



PvE HWG Vast Huisartssysteem

Huisarts Waarneem Gegevens

Datum: 5 juni 2024
Status: Definitief
Versie: 8.3.0.0
Classificatie: Openbaar
Eigenaar: VZVZ
Revisie: 02

Documenthistorie

Documentversies

Datum	Status	Versie	Omschrijving
05-06-2024	Definitief	8.3.0.0	Toegevoegd systeemrollen: • Mandaatregistratie; • Inschrijftoken beherend systeem; • Token beherend systeem; • Mandaattoken beherend systeem. Toegevoegd eis: • GBX.FBH.e4070.1.
02-11-2023	Definitief	8.3.0.0	Het betreft een herziening van de inhoud van de document. Diverse eisen waren onterecht meegenomen. Daarnaast zijn de referenties naar andere documentatie bijgewerkt.
26-09-2023	Definitief	8.3.0.0	Het betreft een herziening van de inhoud van de document. Diverse eisen waren onterecht meegenomen.
01-09-2022	Definitief	8.3.0.0	Het betreft de definitieve PvE HWG 6.12.15 die aangepast is voor de AORTA 8.3 infrastructuur. Voortaan zullen de versienummers van het document overeen komen met de versie van de infrastructuur.

Inhoudsopgave

Documenthistorie	2
1 AORTA Eisen Kwaliteit Aangesloten Systemen	7
1.1 Betrouwbaarheid	7
1.1.1 Borgen van de betrouwbaarheid bij grote storingen.....	7
1.1.2 Borgen van de betrouwbaarheid bij kleine storingen.....	8
1.1.3 Minimaliseren van de impact van gepland onderhoud	8
1.1.4 Borgen van de beschikbaarheid van een GBx.....	9
1.2 Beveiligbaarheid.....	10
1.2.1 Beveiligde opslag	10
1.2.2 Een GBx beschikt over een geldig UZI/PKIO-servercertificaat	11
1.2.3 Borgen van plicht tot uitwisselen van patiëntgegevens	11
1.2.4 Beveiliging van patiëntgegevens in het GBx.....	12
1.2.5 Borgen betrouwbare koppeling tussen pas en applicatie.....	12
1.3 Prestatie-efficiëntie.....	13
1.3.1 Genereren time-out.....	13
1.3.2 Tijdige verwerking van berichten	14
1.3.3 Borgen van minimale verwerkingssnelheid	14
1.4 Uitwisselbaarheid.....	16
1.4.1 Aansluiting op productie-omgeving LSP	17
1.4.2 Tijdsynchronisatie GBx en ZIM.....	17
1.4.3 Gebruik van IP en DNS.....	18
1.4.4 Communicatie met het LSP via een GZN	18
2 AORTA Eisen Kwaliteit Applicatie.....	20
2.1 Uitwisselbaarheid.....	20
2.1.1 Kenbaar maken Certificate Authorities.....	22
2.1.2 Ondersteunen servercertificaten en ondertekeningalgoritmen.....	22
2.1.3 Bevorderen interoperabiliteit bij berichtuitwisseling	22
2.1.4 Juiste afhandeling van SOAP headers	23
2.1.5 Protocolstack voor berichtuitwisseling	23
2.2 Beveiligbaarheid.....	24
2.2.1 Hardening	24
2.2.2 Beveiligen van tokens	25
2.2.3 Opzetten beveiligde verbinding vanuit de ZIM met een GBx.....	25
2.2.4 Opzetten en gebruiken van TLS-sessies	26
2.2.5 Instellen configuratieparameters t.b.v. communicatie en authenticatie van de ZIM.....	26

2.2.6	Opzetten beveiligde verbinding met de ZIM	26
2.2.7	Toegangslog bijhouden.....	27
2.2.8	Toegang systeem met tweefactorauthenticatie	28
3	Eisen Infrastructurele Systeemrollen Vast huisartssysteem	29
3.1	Applicatiebeheer	29
3.1.1	Bevestigen applicatiekoppeling	31
3.1.2	Verifiëren applicatiekoppeling	31
3.1.3	Wijzigen TKID applicatie	32
3.2	Generieke eisen.....	34
3.2.1	Onderscheiden van fictieve gegevens.....	34
3.3	Opleverend Systeem	35
3.3.1	Verwerken en beantwoorden opvraag.....	35
3.3.2	Bijhouden van de verwijzindex	35
3.3.3	Afzonderlijk instellen afscherming per doelgroep.....	36
3.3.4	Opt-in controle.....	36
3.3.5	Compatibiliteit bieden met de diverse (zorg)toepassingen	37
3.3.6	Afschermen patiëntgegevens op doelgroep	38
3.3.7	Afschermen van patiëntgegevens	38
3.3.8	Vrijgeven van patiëntgegevens.....	38
3.3.9	Retourneren van opgevraagde patiëntgegevens.....	39
3.4	Patiëntadministratie	40
3.4.1	Gebruik van geverifieerde BSN's.....	40
3.4.2	Opzoeken en tonen patiëntgegevens.....	41
3.4.3	Bijhouden opt-in	41
3.4.4	Bijhouden behandelrelatie	42
3.4.5	Controleren geldigheid van een WID.....	42
3.4.6	Definitief koppelen van patiëntgegevens aan een BSN	43
3.4.7	Voorlopig koppelen van patiëntgegevens aan een BSN	44
3.4.8	Verwerken geboortedatums waarin nullen zijn opgenomen	44
3.5	Primaire interacties - ontvangend systeem	45
3.5.1	Ontvangen patiëntgegevens	45
3.5.2	Opslaan ontvangen patiëntgegevens	46
3.5.3	Ontvangen en verwerken van opgestuurde patiëntgegevens.....	46
3.6	Verwijzindex.....	47
3.6.1	Synchroniseren van de lokale administratie met de verwijzindex	47
3.6.2	Heraanmelden van patiëntgegevens	49
3.6.3	Afmelden van patiëntgegevens	49
3.6.4	Aanmelden van patiëntgegevens.....	50

3.7	Mandaatregistratie	51
3.7.1	Uniformiteit mandaat	51
3.7.2	Waarschuwen verlopen mandaten	52
3.7.3	Verwijderen mandaten	52
3.7.4	Logging mandaten	53
3.7.5	Gebruik mandaattokens	53
3.7.6	Beheren mandaattokens	54
3.7.7	Inzichtelijk maken mandaatautorisatie	54
3.7.8	Beheren gemandateerde groepen	54
3.7.9	Beheren mandaat autorisatieregel	55
3.7.10	Beheren van mandaten	56
3.8	Mandaattoken beherend systeem	57
3.8.1	Beheren mandaattokens	57
3.9	Inschrijftoken beherend systeem	58
3.9.1	Inhoud inschrijftoken	58
3.9.2	Geldigheidsduur inschrijftoken	58
3.9.3	Creëren inschrijftoken	59
3.9.4	Beperken gebruik inschrijftokens	59
3.10	Token beherend systeem	60
3.10.1	Verwijderen tokens	60
3.10.2	Toegankelijkheid tokens	60
3.10.3	Voorkomen misbruik tokens	61
4	HWg Eisen aan de beheerorganisatie	62
4.1	Afmelden patiënt na overlijden	62
4.2	Wijzigen logging	63
4.3	Vernietigen loggegevens	63
4.4	Uitschakelen logging	64
4.5	Toegangsbeheer tot logging	64
4.6	Loggen toegangsregeling	64
4.7	Loggen inzage logging	65
4.8	Bewaartermijn loggegevens	65
4.9	Voldoen aan wet- en regelgeving	66
4.10	Vernietigen materialen volgens standaarden	66
4.11	Een GBx valt onder Nederlandse wet- en regelgeving	66
4.12	Kennisvergaring m.b.t. GBX-beheer	67
4.13	Bijhouden van een beheerlog	67
4.14	Beperking inzage door beheerder	68
4.15	Actueel houden van het applicatieregister	68

4.16	Systeembeheer van een GBx	68
4.17	Beheren van en toegang verschaffen tot de toegangslog.....	69
4.18	Toekennen functiescheiding tussen systeemgebruikers	69
4.19	Instrueren systeemgebruikers over beveiligingsbeleid	70
4.20	Ondersteuning van gebruikers bij problemen met de landelijke uitwisseling van informatie.....	70
5	Eisen voor specifieke zorgtoepassingssysteemrollen.....	72
5.1	Opleveren Professionele Samenvatting	72
5.2	Ontvangen Waarneembericht.....	73

1 AORTA Eisen Kwaliteit Aangesloten Systemen

1.1 Betrouwbaarheid

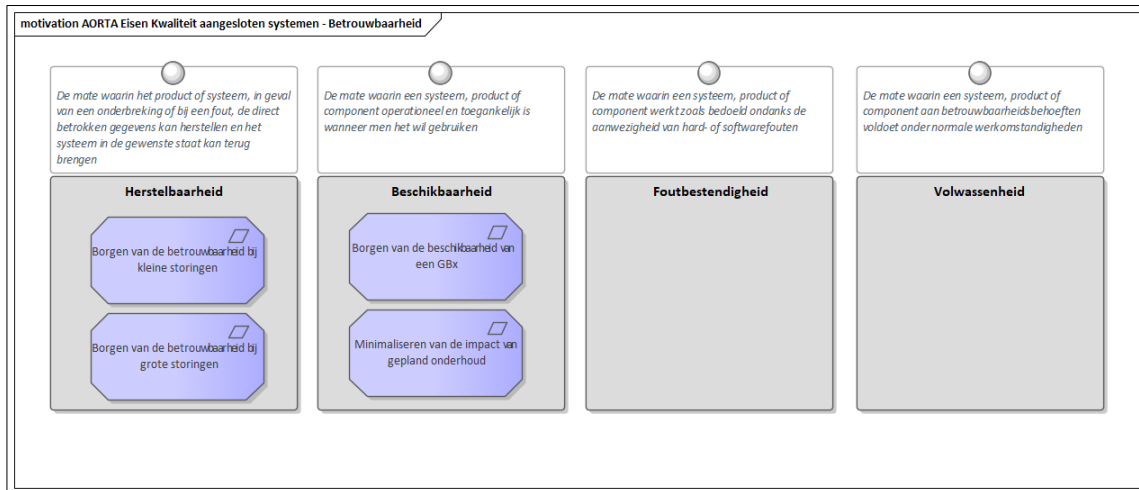


Figure 1 : AORTA Eisen Kwaliteit aangesloten systemen - Betrouwbaarheid

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

1.1.1 Borgen van de betrouwbaarheid bij grote storingen

Alias: GBX.BET.e4020.1

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

Vzvv_Moscow: Verplicht (Must)
Vzvv_Req_Verificatie: Monitoring
Vzvv_Req_Soort: Non-Functional

Vzvvz_Req_Type: Product

1.1.2 Borgen van de betrouwbaarheid bij kleine storingen

Alias: GBX.BET.e4010.1

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

Vzvvz_Moscow: Verplicht (Must)

Vzvvz_Req_Verificatie: Monitoring

Vzvvz_Req_Soort: Functional

Vzvvz_Req_Type: Product

1.1.3 Minimaliseren van de impact van gepland onderhoud

Alias: GBX.BES.e4020.2

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

Vzvvz_Moscow: Verplicht (Must)

Vzvvz_Req_Verificatie: Monitoring

Vzvvz_Req_Soort: Non-Functional

Vzvvz_Req_Type: Product

1.1.4 Borgen van de beschikbaarheid van een GBx

Alias: GBX.BES.e4010

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

Vzvv_Moscow: Verplicht (Must)
Vzvv_Req_Verificatie: Monitoring
Vzvv_Req_Soort: Non-Functional
Vzvv_Req_Type: Product

1.2 Beveiligbaarheid

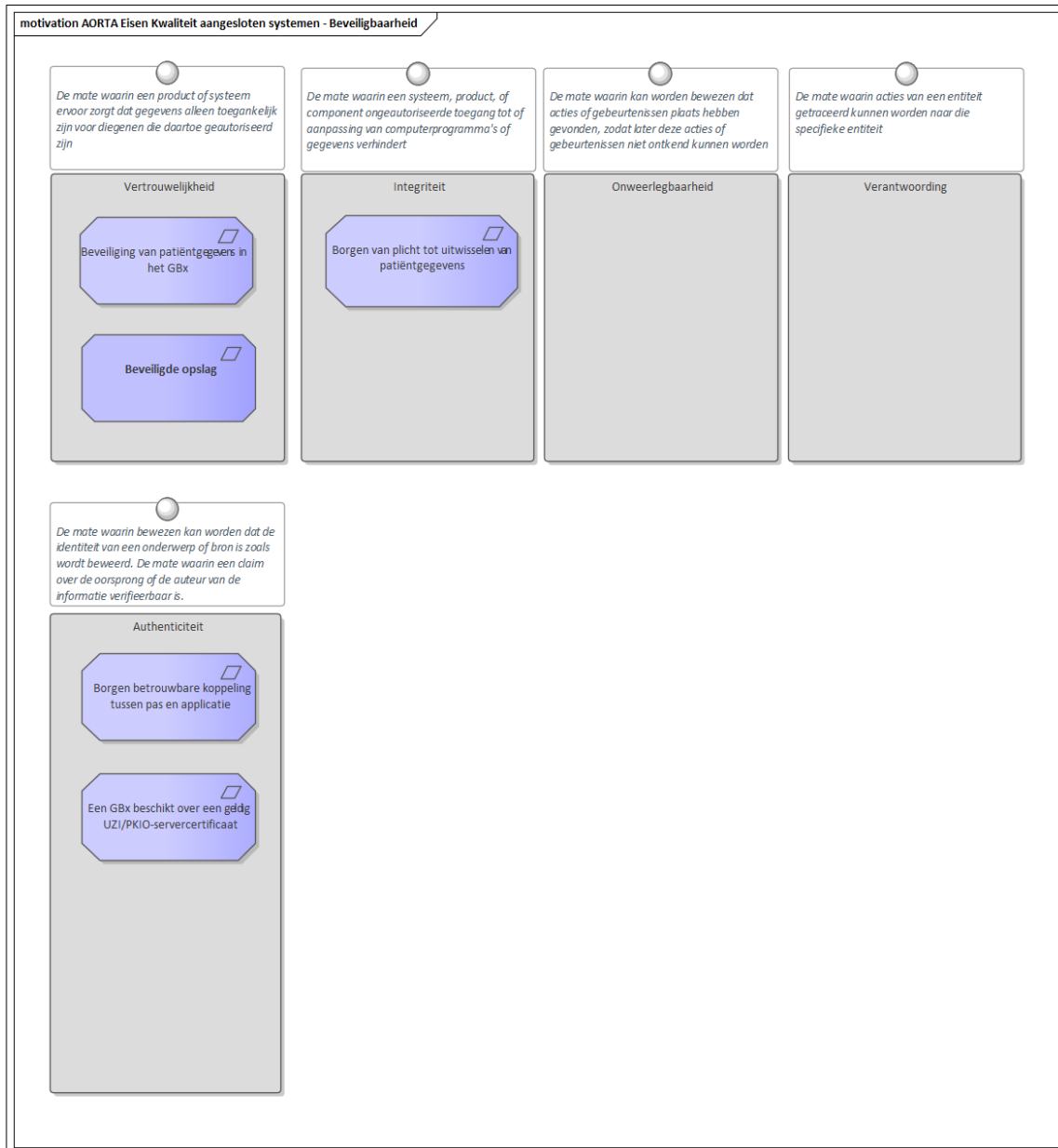


Figure 2 : AORTA Eisen Kwaliteit aangesloten systemen - Beveiligbaarheid

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

Dit schema toont de subcategorieën van Beveiligbaarheid volgens ISO 25010.

1.2.1 Beveiligde opslag

Alias: SYS.BVL.e4010.1

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

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

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

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

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

Vzvv_Moscow: Verplicht (Must)
 Vzvv_Req_Verificatie: Aansluittoets
 Vzvv_Req_Soort: Functional
 Vzvv_Req_Type: Product

1.2.3 Borgen van plicht tot uitwisselen van patiëntgegevens

Alias: GBX.BVL.e4070

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

Vzvv_Moscow: Verplicht (Must)
 Vzvv_Req_Verificatie: Monitoring
 Vzvv_Req_Soort: Functional
 Vzvv_Req_Type: Product

1.2.4 Beveiliging van patiëntgegevens in het GBx

Alias: GBX.BVL.e4060

Details
Eis: Voor een GBx moet zijn gedefinieerd: 1. welke landelijke toepassingen en systeemrollen worden ondersteund en gebruikt; 2. hoe de grenzen van het GBx lopen door de ICT-voorzieningen van de organisatie; 3. hoe en wanneer patiëntgegevens die grenzen kunnen passeren; 4. hoe wordt gewaarborgd dat patiëntgegevens in de dossiers en postbussen niet kunnen lekken naar onbetrouwbare bestemmingen; 5. hoe wordt gewaarborgd dat patiëntgegevens uit onbetrouwbare bronnen niet kunnen terechtkomen in de dossiers en postbussen of de ZIM; 6. hoe wordt gewaarborgd dat anderen dan bevoegde gebruikers geen fysieke toegang tot (delen van) het GBx kunnen krijgen. Toelichting bij eis: Deze eis is nodig om te voorkomen dat patiëntgegevens, bijvoorbeeld via een andere applicatie, door willekeurige medewerkers kunnen worden benaderd terwijl de organisatie zijn GBx heeft beveiligd met firewalls, authenticatie- en vertrouwensmiddelen.

Vzvv_Moscow: Verplicht (Must)

Vzvv_Req_Verificatie: Documentverificatie

Vzvv_Req_Soort: Non-Functional

Vzvv_Req_Type: Product

1.2.5 Borgen betrouwbare koppeling tussen pas en applicatie

Alias: GBX.BVL.e4050.1

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

Vzvv_Moscow: Verplicht (Must)

Vzvvz_Req_Verificatie: Audit
 Vzvvz_Req_Soort: Functional
 Vzvvz_Req_Type: Product

1.3 Prestatie-efficiëntie

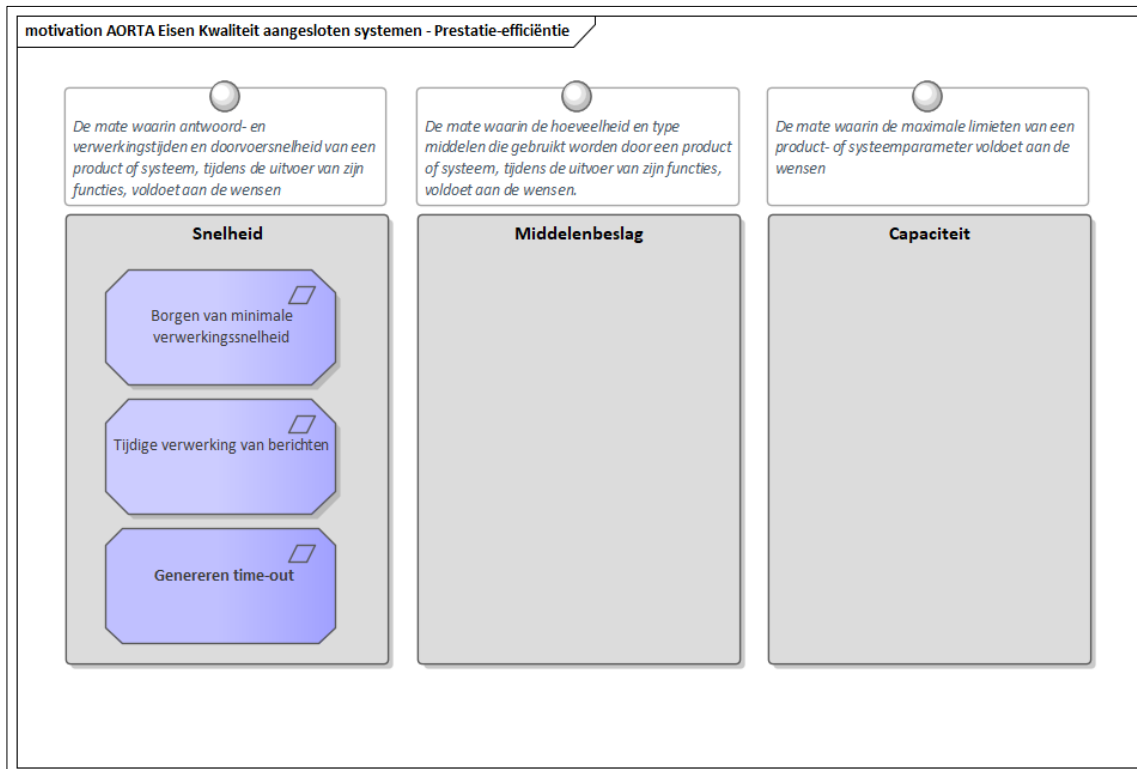


Figure 3 : AORTA Eisen Kwaliteit aangesloten systemen - Prestatie-efficiëntie

1.3.1 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 (timeout) 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. Voorsnog blijft de waarde zoals opgenomen in deze eis gehandhaaft. 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

1.3.2 Tijdige verwerking van berichten

Alias: GBX.PST.e4015

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

Vzvv_Moscow: Verplicht (Must)
Vzvv_Req_Verificatie: Monitoring
Vzvv_Req_Soort: Non-Functional
Vzvv_Req_Type: Product

1.3.3 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.

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

1.4 Uitwisselbaarheid

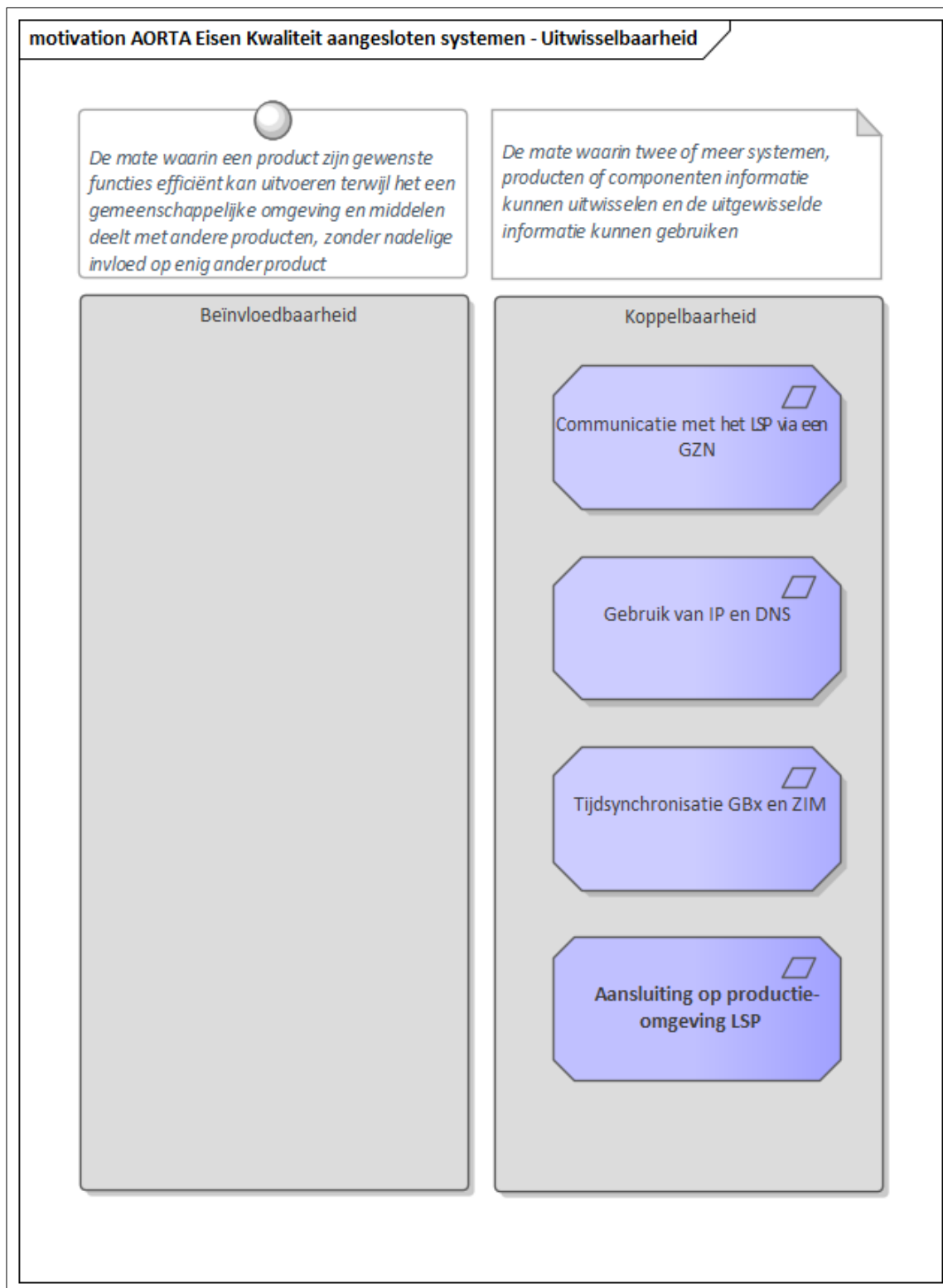


Figure 4 : AORTA Eisen Kwaliteit aangesloten systemen - Uitwisselbaarheid

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

Dit diagram toont de subcategorieën zoals gedefinieerd door ISO 25010.

1.4.1 Aansluiting op productie-omgeving LSP

Alias: GBX.CON.e4120

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

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Monitoring

Vzvv_Req_Soort: Non-Functional

Vzvv_Req_Type: Product

1.4.2 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 toezichthouder of patiënt een geval van vermeend onrechtmatige uitwisseling van patiëntgegevens wil onderzoeken en daartoe zowel de lokale toegangslog van het GBx als de centrale toegangslog van het LSP wil raadplegen. Deze eis betekent voor de organisatie dat er binnen het GBx een NTP-client is geïnstalleerd en dat deze is afgestemd op de NTP-server van de ZIM. Ook is het mogelijk dat de ZIM 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 (Must)

Vzvv_Req_Verificatie: Monitoring

Vzvv_Req_Soort: Non-Functional

Vzvv_Req_Type: Product

1.4.3 Gebruik van IP en DNS

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

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

Vzvv_Moscow: Verplicht (Must)
Vzvv_Req_Verificatie: Aansluittoets
Vzvv_Req_Soort: Non-Functional
Vzvv_Req_Type: Product

1.4.4 Communicatie met het LSP via een GZN

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

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

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

2 AORTA Eisen Kwaliteit Applicatie

2.1 Uitwisselbaarheid

motivation AORTA Eisen Kwaliteit applicatie - Uitwisselbaarheid

De mate waarin een product zijn gewenste functies efficiënt kan uitvoeren terwijl het een gemeenschappelijke omgeving en middelen deelt met andere producten, zonder nadelige invloed op enig ander product

Beïnvloedbaarheid

Kenbaar maken Certificate Authorities

De mate waarin twee of meer systemen, producten of componenten informatie kunnen uitwisselen en de uitgewisselde informatie kunnen gebruiken

Koppelbaarheid

Protocolstack voor berichtuitwisseling

Juiste afhandeling van SOAP headers

Bevorderen interoperabiliteit bij berichtuitwisseling

Ondersteunen servercertificaten en ondertekeningalgoritmen

Figure 5 : AORTA Eisen Kwaliteit applicatie - Uitwisselbaarheid

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

2.1.1 Kenbaar maken Certificate Authorities

Alias: GBX.CON.e4100

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

Vzvv_Moscow: Verplicht (Must)

Vzvv_Req_Verificatie: Aansluittoets

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

2.1.2 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 ondertekeningalgoritme. Toelichting bij eis: Het UZI-register geeft UZI-servercertificaten uit onder één of meerdere certificaatbomen. In het geval er onder diverse certificaatbomen UZI-servercertificaten wordt uitgegeven, is het zaak om alle servercertificaten uitgegeven onder de diverse certificaatbomen te kunnen ondersteunen. Een GBX-communicatieserver dient te zijn ingericht op het ondertekeningalgoritme SHA-256.

Vzvv_Moscow: Verplicht (Must)

Vzvv_Req_Verificatie: Monitoring

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

2.1.3 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

2.1.4 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'.

Vzvv_Moscow: Verplicht (Must)

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

2.1.5 Protocolstack voor berichtuitwisseling

Alias: GBX.CON.e4060.2

Details
Eis:

Het GBx dient voor berichtuitwisseling met de ZIM de volgende protocolstack te gebruiken:

- HL7v3
- SOAP v1.1
- SAML 2.0
- HTTP v1.1
- TLS v1.2/TLS v1.3
- TCP
- IPv4

Toelichting bij eis:

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

Voor de versie van TLS geldt dat de beveiligingsrichtlijnen van NCSC worden gevolgd indien redelijkerwijs mogelijk. Alle deelnemers dienen minimaal TLS 1.2 te ondersteunen, tenzij het ook mogelijk is om TLS 1.3 te ondersteunen. Bij de TLS-handshake dient de hoogste toegestane TLS-versie gekozen te worden die beide partijen ondersteunen.

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

Vzvv_Moscow: Verplicht (Must)
Vzvv_Req_Verificatie: Aansluittoets
Vzvv_Req_Soort: Functional
Vzvv_Req_Type: Product

2.2 Beveiligbaarheid

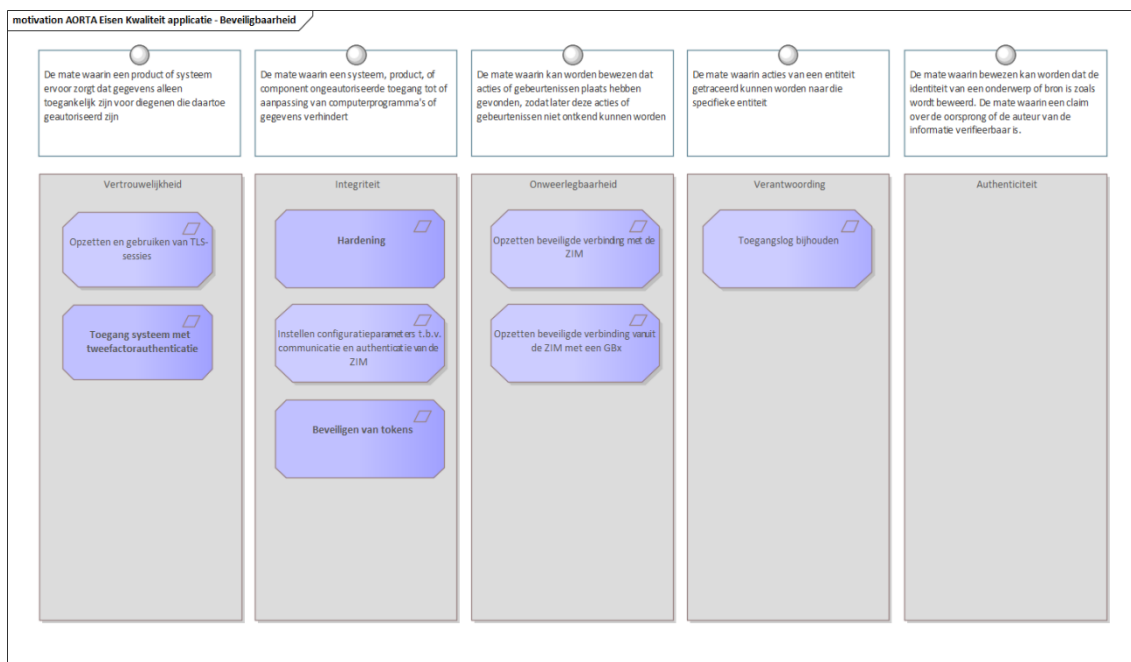


Figure 6 : AORTA Eisen Kwaliteit applicatie - Beveiligbaarheid

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

2.2.1 Hardening

Alias: SYS.BVL.e4065

Details
Eis: Er dient hardening op de diverse systeemlagen te worden toegepast. Het gaat hierbij om hardening op het niveau van operating system, middleware en database. Alle 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

2.2.2 Beveiligen van tokens

Alias: GBX.FBH.e4070.1

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

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

2.2.3 Opzetten beveiligde verbinding vanuit de ZIM met een GBx

Alias: GBX.CON.e4090.2

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

Vzvv_Moscow: Conditioneel.
 Vzvv_Req_Verificatie: Acceptatietest
 Vzvv_Req_Soort: Functional
 Vzvv_Req_Type: Product

2.2.4 Opzetten en gebruiken van TLS-sessies

Alias: GBX.CON.e4070.2

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

Vzvv_Moscow: Verplicht (Must)

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

2.2.5 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 (Must)

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

2.2.6 Opzetten beveiligde verbinding met de ZIM

Alias: GBX.CON.e4080.5

Details
Eis: Het GBx dient voor het landelijk uitwisselen van patiëntgegevens een TLS-sessie met de ZIM met de volgende kenmerken op te zetten: 1. tweezijdige authenticatie met behulp van het servercertificaat van de ZIM en * (indien tokenauthenticatie) het servercertificaat van het GBx voor vertrouwensniveau midden

* het servercertificaat van het GBx voor vertrouwensniveau laag {GBK} en midden

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

Toelichting bij eis:

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

Dit betekent voor de organisatie dat hij of zijn XIS-leverancier de bovenstaande parameters moet instellen in de TLS-library in de betrokken applicatie(s) en/of de eventuele communicatieserver. Het GBx is niet in staat te controleren of de ZIM daadwerkelijk het (server)certificaat van de GBx opvraagt, maar mag er impliciet van uitgaan dat dit gebeurt en dat de ZIM het certificaat ook controleert. Hiermee wordt tweezijdige authenticatie bewerkstelligd.

Vzvv_Moscow: Conditioneel.

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

2.2.7 Toegangslog bijhouden

Alias: GBX.LOG.e4015.1

Details

Eis:

Het systeem moet de volgende berichtuitwisselingen loggen:

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

De log bevat per berichtuitwisseling tenminste:

1. de identiteit van de patiënt/cliënt (BSN)
2. identiteit van de opvragende/versturende en bestemde organisatie
3. de functie en identiteit van de opvragende of versturende zorgverlener of medewerker of patiënt.
4. type van de uitgevoerde gebruikersinteractie
5. het tijdstip en tijdzone (ten opzichte van UTC) van de gebruikersinteractie
6. de bericht-id van het ontvangen (opvraag- of bevestig-) bericht
7. de bericht-id van het verzonden (oplever- of opdracht-) bericht
8. de gegevenssoorten of contextcodes van de verzonden en ontvangen patiëntstukken;
9. een indicatie van eventueel opgetreden foutsituaties met betrekking tot het ontvangen en verzenden van de berichten.

Toelichting bij eis:

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

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

- wat voor soort patiëntstukken wanneer zijn toegestuurd aan welke andere zorgaanbieder of ZIM;
- welke inhoud die patiëntstukken precies hadden;
- wat voor soort patiëntstukken wanneer zijn opgevraagd door welke patiënt vanuit welke organisatie.

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

Vzvv_Moscow: Verplicht (Must)
Vzvv_Req_Verificatie: Acceptatietest
Vzvv_Req_Soort: Functional
Vzvv_Req_Type: Product

2.2.8 Toegang systeem met tweefactorauthenticatie

Alias: GBX.BVL.e4150

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

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

3 Eisen Infrastructurele Systeemrollen

Vast huisartssysteem

3.1 Applicatiebeheer

motivation Eisen Infrastructurele Systemrollen - Applicatiebeheer

Applicatieregister raadplegend systeem

Applicatieregister bewerkend systeem

Wijzigen TKID applicatie

Koppeling verifiërend systeem

Verifiëren applicatiekoppeling

Koppeling bevestigend systeem

Bevestigen applicatiekoppeling

Figure 7 : Eisen Infrastructurele Systeemrollen - Applicatiebeheer

3.1.1 Bevestigen applicatiekoppeling

Alias: GBX.APR.e4160

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

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

3.1.2 Verifiëren applicatiekoppeling

Alias: GBX.APR.e4140

Details
Beginsituatie De gebruiker is lokaal ingelogd op vertrouwensniveau laag of hoger.
Trigger De gebruiker initieert de functie via het systeem.
Interacties 1. Het systeem verzendt een verifiërenApplicatiekoppeling bericht naar de ZIM of een ander GBX conform IH AORTA. 2. Het systeem ontvangt een verifiërenApplicatiekoppelingAntwoord bericht 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 Het bericht moet een authenticatietoken kunnen bevatten.
Responsetijd -
Betrouwbaarheid Garantie geven dat versturen van gegevens niet zonder kennisgeving gestaakt wordt

Toelichting

-

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

3.1.3 Wijzigen TKID applicatie

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

Details

Beginsituatie

De gebruiker is lokaal ingelogd op vertrouwensniveau laag of hoger.

Trigger

De gebruiker initieert de functie via het systeem.

Interacties

1. Het systeem verzendt een *beherenTKID*-bericht naar de ZIM conform [IH AORTA](#).
2. 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 'beheren TKID'-bericht, het gewenste TKID ingestuurd te worden.

Er mogen alleen TKID's ingestuurd worden, die door de afgenomen XIS-applicatiesoftware zijn verkregen naar aanleiding van een positieve acceptatie. De beheerder of het systeem van een bij een zorgaanbieder geïnstalleerde applicatie dient alleen die TKID's in te sturen waarvan alle systeemrollen ook daadwerkelijk door de geïnstalleerde applicatie ondersteund worden.

Er kunnen meerdere TKID's in het bericht opgenomen worden. Zodra een TKID niet bekend is, wordt er een foutcode (INVALIDETKID) met bijbehorende foutmelding (zie [Foutentabel](#)) gegenereerd. De mogelijk overige correcte TKID's worden niet verwerkt in het applicatieregister. Alle TKID's dienen opnieuw ingestuurd te worden.

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

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

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

Terugzetten oude functionaliteit (met een eerder verkregen TKID).

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

3.2 Generieke eisen

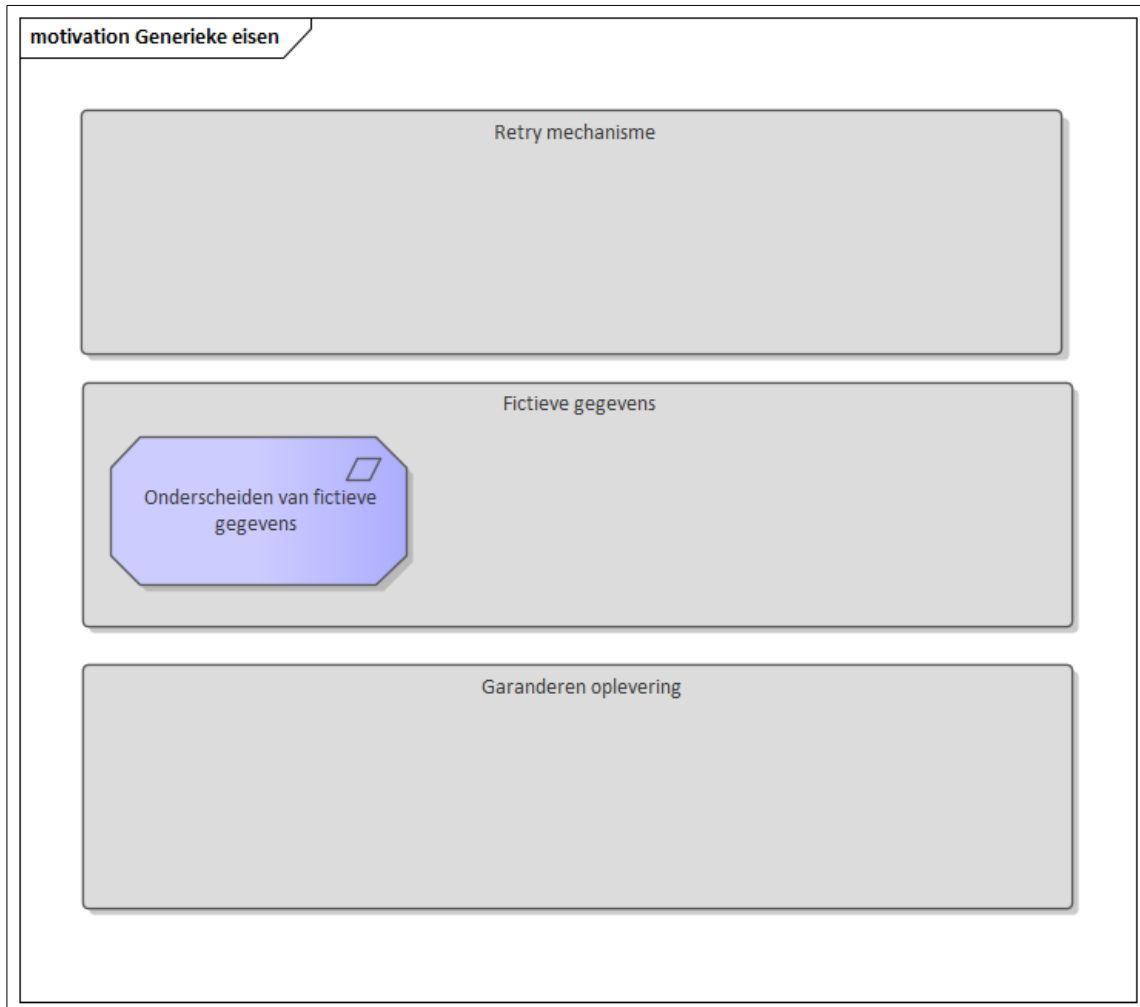


Figure 8 : Generieke eisen

3.2.1 Onderscheiden van fictieve gegevens

Alias: GBX.BVL.e4090

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

Vz vz_Moscow: Verplicht (Must)
Vz vz_Req_Verificatie: Acceptatietest
Vz vz_Req_Soort: Functional
Vz vz_Req_Type: Product

3.3 Opleverend Systeem

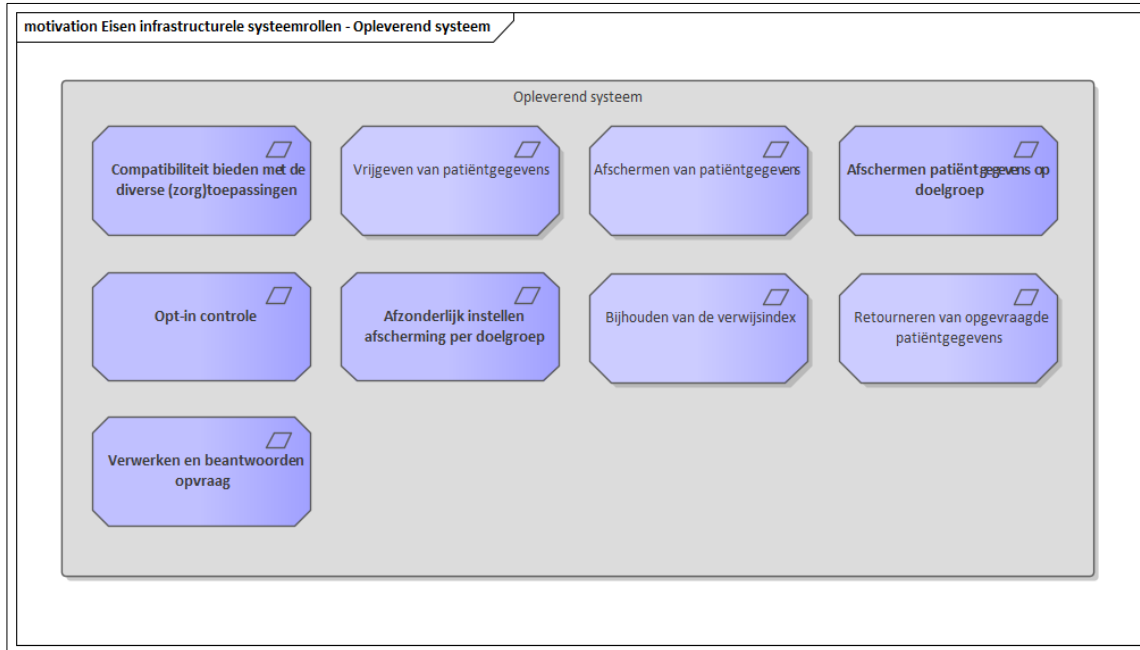


Figure 9 : Eisen infrastructurele systeemrollen - Opleverend systeem

3.3.1 Verwerken en beantwoorden opvraag

Alias: GBX.OPV.e4590

Details
Eis: Het opleverende systeem dient een opvraag te kunnen verwerken en een antwoord te kunnen versturen zoals gespecificeerd in de implementatiehandleiding van de zorgtoepassing. Toelichting bij eis: De implementatiehandleiding van een zorgtoepassing is opgenomen in Art-Decor (https://decor.nictiz.nl/pub/vzvz/). Hierin is voor elke systeemrol gespecificeerd welke interacties er ondersteund dienen te worden.

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

3.3.2 Bijhouden van de verwijsindex

Alias: GBX.OPV.e4540.2

Details
Eis: Alle in het systeem beschikbare patiëntgegevens, waarvoor het systeem fungeert als bronsysteem patiëntgegevens, moeten bij de verwijsindex worden aangemeld, heraangemeld en afgemeld. Dit dient te geschieden onder vermelding van de gegevenssoort waartoe de patiëntgegevens behoren.

Het systeem dient een gegevenssoort aan te melden indien het beschikt over, tot de gegevenssoort behorende, vrijgegeven gegevens voor een patiënt.
Het systeem dient een gegevenssoort heraan te melden indien er iets wijzigt in de lokale registratie van de tot de gegevenssoort behorende, aangemelde gegevens voor een patiënt.
Het systeem dient een gegevenssoort af te melden indien het niet langer beschikt over, tot de gegevenssoort behorende, vrijgegeven gegevens voor een patiënt.
Patiëntgegevens mogen slechts bij de verwijfsindex zijn aangemeld, wanneer er sprake is van een definitieve koppeling met het BSN.
Toelichting bij eis: Aanmelden is alleen toegestaan indien uit de opt-in-registratie van het systeem expliciet blijkt dat de patiënt akkoord is gegaan met het beschikbaar maken van zijn medische gegevens aan andere zorgaanbieders.
Patiëntgegevens en gegevenssoorten worden gedefinieerd in domeinspecificaties.
Als kopie aangemerkte patiëntgegevens mogen niet worden aangemeld.
Aangemelde patiëntgegevens kunnen via AORTA worden opgevraagd.

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

3.3.3 Afzonderlijk instellen afscherming per doelgroep

Alias: GBX.OPV.e4536

Details
Eis: Afscherming van gegevens voor bevraging door patiënten en zorgverleners moet afzonderlijk ingesteld kunnen worden.
Toelichting bij eis: Het kan mogelijk zijn dat een patiënt gegevens voor andere zorgaanbieders wil laten afschermen, maar dat hij die gegevens wel zelf wil kunnen ontvangen (of andersom).
Het aggregatieniveau van afscherming voor beide doelgroepen is opgenomen in eis GBX.OPV.e4530.
Conditie: Deze eis geldt indien er zowel gegevens beschikbaar worden gesteld aan patiënten en aan zorgaanbieders.

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

3.3.4 Opt-in controle

Alias: GBX.OPV.e4560.2

Details
Eis:

Alvorens gegevens van een patiënt op te leveren, dient er expliciet gecontroleerd te worden of er een opt-in geregistreerd staat van de patiënt in het geval:

- er een AORTA access token wordt ontvangen, waarin een attest claim is opgenomen met de waarde 'BRON';
- er een HL7v3-bericht wordt ontvangen.

Deze controle dient te worden overgeslagen indien de opvrager een patiënt is (rolcode 'P') en in het geval van een FHIR-request in combinatie met een AORTA access token met een andere waarde dan 'BRON'.

Toelichting bij eis:

Om te voorkomen dat een zorgverlener patiëntgegevens kan opvragen zonder een expliciete toestemming van de patiënt, is het van belang dat het systeem een controle doet op het aanwezig zijn van een geregistreerde opt-in voor de specifieke binnenkomende opvraag.

Indien er sprake is van een FHIR-request, dan zal dit request begeleid worden door een AORTA-access token. Dit token bevat een attest claim, op basis waarvan bepaald kan worden hoe de bron om moet gaan met de toestemmingscontrole. Indien wordt verwacht dat de bron de patiënttoestemming controleert, dan is dit aangegeven door de waarde 'BRON'.

Huidige zorgsystemen registreren alleen de opt-ins voor het opvragen van patiëntgegevens door zorgverleners. Een patiënt geeft geen uitdrukkelijke toestemming bij de zorgaanbieder om zijn eigen gegevens op te vragen. Er is in het systeem dan ook geen opt-in registratie voor het opvragen van gegevens door de patiënt zelf. Echter, de patiënt heeft het recht om zijn eigen gegevens op te kunnen vragen. In het geval van een opvraag door een patiënt dient de aanwezigheid van een opt-in dan ook overgeslagen te worden.

De controle of de opvrager een patiënt is moet gebeuren op basis van de rolcode van de 'overseer' van het bericht.

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

3.3.5 Compatibiliteit bieden met de diverse (zorg)toepassingen

Alias: GBX.OPV.e4550.1

Details
Eis: Een bronsysteem moet bevestigingen van diverse actoren en vanuit diverse organisaties kunnen verwerken. Toelichting bij eis: De volgende actoren of groep van actoren moeten door het bronsysteem worden ondersteunt als opvrager (of opvraagverantwoordelijke): • Een zorgverlener op basis van UZI; • Een burger op basis van BSN. De volgende organisaties moeten door het bronsysteem worden ondersteunt als organisatie vanuit waar opgevraagd wordt: • Resource Broker VnC; • Patiëntenportaal (GBP); • Goed beheerde organisatie (GBO).

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Acceptatietest

Vzvvz_Req_Soort: Functional

Vzvvz_Req_Type: Product

3.3.6 Afschermden patiëntgegevens op doelgroep

Alias: GBX.OPV.e4535.1

Details
Eis: Patiëntgegevens dienen afgeschermd te kunnen worden voor bevestigingen door patiënten en/of door zorgverleners. Toelichting bij eis: Het aggregatieniveau van afscherming voor beide doelgroepen is opgenomen in eis Afschermden van patiëntgegevens.

Vzvvz_Moscow: Verplicht

Vzvvz_Req_Verificatie: Acceptatietest

Vzvvz_Req_Soort: Functional

Vzvvz_Req_Type: Product

3.3.7 Afschermden van patiëntgegevens

Alias: GBX.OPV.e4530

Details
Eis: Vrijgegeven patiëntgegevens moeten op verschillende aggregatieniveaus kunnen worden afgeschermd. De aggregatieniveaus zijn beschreven in de domeinspecificatie waartoe de gegevens behoren. Na het afschermden van patiëntgegevens moet zo nodig (conform Bijhouden van de verwijzindex) de verwijzindex worden bijgewerkt. Toelichting bij eis: Afschermden patiëntgegevens kunnen niet via AORTA worden opgevraagd. Deze eis is nodig zodat een zorgverlener op verzoek van een patiënt bepaalde gegevens kan afschermden.

Vzvvz_Moscow: Verplicht

Vzvvz_Req_Verificatie: Acceptatietest

Vzvvz_Req_Soort: Functional

Vzvvz_Req_Type: Product

3.3.8 Vrijgeven van patiëntgegevens

Alias: GBX.OPV.e4520

Details
Eis: Patiëntgegevens moeten na vastlegging, automatisch of op commando van de gebruiker, vrijgegeven kunnen worden. Vrijgeven moet kunnen op verschillende aggregatieniveaus, zoals beschreven in de domeinspecificatie waartoe de gegevens behoren. Na het vrijgeven van patiëntgegevens moet zo nodig (conform Bijhouden van de verwijzindex) de verwijzindex worden bijgewerkt. Toelichting bij eis: Slechts vrijgegeven patiëntgegevens kunnen via AORTA worden opgevraagd.

Het vrijgeven van patiëntgegevens kan zowel op commando als automatisch gebeuren. Als op commando vrijgeven onwerkbaar is, mag dit automatisch gebeuren. Het is aan te raden de gebruiker hierover te informeren.

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

3.3.9 Retourneren van opgevraagde patiëntgegevens

Alias: GBX.OPV.e4510.3

Details
Beginsituatie • Het systeem beschikt over de voor deze functie vereiste vertrouwensmiddelen, • Het systeem heeft de opgevraagde patiëntgegevens aangemeld bij de VWI. • Er is een opt-in geregistreerd in het systeem. Trigger Het systeem ontvangt een opvragenPatiëntgegevens-bericht Interacties Het systeem retourneert een opleverenPatiëntgegevens-bericht, zoals beschreven in het PvE voor de concrete systeemrol. Resultaat Het bericht is afgehandeld en de opgevraagde gegevens zijn, indien toegestaan, binnen de gestelde responsetijd geretourneerd. Uitzonderingen Uitzonderingen zijn beschreven in de Foutentabel. Opties Het geretourneerde bericht bevat alle, in het systeem aanwezige, vrijgegeven patiëntgegevens, die voldoen aan de criteria die zijn meegegeven in het opvragenPatiëntgegevens-bericht, en waarbij sprake is van een definitieve koppeling met het BSN. De criteria zijn beschreven in het PvE voor de concrete systeemrol. In het geval het bronsysteem, om welke reden dan ook, niet alle opgevraagde gegevens kan retourneren, dient er een foutmelding te worden verstuurd. Deze foutmelding dient door het bronsysteem te worden verstuurd, tezamen met de patiëntgegevens die wel opgeleverd kunnen worden. Als kopie aangemerkte gegevens mogen niet worden geretourneerd. Responsetijd Bij het beantwoorden van een opvragenPatiëntgegevens-bericht moet rekening gehouden worden met dat dit gebeurt vòòr het tijdstip dat in het bericht is meegegeven (). Indien het niet mogelijk is om de gevraagde gegevens tijdig op te leveren, dient zo snel mogelijk een melding naar de ZIM gestuurd te worden. Het systeem dient in staat te zijn kilobytes aan berichtinhoud per seconde te retourneren. Betrouwbaarheid - Toelichting -

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

3.4 Patiëntadministratie

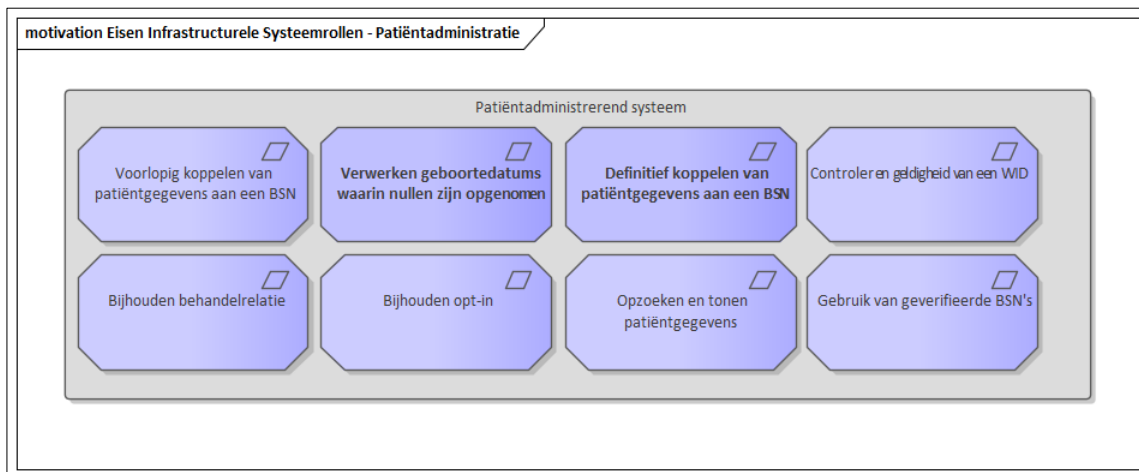


Figure 10 : Eisen Infrastructurele Systeemrollen - Patiëntadministratie

3.4.1 Gebruik van geverifieerde BSN's

Alias: GBX.IDA.e4060.1

Details
Eis: Het systeem moet aan <u>Opzoeken en tonen patiënteninformatie</u>, <u>Voorlopig koppelen van patiëntgegevens aan een BSN</u>, <u>Controleren geldigheid van een WID</u>, en <u>Bijhouden behandelrelatie</u> voldoen of (bij implementatie in een GBZ) een koppeling kunnen leggen met een derde systeem dat aan die eisen voldoet. Een systeem die gebruik maakt van een extern patiëntadministrerend systeem is verplicht om te controleren of een BSN daadwerkelijk aan alle AORTA eisen voldoet m.b.t. het BSN. Toelichting bij eis: Ieder GBZ moet over een patiëntadministratie beschikken, maar een XIS hoeft die niet per se in te bouwen. Het staat een GBZ vrij een eigen patiëntadministrerend systeem te kiezen dat voldoet aan de genoemde eisen. De systeemrol van Patiëntadministrerend systeem is daarmee niet verplicht voor XIS-typekwalificatie, maar een GBZ moet wel aantoonbaar over een dergelijk systeem beschikken en dit met het gebruikte XIS hebben gekoppeld om zodoende te kunnen garanderen dat er in de XIS-instantie met geverifieerde BSN's gewerkt wordt. Die gerefereerde eisen hoeven dan niet voor de XIS-typekwalificatie te worden ingebouwd. Hoe de controle wordt gedaan op de geldigheid van een BSN is aan de XIS-applicatie. Het is denkbaar dat de XIS-applicatie het patiëntadministrerende systeem actief benaderd, maar het is ook mogelijk dat de XIS-applicatie de statussen van een BSN toegezonden krijgt. Er mogen in géén geval BSN's in een bericht worden opgenomen die niet voldoen aan de AORTA eisen.

Vzvv_Moscow: Verplicht

Vzvvz_Req_Verificatie: Acceptatietest

Vzvvz_Req_Soort: Functional

Vzvvz_Req_Type: Product

3.4.2 Opzoeken en tonen patiëntgegevens

Alias: GBX.IDA.e4010.1

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

Vzvvz_Moscow: Verplicht

Vzvvz_Req_Verificatie: Acceptatietest

Vzvvz_Req_Soort: Functional

Vzvvz_Req_Type: Product

3.4.3 Bijhouden opt-in

Alias: GBX.IDA.e4100.1

Details
Eis: Het systeem moet in de lokale patiëntadministratie een zogenaamde opt-in-registratie bijhouden waarin voor iedere patiënt/cliënt wordt geregistreerd of de patiënt/cliënt wel of niet akkoord is met het beschikbaar stellen van zijn medische gegevens aan andere zorgaanbieders die bij de behandeling van de patiënt betrokken zijn. Deze opt-in-registratie moet de mogelijkheid bieden aan de gebruiker om per patiënt te registreren: 1. of de patiënt gevraagd is om akkoord te gaan met het beschikbaar stellen van zijn medische gegevens aan andere zorgaanbieders (opt-in); 2. of de patiënt naar aanleiding van deze vraag akkoord is gegaan; 3. de datum waarop de patiënt akkoord is gegaan; 4. de einddatum van de geldigheid van de opt-in; 5. een unieke identificatie van de set van voorwaarden waarmee de patiënt heeft ingestemd. Toelichting bij eis: De geldigheid van de opt-in kan onbeperkt zijn.

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

Eis vervalt na migratie naar Mitz

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

3.4.4 Bijhouden behandelrelatie

Alias: GBX.IDA.e4050

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

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

3.4.5 Controleren geldigheid van een WID

Alias: GBX.IDA.e4040

Details
Eis: Het systeem moet voor een geselecteerde patiënt/cliënt de gebruiker de mogelijkheid bieden: 1. het 'in omloop mogen zijn' van het WID te controleren door raadplegen van de SBV-Z op basis van aard en nummer van het WID;

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

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

3.4.6 Definitief koppelen van patiëntgegevens aan een BSN

Alias: GBX.IDA.e4030

Details
Eis: Het systeem moet voor een geselecteerde patiënt/cliënt de gebruiker: • de mogelijkheid bieden gewaarschuwd te worden indien nog niet is vastgesteld dat het BSN hoort bij de patiënt/cliënt; • de mogelijkheid bieden in de lokale patiëntenindex vast te leggen dat hij heeft vastgesteld dat het betreffende BSN hoort bij de patiënt/cliënt, onder vermelding van: 1. de manier van vaststellen: i. Controle van echtheid en geldigheidsdatum van WID en de gelijkenis van de in de WID genoemde identificerende gegevens, ii. Vergewissen, 1. Datum en tijd van vaststellen, 2. indien beschikbaar het UZI-nummer of anders een unieke identificatie van de gebruiker, en het UZI-nummer van mandaterende zorgverlener indien van toepassing. 3. zorgaanbieder-id van de gebruiker; 4. in geval van WID-controle: aard en nummer van het WID. Daarmee is het BSN definitief gekoppeld. Toelichting bij eis: Dit is belangrijk voor een zorgaanbieder die (geautomatiseerd) wil vaststellen of is voldaan aan de eventuele wettelijke verplichting om de identiteit vast te stellen aan de hand van een WID. Merk op dat de toelichting op Wet gebruik burgerservicenummer in de zorg artikel 26 een grote verantwoordelijkheid legt bij de zorgaanbieder voor de afweging wel/niet WID controleren. Daarom is geautomatiseerde ondersteuning belangrijk. Manier van vaststellen: • Vaststellen identiteit; Bij inschrijving van een patiënt waar nog geen behandelrelatie mee is, is het verplicht de identiteit van de patiënt vast te stellen aan de hand van een Wettelijk Identificatie Document (WID): een paspoort, Nederlands rijbewijs, Nederlandse ID-kaart of Nederlands vreemdelingendocument.

- WID-controle; Indien er wordt getwijfeld over de geldigheid van een identiteitsdocument, kan bij de Sectorale Berichten Voorziening in de Zorg (SBV-Z) een WID-controle worden uitgevoerd. Dit kan via een zorginformatiesysteem of via de website van SBV-Z.
- Opvragen/verifiëren BSN; Hierna moet het BSN geverifieerd worden en registreren worden dat deze verificatie heeft plaatsgevonden. Alle door VZVZ geaccepteerde zorginformatiesystemen ondersteunen deze mogelijkheid. Komt BSN van een patiënt via een andere zorgverlener? Dan hoeft het niet opnieuw geverifieerd te worden. Ook als het nummer direct uit de BRP komt, kunt BSN-verificatie achterwege worden gelaten.

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

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

3.4.7 Voorlopig koppelen van patiëntgegevens aan een BSN

Alias: GBX.IDA.e4020

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

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

3.4.8 Verwerken geboortedatums waarin nullen zijn opgenomen

Alias: GBX.IDA.e4015

Details
Eis: Een geboortedatum die teruggegeven wordt door de SBV-Z kan nullen bevatten (jjjjmm00, jjjj0000 of 00000000). Het XIS moet in staat zijn hiermee adequaat om te gaan zonder dat de applicatie vastloopt. Toelichting bij eis: Deze eis leidt tot de volgende aanvullende eisen:

1. Alle XISsen moeten naast de mogelijkheid om een BSN op te vragen of te verifiëren op basis van de Zoekpaden 1 en 2, ook de dienst opvragen van persoonsgegevens op basis van een ingevoerd BSN inbouwen.
2. Bij het overnemen van de gegevens uit de SBV-Z moet het voor de gebruiker mogelijk zijn om de geboortedatum aan te passen voor het opslaan, indien het systeem meldt dat de gegevens niet in de database kunnen worden opgeslagen.
3. Bij het aanpassen van de geboortedatum in een databasegeaccepteerde datum moet er een indicatie komen dat de geboortedatum handmatig is aangepast. (bijvoorbeeld andere kleur of een indicatie erbij). Nog mooier is de opgeleverde datum opslaan in een (apart) tekstveld.
4. De dienst 'opvragen persoonsgegevens op basis van BSN' moet kunnen worden uitgevoerd, ook als er al persoonsgegevens bekend zijn maar de verificatie mislukt is vanwege de geboortedatum. Hierbij kan er een dialoogvenster 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.

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

3.5 Primaire interacties - ontvangend systeem

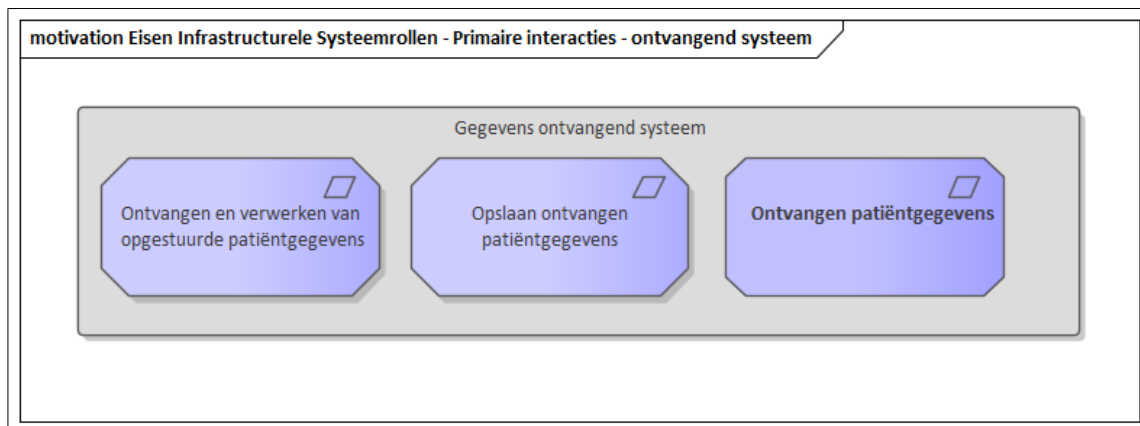


Figure 11 : Eisen Infrastructurele Systeemrollen - Primaire interacties - ontvangend systeem

3.5.1 Ontvangen patiëntgegevens

Alias: GBX.OPV.e4200

Details
Eis: Het ontvangende systeem dient ontvangen patiëntgegevens te kunnen verwerken en een antwoord te kunnen versturen zoals gespecificeerd in de implementatiehandleiding van de zorgtoepassing. Toelichting bij eis: De implementatiehandleiding van een zorgtoepassing is opgenomen in Art-Decor (https://decor.nictiz.nl/pub/vzvv/) voor HL7v3 en in github (https://vzvzn.github.io/VZVZ-FHIR-api/) voor

FHIR-toepassingen. Daarnaast is de toepassing beschreven in confluence (www.public.vzviz.nl). Hierin is voor elke systeemrol gespecificeerd welke interacties er ondersteund dienen te worden.

Vzviz_Moscow: Verplicht
 Vzviz_Req_Verificatie: Acceptatietest
 Vzviz_Req_Soort: Functional
 Vzviz_Req_Type: Product

3.5.2 Opslaan ontvangen patiëntgegevens

Alias: GBX.STU.e4520

Details
Eis: Wanneer patiëntgegevens, die conform Ontvangen en verwerken van opgestuurde patiëntgegevens 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. Om redundantie van informatie te voorkomen mogen als kopie aangemerkte patiëntgegevens niet bij de verwijzindex worden aangemeld en niet worden opgeleverd bij het verwerken van een opvraagverzoek. Wanneer een gebruiker, als kopie aangemerkte, gegevens raadpleegt is het raadzaam om aan te geven dat het een kopie betreft, en dat de gegevens mogelijk zijn verouderd.

Vzviz_Moscow: Verplicht
 Vzviz_Req_Verificatie: Acceptatietest
 Vzviz_Req_Soort: Functional
 Vzviz_Req_Type: Product

3.5.3 Ontvangen en verwerken van opgestuurde patiëntgegevens

Alias: GBX.STU.e4510

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

Berichten kunnen zijn geadresseerd aan een applicatie die niet de applicatie is van de zorgverlener die het bericht moet krijgen. Het GBX moet er in dat geval voor zorgen het bericht bij de juiste applicatie wordt afgeleverd.

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

3.6 Verwijsindex

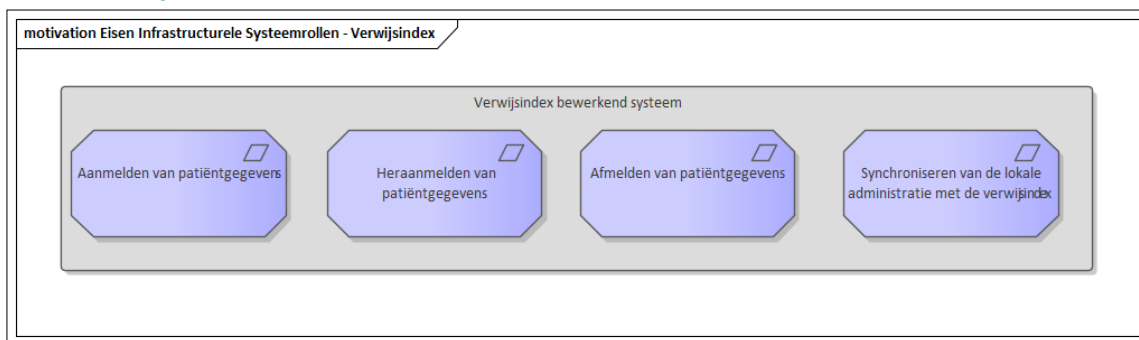


Figure 12 : Eisen Infrastructurele Systeemrollen - Verwijsindex

3.6.1 Synchroniseren van de lokale administratie met de verwijsindex

Alias: GBX.SYNC.e4010.1

Details

Beginsituatie

Er zijn:

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

Trigger

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

Interacties

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

Resultaat

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

Uitzonderingen

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

Responsetijd

-

Betrouwbaarheid

-

Toelichting

Het systeem moet indien er aanleiding toe is of in

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

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

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

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

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

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

3.6.2 Heraanmelden van patiëntgegevens

Alias: GBX.VWI.e4020.3

Details
Beginsituatie - De gebruiker is lokaal ingelogd op vertrouwensniveau laag of hoger. - Er zijn gegevens beschikbaar gekomen om her aan te melden. - Voor de onderhavige patiënt is opt-in geregistreerd. Trigger - De gebruiker initieert de functie via het systeem, of - Het systeem initieert de functie automatisch n.a.v. het vrijgeven nieuwe gegevens of het afschermen, bijwerken van bestaande patiëntgegevens. Interacties - Het systeem verzendt een publicerenGegevens bericht naar de ZIM conform IH AORTA. - Het systeem ontvangt een bevestiging conform IH AORTA. Resultaat - De verwijzing is opgenomen in de verwijzindex, er is een bevestigingsbericht ontvangen door het systeem en er wordt een melding getoond aan de gebruiker (trigger 1). - De verwijzing is opgenomen in de verwijzindex en er is een bevestigingsbericht ontvangen door het systeem (trigger 2). Uitzonderingen Uitzonderingen zijn beschreven in de Foutentabel. Opties Wanneer de gebruiker een GBZ-beheerder is dient er gebruik te worden gemaakt van fictieve BSN's en van fictieve gegevens. Responsetijd - Betrouwbaarheid Garantie geven dat gegevens in zendende en ontvangende systeem overeenstemmen Toelichting Elke keer als de gebruiker nieuwe gegevens heeft toegevoegd, moet dit worden heraangemeld bij de VWI. Dit is nodig om ervoor te zorgen dat de verwijzingen in de VWI actueel blijven. Als het LSP, bij een poging tot heraanmelden, aan een GBZ terugmeldt dat de categorie niet bestaat in de verwijzindex, dan probeert het GBZ automatisch alle vrijgegeven patiëntstukken in die categorie aan te melden. Het heraanmelden dient te gebeuren binnen 15 minuten, nadat er nieuwe patiëntstukken zijn vrijgegeven.

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

3.6.3 Afmelden van patiëntgegevens

Alias: GBX.VWI.e4030.2

Details
Beginsituatie De gebruiker is lokaal ingelogd op vertrouwensniveau laag of hoger. Trigger - De gebruiker initieert de functie via het systeem, of - Het systeem initieert de functie automatisch indien er geen vrijgegeven patiëntstukken meer zijn aangemeld onder het betreffende categorie-id, of

3. Het systeem initieert de functie automatisch wanneer voor een patiënt opt-out geregistreerd wordt, indien voor deze zelfde patiënt eerder opt-in geregistreerd was en op basis hiervan gegevens waren aangemeld. Interacties 1. Het systeem verzendt een afmeldenGegevens bericht naar de ZIM conform IH AORTA. 2. Het systeem ontvangt een bevestiging conform IH AORTA. Resultaat • De verwijzing is afgemeld in de verwijzindex, er is een bevestigingsbericht ontvangen door het systeem en er wordt een melding getoond aan de gebruiker (trigger 1). • De verwijzing is afgemeld in de verwijzindex en er is een bevestigingsbericht ontvangen door het systeem (trigger 2 en 3). Uitzonderingen Uitzonderingen zijn beschreven in de Foutentabel. Opties Wanneer de gebruiker een GBZ-beheerder is dient er gebruik te worden gemaakt van fictieve BSN's en van fictieve gegevens. Responsetijd - Betrouwbaarheid Garantie geven dat gegevens in zendende en ontvangende systeem overeenstemmen Toelichting Afmelden van gegevens is nodig om ervoor te zorgen dat de ZIM het systeem niet langer zal vragen naar deze gegevens. Het systeem moet aan de gebruiker een faciliteit bieden om bij het systeem aan te geven dat het een afmelding moet doen voor alle patiënten waarvoor geen opt-in is verkregen.

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

3.6.4 Aanmelden van patiëntgegevens

Alias: GBX.VWI.e4010.3

Details
Beginsituatie 1. De gebruiker is lokaal ingelogd op vertrouwensniveau laag of hoger. 2. Voor de onderhavige patiënt is opt-in geregistreerd. Trigger 1. De gebruiker initieert de functie via het systeem, of 2. Het systeem initieert de functie automatisch n.a.v. het vrijgeven van patiëntgegevens. Interacties 1. Het systeem verzendt een publicerenGegevens bericht naar de ZIM conform IH AORTA. 2. Het systeem ontvangt een bevestiging conform IH AORTA. Resultaat • De verwijzing is opgenomen in de verwijzindex, er is een bevestigingsbericht ontvangen door het systeem en er wordt een melding getoond aan de gebruiker (trigger 1). • De verwijzing is opgenomen in de verwijzindex en er is een bevestigingsbericht ontvangen door het systeem (trigger 2). Uitzonderingen Uitzonderingen zijn beschreven in de Foutentabel. Opties

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

Responsetijd

-

Betrouwbaarheid

Garantie geven dat gegevens in zendende en ontvangende systeem overeenstemmen

Toelichting

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

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

3.7 Mandaatregistratie

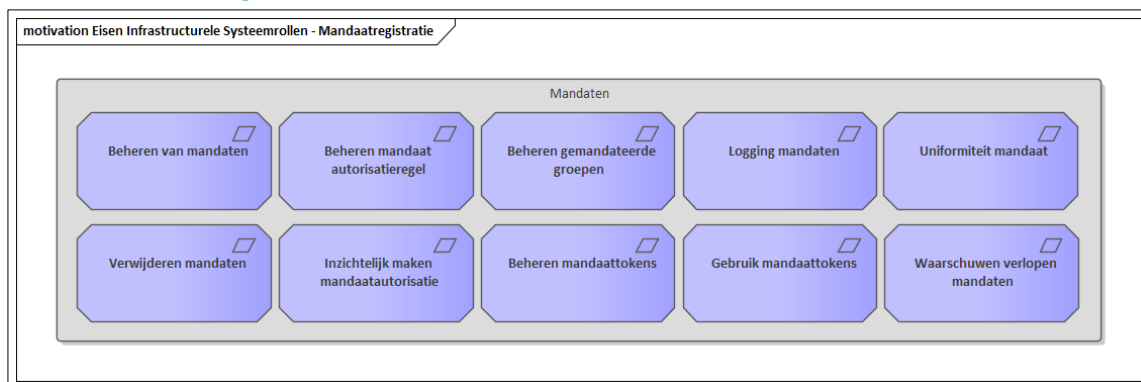


Figure 13 : Eisen Infrastructurele Systeemrollen – Mandaatregistratie

De systeemrol Mandaatregistratie is optioneel voor vaste huisartssystemen. Indien een vaste huisartssysteem gebruikt maakt van mandaten, dan is deze systeemrol verplicht. Deze systeemrol is optioneel ook nodig in combinatie met Mitz.

3.7.1 Uniformiteit mandaat

Alias: GBX.AUT.e4515

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

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Acceptatietest

Vz vz_Req_Soort: Functional

Vz vz_Req_Type: Product

3.7.2 Waarschuwen verlopen mandaten

Alias: GBX.AUT.e4522.1

Details
Eis: Een mandaterende en de in de autorisatieregeling 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.

Vz vz_Moscow: Verplicht

Vz vz_Req_Verificatie: Acceptatietest

Vz vz_Req_Soort: Functional

Vz vz_Req_Type: Product

3.7.3 Verwijderen mandaten

Alias: GBX.AUT.e4521.1

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

Vz vz_Moscow: Conditioneel

Vz vz_Req_Verificatie: Acceptatietest

Vzvvz_Req_Soort: Functional

Vzvvz_Req_Type: Product

3.7.4 Logging mandaten

Alias: GBX.AUT.e4516

Details
Eis: Met betrekking tot het mandaattoken dienen drie zaken gelogd te worden: 1. Mandaattoken; bij het aanmaken van een mandaattoken dienen de gegevens gelogd te worden zoals opgenomen in GBX.AUT.e4511. 2. Autorisatieregels; bij het aanmaken van een autorisatieregels dienen de gegevens gelogd te worden zoals opgenomen in GBX.AUT.e4514. 3. Groepen; bij elke wijziging aan een groep, dienen de gegevens gelogd te worden zoals opgenomen in GBX.AUT.e4515. In het geval een autorisatieregels geen gebruik maakt van groepen, dan hoeft deze uiteraard ook niet gelogd te worden. In opdracht van VZVZ, van een toezichthouder of van een andere geautoriseerde belanghebbende moeten bovenstaande loggegevens te allen tijden inzichtelijk gemaakt kunnen worden. Toelichting bij eis: Ten behoeve van een audit trail moet precies kunnen worden nagegaan of een mandaattoken terecht gebruikt is. Het is mogelijk om de te loggen gegevens genoemd onder de punten a t/m c in één gecombineerde log op te nemen. Hierbij moet dan wel na elke aanpassing van een van de drie genoemde zaken opnieuw gelogd worden.

Vzvvz_Moscow: Verplicht

Vzvvz_Req_Verificatie: Acceptatietest

Vzvvz_Req_Soort: Functional

Vzvvz_Req_Type: Product

3.7.5 Gebruik mandaattokens

Alias: GBX.AUT.e4520

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

Vzvvz_Moscow: Verplicht

Vzvvz_Req_Verificatie: Acceptatietest

Vzvvz_Req_Soort: Functional

Vzvvz_Req_Type: Product

3.7.6 Beheren mandaattokens

Alias: GBX.AUT.e4519

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

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Monitoring

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

3.7.7 Inzichtelijk maken mandaatautorisatie

Alias: GBX.AUT.e4517

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

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

3.7.8 Beheren gemandateerde groepen

Alias: GBX.AUT.e4514

Details
Eis: In een autorisatieregeling kunnen één of meerdere groepen van gemandateerden worden opgenomen. Een groep bestaat in ieder geval uit de volgende elementen: 1. Unieke identifier; dit kan een nummer of een groepsnaam zijn. 2. Lijst met gemandateerden; een lijst kan bestaan uit bijvoorbeeld UZI-nummer(s) of rollen/functies. Alleen op vertrouwensniveau midden is het mogelijk om de lijst met gemandateerden dynamisch uit te breiden. De identifier hoeft niet aangepast te worden bij uitbreiding van de lijst met gemandateerden.

Toelichting bij eis:

Door het gebruik van groepen in een autorisatieregel is het mogelijk om dynamisch rolcode's of UZI-nummers toe te voegen aan de lijst met gemandateerden.

Mocht er gebruik worden gemaakt van een andere waarde dan UZI-nummer of rolcode, dan dient vanuit de logging ontegenzeggelijk te worden aangetoond welke UZI of rolcode er aan de waarde gekoppeld is.

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

3.7.9 Beheren mandaat autorisatieregel

Alias: GBX.AUT.e4513.1

Details

Eis:

Een mandaat kan alleen afgegeven worden op basis van een autorisatieregel. Een autorisatieregel bepaalt of een bepaalde zorgverlener gebruik mag maken van een specifiek mandaat.

De precieze invulling van een autorisatieregel is niet gespecificeerd. Dit is ter invulling van de zorginstelling. Een autorisatieregel moet in ieder geval wel de volgende attributen bevatten:

1. Lijst met werkcontext(en); De werkcontext(en) bepaalt de context(en) waarbinnen een mandaat geldig is. Dit kan bijvoorbeeld gekoppeld zijn aan een afdeling of een werkproces.
2. Lijst met gemandateerden; Dit kunnen UZI-nummer(s), lokale zorgverleneridentificaties of (lokaal gedefinieerde) rollen zijn. Er kan ook een groep(en) ([GBX.AUT.e4514](#)) worden opgenomen waar rolcodes of UZI-nummers aan gekoppeld zijn. Door het gebruik van groep(en) is het mogelijk om dynamisch rolcodes of UZI-nummers toe te voegen aan de lijst van gemandateerden.
3. Uniek identificatiekenmerk; Een autorisatieregel moet uniek gekenmerkt worden. Een uniek gekenmerkte autorisatieregel behorende bij een afgegeven mandaat mag niet veranderlijk zijn.

Toelichting bij eis:

Lokaal moet duidelijk en uniek geregistreerd zijn hoe er invulling is gegeven aan een autorisatieregel. Op verzoek (van bijvoorbeeld een toezichthouder) moet kunnen worden aangetoond dat een gemandateerde ten tijde van het versturen van een bericht onder mandaat, inderdaad gerechtigd was om gebruik te maken van het mandaattoken ([GBX.AUT.e4517](#)).

Om een flexibel mandaat in te richten is het aan te raden om gebruik te maken van dynamische groepen in de autorisatieregel. Een groep wordt aangeduid door middel van een groepsnaam. De UZI-nummers die direct of indirect (door middel van de rolcode) gekoppeld worden aan een groepsnaam moeten op een veilige manier worden beheerd (eis [GBX.AUT.e4514](#)).

Indien een lokale gebruikersidentificatie wordt gebruikt, dan kan het LSP alleen bevestigd worden via de conditionele query. Dit zal dan in een zorgtoepassing specifiek worden vereist.

Een autorisatieregel mag niet aangepast worden. De attributen die zijn opgenomen in verwijzingen (zoals bijvoorbeeld bij de onder b. genoemde groepen) mogen wel worden aangepast.

Autorisatieregels en de invulling met betrekking tot de werkcontext en de lijst met gemandateerden dienen in een beveiligde container te worden opgeslagen. Deze mogen alleen door een geautoriseerde medewerker worden ingezien en aangepast.

Vzvv_Moscow: Verplicht

Vzvvz_Req_Verificatie: Acceptatietest

Vzvvz_Req_Soort: Functional

Vzvvz_Req_Type: Product

3.7.10 Beheren van mandaten

Alias: GBX.AUT.e4511

Details
Eis: Een zorgverlener moet, wanneer hij lokaal is ingelogd op vertrouwensniveau midden, mandaten kunnen vastleggen, inzien en intrekken. Gebruikers mogen uitsluitend mandaten vastleggen waarvoor zij mandaterende zijn. Voor een mandaat worden tenminste de volgende gegevens vastgelegd: 1. de ingangsdatum van het mandaat; 2. de einddatum van het mandaat; 3. het UZI-nummer van de mandaterende zorgverlener; 4. de rolcode van de mandaterende zorgverlener; 5. het abonneenummer (URA) van de zorgaanbieder waarbinnen het mandaat geldig moet zijn; 6. de autorisatieregels (zie eis GBX.AUT.e4513) op basis waarvan een mandaat verkregen kan worden; 7. een unieke identifier. Toelichting bij eis: Met betrekking tot deze eis worden de volgende subeisen gedefinieerd: • Het wijzigen van een mandaat is niet toegestaan. Het systeem dient in dat geval een nieuw mandaat aan te maken. Hierbij dient dus een nieuwe unieke identifier te worden opgenomen. • De einddatum van het mandaat mag door een mandaatverlener leeg gelaten worden. In dat geval moet het systeem de vervaldatum van het handtekeningcertificaat opnemen als einddatum. • De mandaatverlener mag geen einddatum invullen die na de geldigheidstermijn van zijn handtekeningcertificaat ligt. Het systeem dient dan een duidelijk foutmelding te genereren voor de gebruiker. • De ingangsdatum van het mandaat mag in de toekomst liggen. • Er kan alleen een mandaat worden afgesloten voor de eigen organisatie. • Er dient een verwijzing naar een autorisatieregels te zijn opgenomen. Dit kan bijvoorbeeld door middel van een URI, die verwijst naar de daadwerkelijke inhoud van een autorisatieregels. • Een autorisatieregels is niet uniek gekoppeld aan een mandaat. Het is dus mogelijk om naar dezelfde autorisatieregels te verwijzen in meerdere mandaten.

Vzvvz_Moscow: Verplicht

Vzvvz_Req_Verificatie: Acceptatietest

Vzvvz_Req_Soort: Functional

Vzvvz_Req_Type: Product

3.8 Mandaattoken beherend systeem

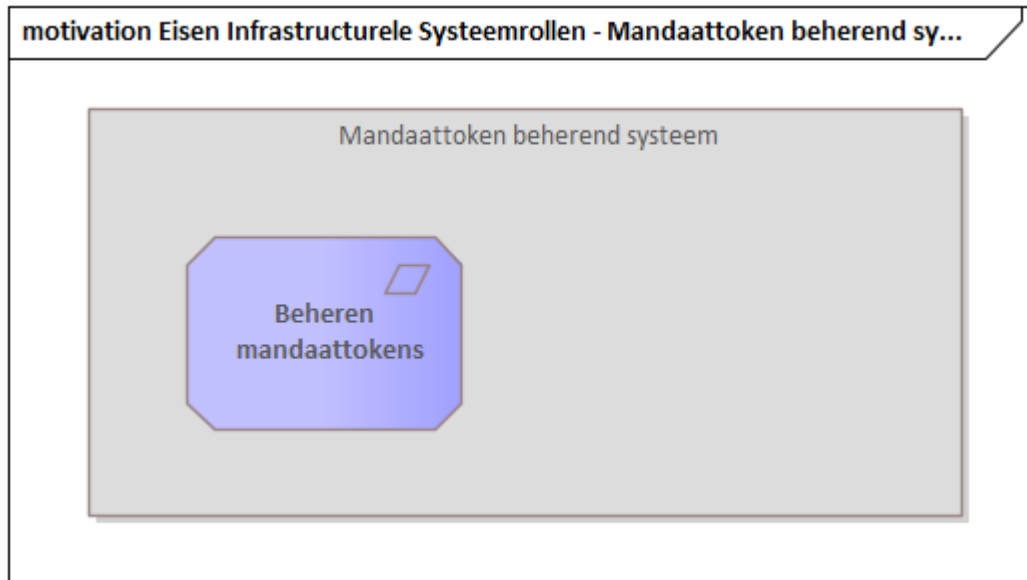


Figure 14 : Eisen Infrastructurele Systeemrollen - Mandaattoken beherend systeem

De systeemrol Mandaattoken beherend systeem is optioneel voor vaste huisartssystemen. Indien een vaste huisartssysteem gebruikt maakt van mandaten, dan is deze systeemrol verplicht. Deze systeemrol is optioneel ook nodig in combinatie met Mitz.

3.8.1 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.

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

3.9 Inschrijftoken beherend systeem

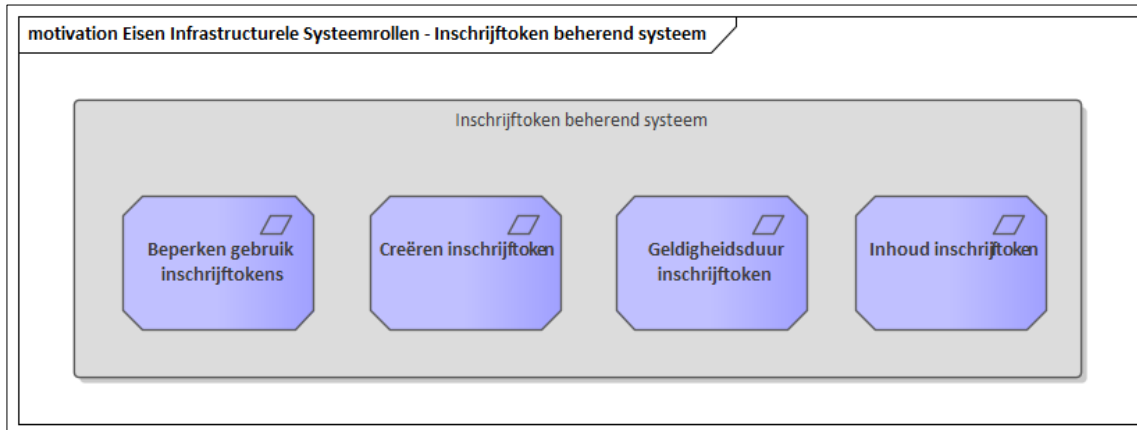


Figure 15 : Eisen Infrastructurele Systeemrollen - Inschrijftoken beherend systeem

Het inschrijftoken beherend systeem is optioneel voor vaste huisartssystemen. Het is mogelijk dat deze gebruikt wordt in combinatie met Mitz en in de toekomst voor het gebruik van de conditionele berichten. Vooralsnog wordt die laatste nog niet ondersteund door vaste huisartssystemen. Mocht deze behoefte er wel zijn, dan dient dit PvE uitgebreid te worden met aanvullende eisen m.b.t. het gebruik van conditionele berichten.

3.9.1 Inhoud inschrijftoken

Alias: GBX.OPV.e4060.2

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

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

3.9.2 Geldigheidsduur inschrijftoken

Alias: GBX.OPV.e4100.1

Details
Eis: Een inschrijftoken heeft een maximale geldigheidsduur van 1,5 jaar. Toelichting:

Een inschrijftoken kent een beperkte geldigheidsduur. Het is echter mogelijk om dezelfde informatie in het inschrijftoken opnieuw te ondertekenen (zie eis GBX.OPV.e4050).

De geldigheid van het UZI-certificaat waarmee het inschrijftoken is ondertekend heeft geen invloed op de geldigheid van het inschrijftoken.

Een inschrijftoken heeft een maximale geldigheidsduur van 1,5 jaar.

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

3.9.3 Creëren inschrijftoken

Alias: GBX.OPV.e4050

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

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

3.9.4 Beperken gebruik inschrijftokens

Alias: GBX.OPV.e4120

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

Vzvv_Moscow: Verplicht
Vzvv_Req_Verificatie: Monitoring
Vzvv_Req_Soort: Functional

Vzvvz_Req_Type: Product

3.10 Token beherend systeem

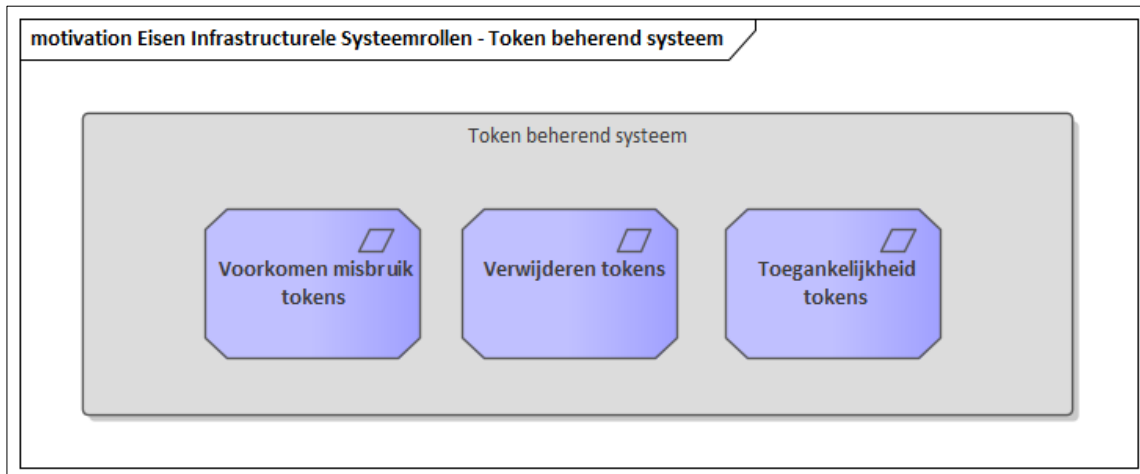


Figure 16 : Eisen Infrastructurele Systeemrollen - Token beherend systeem

De systeemrol Token beherend systeem is optioneel voor vaste huisartssystemen. Indien een vaste huisartssysteem gebruikt maakt van mandaattokens, inschrijftokens of consenttokens, dan is deze systeemrol verplicht.

3.10.1 Verwijderen tokens

Alias: GBX.OPV.e4110

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

Vzvvz_Moscow: Verplicht

Vzvvz_Req_Verificatie: Acceptatietest

Vzvvz_Req_Soort: Functional

Vzvvz_Req_Type: Product

3.10.2 Toegankelijkheid tokens

Alias: GBX.OPV.e4160.1

Details
Eis:

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

Toelichting:

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

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

Vz vz_Moscow: Verplicht

Vz vz_Req_Verificatie: Audit

Vz vz_Req_Soort: Functional

Vz vz_Req_Type: Product

3.10.3 Voorkomen misbruik tokens

Alias: GBX.OPV.e4170

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

Vz vz_Moscow: Verplicht

Vz vz_Req_Verificatie: Audit

Vz vz_Req_Soort: Functional

Vz vz_Req_Type: Product

4 HWg Eisen aan de beheerorganisatie

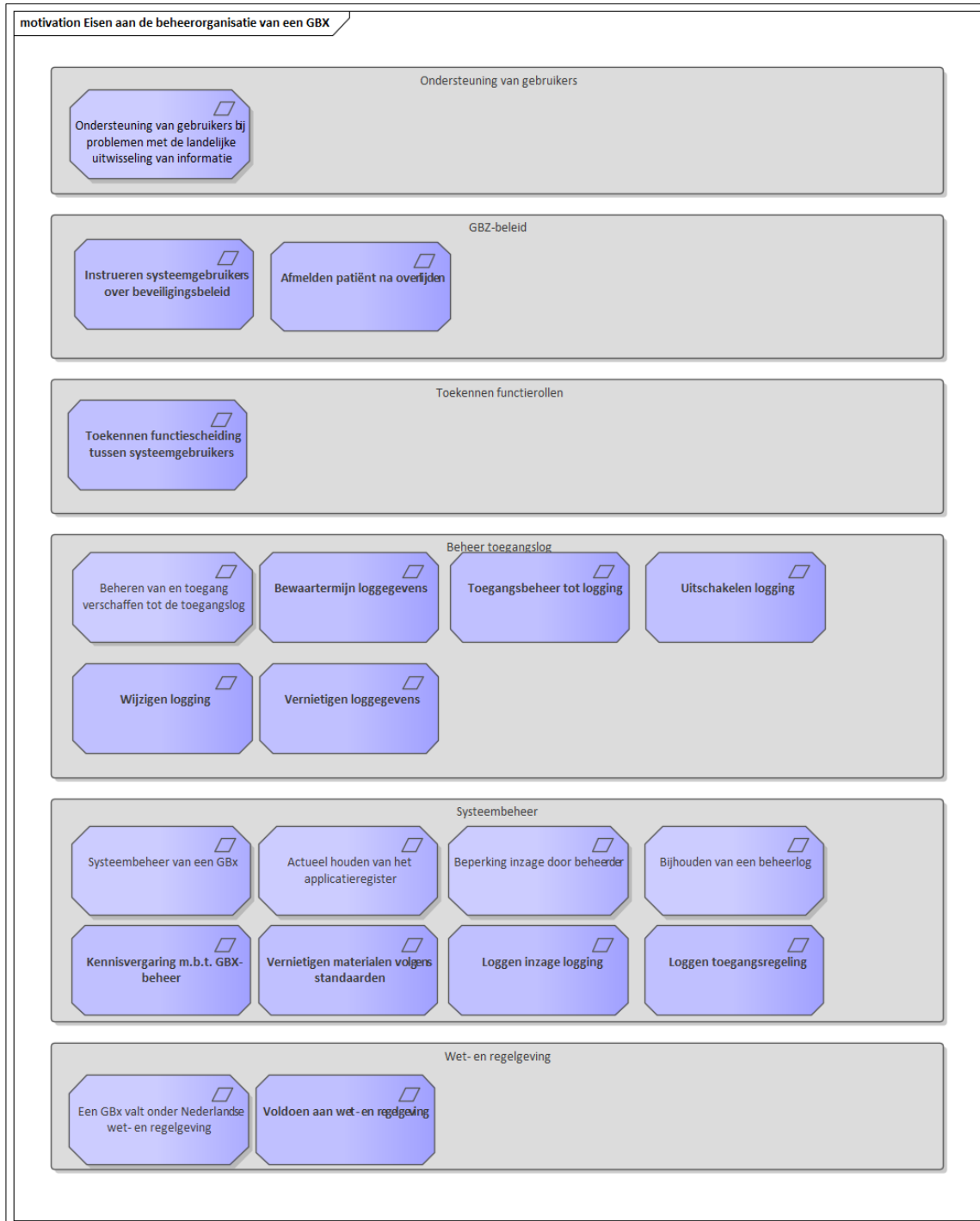


Figure 17 : Eisen aan de beheerorganisatie van een GBX

4.1 Afmelden patiënt na overlijden

Alias: GBX.FBH.e4090

Details
Eis: Patiënten dienen na overlijden binnen een maand te worden afgemeld in het LSP, tenzij expliciet anders vereist wordt. Toelichting bij eis: Afmelding in het LSP beslaat het (mogelijk) afmelden in de verwijzindex en het abonnementenregister. Het streven is om het abonnementenregister zuiver te houden ten behoeve van de kwaliteit van AORTA en de garanties met betrekking tot de prestaties. Indien abonnementen niet meer gebruikt worden, dan dienen deze afgemeld te worden in het abonnementregister. Het is de verantwoordelijkheid van de zorgaanbieder om zorg te dragen voor de informatiebeschikbaarheid van zijn patiënten. Echter, om te voorkomen dat gegevens van overleden patiënten onnodig in de verwijzindex blijven staan, is het wenselijk om de verwijzing te verwijderen. Het is mogelijk dat bepaalde informatie na overlijden nog voor een beperkte duur beschikbaar moet blijven. Het is aan de zorgaanbieder om deze inschatting te maken. Vooralsnog is er een tijdsbestek van een maand voorgesteld, waarbinnen de afmeldingen gedaan dienen te worden.

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

4.2 Wijzigen logging

Alias: AGE.LOG.e4060

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

Vzvv_Moscow: n/a
Vzvv_Req_Verificatie: n/a
Vzvv_Req_Soort: n/a
Vzvv_Req_Type: n/a

4.3 Vernietigen loggegevens

Alias: AGE.LOG.e4050

Details
Eis: Loggegevens moeten bij het verstrijken van <log_bewaartermijn> automatisch worden verwijderd uit de actieve log en uit het archief. De logregels moeten op een zodanige wijze vernietigd worden dat de data niet te reconstrueren is. Dit betekent ook dat eventueel reservekopieën verwijderd/vernietigd/volledig overschreven zijn. Toestemming Conform NEN 7513:2018 paragraaf 8.5.

Elke afsprakenstelsel/architectuur dient expliciet invulling te geven aan de waarde voor `<log_bewaartermijn>`. Indien deze waarde ontbreekt dan geldt de standaard waarde van 5 jaar.

Vz vz_Moscow: n/a
 Vz vz_Req_Verificatie: n/a
 Vz vz_Req_Soort: n/a
 Vz vz_Req_Type: n/a

4.4 Uitschakelen logging

Alias: AGE.LOG.e4030

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

Vz vz_Moscow: n/a
 Vz vz_Req_Verificatie: n/a
 Vz vz_Req_Soort: n/a
 Vz vz_Req_Type: n/a

4.5 Toegangsbeheer tot logging

Alias: AGE.LOG.e4040

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

Vz vz_Moscow: n/a
 Vz vz_Req_Verificatie: n/a
 Vz vz_Req_Soort: n/a
 Vz vz_Req_Type: n/a

4.6 Loggen toegangsregeling

Alias: AGE.LOG.e4070

Details
Eis: Elke wijziging in de toegangsregeling dient te worden gelogd. Hierbij moet onweerlegbaar kunnen worden vastgesteld welke persoon met welke rol welke specifieke aanpassing heeft doorgevoerd.

Toelichting
Conform NEN 7513:2018 Paragraaf 6.3

Vzvv_Moscow: n/a
Vzvv_Req_Verificatie: n/a
Vzvv_Req_Soort: n/a
Vzvv_Req_Type: n/a

4.7 Loggen inzage logging

Alias: AGE.LOG.e4020

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

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

4.8 Bewaartermijn loggegevens

Alias: AGE.LOG.e4010

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

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

4.9 Voldoen aan wet- en regelgeving

Alias: GBX.ALG.e4010

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

Vzvv_Moscow: Verplicht (Must)

Vzvv_Req_Verificatie: Eigenverklaring

Vzvv_Req_Soort: Non-Functional

Vzvv_Req_Type: Product

4.10 Vernietigen materialen volgens standaarden

Alias: GBX.SBH.e4070

Details
Eis: Om te voorkomen dat privacygevoelige of beveiliging gerelateerde gegevens achterblijven en in ongewenste handen vallen dienen niet (meer) gebruikte websites, apps, informatie of code te worden vernietigd volgens de standaard DoD 5220.22-M (E). Te vervangen fysieke opslagmedia dienen gecontroleerd vernietigd te worden volgens DIN 32757. Toelichting bij eis: Er is een proces nodig dat controleert of gegevens nog noodzakelijk zijn en te verwijderen gegevens voorgoed vernietigt.

Vzvv_Moscow: Verplicht (Must)

Vzvv_Req_Verificatie: Eigenverklaring

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Business

4.11 Een GBx valt onder Nederlandse wet- en regelgeving

Alias: GBX.CON.e4050.1

Details
Eis: De technische infrastructuur van het GBX dient zich in de Europese Unie te bevinden. De voertaal met de zorgaanbieder en de organisatie die het GBx beheert en exploiteert is Nederlands. Met betrekking tot de contracten tussen de zorgaanbieder en bovengenoemde moet de Nederlandse wet- en regelgeving van toepassing zijn. De zorgaanbieder en de organisatie's die het GBX beheert en exploiteert dient in Nederland gevestigd te zijn.

In de contracten tussen de zorgaanbieder en bovengenoemde moet de Nederlandse wet- en regelgeving van toepassing zijn.

Toelichting bij eis:

Dit is nodig om er voor te zorgen dat de infrastructuur en dienstverlening volledig onder Nederlandse wet- en regelgeving valt. De exploitant dient waarborgen actief te hebben die voorkomen dat gegevens oneigenlijk gebruikt kunnen worden en te voldoen aan de privacy wetgeving.

Vzvv_Moscow: Verplicht (Must)

Vzvv_Req_Verificatie: Aansluittoets

Vzvv_Req_Soort: Non-Functional

Vzvv_Req_Type: Product

4.12 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.

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Aansluittoets

Vzvv_Req_Soort: Non-Functional

Vzvv_Req_Type: Product

4.13 Bijhouden van een beheerlog

Alias: GBX.SBH.e4050

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

Vzvv_Moscow: Verplicht (Must)

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Non-Functional

Vzvvz_Req_Type: Product

4.14 Beperking inzage door beheerder

Alias: GBX.SBH.e4040.3

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

Vzvvz_Moscow: Verplicht (Must)

Vzvvz_Req_Verificatie: Acceptatietest

Vzvvz_Req_Soort: Non-Functional

Vzvvz_Req_Type: Product

4.15 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.

Vzvvz_Moscow: Verplicht (Must)

Vzvvz_Req_Verificatie: Documentverificatie

Vzvvz_Req_Soort: Non-Functional

Vzvvz_Req_Type: Product

4.16 Systeembeheer van een GBx

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

Details
Eis: De rol van systeembeheerder moet door de organisatie expliciet benoemd en belegd zijn.

De systeembeheerder en diens vervanger(s) dienen met actuele telefoonnummers bekend te zijn bij de LSP-beheerder en de centrale AORTA servicedesk. Tenminste één beheerder dient altijd bereikbaar te zijn en in staat om de nodige beheertaken uit te voeren.

De systeembeheerder dient verzoeken van het LSP met betrekking tot het configureren van het GBx en het activeren/deactiveren van op het LSP aangesloten systeem in te willigen.

Toelichting bij eis:

Deze eis zorgt ervoor dat een systeembeheerder altijd kan worden gewaarschuwd als er problemen zijn met een GBx, die ingrijpen van de systeembeheerder vergen.

Vzvv_Moscow: Verplicht (Must)

Vzvv_Req_Verificatie: Documentverificatie

Vzvv_Req_Soort: Non-Functional

Vzvv_Req_Type: Product

4.17 Beheren van en toegang verschaffen tot de toegangslog

Alias: GBX.SBH.e4010

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

Vzvv_Moscow: Verplicht (Must)

Vzvv_Req_Verificatie: Audit

Vzvv_Req_Soort: Non-Functional

Vzvv_Req_Type: Product

4.18 Toekennen functiescheiding tussen systeemgebruikers

Alias: GBX.FBH.e4025

Details
Eis: Het autorisatiebeleid binnen een organisatie moet rekening houden met het onderscheid tussen systeemgebruikers die gebruik mogen maken van LSP-functionaliteiten en systeemgebruikers die geen toegang tot deze functionaliteiten mogen hebben. De verantwoordelijke voor het toekennen van

autorisaties binnen de organisatie dient in het systeem de juiste autorisaties toe te kennen aan de systeemgebruikers.

Toelichting:

GBZ-en zouden een additionele toegangscontrole moeten implementeren voor het initiëren van interacties met het LSP. Een medewerker met toegang tot het systeem van een GBZ zou niet automatisch ook toegang moeten hebben tot de functies om het LSP te bevragen.

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Non-Functional

Vzvv_Req_Type: Product

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 NEN 7510, 7.2.2.

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Monitoring

Vzvv_Req_Soort: Non-Functional

Vzvv_Req_Type: Product

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.

Vzvv_Moscow: Verplicht (Must)

Vzvv_Req_Verificatie: Aansluittoets

Vzvv_Req_Soort: Non-Functional

Vzvv_Req_Type: Product

5 Eisen voor specifieke zorgtoepassingssysteemrollen

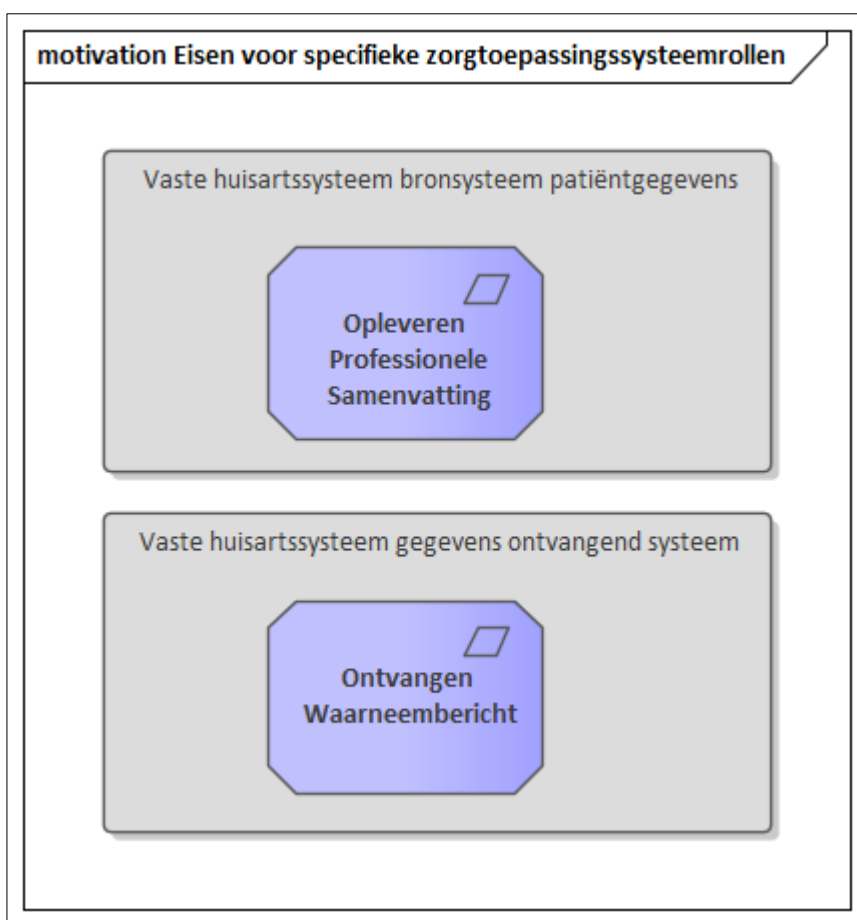


Figure 18 : Eisen voor specifieke zorgtoepassingssysteemrollen

5.1 Opleveren Professionele Samenvatting

Alias:

Details

Eis:

Het systeem moet het opvragen professionele samenvattingsbericht(QUPC_IN990001NL) kunnen ontvangen. Als antwoord op dit bericht dient het systeem een opleveren professionele samenvattingsbericht(QUPC_IN990002NL) terug te sturen.

Toelichting bij eis:

De specificatie van het opvragen en opleveren professionele samenvattings-bericht zijn opgenomen in de art-decorpublicatie van de zorgtoepassing.

Vzvz_Moscow: Verplicht

Vzvz_Req_Verificatie: Acceptatietest

Vzvz_Req_Soort: Functional

Vz vz_Req_Type: Product

5.2 Ontvangen Waarneembericht

Alias:

Details
Eis: Het systeem moet het waarneembericht (REPC_IN990003NL) kunnen ontvangen. Toelichting bij eis: De specificatie van het Waarneembericht is opgenomen in de art-decorpublicatie van de zorgtoepassing.

Vz vz_Moscow: Verplicht

Vz vz_Req_Verificatie: Acceptatietest

Vz vz_Req_Soort: Functional

Vz vz_Req_Type: Product