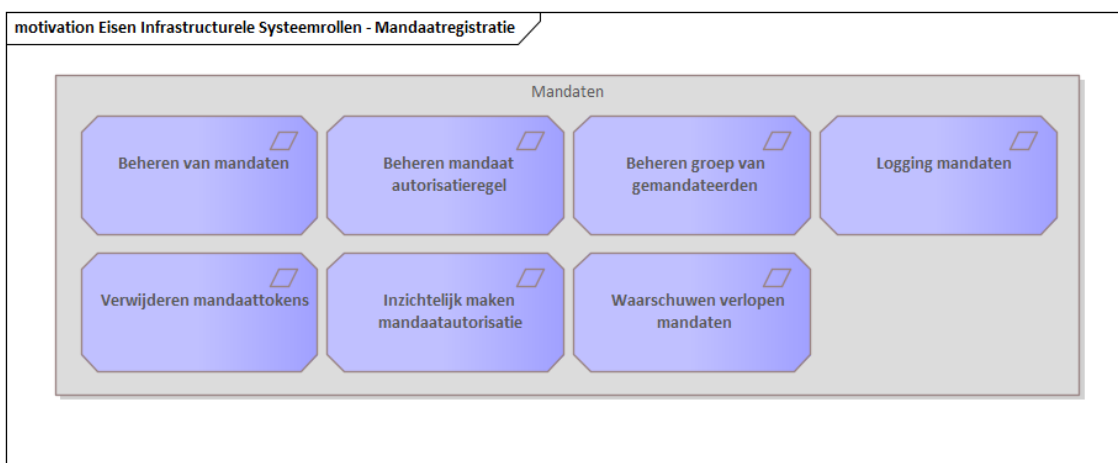


Figure 4 : Eisen Infrastructurele Systeemrollen – Mandaatregistratie

2.1.4.1 Waarschuwen verlopen mandaten

Alias: GBX.AUT.e4522.1

Details
Eis: Een mandaterende en de in de autorisatieregel opgenomen gemandateerde zorgverlener(s) moeten via een melding op de hoogte worden gebracht als respectievelijk zijn gegeven mandaat of zijn verkregen mandaat binnen een tijdsbestek van 1 maand komt te verlopen. Toelichting bij eis: Er moet voorkomen worden dat door een verlopen mandaat het zorgproces in gedrang komt.

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

Vzvv_Moscow: Verplicht
Vzvv_Req_Verificatie: Acceptatietest
Vzvv_Req_Soort: Functional
Vzvv_Req_Type: Product

2.1.4.2 Verwijderen mandaattokens

Alias: GBX.AUT.e4521.4

Details
Eis: Verlopen mandaattokens moeten in de volgende gevallen uit het systeem worden verwijderd: 1. De einddatum van het mandaattoken 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 mandaattoken. Toelichting bij eis: Er moet voorkomen worden dat verlopen mandaattokens in het systeem achterblijven en mogelijk onterecht gebruikt worden. Indien een certificaat (waarmee het mandaattoken is ondertekend) 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. • 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.

Vzvv_Moscow: Verplicht
Vzvv_Req_Verificatie: Acceptatietest
Vzvv_Req_Soort: Functional
Vzvv_Req_Type: Product

2.1.4.3 Logging mandaten

Alias: GBX.AUT.e4516.3

Details
Eis: Met betrekking tot het mandaattoken dienen vier 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. Mandaattoken; bij het verwijderen van een mandaattoken dient de einddatum en de unieke identifier van het mandaattoken gelogd te worden. 3. Autorisatieregels; bij het aanmaken van een autorisatieregels dienen de gegevens gelogd te worden zoals opgenomen in GBX.AUT.e4514. In opdracht van VZVZ, van een toezichthouder of van een andere geautoriseerde belanghebbende moeten bovenstaande loggegevens te allen tijde 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, zoals zijn benoemd in de eis, in één gecombineerde log op te nemen. Hierbij moet dan wel na elke aanpassing van een van de drie genoemde zaken opnieuw gelogd worden.

Vzvv_Moscow: Verplicht
Vzvv_Req_Verificatie: Acceptatietest
Vzvv_Req_Soort: Functional
Vzvv_Req_Type: Product

2.1.4.4 Inzichtelijk maken mandaatautorisatie

Alias: GBX.AUT.e4517.1

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

Vzvv_Moscow: Verplicht
Vzvv_Req_Verificatie: Acceptatietest
Vzvv_Req_Soort: Functional
Vzvv_Req_Type: Product

2.1.4.5 Beheren groep van gemandateerden

Alias: GBX.AUT.e4514.4

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

Vzvv_Moscow: Verplicht
Vzvv_Req_Verificatie: Acceptatietest
Vzvv_Req_Soort: Functional

Vzvvz_Req_Type: Product

2.1.4.6 Beheren mandaat autorisatiereg

Alias: GBX.AUT.e4513.3

Details
Eis: Een mandaat kan alleen afgegeven worden op basis van een autorisatiereg. Een autorisatiereg bepaalt of een bepaalde zorgverlener gebruik mag maken van een specifiek mandaat. De precieze invulling van een autorisatiereg is niet gespecificeerd. Dit is ter invulling van de zorginstelling. Een autorisatiereg moet in ieder geval wel de volgende attributen bevatten: 1. Lijst met werkcontext(en); De werkcontext(en) bepaalt de context(en) waarbinnen een mandaat geldig is. Dit kan bijvoorbeeld gekoppeld zijn aan een afdeling of een werkproces. 2. Lijst met gemandateerden; Dit kunnen UZI-nummer(s), lokale zorgverleneridentificaties of (lokaal gedefinieerde) rollen zijn. Er kan ook een groep(en) (GBX.AUT.e4514) worden opgenomen waar rolcodes of UZI-nummers aan gekoppeld zijn. Door het gebruik van groep(en) is het mogelijk om dynamisch rolcodes of UZI-nummers toe te voegen aan de lijst van gemandateerden. 3. Uniek identificatiekenmerk; Een autorisatiereg moet uniek gekenmerkt worden. Een uniek gekenmerkte autorisatiereg 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 autorisatiereg. 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 autorisatiereg. Een groep wordt aangeduid door middel van een groepsnaam. De UZI-nummers die direct of indirect (door middel van de rolcode) gekoppeld worden aan een groepsnaam moeten op een veilige manier worden beheerd (eis GBX.AUT.e4514). Indien een lokale gebruikersidentificatie wordt gebruikt, dan kan het LSP alleen bevraagd worden via de conditionele query. Dit zal dan in een zorgtoepassing specifiek worden vereist. Een autorisatiereg mag niet aangepast worden. De attributen die zijn opgenomen in verwijzingen (zoals bijvoorbeeld bij de onder punt 2 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. Autorisatieregels mogen alleen door een geautoriseerde medewerker worden ingezien. De lijst met gemandateerden mag alleen door een geautoriseerde medewerker worden aangepast.

Vzvvz_Moscow: Verplicht

Vzvvz_Req_Verificatie: Acceptatietest

Vzvvz_Req_Soort: Functional

Vzvvz_Req_Type: Product

2.1.4.7 Beheren van mandaten

Alias: GBX.AUT.e4511.3

Details
Eis: Een zorgverlener moet, wanneer hij lokaal is ingelogd op vertrouwensniveau midden, mandaten kunnen vastleggen, inzien en intrekken.

Gebruikers mogen uitsluitend mandaten vastleggen waarvoor zij mandaterende zijn. Voor het inzien en intrekken geldt dat dit mag voor elk in het systeem beschikbare mandaat.

Voor een mandaat worden tenminste de volgende gegevens vastgelegd:

1. de ingangsdatum van het mandaat;
2. de einddatum ('NotOnOrAfter') 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. een verwijzing naar een autorisatieregel (zie eis GBX.AUT.e4513);
7. een unieke identifier.

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.

Toelichting bij eis:

-

Vz vz_Moscow: Verplicht

Vz vz_Req_Verificatie: Acceptatietest

Vz vz_Req_Soort: Functional

Vz vz_Req_Type: Product

2.1.5 Mandaattoken beherend systeem

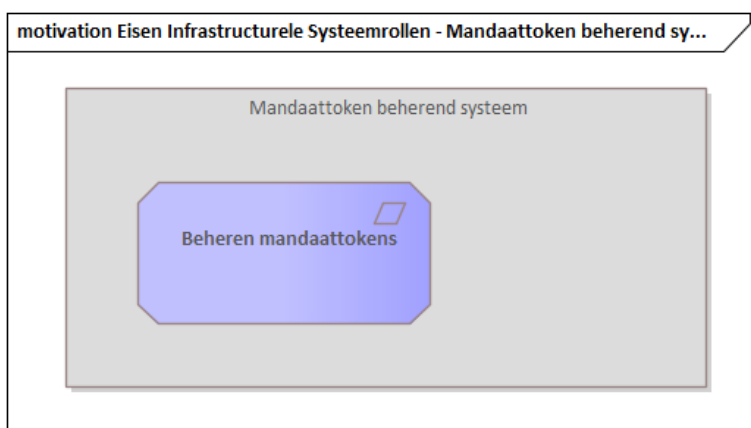


Figure 5 : Eisen Infrastructurele Systeemrollen - Mandaattoken beherend systeem

2.1.5.1 Beheren mandaattokens

Alias: GBX.AUT.e4519

Details
Eis: Mandaattokens dienen in een beveiligde container te worden opgeslagen. Een gebruiker krijgt door middel van een beveiligde verbinding alleen gebruik over die mandaattokens waarvoor het is geautoriseerd. Toelichting bij eis: Er moet voorkomen worden dat mandaattokens onderschept, gelezen en vervolgens misbruikt worden. Door middel van implementatie van een beveiligde container krijgen medewerkers alleen gebruik over die mandaattokens waarvoor ze zijn geautoriseerd. De beveiligde container moet het onmogelijk maken om een mandaattoken te stelen.

Vz vz_Moscow: Verplicht
Vz vz_Req_Verificatie: Monitoring
Vz vz_Req_Soort: Functional
Vz vz_Req_Type: Product

2.1.6 Patiëntadministratie

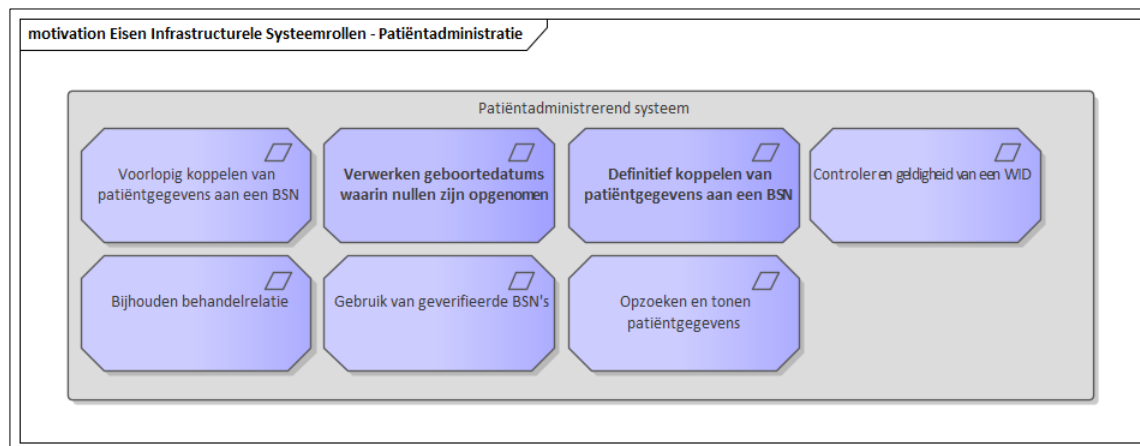


Figure 6 : Eisen Infrastructurele Systeemrollen - Patiëntadministratie

2.1.6.1 Gebruik van geverifieerde BSN's

Alias: GBX.IDA.e4060.1

Details
Eis: Het systeem moet aan GBX.IDA.e4010, GBX.IDA.e4020, GBX.IDA.e4040 en GBX.IDA.e4050 voldoen of (bij implementatie in een GBZ) een koppeling kunnen leggen met een derde systeem dat aan die eisen voldoet. Een systeem dat gebruik maakt van een extern patiëntadministrerend systeem is verplicht om te controleren of een BSN daadwerkelijk aan alle AORTA eisen voldoet. 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 <i>Patiëntadministrerend systeem</i> 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.

Vzvv_Moscow: Verplicht
Vzvv_Req_Verificatie: Acceptatietest
Vzvv_Req_Soort: Functional
Vzvv_Req_Type: Product

2.1.6.2 Opzoeken en tonen patiëntgegevens

Alias: GBX.IDA.e4010.2

Details
Eis: Het systeem moet een gebruiker de mogelijkheid bieden een patiënt op te zoeken in de 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 het opnemen van de BSN in de patiëntadministratie 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.

Vzvv_Moscow: Verplicht
Vzvv_Req_Verificatie: Acceptatietest
Vzvv_Req_Soort: Functional
Vzvv_Req_Type: Product

2.1.6.3 Bijhouden behandelrelatie

Alias: GBX.IDA.e4050.1

Details
Eis: Het systeem moet een gebruiker de volgende mogelijkheden bieden in de lokale patiëntadministratie voor een patiënt/cliënt. De status van de behandelrelatie inzien, waarbij wordt getoond: 1. of een behandelrelatie bestaat, en zo ja met welke zorgverleners (in ieder geval o.b.v. UZI) een behandelrelatie bestaat; 2. ten behoeve van welke zorgaanbieder (in ieder geval o.b.v. 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.

Vzvv_Moscow: Optioneel

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

2.1.6.4 Controleren geldigheid van een WID

Alias: GBX.IDA.e4040.1

Details

Eis:

Het systeem moet voor een geselecteerde patiënt/cliënt de gebruiker de mogelijkheid bieden:

1. het 'in omloop mogen zijn' van het WID te controleren door raadplegen van de SBV-Z op basis van aard en nummer van het WID;
2. in de lokale patiëntenindex vast te leggen dat hij 'het in omloop mogen zijn' van het WID heeft gecontroleerd, onder vermelding van:
 - resultaat van de controle;
 - datum en tijd;
 - indien beschikbaar het UZI-nummer of anders een unieke identificatie van de gebruiker;
 - aard en nummer van het WID.
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.

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

2.1.6.5 Definitief koppelen van patiëntgegevens aan een BSN

Alias: GBX.IDA.e4030.3

Details

Eis:

Het systeem moet voor een geselecteerde patiënt/cliënt de gebruiker:

- de mogelijkheid bieden gewaarschuwd te worden indien nog niet is vastgesteld dat het BSN hoort bij de patiënt/cliënt;
- de mogelijkheid bieden in de lokale patiëntadministratie vast te leggen dat hij heeft vastgesteld dat het betreffende BSN hoort bij de patiënt/cliënt, onder vermelding van:
 1. de manier van vaststellen:
 - i. Controle van echtheid en geldigheidsdatum van WID en de gelijkenis van de in de WID genoemde identificerende gegevens,
 - ii. Vergewissen,
 2. Datum en tijd van vaststellen,
 3. indien beschikbaar het UZI-nummer of anders een unieke identificatie van de gebruiker, en het UZI-nummer van mandaterende zorgverlener indien van toepassing.
 4. zorgaanbieder-id (URA) van de gebruiker;
 5. in geval van WID-controle: aard en nummer van het WID.

Als gevolg van de uitvoering van de mogelijkheid zoals genoemd onder de tweede bullet, 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 'Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg' (Wabvpz) 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. Verificatie dient in het systeem te worden geregistreerd. Alle door VZVZ geaccepteerde zorginformatiesystemen ondersteunen deze mogelijkheid. Wordt er een BSN verkregen via de AORTA infrastructuur, dan hoeft dit BSN niet opnieuw geverifieerd te worden. Ook als het nummer direct uit de BRP komt, kan BSN-verificatie achterwege worden gelaten.

Het systeem kan hierna overgaan tot het vrijgeven en aanmelden van de bij de patiënt/cliënt behorende gegevens.

Vzvv_Moscow: Optioneel

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

2.1.6.6 Voorlopig koppelen van patiëntgegevens aan een BSN

Alias: GBX.IDA.e4020.1

Details

Eis:

Het systeem moet een gebruiker de mogelijkheid bieden het door een burgerregister geretourneerde BSN te koppelen aan de identificerende gegevens in de gebruikte patientadministratie 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 systeemgebruiker.

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 de 'Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg' (Wabvpz). Voor het landelijk uitwisselen van medische patiëntgegevens moet de SBV-Z of de GBA/BRP zijn geraadpleegd.

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

2.1.6.7 Verwerken geboortedatum waarin nullen zijn opgenomen

Alias: GBX.IDA.e4015.2

Details
Eis: Een geboortedatum die teruggegeven wordt door de SBV-Z kan nullen bevatten (jjjjmm00, jjjj0000 of 00000000). Het XIS moet in staat zijn hiermee adequaat om te gaan zonder dat de applicatie vastloopt. Deze eis leidt tot de volgende aanvullende eisen: 1. Een XIS moet de mogelijkheid hebben om een BSN op te vragen of te verifiëren op basis van de Zoekpaden 1 en 2 conform de SBV-specificaties (https://www.sbv-z.nl/dienstverlening/bsn-verifiëren). 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. 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. Toelichting bij eis: Een indicatie dat een geboortedatum handmatig is aangepast kan bijvoorbeeld worden gerealiseerd door het aangeven door kleur, tekstuele indicatie of door de opgeleverde datum op te slaan in een (apart) tekstveld.

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

2.1.7 Token beherend systeem

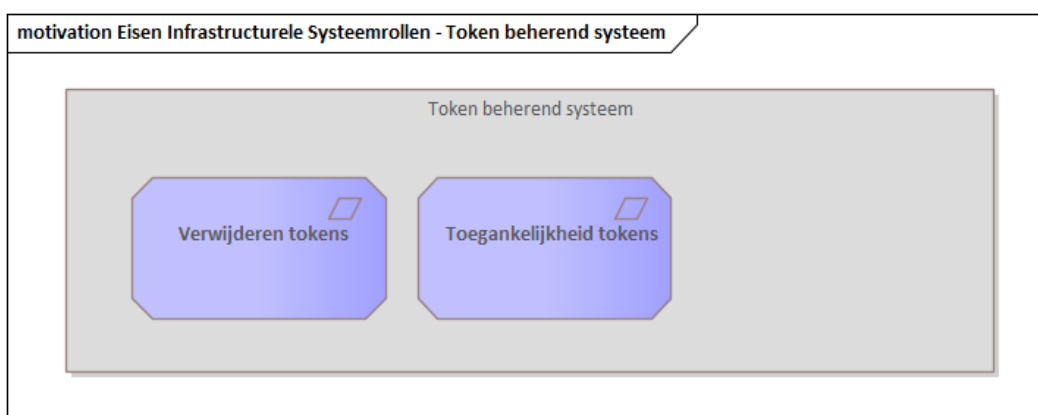


Figure 7 : Eisen Infrastructurele Systeemrollen - Token beherend systeem

2.1.7.1 Verwijderen tokens

Alias: GBX.OPV.e4110.2

Details
Eis:

Indien de geldigheid van een token is verlopen, dan dient deze binnen 24 uur automatisch te worden verwijderd.

Daarnaast moet het voor een gebruiker, die ingelogd is met tweefactorauthenticatie, mogelijk zijn om een token uit het systeem te verwijderen.

Toelichting:

Het verwijderen (en daarmee afwezig zijn) van een token leidt ertoe dat er geen automatische opvraag meer verstuurd mag worden t.b.v. het opvragen van patiëntgegevens van de in het token opgenomen patiënt-id. Dit kan gevolgen hebben voor het werkproces van de gebruiker van het systeem. Het is dan ook aan te raden om de gebruiker(s) van het systeem (tijdig) op de hoogte te stellen van het verwijderen van een token. Hoe hier invulling aan te geven is aan de systeembouwer.

Het gaat hierbij bijvoorbeeld om inschrijf-, mandaat- en consenttokens.

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

2.1.7.2 Toegankelijkheid tokens

Alias: GBX.OPV.e4160.2

Details

Eis:

Om misbruik van tokens door een kwaadwillende te bemoeilijken, moeten de tokens in een beveiligde container worden opgeslagen. Toegang tot de tokens moet alleen mogelijk zijn voor geautoriseerde gebruikers.

Toelichting:

Er worden geen specifieke eisen gesteld aan de rollen die geautoriseerd zijn en aan de wijze van opslag van de tokens. Dit is afhankelijk van de lokale systeemimplementatie. De systeembouwer is verantwoordelijk voor de invulling van deze eis.

Het gaat hierbij alleen om die tokens, die meerdere malen gebruikt kunnen worden, zoals inschrijf-, mandaat en consenttokens.

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Audit

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

2.2 AORTA Eisen Kwaliteit Aangesloten Systemen

2.2.1 Betrouwbaarheid

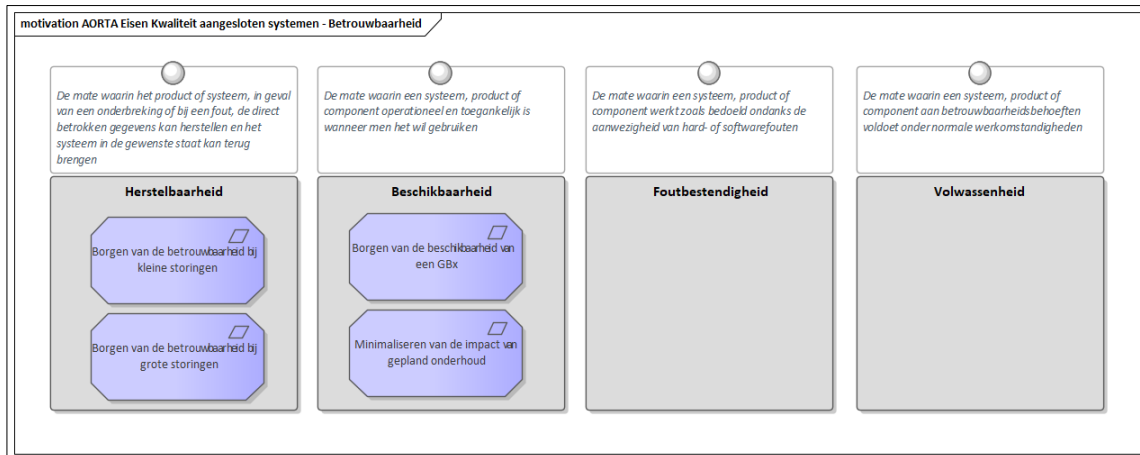


Figure 8 : AORTA Eisen Kwaliteit aangesloten systemen - Betrouwbaarheid

2.2.1.1 Borgen van de betrouwbaarheid bij grote storingen

Alias: GBX.BET.e4020.2

Details
Eis: Grote storingen in een GBx mogen niet meer dan gemiddeld 2 keer per jaar voorkomen en dienen dan binnen 1 dag te zijn opgelost. Toelichting bij eis: De term 'grote storing' is niet SMART gedefinieerd. Het kan vele soorten storingen betreffen. Het doel van deze eis is om te voorkomen dat een GBx na een grote 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 er snel teruggevallen moet kunnen worden op de XIS-leverancier, GZN-leverancier en/of andere ICT-leveranciers. Zo moet bij een grote storing, snel een leverancier beschikbaar zijn om het probleem te verhelpen. Wellicht kunnen zijn ICT-leveranciers hem een 24-uurs onderhoudscontract bieden.

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Monitoring

Vzvv_Req_Soort: Non-Functional

Vzvv_Req_Type: Product

2.2.1.2 Borgen van de betrouwbaarheid bij kleine storingen

Alias: GBX.BET.e4010.1

Details
Eis: Kleine storingen in een GBx mogen niet meer dan gemiddeld 1 keer per maand voorkomen en dienen dan binnen 10 werkdagen te zijn opgelost. Toelichting bij eis: De term 'kleine storing' is niet SMART gedefinieerd. Het kan vele soorten storingen betreffen. Het doel van deze eis is om te voorkomen dat een GBx 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 GBx-beheerder snel beschikbaar kan zijn om het probleem te verhelpen. Wellicht kan zijn XIS-leverancier hem daarbij helpen. De afspraken en procedures zoals opgenomen in de AORTA DAP dienen hierbij gevolgd te worden.

Vzvv_Moscow: Verplicht
Vzvv_Req_Verificatie: Monitoring
Vzvv_Req_Soort: Functional
Vzvv_Req_Type: Product

2.2.1.3 Minimaliseren van de impact van gepland onderhoud

Alias: GBX.BES.e4020.2

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

Vzvv_Moscow: Verplicht
Vzvv_Req_Verificatie: Monitoring
Vzvv_Req_Soort: Non-Functional
Vzvv_Req_Type: Product

2.2.1.4 Borgen van de beschikbaarheid van een GBx

Alias: GBX.BES.e4010.1

Details
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: De beschikbaarheid wordt als een voortschrijdend gemiddelde berekend.

Vzvv_Moscow: Verplicht
Vzvv_Req_Verificatie: Monitoring
Vzvv_Req_Soort: Non-Functional
Vzvv_Req_Type: Product

2.2.2 Beveiligbaarheid

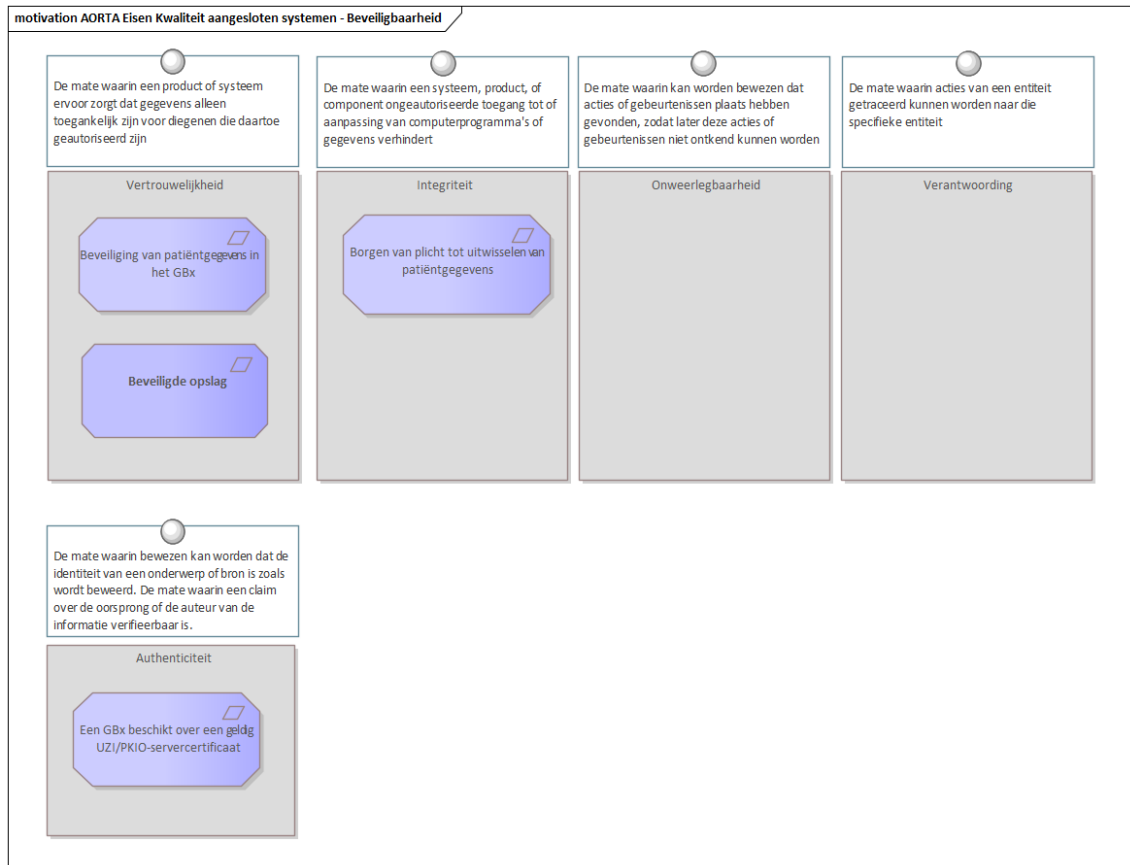


Figure 9 : AORTA Eisen Kwaliteit aangesloten systemen - Beveiligbaarheid

2.2.2.1 Beveiligde opslag

Alias: SYS.BVL.e4010.3

Details
Eis: Data die persoonsgegevens bevatten dienen versleuteld en beveiligd te worden opgeslagen. Het gaat hierbij om alle opgeslagen data (bv. logging en backups). Toelichting bij eis: Alle data met persoonsgegevens dienen geëncrypt te worden. Mocht hiervan met het oog op systeemprestaties van afgeweken worden, dan dient dit overlegd te worden met VZVZ.

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Audit

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

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

Alias: GBX.BVL.e4080.1

Details
Eis:

Een GBx dient een {GBx}UZI- of {GBK}{GBP}{GBO} PKIO-servercertificaat te hebben dat op naam staat van de zorgaanbieder 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.

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Aansluittoets

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

2.2.2.3 Borgen van plicht tot uitwisselen van patiëntgegevens

Alias: GBX.BVL.e4070.1

Details

Eis:

Als een GBx voor een systeemrol is aangesloten op de AORTA-infrastructuur, 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 de AORTA-infrastructuur.

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Monitoring

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

2.2.2.4 Beveiliging van patiëntgegevens in het GBx

Alias: GBX.BVL.e4060

Details

Eis:

Voor een GBx moet zijn gedefinieerd:

1. welke landelijke toepassingen en systeemrollen worden ondersteund en gebruikt;
2. hoe de grenzen van het GBx lopen door de ICT-voorzieningen van de organisatie;
3. hoe en wanneer patiëntgegevens die grenzen kunnen passeren;
4. hoe wordt gewaarborgd dat patiëntgegevens in de dossiers en postbussen niet kunnen lekken naar onbetrouwbare bestemmingen;
5. hoe wordt gewaarborgd dat patiëntgegevens uit onbetrouwbare bronnen niet kunnen terechtkomen in de dossiers en postbussen of de ZIM;
6. hoe wordt gewaarborgd dat anderen dan bevoegde gebruikers geen fysieke toegang tot (delen van) het GBx kunnen krijgen.

Toelichting bij eis:

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

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Documentverificatie

Vzvv_Req_Soort: Non-Functional

Vzvv_Req_Type: Product

2.2.3 Prestatie-efficiëntie

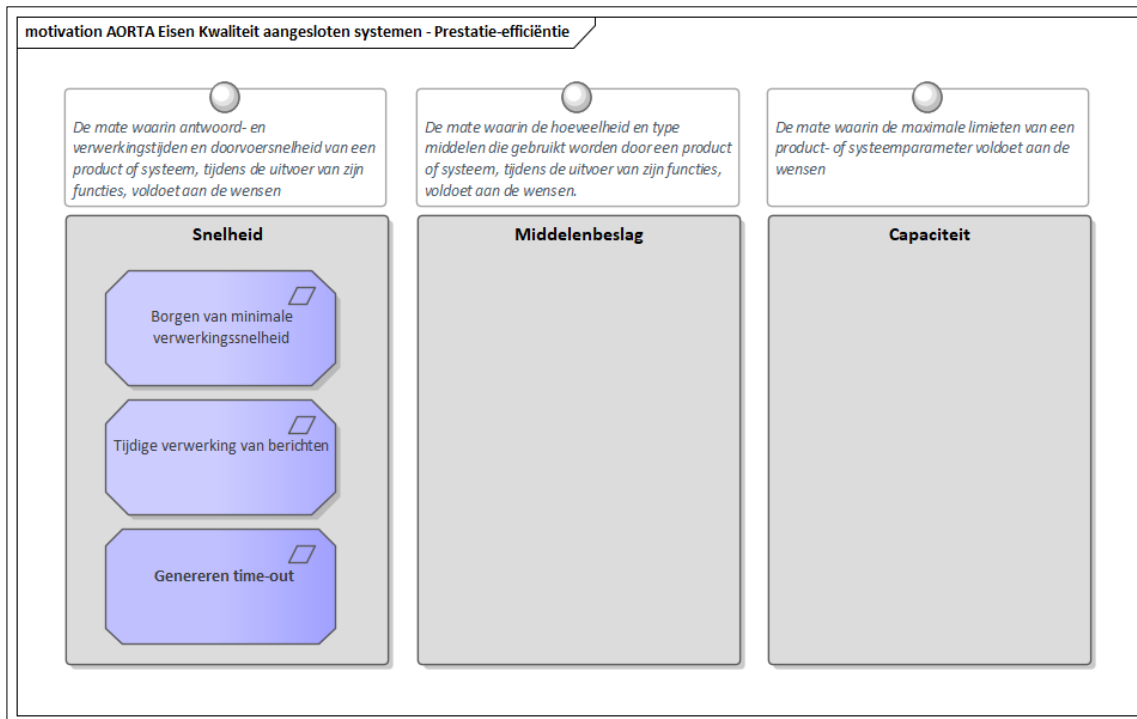


Figure 10 : AORTA Eisen Kwaliteit aangesloten systemen - Prestatie-efficiëntie

2.2.3.1 Genereren time-out

Alias: GBX.PST.e4020

Details
Eis: Het bronsysteem moet binnen 60 seconden na ontvangst van een opvraagbericht een antwoord geven. Indien het bronsysteem constateert dat het niet binnen 60 seconden kan antwoorden, dan dient het bronsysteem een foutmelding te genereren. Toelichting bij eis: Om te voorkomen dat TLS-verbindingen onnodig lang tussen het LSP en GBx-en blijven bestaan, worden de TLS-verbindingen automatisch door het LSP verbroken. Het LSP zal na 60 seconden de verbinding met een bronsysteem verbreken en een foutmelding (time-out) terugsturen naar het initiërende systeem. Indien het bronsysteem zelf kan vaststellen dat er niet binnen de in de eis opgegeven tijd een antwoord verstuurd kan worden, dan dient het bronsysteem een foutmelding (time-out) te versturen. Op deze manier kan voorkomen worden, dat een initiërend systeem onnodig lang hoeft te wachten. De waarde voor de time-out is gebaseerd op voorgaande AORTA-versies. Hierbij is nog geen rekening gehouden met aansluiting op MedMij, die vereist dat een DVZA binnen 60 seconden een antwoord moet geven aan een PGO. Vooralsnog blijft de waarde zoals opgenomen in deze eis gehandhaafd. Het DVZA zal in dat geval na 60 seconden een time-out versturen naar het PGO.

Vzvv_Moscow: Verplicht
Vzvv_Req_Verificatie: Acceptatietest
Vzvv_Req_Soort: Functional
Vzvv_Req_Type: Product

2.2.3.2 Tijdsige verwerking van berichten

Alias: GBX.PST.e4015

Details
Eis: Een GBx dient voor gebruikersinteracties, na het commando van een gebruiker of een daaropvolgende ontvangst van een bericht van de ZIM, binnen 0,3 seconden het aangegeven resultaat te hebben bereikt. Toelichting bij eis: Deze eis is nodig om te voorkomen dat een zorgaanbieder bij zijn GZN of het LSP gaat klagen over te lange responstijden terwijl de oorzaak ligt bij bijvoorbeeld 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 (Application Service Provider) 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.

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Monitoring

Vzvv_Req_Soort: Non-Functional

Vzvv_Req_Type: Product

2.2.3.3 Borgen van minimale verwerkingssnelheid

Alias: GBX.PST.e4010.1

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

Vzvv_Moscow: Verplicht

Vz vz_Req_Verificatie: Monitoring
Vz vz_Req_Soort: Non-Functional
Vz vz_Req_Type: Product

2.2.4 Uitwisselbaarheid

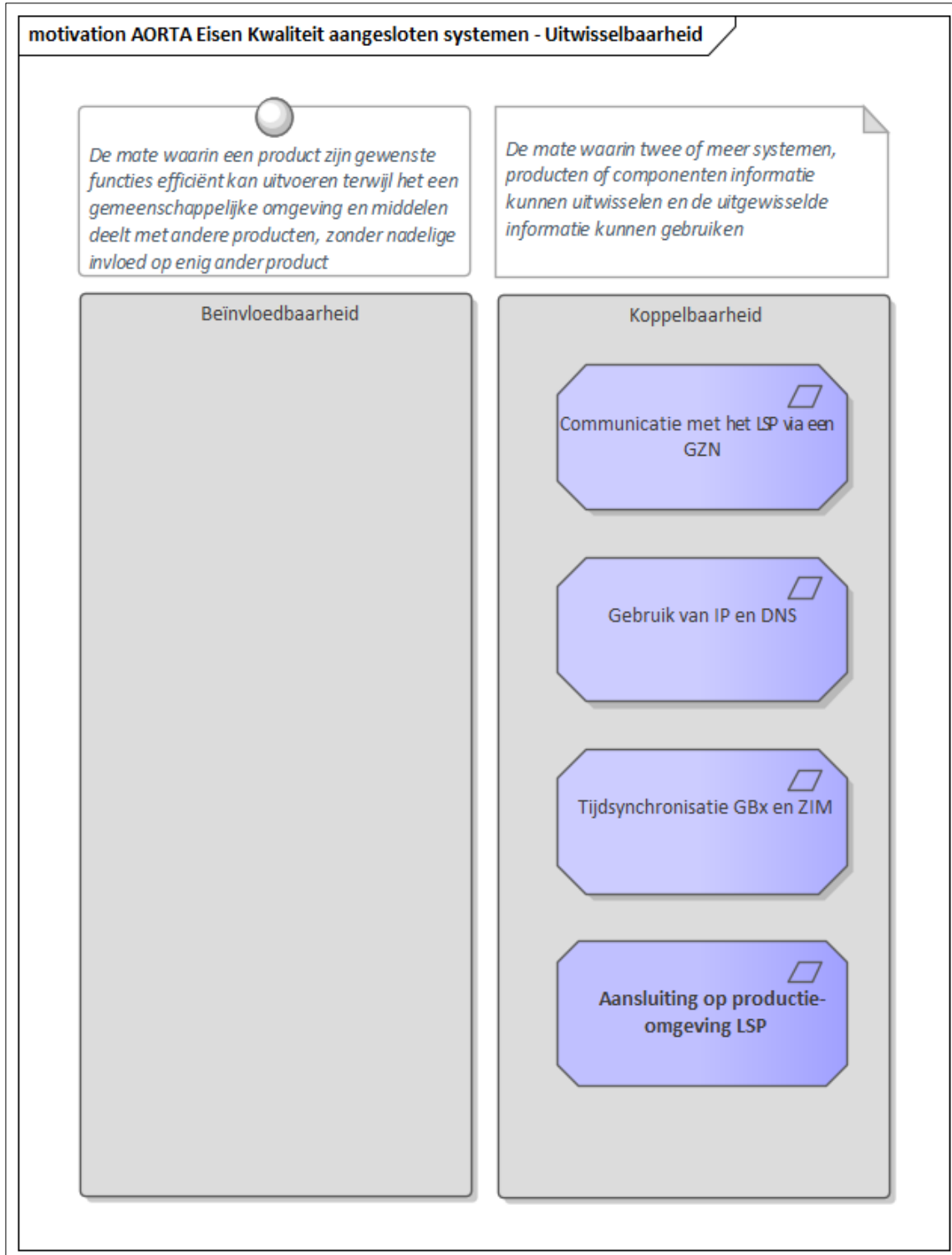


Figure 11 : AORTA Eisen Kwaliteit aangesloten systemen - Uitwisselbaarheid

2.2.4.1 Aansluiting op productie-omgeving LSP

Alias: GBX.CON.e4120.1

Details
Eis: GBx-beheerder moet er namens de verantwoordelijke organisatie van het GBx 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 GBx. Toelichting bij eis: Vanwege mogelijke beveiligingsrisico's en kwaliteitgaranties in de keten mogen er alleen GBx-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.

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Monitoring

Vzvv_Req_Soort: Non-Functional

Vzvv_Req_Type: Product

2.2.4.2 Tijdsynchronisatie GBx en ZIM

Alias: GBX.CON.e4030.2

Details
Eis: Een GBx dient NTP te gebruiken voor tijdsynchronisatie met de ZIM. De 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 toezichhouder 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 tegen een NTP-server om synchroon te blijven met de ZIM.

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Monitoring

Vzvv_Req_Soort: Non-Functional

Vzvv_Req_Type: Product

2.2.4.3 Gebruik van IP en DNS

Alias: GBX.CON.e4020

Details
Eis: Een GBx moet bereikbaar zijn voor de ZIM: 1. {GBx}{GBO} via het IP-adres dat is toegekend aan het GBx en dat is verkregen door DNS-vertaling van de hostnaam van dat GBx; 2. {GBK} via het IP-adres dat door het LSP is toegekend aan het GBK en dat is verkregen door DNS-vertaling van de hostnaam van dat GBK;

3. {GBP} via het IP-adres en de fully qualified domain name (FQDN) die door het LSP zijn toegekend aan het GBP en waarvoor het LSP de DNS-vertaling biedt.

De ZIM moet bereikbaar zijn vanuit een GBx via het IP-adres van de operationele ZIM, dat is verkregen door DNS-vertaling van de hostnaam van de ZIM.

Voor de DNS-vertaling geldt dat:

1. de hostnaam een maximale time-to-live (TTL) heeft voor verversing van de cache;
2. het IP-adres van de ZIM zich binnen een vooraf overeengekomen range bevindt die altijd gerouteerd moet worden naar de GZN;
3. een systeem vanuit de applicatie alleen benaderd mag worden op de FQDN. Vertaling naar IP-adres wordt door de DNS uitgevoerd.

Een GBx mag de volgende IP-adressen niet intern gebruiken:

1. het IP-adres dat door het LSP is uitgegeven voor het GBx als geheel,
2. de IP-adressen die zijn gereserveerd voor de ZIM,
3. de IP-adressen uit het landelijke IP-nummerplan van het LSP.

Toelichting bij eis:

Deze eis is nodig om ervoor te zorgen dat FQDN en IP-adressen op een juiste wijze worden ingesteld. Deze eis is ook nodig voor het gebruik van een ZIM op twee operationele locaties en om IP-netwerkkonflikten te voorkomen.

Deze eis betekent voor de organisatie dat die voor zijn GBx/GBO een FQDN moet krijgen van zijn GZN en deze laten registreren bij het LSP of bij SIDN. De GZN zal daaraan een IP-adres toekennen. De organisatie moet het toegekende IP-adres tenslotte (laten) configureren in zijn netwerkapparatuur binnen zijn GBx. Deze eis betekent dat een applicatie een ZIM expliciet op naam benadert en dat systemen geconfigureerd moeten worden voor het gebruik van DNS. Door middel van DNS-resolving kan voor het GBx transparant gebruik gemaakt worden van de operationele ZIM op locatie 1 of locatie 2.

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Aansluittoets

Vzvv_Req_Soort: Non-Functional

Vzvv_Req_Type: Product

2.2.4.4 Communicatie met het LSP via een GZN

Alias: GBX.CON.e4010.2

Details

Eis:

Een GBx dient via een datacommunicatienetwerk (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.

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Aansluittoets

Vzvv_Req_Soort: Non-Functional

Vzvv_Req_Type: Product

2.3 AORTA Eisen Kwaliteit Applicatie

2.3.1 Beveiligbaarheid

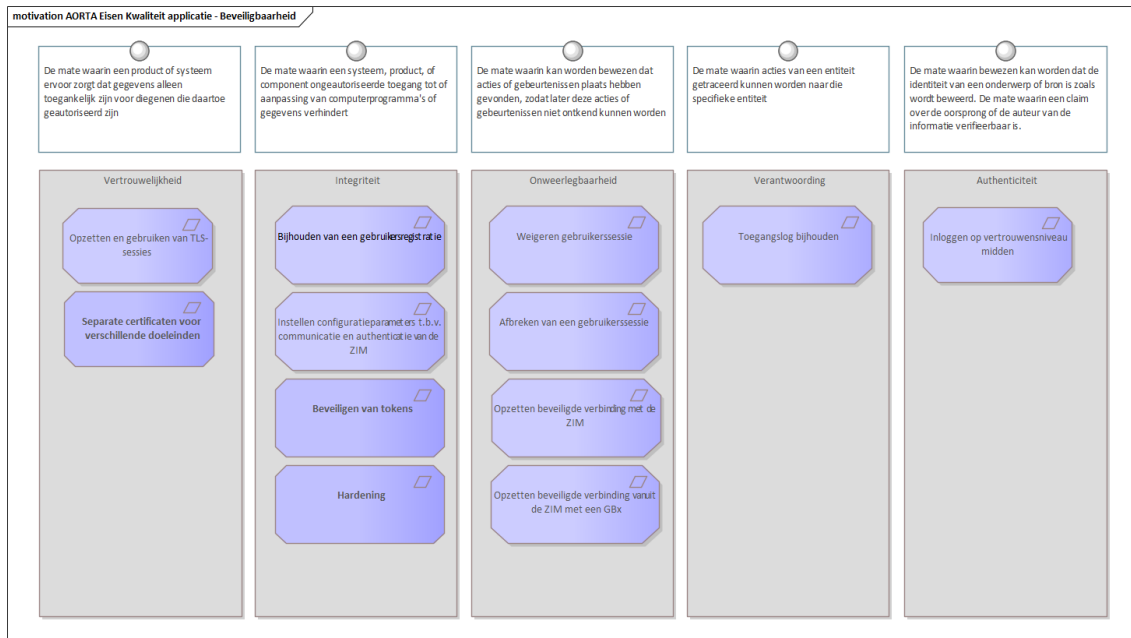


Figure 12 : AORTA Eisen Kwaliteit applicatie - Beveiligbaarheid

2.3.1.1 Hardening

Alias: SYS.BVL.e4065

Details
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.

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Audit

Vzvv_Req_Soort: Non-Functional

Vzvv_Req_Type: Product

2.3.1.2 Opzetten beveiligde verbinding vanuit de ZIM met een GBx

Alias: GBX.CON.e4090.3

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

1. tweezijdige authenticatie met behulp van het UZI-servercertificaat van het GBZ en het servercertificaat van de ZIM,
2. tijdelijke sleutels die elke 5 minuten ververs worden,
3. gebruikmakend van Cipher Suites die door het NCSC minimaal worden gekenmerkt als goed en tevens worden ondersteund door de ZIM. Voor encryptie moet altijd de sterkste vorm als eerste worden geprobeerd,
4. een maximale sessieduur van 8 uur,
5. een maximale ongebruikte TLS-sessie van 15 minuten.

Toelichting bij eis:

Dit is nodig opdat de ZIM een voldoende hoog beveiligingsniveau kan afdwingen bij het opzetten van een TLS-sessie met een GBx.

Dit betekent voor de zorgaanbieder dat hij of zijn XIS-leverancier de bovenstaande parameters moet instellen in de TLS-library in de betrokken XIS-applicatie(s) en/of de eventuele communicatieserver.

Vzvv_Moscow: Conditioneel.

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

2.3.1.3 *Separate certificaten voor verschillende doeleinden*

Alias: GBX.BVL.e4100.2

Details
Eis: Een GBZ dient voor transportbeveiliging een ander servercertificaat te gebruiken dan voor berichtauthenticatie. De verschillende certificaten horen daarbij in verschillende componenten ondergebracht te zijn in de architectuur van het XIS. Toelichting bij eis: Deze eis is conform NIST SP 800-57 norm; iedere XIS zou aparte sleutels moeten hanteren voor verschillende doeleinden. Deze eis impliceert dat een XIS een ander certificaat moet gebruiken voor TLS dan voor het ondertekenen van transactietokens. Conditie: De verplichting voor het gebruik van een separaat certificaat is afhankelijk van de grootte van de zorgaanbiederorganisatie. Deze eis zal in overleg met VZVZ wel of niet toegepast dienen te worden. Deze eis is verplicht voor de zorgaanbiedertypes Ziekenhuis en Zelfstandig Behandelcentra (ZBC).

Vzvv_Moscow: Conditioneel

Vzvv_Req_Verificatie: Audit

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

2.3.1.4 *Opzetten en gebruiken van TLS-sessies*

Alias: GBX.CON.e4070.3

Details
Eis: Het GBx moet na het beschikbaar worden voor de ZIM: • verzoeken van de ZIM voor het opzetten van nieuwe TLS-sessies honoreren ten behoeve van berichtuitwisseling voor andere zorgaanbieders,

- voor gebruikers die landelijk patiëntgegevens willen uitwisselen, een of meer TLS-sessies met de ZIM (her)gebruiken voor berichtuitwisseling.

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.

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

2.3.1.5 Beveiligen van tokens

Alias: GBX.FBH.e4070.2

Details
Eis: Tokens moeten behandeld worden als medische gegevens (volgens de NEN7510). Binnen de organisatie moet er een speciale rol toegewezen (en geautoriseerd) worden om toegang te krijgen tot de diverse opgeslagen tokens (inschrijf-, consent- 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 ter voorkoming van misbruik van de tokens beperkt zijn tot daarvoor aangewezen rollen.

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Audit

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

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

Alias: GBX.FBH.e4050.3

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

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

2.3.1.7 Bijhouden van een gebruikersregistratie

Alias: GBX.FBH.e4030.1

Details

Eis:

Binnen het GBx dient te worden bijgehouden welke UZI-passen worden toegelaten voor gebruik. Deze gebruikersregistratie is uitsluitend toegankelijk voor de rol van autorisatiebeheerder, na authenticatie op basis van een sterk authenticatiemiddel (tweefactorauthenticatie bijvoorbeeld via een UZI-pas).

Toelichting bij eis:

Dit is nodig om te voorkomen dat een willekeurig persoon de gebruikersregistratie kan aanpassen. Dit betekent voor de zorgaanbieder dat hij invulling moet geven aan de rol van autorisatiebeheerder.

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

2.3.1.8 Opzetten beveiligde verbinding met de ZIM

Alias: GBX.CON.e4080.7

Details

Eis:

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

1. tweezijdige authenticatie met behulp van het servercertificaat van de ZIM en het servercertificaat van het GBx;
2. tijdelijke sleutels die elke 5 minuten ververs worden door middel van TLS Secure Renegotiation;
3. gebruikmakend van Cipher Suites die door het NCSC minimaal worden gekenmerkt als goed;
4. gebruikmakend van de sterkste cipher suite die gedeeld wordt met de ZIM;
5. gebruikmakend van de hoogste toegestane TLS-versie die door beide partijen wordt ondersteund;
6. een ongebruikte TLS-sessie van maximaal 15 minuten.

Toelichting bij eis:

Dit is nodig opdat een GBx een voldoende hoog beveiligingsniveau kan afdwingen bij het opzetten van een TLS-sessie met de ZIM.

Dit betekent voor de organisatie dat hij of zijn XIS-leverancier de bovenstaande parameters moet instellen in de TLS-library in de betrokken applicatie(s) en/of de eventuele communicatieserver. Hiermee wordt tweezijdige authenticatie bewerkstelligd.

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

2.3.1.9 Toegangslog bijhouden

Alias: GBX.LOG.e4015.1

Details

Eis:

Het systeem moet de volgende berichtuitwisselingen loggen:

1. Ontvangen opvraagberichten en de daarop verzonden antwoorden;
2. Verzonden opvraagberichten en daarop verkregen antwoorden;
3. Verzonden opdrachtberichten en kennisgevingberichten.

De log bevat per berichtuitwisseling tenminste:

1. de identiteit van de patiënt/cliënt (BSN)
2. identiteit van de opvragende/versturende en bestemde organisatie
3. de functie en identiteit van de opvragende of versturende zorgverlener of medewerker of patiënt.
4. type van de uitgevoerde gebruikersinteractie

5. het tijdstip en tijdzone (ten opzichte van UTC) van de gebruikersinteractie
6. de bericht-id van het ontvangen (opvraag- of bevestig-) bericht
7. de bericht-id van het verzonden (oplever- of opdracht-) bericht
8. de gegevenssoorten of contextcodes van de verzonden en ontvangen patiëntstukken;
9. een indicatie van eventueel opgetreden foutsituaties met betrekking tot het ontvangen en verzenden van de berichten.

Toelichting bij eis:

Dit is nodig opdat aan de hand van de berichtuitwisseling precies achterhaald kan worden:

- {GBx} 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.

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

2.3.1.10 Afbreken van een gebruikerssessie

Alias: GBX.IDA.e4090.1

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

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

2.3.1.11 Weigeren gebruikerssessie

Alias: GBX.IDA.e4085.4

Details
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 en een geaccepteerde applicatie met een geldig UZI-servercertificaat, kan een geldig transactietoken genereren.

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

2.3.1.12 Inloggen op vertrouwensniveau midden

Alias: GBX.IDA.e4080.5

Details
Eis: Het systeem moet een gebruiker de mogelijkheid bieden een gebruikerssessie op vertrouwensniveau midden te starten door: 1. {GBx}{GBK}het invoeren van zijn vertrouwensmiddel op de werkplek en het invoeren van de bijbehorende toegangscode; 2. {GBP} zich op niveau DigiD-midden te authenticeren. {GBx} Een GBx dient hierbij een UZI-pas toe te laten indien: 1. de UZI-pas is geregistreerd in de gebruikerstabel (zie ook eis GBX.FBH.e4030); 2. de UZI-pas nog geldig is; 3. 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 biedt gratis generieke tooling in de vorm van ZORG-ID om de implementatie van het authenticeren met de UZI-pas te ondersteunen.

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Audit

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

2.3.2 Uitwisselbaarheid

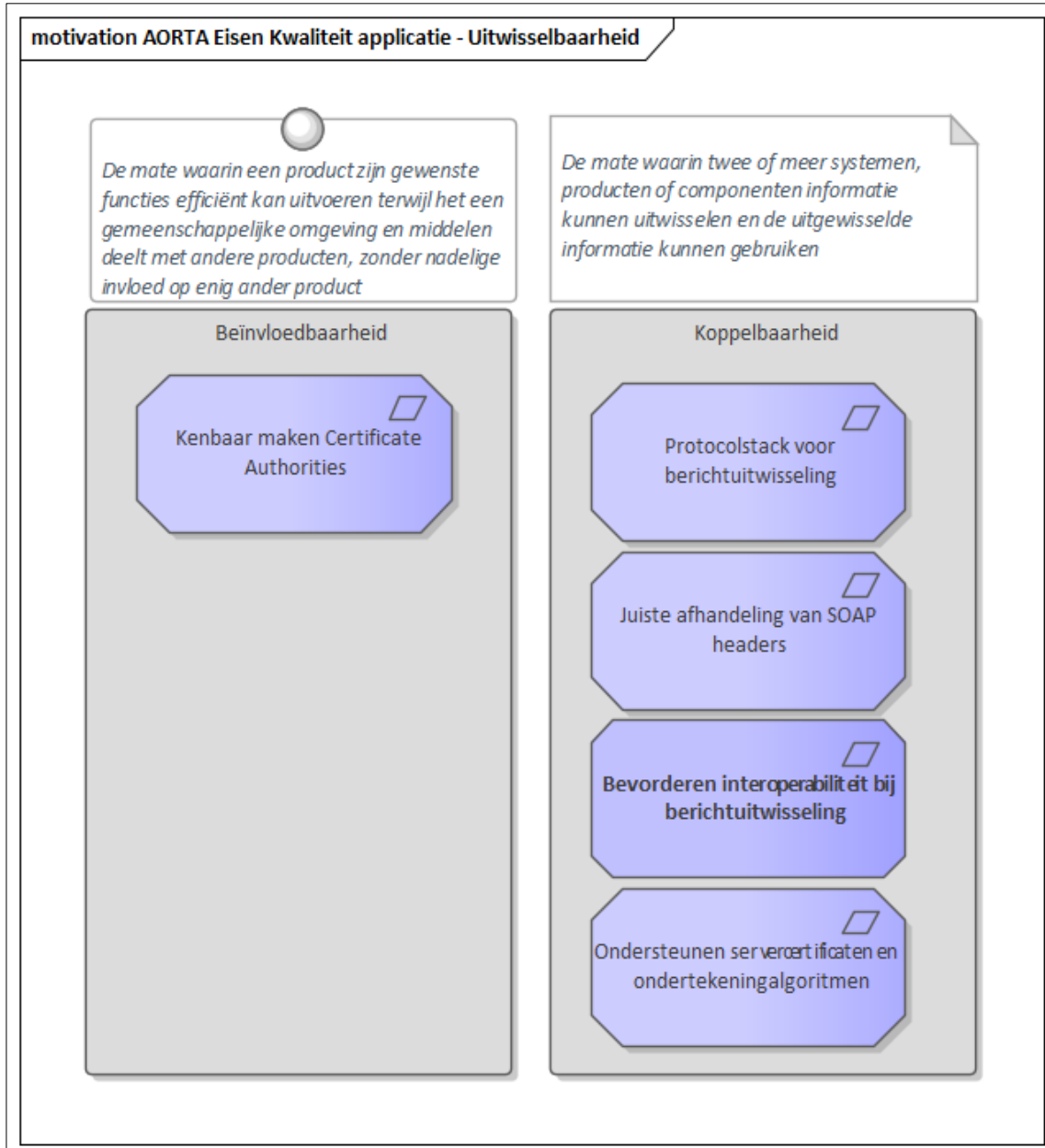


Figure 13 : AORTA Eisen Kwaliteit applicatie - Uitwisselbaarheid

2.3.2.1 Kenbaar maken Certificate Authorities

Alias: GBX.CON.e4100

Details
Eis: Het GBx dient alleen de keten van Certificate Authorities (CA's) van het GBX-certificaat kenbaar te maken aan de ZIM in het "certificate request" bericht van de TLS-handshake, waaronder ook het stamcertificaat (Root CA) van de keten. Toelichting bij eis: Dit is nodig opdat een GBx beperkt kenbaar maakt welke CA's het vertrouwt.

Dit betekent voor de zorgaanbieder dat hij of zijn XIS-leverancier selectief om moet gaan met het aantal CA's waarmee de betrokken XIS-applicatie(s) en/of de eventuele communicatieserver worden opgezet.

Vzvv_Moscow: Verplicht
Vzvv_Req_Verificatie: Aansluittoets
Vzvv_Req_Soort: Functional
Vzvv_Req_Type: Product

2.3.2.2 Ondersteunen servercertificaten en ondertekeningalgoritmen

Alias: GBX.CON.e4110.2

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

Vzvv_Moscow: Verplicht
Vzvv_Req_Verificatie: Monitoring
Vzvv_Req_Soort: Functional
Vzvv_Req_Type: Product

2.3.2.3 Bevorderen interoperabiliteit bij berichtuitwisseling

Alias: GBX.CON.e4066

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

Vzvv_Moscow: Verplicht
Vzvv_Req_Verificatie: Acceptatietest
Vzvv_Req_Soort: Functional
Vzvv_Req_Type: Product

2.3.2.4 Juiste afhandeling van SOAP headers

Alias: GBX.CON.e4065

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

Vzvv_Moscow: Verplicht
Vzvv_Req_Verificatie: Acceptatietest
Vzvv_Req_Soort: Functional
Vzvv_Req_Type: Product

2.3.2.5 Protocolstack voor berichtuitwisseling

Alias: GBX.CON.e4060.3

Details
Eis: Het GBx dient voor berichtuitwisseling met de ZIM de volgende protocolstack te gebruiken: • HL7v3 • SOAP v1.1 • SAML 2.0 • HTTP v1.1 • TLS v1.3 • TCP • IPv4 Toelichting bij eis: Het is niet toegestaan om een lagere protocolversie te hanteren dan die in deze protocolstack vermeld is, zoals bv SSLv2 en SSLv3. Voor de versie van TLS geldt dat de beveiligingsrichtlijnen van NCSC worden gevolgd indien redelijkerwijs mogelijk. Bij de TLS-handshake dient de hoogste toegestane TLS-versie gekozen te worden die beide partijen ondersteunen.

Vzvv_Moscow: Verplicht
Vzvv_Req_Verificatie: Aansluittoets
Vzvv_Req_Soort: Functional
Vzvv_Req_Type: Product

2.4 AORTA Eisen aan de Beheerorganisatie van een GBX

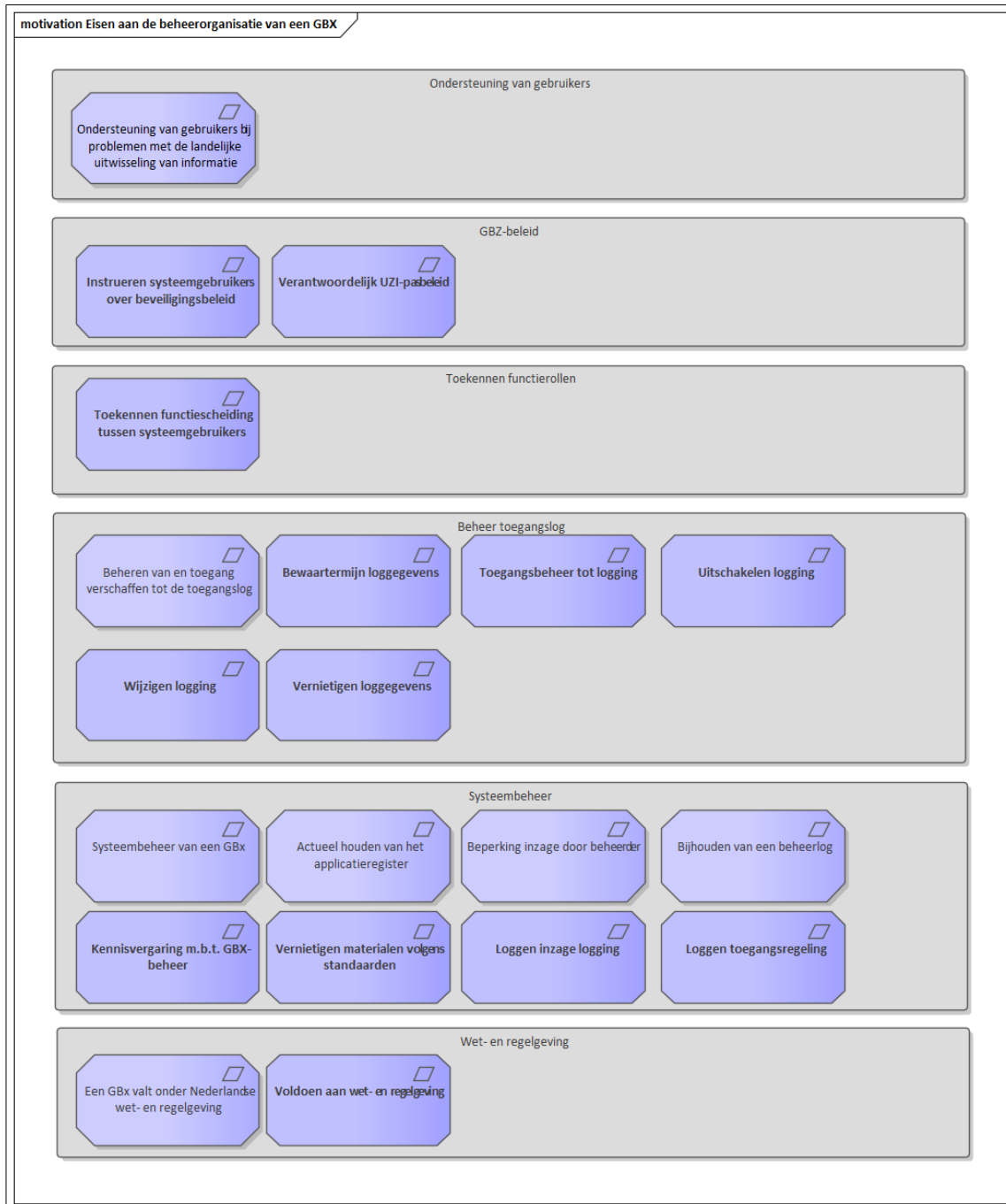


Figure 14 : Eisen aan de beheerorganisatie van een GBX

2.4.1 Wijzigen logging

Alias: AGE.LOG.e4060.1

Details
Eis:

Gegevens in de log mogen niet wijzigbaar of verwijderbaar (alleen in het kader van eis **AGE.LOG.e4050**) zijn. Het niet kunnen wijzigen/verwijderen van loggegevens moet worden afgedwongen door technische maatregelen.

Toelichting:
-

Vz vz_Moscow: Verplicht
Vz vz_Req_Verificatie: Acceptatietest
Vz vz_Req_Soort: Non-Functional
Vz vz_Req_Type: Product

2.4.2 Vernietigen loggegevens

Alias: AGE.LOG.e4050.1

Details
Eis: Loggegevens moeten bij het verstrijken van <i><log_bewaartermijn></i> automatisch worden verwijderd uit de actieve log en uit het archief. De logregels moeten op een zodanige wijze vernietigd worden dat de data niet te reconstrueren is. Dit betekent ook dat eventueel reservekopieën verwijderd/vernietigd/volledig overschreven zijn. Toelichting: Voor de <i><log_bewaartermijn></i> geldt de standaard waarde van 5 jaar.

Vz vz_Moscow: Verplicht
Vz vz_Req_Verificatie: Eigenverklaring
Vz vz_Req_Soort: Non-Functional
Vz vz_Req_Type: Product

2.4.3 Uitschakelen logging

Alias: AGE.LOG.e4030

Details
Eis: Het loggen van de berichtuitwisseling in de toegangslog en het loggen van acties op de toegangslog mogen niet uitgeschakeld kunnen worden. Toelichting bij eis: -

Vz vz_Moscow: Verplicht
Vz vz_Req_Verificatie: Eigenverklaring
Vz vz_Req_Soort: Non-Functional
Vz vz_Req_Type: Product

2.4.4 Toegangsbeheer tot logging

Alias: AGE.LOG.e4040

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

Vzvv_Moscow: Verplicht
Vzvv_Req_Verificatie: Acceptatietest
Vzvv_Req_Soort: Functional
Vzvv_Req_Type: Product

2.4.5 Loggen toegangsregeling

Alias: AGE.LOG.e4070.1

Details
Eis: Elke wijziging in de toegangsregeling dient te worden gelogd. Hierbij moet onweerlegbaar kunnen worden vastgesteld welke persoon met welke rol welke specifieke aanpassing heeft doorgevoerd. Toelichting: Toegangsregeling betreft de autorisatie voor toegang tot medische informatie. Dit kan de toegang tot de logging betreffen, maar ook de toegang tot andere vormen van medische informatie.

Vzvv_Moscow: Verplicht
Vzvv_Req_Verificatie: Acceptatietest
Vzvv_Req_Soort: Functional
Vzvv_Req_Type: Product

2.4.6 Loggen inzage logging

Alias: AGE.LOG.e4020.1

Details
Eis: Elke inzage van de toegangslog dient gelogd te worden. Hierbij moet onweerlegbaar kunnen worden vastgesteld welk persoon inzage heeft gehad in welke specifieke gegevens. Toelichting -

Vzvv_Moscow: Verplicht
Vzvv_Req_Verificatie: Audit
Vzvv_Req_Soort: Functional
Vzvv_Req_Type: Product

2.4.7 Bewaartermijn loggegevens

Alias: AGE.LOG.e4010

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

Vzvv_Moscow: Verplicht
Vzvv_Req_Verificatie: Monitoring

Vzvvz_Req_Soort: Non-Functional

Vzvvz_Req_Type: Business

2.4.8 Voldoen aan wet- en regelgeving

Alias: GBX.ALG.e4010.1

Details
Eis: Een GBx dient te voldoen aan de meest recente definitieve versie van de NEN 7510, NEN 7512 en NEN 7513 normen. Toelichting bij eis: In het 'Besluit elektronische gegevensverwerking door zorgaanbieders' worden de NEN 7510, NEN 7512 en NEN 7513 verplicht gesteld.

Vzvvz_Moscow: Verplicht

Vzvvz_Req_Verificatie: Eigenverklaring

Vzvvz_Req_Soort: Non-Functional

Vzvvz_Req_Type: Product

2.4.9 Vernietigen materialen volgens standaarden

Alias: GBX.SBH.e4070.1

Details
Eis: Om te voorkomen dat privacygevoelige of beveiliging gerelateerde gegevens achterblijven en in ongewenste handen vallen, dienen niet (meer) gebruikte websites, apps, informatie of code te worden vernietigd volgens de standaard NIST 800-88. Te vervangen fysieke opslagmedia dienen gecontroleerd vernietigd te worden volgens DIN 66399. Toelichting bij eis: Er is een proces nodig dat controleert of gegevens nog noodzakelijk zijn en te verwijderen gegevens voorgoed vernietigt.

Vzvvz_Moscow: Verplicht

Vzvvz_Req_Verificatie: Eigenverklaring

Vzvvz_Req_Soort: Functional

Vzvvz_Req_Type: Business

2.4.10 Een GBx valt onder Nederlandse wet- en regelgeving

Alias: GBX.CON.e4050.3

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

Vz vz_Moscow: Verplicht
Vz vz_Req_Verificatie: Aansluittoets
Vz vz_Req_Soort: Non-Functional
Vz vz_Req_Type: Product

2.4.11 Kennisvergaring m.b.t. GBX-beheer

Alias: GBX.SBH.e4060

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

Vz vz_Moscow: Verplicht
Vz vz_Req_Verificatie: Aansluittoets
Vz vz_Req_Soort: Non-Functional
Vz vz_Req_Type: Product

2.4.12 Bijhouden van een beheerlog

Alias: GBX.SBH.e4050.1

Details
Eis: Beheerhandelingen moeten worden vastgelegd in een beheerlog. De organisatie dient de opdrachtgever en toezichthouder inzage te geven in deze beheerlog. In de beheerlog wordt bijgehouden wie 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.

Vz vz_Moscow: Verplicht
Vz vz_Req_Verificatie: Acceptatietest
Vz vz_Req_Soort: Non-Functional
Vz vz_Req_Type: Product

2.4.13 Beperking inzage door beheerder

Alias: GBX.SBH.e4040.4

Details
Eis: De systeembeheerder mag de inhoud van berichten slechts inzien indien dit noodzakelijk is voor het oplossen van problemen, is ingelogd met een tweefactorauthenticatiemiddel en uitsluitend op verzoek van een: • {GBZ} zorgverlener/medewerker; • {GBP} patiënt/klant, een leidinggevende of de Toezichthouder. Toelichting bij eis: Vanuit zijn ondersteunende rol kan het voor een systeembeheerder 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 systeembeheerder expliciet door de organisatieverantwoordelijke is aangewezen.

Vzvv_Moscow: Verplicht
Vzvv_Req_Verificatie: Acceptatietest
Vzvv_Req_Soort: Non-Functional
Vzvv_Req_Type: Product

2.4.14 Actueel houden van het applicatieregister

Alias: GBX.SBH.e4030

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

Vzvv_Moscow: Verplicht
Vzvv_Req_Verificatie: Documentverificatie
Vzvv_Req_Soort: Non-Functional
Vzvv_Req_Type: Product

2.4.15 Systeembeheer van een GBx

Alias: GBX.SBH.e4020.2

Details
Eis: De rol van systeembeheerder moet door de organisatie expliciet benoemd en belegd zijn. De systeembeheerder en diens vervanger(s) dienen met actuele telefoonnummers bekend te zijn bij de LSP-beheerder en de centrale AORTA servicedesk. Op elk moment dient tenminste één systeembeheerder bereikbaar te zijn, die in staat is om de nodige beheertaken uit te voeren. De systeembeheerder dient verzoeken van de LSP-beheerder 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 bereikt kan worden als er problemen zijn met een GBx, die ingrijpen van de systeembeheerder vergen.

Vzvv_Moscow: Verplicht
Vzvv_Req_Verificatie: Aansluittoets
Vzvv_Req_Soort: Non-Functional
Vzvv_Req_Type: Product

2.4.16 Beheren van en toegang verschaffen tot de toegangslog

Alias: GBX.SBH.e4010.1

Details
Eis: De organisatie moet een toegangslogbeheerder benoemen. De toegangslogbeheerder moet verzoeken van de toezichthouder om de lokale toegangslog te raadplegen inwilligen. Toelichting bij eis:

Deze eis is nodig omdat de toezichthouder op AORTA voor het uitvoeren van haar bevoegdheden informatie nodig kan hebben over de gebeurtenissen waarbij het GBx met het LSP informatie heeft uitgewisseld. {GBx} Deze toegangslogbeheerder kan door alle zorgverleners worden gemandateerd om de toegangslog te raadplegen, om zo te voorkomen dat hij voor een verzoek tot raadplegen van de lokale toegangslog inzake een bepaalde patiënt/cliënt steeds de behandelende zorgverleners moet inschakelen. {GBK} Deze toegangslogbeheerder kan worden gemandateerd om de toegangslog te raadplegen door de GBK-verantwoordelijke. {GBP} Deze toegangslogbeheerder dient vóór de aansluiting aan het LSP te worden doorgegeven aan VZVZ.
--

Vzvv_Moscow: Verplicht
Vzvv_Req_Verificatie: Audit
Vzvv_Req_Soort: Non-Functional
Vzvv_Req_Type: Product

2.4.17 Toekennen functiescheiding tussen systeemgebruikers

Alias: GBX.FBH.e4025

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

Vzvv_Moscow: Verplicht
Vzvv_Req_Verificatie: Acceptatietest
Vzvv_Req_Soort: Non-Functional
Vzvv_Req_Type: Product

2.4.18 Verantwoordelijk UZI-pasbeleid

Alias: GBX.FBH.e4017

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

Vzvv_Moscow: Verplicht
Vzvv_Req_Verificatie: Monitoring
Vzvv_Req_Soort: Non-Functional

Vzvvz_Req_Type: Product

2.4.19 Instrueren systeemgebruikers over beveiligingsbeleid

Alias: GBX.FBH.e4015

Details
Eis: Systeemgebruikers binnen een GBZ dienen op de hoogte te zijn van het beveiligingsbeleid en dienen het beveiligingsbeleid na te leven. In het beveiligingsbeleid dient in ieder geval aandacht te zijn voor: • Het gebruik van de systemen en de toegang daartoe; • Het gebruik van de UZI-pas (indien door het XIS gebruikt); hierbij dient in ieder geval de verantwoordelijkheden met betrekking tot het bezit en het gebruik van de UZI-pas benoemd worden. • Het concept van mandatering (indien door het XIS gebruikt); hierbij dient in ieder geval aandacht besteed te worden aan de juiste fijnmazigheid waarop gemandateerd mag worden. De verantwoordelijkheid die wordt weergegeven in een mandaattoken moet bij de reële organisatiestructuur en werkwijze horen. • Het concept van inschrijftoken (indien door het XIS gebruikt). Toelichting: Een GBZ moet concreet beleid maken om het bewustzijn van het beveiligingsbeleid onder de medewerkers en zorgverleners te bevorderen en iedereen te wijzen op zijn verantwoordelijkheden. Beleid om bewustzijn onder personeel te bewerkstelligen horen al standaard onderdeel te zijn van beveiligingsmaatregelen binnen een GBZ. Dit is voorgeschreven in de NEN 7510.

Vzvvz_Moscow: Verplicht

Vzvvz_Req_Verificatie: Monitoring

Vzvvz_Req_Soort: Non-Functional

Vzvvz_Req_Type: Product

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

Alias: GBX.FBH.e4010

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

Vzvvz_Moscow: Verplicht

Vzvvz_Req_Verificatie: Aansluittoets

Vzvvz_Req_Soort: Non-Functional

Vzvvz_Req_Type: Product

2.5 Generieke eisen aan een XIS



Figure 15 : Generieke eisen

2.5.1 Onderscheiden van fictieve gegevens

Alias: GBX.BVL.e4090.1

Details
Eis: Het systeem moet fictieve gegevens opvallend onderscheidend van reguliere gegevens presenteren aan gebruikers. Toelichting bij eis: Deze eis dient om onjuist gebruik van fictieve gegevens te voorkomen in het regulier werkproces. Het is aan de XIS-leverancier om eventueel in afstemming met zijn klant te komen tot een goede onderscheidende weergave van fictieve gegevens.

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

2.6 Eisen XIS-leverancier

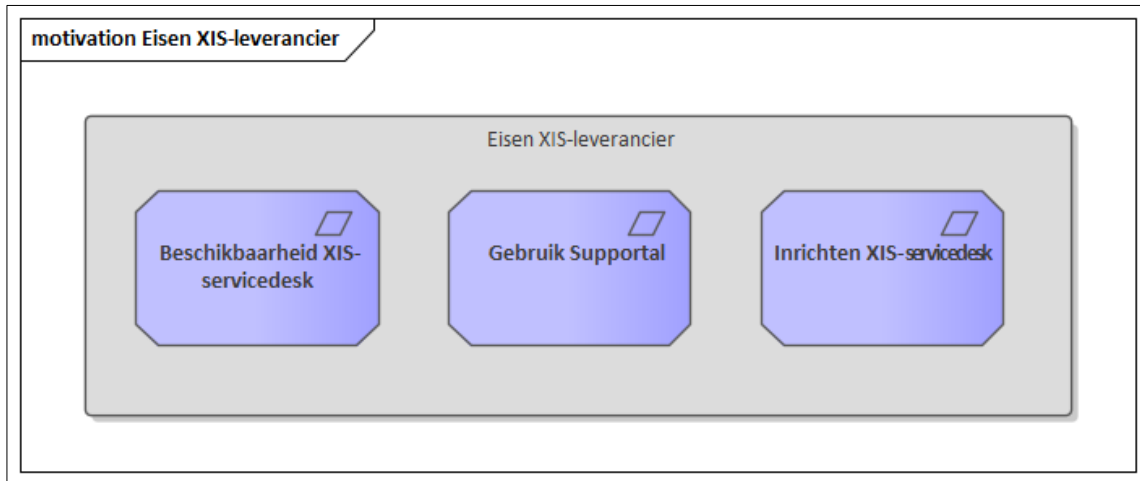


Figure 16 : Eisen XIS-leverancier

2.6.1 Inrichten XIS-servicedesk

Alias: XIS.SVD.e4030.2

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

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Monitoring

Vzvv_Req_Soort: Non-Functional

Vzvv_Req_Type: Business

2.6.2 Gebruik Supportal

Alias: XIS.SVD.e4020

Details

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

Vz vz_Moscow: Verplicht
Vz vz_Req_Verificatie: Monitoring
Vz vz_Req_Soort: Non-Functional
Vz vz_Req_Type: Business

2.6.3 Beschikbaarheid XIS-servicedesk

Alias: XIS.SVD.e4010.2

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

Vz vz_Moscow: Verplicht
Vz vz_Req_Verificatie: Monitoring
Vz vz_Req_Soort: Non-Functional
Vz vz_Req_Type: Business