< PvE GBx Organisatie

Datum: 7 oktober 2020
Publicatie: V8.2.0.0

Inhoudsopgave

1 Inleiding

1.1 Doel en scope

Dit document beschrijft de generieke eisen die worden gesteld aan informatiesystemen om gekoppeld te kunnen worden aan het landelijk schakelpunt (LSP). Een informatiesysteem dat aan deze eisen voldoet wordt aan Goed Beheerd systeem (GBX) genoemd. Specifiek gaat het hier om eisen aan het goed beheerde zorgsysteem, klantloket en patiëntportaal, respectievelijk afgekort tot GBZ, GBK, GBP en GBO. Dit document bevat eisen die worden gesteld aan de beheer- en aan de gebruiksorganisatie en het bevat kwaliteitseisen ("non-functionals") die worden gesteld aan de informatiesystemen. Voor het GBP is het document [PvE GBP]leidend.

Instellingen die niet onder de kwaliteitswet zorginstellingen vallen, en dus geen UZI abonnee kunnen worden, worden als een GBZ behandeld. In het geval de betreffende instellingen afwijken van de eisen voor een GBZ, dan wordt dit specifiek aangegeven.

Voor AORTA is informatiebeveiliging van het grootste belang. Dit programma van eisen bevat een aantal specifieke eisen die gerelateerd zijn aan informatiebeveiliging binnen AORTA. Voor algemeen te treffen maatregelen op het gebied van informatiebeveiliging wordt ervan uitgegaan dat aangesloten partijen voldoen aan geaccepteerde standaarden en normen zoals [ISO27001] of [NEN7510]. De GBx dient te waarborgen dat gegevens niet oneigenlijk ingezien en/of gebruikt kunnen worden.

1.2 Doelgroep voor dit document

De doelgroep van dit document bestaat uit:

1. Productmanagers, architecten, ontwerpers en testers van XIS-leveranciers, regio-organisaties en VZVZ;
2. (Vertegenwoordigers van) zorgverleners.

1.3 Documenthistorie

Versie	Datum	Omschrijving
6.10.0.0	12-okt-2011	Initiële opzet document op basis van oorspronkelijke PvE's GBZ/GBK/GBP
6.10.0.0	12-okt-2011	Eisen aan 'Selecteren burger' verplaatst naar PvE Klantenloket
6.10.0.0	12-okt-2011	Connectiviteitseisen toegevoegd Kwalificatiecriteria verwijderd
6.10.0.0	12-okt-2011	RFC 24449: Eisen betreffende selecteren patiënt aangepast
6.10.0.0	12-okt-2011	RFC 24873: Obsolete ciphersuites uitgefaseerd en nieuwe verplicht gesteld
6.10.0.0	12-okt-2011	RFC 35173: Eisen aan 'Selecteren patiënt' verplaatst naar PvE Infrastructurele systeemrollen. Eis met betrekking tot presentatie fictieve gegevens verplaatst naar PvE Infrastructurele systeemrollen.
6.10.0.0	12-okt-2011	RFC 35208: Aanpassing binnen het onderdeel Selecteren burger

6.10.0.0	12-okt-2011	RFC 42686: Implementatie gastgebruik aangepast
6.10.0.0	12-okt-2011	RFC 42949: Herzien datamodel applicatieregister
6.10.0.0	12-okt-2011	RFC 46035: Eisen t.b.v het gebruik van whitelists toegevoegd.
6.11.0.0	5-dec-2012	RFC 46058: Toelichting op GBX.CON .e4080.1 uitgebreid. RFC 50926: Aansluiten zonder UZI-servercertificaat. RFC 51771: TLS 1.2 ondersteuning van de ZIM en de nieuw aan te sluiten GBx en optioneel SNI ondersteuning RFC 24873: SNI Server Name Indication
6.11.0.0	5-dec-2012	RFC 52441: GBZ moet controleren op verlopen en ingetrokken passen. Weggevallen eis opnieuw opgenomen als: GBX.IDA.e4085
6.11.1.0	21-feb-2013	Review
6.12.0.0	12-aug-2013	RfC 59337: GBX.LOG.e4010 : Niet logbare zaken weggehaald en andere toegevoegd. RfC 59336: GBX.LOG.e4010 bestaat al in de PvE Infrastructurele Systeemrollen. De eis in dit document is veranderd naar GBX.LOG.e4015. RfC 53482: GBX in NL? Aanpassen aan EU wetgeving Wijziging aan eis GBX.CON.e4050 RfC 60342: Betrouwbaarheidseisen GBX.BET.e4010 en GBX.BET.e4020 toegevoegd. RfC 60343: GBZ latency toegevoegd, eis GBX.PST.e4015. RfC 60470: GBX.CON.e4090.1, GBX.CON.e4110, GBX.CON.e4080; alleen G21 certificaten ondersteunen RfC 60477: verwijdering Sessieauthenticatie; GBX.CON.e4070, GBX.CON.e4080
6.12.0.0	24-okt-2013	RfC 60921: zim-max-sessie-aantal in GBX.PST.e4020 niet gedefinieerd. Aangezien dit er toch maximaal 1 is, is de eis verwijderd.
6.12.2.0	27-nov-2013	RfC 60470: Naast GBX.CON.e4090.1, GBX.CON.e4110 (zie wijziging 12-aug-2013), zijn ook GBX.BVL.e4050.1 en GBX.IDA.e4080.1 aangepast op het niet meer hoeven te ondersteunen van oude UZI-passen.
6.12.5.0	1-juni-2016	RfC 62084: GBP.SBH.e4050 aangepast conform NEN 7513
6.12.5.0	1-juni-2016	RfC 60478: Sessieauthenticatieoptie verwijderd GBX.FBH.e4060.1

6.12.5.0	1-juni-2016	Eis GBX.IDA.e4090 punt d) is specifiek voor GBP. Zelfde eis komt ook voor in AORTA_GBP_PvE_Organisatie. Daarom in dit document de aanduiding GBP en punt d) verwijderd._
6.12.5.0	1-juni-2016	Eis GBP.LOG.e4020 verwijderd omdat de scope alleen GBP betreft en deze dus al in document AORTA_GBP_PvE_Organisatie is opgenomen.
6.12.5.0	1-juni-2016	RfC 59615. Eis GBX.FBH.e4030 verruimt zodat de (gast)ge-bruikerregistratie op basis van sterke authenticatie (en niet alleen de UZI-pas) wordt toegestaan.
6.12.5.0	1-juni-2016	RfC 64571. Eis GBX.IDA.e4090 punt c) versoepeld zodat de onbruik time-out van een applicatie instelbaar moet zijn met een maximum van 60 minuten.
6.12.5.0	1-juni-2016	Eisen in lijn gebracht met ontwikkelingen op GBP-gebied, veiligheidsrisico's op GZN-gebied en veiligheidsbevindingen bij GBZ'en die als SaaS worden ontsloten.
6.12.5.0	1-juni-2016	RfC 52817: Expliciet controleren PIN en UZI-pas combinatie (eis GBX.IDA.e4085)
8.0.1.0	15-mei-2017	RfC 75284: BSN in query (eis GBx.LOG.e4015)
8.0.1.0	15-mei-2017	Naamgeving: Zorg Service Provider (ZSP) is Goedbeheerd Zorg Netwerk (GZN) geworden.
8.0.1.0	15-mei-2017	RfC 64820: In de publicatieversies voor 6.12.15.0 wordt er gesuggereerd dat het LSP de mogelijkheid voor Server Name Indication (SNI) ondersteunt. Dit is echter niet het geval. SNI wordt niet ondersteund door de COTS-producten waar het LSP van afhankelijk is. In de toelichting van eis GBX.CON.e4060.1 is het mogelijke gebruik van SNI verwijderd. In een erratum op 6.12.2.0 van 8 september 2014 is dit probleem al eerder geaddresseerd.
8.0.1.0	15-mei-2017	RfC 63910: Nieuw TKID Wijzigingsbericht leidt tot wijziging GBX.FBH.e4060 en vervallen van GBX.FBX.e4070.
8.0.1.0	15-mei-2017	RfC 72121: TLS 1.2 verplicht voor alle GBx'en. Eisen: GBX.CON.e4060.1, GBX.CON.e4080.3 en GBX.CON.e4090.2
8.0.1.0	15-mei-2017	RfC 71719: PKIO/UZI certificaten gaan over naar de Public G3/Private G1 generatie
8.0.1.0	15-mei-2017	RfC 76233: Aanpassen eisen m.b.t. configuratieparameters (Eis GBX.FBH.e4050.1 en GBX.FBH.e4060.1 opgenomen in GBX.FBH.e4050.2)

8.0.1.0	15-mei-2017	RfC 76305: Verplichting NEN751x
8.0.1.0	15-mei-2017	RfC 76210: Aanpassen Cipher Suites.
8.0.2.0	31-jan-2018	INI-8417: Aanpassen toelichting GBX.CON.e4030
8.0.3.0	1-juli-2018	INI-8563: Aanpassing eis GBX.CON.e4050.1. Aansluiting op LSP van buiten Nederland.
8.0.3.0	1-juli-2018	INI-8420: Eis GBX.IDA.e4070 verwijderd. Dit wordt al geborgd door NEN7510. INI-8421: Herschrijven eis GBX.IDA.e4085.1 INI-7149: In eis GBX.LOG.e4015 is expliciet opgenomen dat alle gegevenssoorten en contextcodes binnen een berichtuitwisseling gelogd moeten worden. INI-7329: GBX.SBH.e4060 verplicht volgen van een VZVZ GBx-workshop bij toetreden op productie INI-6829: Eis GBX.IDA.e4080.1 aangepast. Bij het inloggen dient er ook een sign actie te worden gedaan op de certificaten van de UZI-pas. INI-8694 ALG.e4010: verwijzing naar wetgeving geactualliseerd.
8.1.0.0	1-aug-2019	INI-8967: Verduidelijken GBX.IDA.e4080.2
8.1.0.0	1-aug-2019	INI-8826: Verwijzing naar AORTA DAP opgenomen in eis GBX.BET.e4010 en GBX.BET.e4020. INI-8694 ALG.e4010: toegevoegd dat wanneer GBZ-beheer door de zorgaanbieder wordt uitbesteed, deze partij aan de NEN-7510 normering moet voldoen. INI-8877: Toegevoegd eis GBX.FBH.e4070 INI-9038: Toegevoegd eis GBX.FBH.e4025; Toekennen functiescheiding systeemgebruikers INI-9039: Toegevoegd eis GBX.FBH.e4015; Informeren beveiligingsbeleid INI-9040: Toegevoegd eis GBX.FBH.e4017; Zorgdragen voor UZI-passen INI-9041: Toegevoegd eis GBX.FBH.e4018; geen overmatige bevragingen
8.2.0.0	12-aug-2020	INI-8598: Gewijzigde eis GBX.CON.e4090.3. Sterkste encryptie moet eerst worden geprobeerd.

1.4 Uitleg presentatie van eisen

De eisen die in dit document zijn opgenomen, worden uniform gepresenteerd waardoor ze makkelijker leesbaar zijn geworden. De gebruikte tabel per eis bevat onder andere

aparte aanduidingen voor de scope, het karakter en de verificatiewijze. Hieronder wordt kort aangegeven wat de termen in deze velden aanduiden.

Scope:

- GBZ: geldig voor een goed beheerd zorgsysteem.
- GBK: geldig voor een goed beheerd klantenloket.
- GBP: geldig voor een goed beheerd patiëntenportaal.
- GBO: geldig voor een goed beheerde organisatie (organisatie die geen UZI abonnee is).
- Geldig voor een {GBZ, GBK, GBP, GBO} of een subset hiervan.

Karakter:

- Verplicht: de eis is verplicht voor de in de scope genoemde systemen
- Optioneel: de eis is niet verplicht, maar als de functionaliteit wordt geboden, dan moet die voldoen aan hetgeen in de eis is beschreven.
- Conditioneel: de eis is verplicht onder de conditie die is gesteld in het veld "Condities".

Verificatiewijze (geeft een indicatie van de wijze waarop de eis wordt getoetst):

- Test: het successcenario en de uitzonderingen worden getest.
- Demo: slechts het successcenario wordt aangetoond.
- Review: het ontwerp wordt beoordeeld.
- Monitoring: achteraf wordt vastgesteld of aan de eis is voldaan.

Bovendien worden sommige stukken tekst voorafgegaan door een 'tag', die aangeeft dat dat die tekst specifiek van toepassing is onder de conditie aangeduid door de tag. Bijvoorbeeld: {GBZ} geeft aan dat een stuk van de eis of toelichting specifiek van toepassing is binnen een GBZ, maar dus niet binnen een GBK,GBP of GBO. Schuingedrukte tekst tussen vishaken duidt een parameter aan, zoals <*gbx-verwerkingssnelheid-sturen*>. De waarde hiervan wordt ingevuld in systeemroldocumenten.

1.5 Gebruikte generieke termen

De eisen in dit document zijn voortgekomen uit de programma's van eisen aan een goed beheerd zorgsysteem, klantenloketsysteem en patiëntenportaal, respectievelijk afgekort tot GBZ, GBK,GBP en GBO. Vanwege de oorsprong van de hier gestelde eisen zijn er enkele termen ingevoerd die generiek invulling geven aan afgeleide specifieke termen. In de onderstaande tabel wordt duidelijk gemaakt welke generieke termen corresponderen met oorspronkelijke specifieke termen.

Generieke term	GBZ-term	GBK-term	GBP-term	GBO-term
GBX	GBZ	GBK	GBP	GBO
Gebruiker	Zorgverlener/medewerker	Klantloketmedewerker	Burger/Patiënt	Niet UZI geregistreerde
Authenticatiemiddel	UZI-pas	PKIO-pas	WID-Document	Nvt

Beheerder	GBZ-beheerder	GBK-beheerder	GBP-beheerder	GBO-beheerder
Toezichthouder	CBP/IGZ/VZVZ	IGZ/CBP	IGZ/CBP	IGZ/CBP
Organisatie	Zorgaanbieder	Klantloketorganisatie		Niet UZI organisatie
Systeem	XIS	Klantenloket	Patiëntenportaal	XIS
Opdrachtnemer	XIS-leverancier	GBK-opdrachtnemer	GBP-opdrachtnemer	XIS-leverancier
Opdrachtgever	VZVZ	GBK-opdrachtgever	GBP-opdrachtgever	GBO-opdrachtgever
Vertrouwensmiddel	UZI-servercertificaat	PKIO-servercertificaat	PKIO-servercertificaat	PKIO-servercertificaat

2 Eisen aan de beheerorganisatie van een GBX

2.1 Ondersteuning van gebruikers

Aan de servicedesk van een GBX worden de volgende eisen gesteld ten behoeve van de ondersteuning van de gebruikers.

GBX.FBH.e4010	
De GBX-servicedesk dient gebruikers te ondersteunen bij GBX-, GZN- en LSP-gerelateerde problemen. De GBX-servicedesk dient: a) Gebruikers een inschatting te geven van de verwachte oplostermijn; b) Gebruikers regelmatig te informeren over de voortgang van de oplossing; c) Voor noodgevallen telefonisch bereikbaar te zijn voor gebruikers, de GZN en het LSP; d) Incidenten en problemen te registreren en beheren.	
Functie	Ondersteuning van gebruikers bij problemen met de landelijke uitwisseling van informatie.
Scope	GBZ/GBK/GBP/GBO
Karakter	Verplicht
Condities	-
Toelichting	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.
Verificatiewijze	Review, Monitoring
Voorheen	GBZ·EE·GBO·e01 GBZ·EE·GBO·e02 GBZ·EE·GBO·e03 GBZ·EE·GBO·e05

2.2 GBZ-beleid

De organisatie dient een duidelijk beleid te hebben met betrekking tot verschillende aspecten binnen een GBZ. Daarnaast moeten systeemgebruikers geinstrueerd worden over het gevoerde beleid. Dit hoofdstuk beschrijft de eisen die gelden met betrekking tot het beleid binnen een GBZ en het instrueren van systeemgebruikers.

GBX.FBH.e4015
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).	
Functie	Instrueren systeemgebruikers over beveiligingsbeleid
Scope	GBZ/GBK/GBP/GBO
Karakter	Verplicht
Condities	-
Toelichting	Een GBZ moet concreet beleid maken om het bewustzijn van het beveilingsbeleid 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.
Verificatiewijze	Monitoring
Voorheen	

GBX.FBH.e4017	
Een organisatie moet zorgdragen dat er voldoende UZI-passen binnen een organisatie actief zijn. Het aantal benodigde UZI-passen is afhankelijk van de organisatiestructuur en de toepassing waarbinnen een UZI-pas wordt gebruikt.	
Functie	Verantwoordelijk UZI-pasbeleid
Scope	GBZ/ GBO
Karakter	Verplicht
Condities	-
Toelichting	Zorgaanbieders waar veel zorgverleners werkzaam zijn mogen niet uit kostenoverwegingen besparen op UZI-passen en daarom bijvoorbeeld de mandatering in de gehele organisatie bij een of enkele specialisten leggen. Er dient goed afgewogen te worden wie verantwoordelijk is voor bepaalde interacties met het LSP. Verantwoordelijkheid wordt onder andere bepaald door de rol van de zorgverlener en het hebben van een (afgeleide) behandelrelatie met een patiënt.
Verificatiewijze	Monitoring
Voorheen	

GBX.FBH.e4018
Er mogen geen overmatige bevragingen van patiëntgegevens worden gedaan. In het geval van een bevraging door het systeem dient er een duidelijke trigger voor de bevraging te zijn. Indien een systeemgebruiker zelf een bevraging initiëert is het de verantwoordelijkheid van de systeemgebruiker om te bepalen of het gaat om een overmatige bevraging.

Functie	Voorkomen overmatige bevraging van patiëntgegevens
Scope	GBZ/GBO
Karakter	Verplicht
Condities	-
Toelichting	Een overmatige bevraging van patiëntgegevens is een LSP-bevraging zonder een duidelijke noodzaak voor de betreffende patiënt. Het betreft hier bijvoorbeeld een bevraging zonder een duidelijke trigger, door een systeem, met als doel de lokale database aan te vullen met de meest recente patiëntinformatie (synchronisatie). Een duidelijke trigger kan bijvoorbeeld een afspraak zijn met de patiënt of een signaal als gevolg van een afgesloten abonnement.
Verificatiewijze	Monitoring
Voorheen	

2.3 Toekennen functierollen

Binnen een systeem is het mogelijk om diverse autorisatierollen te onderscheiden. Dit hoofdstuk beschrijft de eisen die betrekking hebben op het toekennen van autorisatierollen aan de systeemgebruikers.

GBX.FBH.e4020	
Er moet functiescheiding toegepast worden tussen systeemgebruikers die gerechtigd zijn om inschrijftokens op te stellen en gebruikers die het LSP kunnen bevragen.	
Functie	Toekennen functiescheiding tussen systeemgebruikers m.b.t. inschrijftokens
Scope	GBZ/GBO
Karakter	Conditioneel/Optioneel
Condities	Deze eis geldt indien er gebruik wordt gemaakt van inschrijftokens. Deze eis is niet verplicht, maar voor met name grote organisaties wel aan te raden.
Toelichting	Deze eis moet de kans verlagen dat gegevens van een oneigenlijke patient worden bevraagd, doordat medewerkers niet zowel patiënten mogen inschrijven als betrokken zijn bij de medische processen. Met name bij zorgaanbieders van een grotere omvang zal dit goed toe te passen zijn en aansluiten bij de bestaande werkprocessen. De aanpassingen zijn vooral beleidsmatig en procedureel van aard. Het toepassen van deze maatregel is mogelijk al bestaande praktijk of kan anders wellicht met beperkte inspanning worden gerealiseerd. Voor kleine zorgaanbieders is dit mogelijk niet altijd haalbaar.
Verificatiewijze	Monitoring
Voorheen	

GBX.FBH.e4025	
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.	
Functie	Toekennen functiescheiding tussen systeemgebruikers
Scope	GBZ/GBO
Karakter	Verplicht
Condities	-
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.
Verificatiewijze	Monitoring
Voorheen	

2.4 Beheer van de toegangslog

Een GBX moet een toegangslog bijhouden en beheren.

GBX.SBH.e4010	
De organisatie moet een toegangslogbeheerder benoemen. De toegangslogbeheerder moet verzoeken van de toezichthouder om de lokale toegangslog te raadplegen inwilligen.	
Functie	Beheren van en toegang verschaffen tot de toegangslog.
Scope	GBZ/GBK/GBP/GBO
Karakter	Verplicht
Condities	-
Toelichting	Deze eis is nodig omdat de toezichthouder op AORTA voor het uitvoeren van zijn bevoegdheden informatie nodig kan hebben over de gebeurtenissen waarbij het GBX met het LSP informatie heeft uitgewisseld. {GBZ} Deze toegangslogbeheerder kan door alle zorgverleners worden gemandateerd om de toeganslog 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.
Verificatiewijze	Review
Voorheen	GBZ·EE·LOG·e01

	GBK·EE·LOG·e01 GBZ·EE·LOG·e02 GBK·EE·LOG·e02

2.5 Systeembeheer

Een GBX moet aan de onderstaande eisen aan het systeembeheer voldoen.

GBX.SBH.e4020	
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.	
Functie	Systeembeheer van een GBX.
Scope	GBZ/GBK/GBP/GBO
Karakter	Verplicht
Condities	-
Toelichting	Deze eis zorgt ervoor dat een systeembeheerder altijd kan worden gewaarschuwd als er problemen zijn met een GBX, die ingrijpen van de systeembeheerder vergen.
Verificatiewijze	Review
Voorheen	GBZ·EE·OND·e01 GBZ·EE·OND·e02 GBZ·EE·OND·e03 GBZ·EE·GBO·e04 GBK·EE·OND·e01 GBK·EE·OND·e02 GBK·EE·OND·e03

GBX.SBH.e4030	
De systeembeheerder moet de status van de door hem beheerde GBX-applicaties in het applicatieregister actueel houden.	
Functie	Actueel houden van het applicatieregister.
Scope	GBZ/GBO/GBK/GBP
Karakter	Verplicht
Condities	-
Toelichting	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.

Verificatiewijze	Review
Voorheen	GBZ·EE·ACT·e02

GBX.SBH.e4040.1	
De systeembeheerder mag de inhoud van berichten slechts inzien indien dit noodzakelijk is voor het oplossen van problemen en uitsluitend op verzoek van een zorgverlener/medewerker.	
Functie	Inzage beheerder.
Scope	GBZ/GBK/GBP/GBO
Karakter	Verplicht
Condities	-
Toelichting	Vanuit zijn ondersteunende rol kan het voor 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.
Verificatiewijze	Review
Voorheen	GBZ·EE·LOG·e03 GBK·EE·LOG·e03

GBX.SBH.e4050	
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.	
Functie	Bijhouden van een beheerlog.
Scope	GBZ/GBK/GBP/GBO
Karakter	Verplicht
Condities	-
Toelichting	De beheerlog ondersteunt de controle op de juiste werking van systemen en de controle op het volgen van procedures.
Verificatiewijze	Review
Voorheen	GBK·EE·BVL·e25 GBP·EE·BVL·e17

GBX.SBH.e4060
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.	
Functie	Met voldoende kennis het GBX beheren
Scope	GBZ/GBO
Karakter	Verplicht
Condities	-
Toelichting	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.
Verificatiewijze	Review, Monitoring
Voorheen	

3 Kwaliteitseisen aan de aangesloten systemen

3.1 Algemeen

GBX.ALG.e4010	
Een GBX dient aantoonbaar te voldoen aan de NEN751x normen.	
Functie	Voldoen aan regel- en wetgeving
Scope	GBZ/GBO
Karakter	Verplicht
Condities	-
Toelichting	In het Besluit elektronische gegevensverwerking door zorgaanbieders [Besluit EGDZ] wordt • in artikel 3 lid 2 gesteld dat een zorgaanbieder overeenkomstig het bepaalde in NEN 7510 en NEN 7512, zorg draagt voor een veilig en zorgvuldig gebruik van het zorginformatiesysteem en een veilig en zorgvuldig gebruik van het elektronisch uitwisselingssysteem (i.c. het LSP) waarop hij is aangesloten; • in artikel 3 lid 3 gesteld de netwerkverbindingen moeten voldoen aan het bepaalde in NEN 7512; • in artikel 5 lid 1 gesteld dat de logging van zorgaanbieders moet voldoen aan het bepaalde in NEN 7513. XIS-leveranciers leveren diensten en/of producten aan zorgaanbieders. In het algemeen geldt dat de XIS-leverancier geen toegang heeft tot de persoonsgegevens, die de zorgaanbieder verwerkt met behulp van de diensten en/of producten. Een XIS-leverancier ontwikkelt, test en/of verkoopt de software. Een XIS-leveranciers ondersteunt het gebruik van de software, maar beheert en/of verwerkt geen persoonsgegevens. De zorgaanbieder is zelf verantwoordelijk voor dat beheer en de verwerking. De software is doorgaans lokaal geïnstalleerd of staat in een private cloud bij de zorgaanbieder. Wanneer (een deel van) het GBZ-beheer door de zorgaanbieder is uitbesteed aan een derde partij, heeft deze toegang tot, en verwerkt daardoor, de persoonsgegevens die in een dienst en/of product (bijvoorbeeld: een softwareapplicatie) worden verwerkt door een zorgaanbieder. De software wordt doorgaans aangeboden als SaaS-dienst (Software as a Service) en/of staat in de (publieke) cloud. Voorbeelden zijn: Software Service Providers, SAAS-aanbieders en cloud-aanbieders.
Verificatiewijze	Dit kan ingevuld kan worden door: 1) NEN7510 certificaat van de verantwoordelijke zorgaanbieder en/of 2) In geval van GBZ-beheer door een externe partij: NEN7510 certificaat of ISO27001 certificaat aangevuld met

	aanvullende audit verklaring NEN7510 van die externe partij.
Voorheen	-

3.2 Connectiviteit

GBX.CON.e4010	
Een GBX dient via een DCN[1] van een gekwalificeerde GZN[2] te communiceren met het LSP.	
Functie	Communicatie met het LSP via een GZN.
Scope	GBZ/GBO
Karakter	Verplicht
Condities	-
Toelichting	Organisaties kunnen bij VZVZ Servicecentrum verifiëren of een netwerkaanbieder over een GZN-kwalificatie beschikt.
Verificatiewijze	Review
Voorheen	GBZ·IE·CON·e01

GBX.CON.e4020

Een GBX moet bereikbaar zijn voor de ZIM:

a) {GBZ}{GBO} via het IP-adres dat is toegekend aan het GBZ en dat is verkregen door DNS-vertaling van de hostnaam van dat GBZ;
b) {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;
c) {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:

a) de hostnaam een maximale time-to-live (TTL) heeft voor verversing van de cache;
b) het IP-adres van de ZIM zich binnen een vooraf overeengekomen range bevindt die altijd gerouteerd moet worden naar de GZN;
c) 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:

a) het IP-adres dat door het LSP is uitgegeven voor het GBX als geheel,
b) de IP-adressen die zijn gereserveerd voor de ZIM,
c) de IP-adressen uit het landelijke IP-nummerplan van het LSP.

[1] Datacommunicatienetwerk, zie verder [Arch_AORTA]

[2] Goedbeheerd Zorg Netwerk, zie verder [PvE GZN]

Functie	Gebruik van IP en DNS.
Scope	GBZ/GBK/GBP/GBO
Karakter	Verplicht
Condities	-
Toelichting	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 GBZ/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.
Verificatiewijze	Demo
Voorheen	GBZ·IE·CON·e02 GBZ·IE·CON·e05 GBK·IE·CON·e01 GBK·IE·CON·e04 GBP·IE·CON·e02 GBP·IE·CON·e03

GBX.CON.e4030	
Een GBX dient NTP te gebruiken voor tijdsynchronisatie met de ZIM. De tijdklok van een GBX mag niet meer dan een halve seconde afwijken van de tijdklok van de ZIM.	
Functie	Tijdsynchronisatie GBX en ZIM.
Scope	GBZ/GBK/GBP/GBO
Karakter	Verplicht
Condities	-
Toelichting	Deze eis is nodig om te voorkomen dat de tijdklok van het GBZ/GBO gaat afwijken van de tijdklok van de ZIM. Voor eenzelfde interactie tussen een GBX en de ZIM moeten beide systemen immers dezelfde tijdstempels loggen. Dit is belangrijk wanneer de toezichthouder of patiënt een geval van vermeend onrechtmatige uitwisseling van patiëntgegevens wil onderzoeken en daartoe zowel de lokale toegangslog van het GBX als de centrale toegangslog van het LSP wil raadplegen.
Verificatiewijze	Demo
Voorheen	GBZ·IE·CON·e04

	GBZ·IE·BTW·e01 GBZ·EE·CON·e03 GBK·IE·CON·e03 GBK·IE·BTW·e01 GBK·EE·CON·e03 GBP·IE·CON·e05 GBP·IE·BTW·e01

GBX.CON.e4050.2	
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.	
Functie	Een GBX valt onder Nederlandse wet- en regelgeving
Scope	GBZ/GBK/GBP/GBO
Karakter	Verplicht
Condities	-
Toelichting	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.
Verificatiewijze	Review
Voorheen	GBK·IE·BVL·e07 GBP·IE·INF·e09

3.3 Beveiliging

De aangesloten informatiesystemen moeten voldoen aan de volgende eisen betreffende gebruikte vertrouwensmiddelen en daarmee samenhangende software.

GBX.BVL.e4050.1

Een GBX moet zodanig zijn ingericht dat:

a) passen met SHA-256-certificaten (uitgegeven onder de op het moment geldende certificaatboom) gelezen en gebruikt kunnen worden;
b) paslezers gekoppeld zijn aan werkplekken van gebruikers;
c) de PIN-code die ten behoeve van een authenticatiemiddel wordt ingetoetst op een werkplek, exclusief wordt aangeboden aan de gekoppelde paslezer,
d) geborgd wordt dat:
    - {GBZ} 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;
- {GBZ} de auteur inderdaad is gemandateerd door de in het bericht vermelde (eind)verantwoordelijke, of dezelfde persoon is;
- {GBZ} 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.

e) {GBZ}alle gegevens in berichten die ten behoeve van een gebruiker worden ontvangen exclusief aan die gebruiker worden gepresenteerd;
f) {GBK} alle gegevens in HL7-berichten die ten behoeve van een patiëntopdracht worden ontvangen exclusief gekoppeld worden aan de betreffende patiëntopdracht.

Functie	Borgen betrouwbare koppeling tussen pas en applicatie.
Scope	GBZ/GBK
Karakter	Verplicht
Condities	-
Toelichting	-
Verificatiewijze	Demo
Voorheen	GBZ·IE·BVL·e03 GBK·IE·BVL·e04

GBX.BVL.e4060

Voor een GBX moet zijn gedefinieerd:

a) welke landelijke toepassingen en systeemrollen worden ondersteund en gebruikt,
b) hoe de grenzen van het GBX lopen door de ICT-voorzieningen van de organisatie
c) hoe en wanneer patiëntgegevens die grenzen kunnen passeren;
d) hoe wordt gewaarborgd dat patiëntgegevens in de dossiers en postbussen niet kunnen lekken naar onbetrouwbare bestemmingen,
e) hoe wordt gewaarborgd dat patiëntgegevens uit onbetrouwbare bronnen niet kunnen terechtkomen in de dossiers en postbussen of de ZIM,
f) hoe wordt gewaarborgd dat anderen dan bevoegde gebruikers geen fysieke toegang tot (delen van) het GBX kunnen krijgen.

Functie	Beveiliging van patiëntgegevens in het GBX.
Scope	GBZ/GBK/GBP/GBO
Karakter	Verplicht
Condities	-
Toelichting	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.

Verificatiewijze	Review, Monitoring
Voorheen	GBZ·IE·BVL·e04 GBK·IE·BVL·e05 GBP·IE·BVL·e04

GBX.BVL.e4070	
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 regie van de ZIM.	
Functie	Borgen van plicht tot uitwisselen van patiëntgegevens.
Scope	GBZ/GBO
Karakter	{GBZ}{GBO}Verplicht
Condities	-
Toelichting	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.
Verificatiewijze	Review
Voorheen	GBZ·IE·BVL·e05 GBK·IE·BVL·e06

GBX.BVL.e4080	
Een GBX dient een {GBZ}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.	
Functie	Een GBX beschikt over een geldig UZI/PKIO-servercertificaat.
Scope	GBZ/GBK/GBP/GBO
Karakter	Verplicht
Condities	-
Toelichting	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.
Verificatiewijze	Review
Voorheen	GBP·IE·BVL·e01

3.4 Beschikbaarheid

Om beschikbaarheid te garanderen moeten de systemen voldoen aan de volgende eisen.

GBX.BES.e4010
Met uitzondering van gepland onderhoud dient een GBX-applicatie te allen tijde

beschikbaar te zijn voor het afhandelen van berichten. {GBZ}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.	
Functie	Borgen van de beschikbaarheid van een GBX.
Scope	GBZ/GBK/GBO
Karakter	Verplicht/{GBZ}Conditioneel
Condities	Bronsysteem patiëntgegevens, Gegevens ontvangend systeem
Toelichting	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 computers 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.
Verificatiewijze	Review, monitoring
Voorheen	GBZ·IE·BES·e01 GBK·IE·BES·e01 GBP·IE·BES·e01

GBX.BES.e4020	
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.	
Functie	Minimaliseren van de impact van gepland onderhoud.
Scope	GBZ/GBK
Karakter	Verplicht/{GBZ}Conditioneel
Condities	Bronsysteem patiëntgegevens, Gegevens ontvangend systeem
Toelichting	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. Omdat het GBK signaleringen kan ontvangen, is de eis verplicht voor GBK.
Verificatiewijze	Review, monitoring
Voorheen	GBZ·EE·BES·e01

	GBK·EE·BES·e01

3.5 Betrouwbaarheid

Om een bepaalde mate van betrouwbaarheid te garanderen moeten de systemen voldoen aan de volgende eisen.

GBX.BET.e4010	
Kleine storingen in een GBx mogen niet meer dan gemiddeld *<aantal_kleine_storingen>* keer per maand voorkomen (MTBF) en dienen dan binnen *<oplostijd_kleine_storingen>* (MTTR) te zijn opgelost.	
Functie	Borgen van de betrouwbaarheid van een GBX.
Scope	GBZ/GBO
Karakter	Verplicht
Toelichting	Deze eis is nodig om te voorkomen dat een GBZ al te vaak uitvalt en na een eenvoudig te verhelpen storing meteen langere tijd onbeschikbaar blijft. In de praktijk blijkt het herstarten van onverhoopt vastgelopen computers vaak voldoende om snel weer beschikbaar te zijn. Deze eis betekent voor de zorgaanbieder dat zijn ICT-voorzieningen professioneel moet (laten) beheren. Dit vergt periodieke controle met eventueel preventief onderhoud. Verder moet een onverhoopte storing meteen worden gesignaleerd, zodat een GBZ-beheerder snel beschikbaar kan zijn om het probleem te verhelpen. Wellicht kan zijn XIS-leverancier hem daarbij helpen. Indien de zorgaanbieder een ASP-leverancier heeft geselecteerd voor zijn XIS, zal hij dit wellicht geheel delegeren aan die ASP-leverancier. De afspraken en procedures zoals opgenomen in de [AORTA DAP] dienen hierbij gevolgd te worden. Voor de waarden *<aantal_kleine_storingen>* en *<oplostijd_kleine_storingen>* moeten de waardes gehanteerd worden zoals zijn opgenomen in de [AORTA DAP]. Deze eis dient als kapstokeis. Het is mogelijk dat de tekst en variabele namen in de [AORTA DAP] afwijken van deze eis.
Verificatiewijze	Review, monitoring
Voorheen	GBZ·IE·BES·e02

GBX.BET.e4020	
Grote storingen in een GBZ mogen niet meer dan gemiddeld *<aantal_grote_storingen>* keer per jaar voorkomen (MTBF) en dienen dan binnen *<oplostijd_grote_storingen>* (MTTR) te zijn opgelost.	
Functie	Borgen van de beschikbaarheid van een GBX.
Scope	GBZ/ GBO

Karakter	Verplicht
Toelichting	Deze eis is nodig om te voorkomen dat een GBZ na een ernstige storing zeer lang onbeschikbaar blijft, omdat er bijvoorbeeld 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. De afspraken en procedures zoals opgenomen in de [AORTA DAP] dienen hierbij gevolgd te worden. Voor de waarden *<aantal_grote_storingen>* en *<oplostijd_grote_storingen>* moeten de waardes gehanteerd worden zoals zijn opgenomen in de [AORTA DAP]. Deze eis dient als kapstokeis. Het is mogelijk dat de tekst en variabele namen in de [AORTA DAP] afwijken van deze eis.
Verificatiewijze	Review, monitoring
Voorheen	GBZ·IE·BES·e03

3.6 Prestaties

Een GBX moet voldoen aan de volgende eisen betreffende capaciteit en responstijden.

GBX.PST.e4010

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

Interactiemechanisme	**Minimale verwerkingssnelheid**
Sturen van gegevens	*<GBx-verwerkingssnelheid>*
Opvragen van gegevens	*<GBx-opleversnelheid>*

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.

Functie	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.

Scope	GBZ/GBK/GBO
Karakter	Conditioneel
Condities	Bronsysteem patiëntgegevens, Gegevens ontvangend systeem
Toelichting	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.
Verificatiewijze	Review, monitoring
Voorheen	GBZ·IE·RSP·e02 GBZ·IE·RSP·e03 GBZ·IE·CAP·e02 GBK·IE·CAP·e01

GBX.PST.e4015	
Een GBZ 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.	
Functie	Deze eis is nodig opdat een XIS-applicatie tijdig berichten van de ZIM of de gebruiker kan verwerken.
Scope	GBZ/GBK/GBO
Karakter	Verplicht
Condities	-
Toelichting	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.
Verificatiewijze	Review
Voorheen	GBZ·IE·RSP·e01

4 Eisen aan de applicatie

Een GBX-applicatie dient te voldoen aan de volgende eisen.

4.1 Inloggen en uitloggen van een gebruiker

GBX.IDA.e4080.3

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

a) {GBZ}{GBK}het invoeren van zijn vertrouwensmiddel op de werkplek en het invoeren van de bijbehorende toegangscode;
b) {GBP} zich op niveau DigiD-midden te authenticeren.

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

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

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

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

Functie	Inloggen op vertrouwensniveau midden
Scope	GBZ/GBK/GBP
Karakter	Verplicht
Condities	-
Toelichting	Dit is nodig opdat gebruikers in staat worden gesteld tot het landelijk uitwisselen van gegevens op vertrouwensniveau midden. VZVZ levert gratis generiek tooling in de vorm van Zorg-ID om de implementatie van het authenticeren met de UZI-pas te ondersteunen.
Verificatiewijze	Test
Voorheen	GBX.IDA.e4080.1

GBX.IDA.e4085.2

Het GBx dient het starten van een gebruikersessie met het LSP op vertrouwensniveau midden te weigeren indien:

a) de geldigheidstermijn van het transactietoken is verlopen of nog niet is aangevangen;
b) het transactietoken niet correct is ondertekend;
c) het certificaat, waarmee het transactietoken is getekend, op een geldige lijst staat van ingetrokken certificaten (CRL) van het UZI-register;
d) het transactietoken is geweigerd door het LSP.

Functie	Het blokkeren van ingetrokken, verlopen passen en niet authentieke passen.
Scope	GBZ
Karakter	Verplicht
Condities	-
Toelichting	Deze eis is conform de regels van PKI Overheid. Er moet voorkomen worden dat een GBZ toegang geeft als gevolg van een ongeldige UZI-pas. Alleen een gebruiker die een UZI-pas heeft en de pincode weet, kan een geldig transactietoken genereren.
Verificatiewijze	Test
Voorheen	GBX.IDA.e4085.1

GBX.IDA.e4090	
Het systeem moet een gebruikersessie voor het landelijk uitwisselen van patiëntgegevens op vertrouwensniveau laag of midden afsluiten: a) op commando van de gebruiker (zoals een muisklik of toetsencombinatie); b) door uitnemen van het vertrouwensmiddel door de zorgverlener/medewerker; c) wanneer de applicatie gedurende <*gebruiker-max-applicatie-onbruik*> niet is gebruikt; De parameter <*gebruiker-max-applicatie-onbruik*> is binnen de applicatie instelbaar, naar redelijkheid en risico, en heeft een maximale waarde van 60 minuten.	
Functie	Afbreken van een gebruikersessie.
Scope	GBZ/GBK/GBO
Karakter	Verplicht
Condities	-
Toelichting	Dit is nodig opdat een gebruiker zelf zijn gebruikersessie kan uitloggen met de zekerheid dat niemand anders zijn sessie kan voortzetten en vervolgens zijn bevoegdheden kan misbruiken. Daarnaast is deze eis nodig om te tegen te gaan dat een in onbruik geraakte sessie door een onbevoegde kan worden misbruikt.
Verificatiewijze	Test
Voorheen	GBZ·AE·INL·e05 GBZ·AE·INL·e06 GBK·AE·INL·e04 GBK·AE·INL·e05 GBP·AE·INL·e04 GBP·AE·INL·e05

4.2 Toegangslog

Het GBX moet een lokale toegangslog bijhouden en daarbij voldoen aan de volgende eisen.

GBX.LOG.e4015	
Het systeem moet de volgende berichtuitwisselingen loggen: a) Ontvangen opvraagberichten en de daarop verzonden antwoorden; b) Verzonden opdrachtberichten en kennisgevingberichten. De log bevat per berichtuitwisseling tenminste: 1) de identiteit van de patiënt/cliënt (BSN); 2) identiteit van de opvragende/versturende organisatie; 3) de functie en identiteit van de opvragende of versturende zorgverlener (UZI), medewerker (UZI) of patiënt (BSN); 4) type en volgnummer 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.	
Functie	Dit is nodig opdat aan de hand van de berichtuitwisseling precies achterhaald kan worden: a) {GBZ}{GBO}wat voor soort patiëntstukken wanneer zijn opgevraagd door welke zorgverlener/medewerker van welke andere zorgaanbieder; b) {GBK} wat voor soort opvragingen, opdrachten en kennisgevingen wanneer zijn verzonden resp. ontvangen door welke klantenloketmedewerker; c) wat voor soort patiëntstukken wanneer zijn toegestuurd aan welke andere zorgaanbieder of ZIM; d) welke inhoud die patiëntstukken precies hadden; e) {GBP} wat voor soort patiëntstukken wanneer zijn opgevraagd door welke patiënt vanuit welke organisatie.
Scope	GBZ/GBK/GBO
Karakter	Verplicht
Condities	-
Toelichting	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.
Verificatiewijze	Test
Voorheen	GBZ·AE·LOG·e01 GBZ·AE·LOG·e02 GBZ·AE·RLO·e02 GBK·AE·LOG·e01 GBK·AE·LOG·e02

4.3 Connectiviteit

Om de interoperabiliteit tussen alle op de landelijke infrastructuur aangesloten systemen te garanderen moeten GBX'en aan de volgende connectiviteitseisen voldoen.

GBX.CON.e4060.1	
Het GBX dient voor berichtuitwisseling met de ZIM de volgende protocolstack te gebruiken: • HL7v3 • SOAP v1.1 • HTTP v1.1 • TLS v1.2 • TCP • IPv4	
Functie	Protocolstack voor berichtuitwisseling.
Scope	GBZ/GBK/GBP/GBO
Karakter	Verplicht
Condities	-
Toelichting	Het is niet toegestaan om een lagere protocolversie te hanteren dan die in deze protocolstack vermeld is, zoals bv SSLv2 en SSLv3.
Verificatiewijze	Test
Voorheen	GBZ·AE·CON·e01 GBK·AE·CON·e04 GBP·AE·CON·e01

GBX.CON.e4065	
Het GBX volgt voor de afhandeling van SOAP-headers in berichten de aanwijzingen zoals beschreven in [IH Transport].	
Functie	Juiste afhandeling van SOAP headers.
Scope	GBZ/GBK/GBP/GBO
Karakter	Verplicht
Condities	-
Toelichting	Het gaat hierbij onder andere om het op de juiste wijze in acht nemen van SOAP-headerattributen 'mustUnderstand' and 'actor'.
Verificatiewijze	Test
Voorheen	-

GBX.CON.e4066	
Het GBX volgt voor berichtuitwisseling als bedoeld in eis GBX.CON.e4060 de WS-I Basic Profile 1.0 specificaties.	
Functie	Bevorderen interoperabiliteit bij berichtuitwisseling.
Scope	GBZ/GBK/GBP/GBO
Karakter	Verplicht
Condities	-
Toelichting	-
Verificatiewijze	Test
Voorheen	-

GBX.CON.e4070.2	
Het GBX moet na het beschikbaar worden voor de ZIM: a) verzoeken van de ZIM voor het opzetten van nieuwe TLS-sessies honoreren ten behoeve van berichtuitwisseling voor andere zorgaanbieders, b) {GBZ}{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.	
Functie	Opzetten en gebruiken van TLS-sessies.
Scope	GBZ/GBK/GBP/GBO
Karakter	Verplicht
Condities	-
Toelichting	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.

Verificatiewijze	Test
Voorheen	GBZ·AE·CON·e02 GBK·AE·CON·e05 GBP·AE·CON·e02

GBX.CON.e4080.3	
Het GBX dient voor het landelijk uitwisselen van patiëntgegevens een TLS-sessie met de ZIM met de volgende kenmerken op te zetten: a) tweezijdige authenticatie met behulp van het servercertificaat van de ZIM en i. het servercertificaat van het GBX voor vertrouwensniveau midden; ii. het servercertificaat van het GBX voor vertrouwensniveau laag {GBK} en midden; b) tijdelijke sleutels die ververst worden elke i. *<applicatie-max-sleutel-duur>* c) gebruikmakend van Cipher Suites die door het NCSC minimaal worden gekenmerkt als voldoende; d) gebruikmakend van de sterkste cipher suite die gedeeld wordt met de ZIM; e) een ten hoogste ongebruikte TLS-sessie van: i. *<applicatie-max-sessie-onbruik>*	
Functie	Dit is nodig opdat een GBX een voldoende hoog beveiligingsniveau kan afdwingen bij het opzetten van een TLS-sessie met de ZIM.
Scope	GBZ/GBK/GBP/GBO
Karakter	Conditioneel
Condities	Het initiatief voor het opzetten van de hier bedoelde TLS-sessie ligt bij het GBX.
Toelichting	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. Zie ook **GBX.CON.e4060**
Verificatiewijze	Test
Voorheen	GBZ·AE·CON·e03 GBK·AE·CON·e06 GBP·AE·CON·e03

GBX.CON.e4090.3
Het GBX dient voor het landelijk uitwisselen van patiëntgegevens een TLS-sessie met de ZIM met de volgende kenmerken te accepteren: a) tweezijdige authenticatie met behulp van het UZI- of PKIO-servercertificaat van het GBZ en het servercertificaat van de ZIM, b) tijdelijke sleutels die elke *<systeem-max-sleutel-duur>* ververst worden,

c) gebruikmakend van Cipher Suites die door het NCSC minimaal worden gekenmerkt als voldoende(goed dus altijd ook) en tevens worden ondersteund door de ZIM. Voor encryptie moet altijd de sterkste vorm als eerste worden geprobeerd, d) een maximale sessieduur van <*systeem-max-sessie-duur*>, e) een ten hoogste ongebruikte TLS-sessie van <*systeem-max-sessie-onbruik*>.	
Functie	Dit is nodig opdat de ZIM een voldoende hoog beveiligingsniveau kan afdwingen bij het opzetten van een TLS-sessie met een GBX.
Scope	GBZ/GBK/GBP/GBO
Karakter	Conditioneel
Condities	Het initiatief voor het opzetten van de hier bedoelde TLS-sessie ligt bij de ZIM.
Toelichting	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.
Verificatiewijze	Test
Voorheen	GBZ·AE·CON·e04

GBX.CON.e4100	
Het GBX dient alleen de keten van Certificate Authorities (CA's) van het ZIM-certificaat kenbaar te maken in het "certificate request" bericht van de TLS-handshake, waaronder ook het stamcertificaat (Root CA) van de keten.	
Functie	Dit is nodig opdat een GBZ beperkt kenbaar maakt welke CA's het vertrouwt.
Scope	GBZ/GBO
Karakter	Verplicht
Condities	-
Toelichting	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.
Verificatiewijze	Test
Voorheen	GBZ·AE·CON·e05

GBX.CON.e4110.2	
Het GBx dient UZI/PKIo-servercertificaten van de (verschillende) generatie(s) te ondersteunen zoals beschikbaar wordt gesteld door het UZI-Register ([UZI-Register]). Er moet gebruik worden gemaakt van het SHA-256 ondertekeningsalgoritme.	
Functie	Ondersteunen servercertificaten en ondertekeningalgoritmen.

Scope	GBZ/GBO/GBK/GBP
Karakter	Verplicht
Condities	-
Toelichting	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.
Verificatiewijze	Demo
Voorheen	GBZ·IE·BVL·e07

4.4 Beheer van zorgapplicaties

Een beheerder zal voor de applicatie(s) die hij beheert detailinformatie willen ontvangen voordat hij of zij een wijziging aan de geregistreerde applicatiegegevens aanbrengt.

Daarnaast zal de beheerder ook lokaal en centraal geregistreerde applicatiegegevens willen wijzigen of laten wijzigen. Belangrijk is om daarbij op te merken dat de lokaal geconfigureerde instellingen overeen moeten komen met die uit het centrale applicatieregister.

GBX.FBH.e4030	
Binnen het GBZ dient te worden bijgehouden welke UZI-passen worden toegelaten voor gebruik. Deze gebruikersregistratie is uitsluitend toegankelijk voor gebruikers van de gastheerinstelling, na authenticatie op basis van een sterke authenticatie (2 factor-authenticatie bijvoorbeeld via een UZI-pas) van diezelfde gastheerinstelling.	
Functie	Het bijhouden van een gebruikersregistratie.
Scope	GBZ
Karakter	Verplicht
Condities	-
Toelichting	Dit is nodig om te voorkomen dat een willekeurig persoon de gebruikersregistratie kan aanpassen. Deze bevoegdheid komt bij een specifiek persoon te liggen. Dit betekent voor de zorgaanbieder dat hij moet zorgen dat de bovenstaande rol van autorisatiebeheerder door een van zijn medewerkers wordt ingevuld.
Verificatiewijze	Review
Voorheen	GBZ·AE·BZA·e10 GBZ·AE·BZA·e11

GBX.FBH.e4050.2

De GBx-beheerder moet de volgende configuratieparameters in het GBx kunnen instellen: a) URI en hostnaam van de ~~operationele~~ ZIM; b) applicatie-id van de eigen applicatie; c) applicatie-id van het schakelpunt waarop kan worden aangesloten.	
Functie	Dit is nodig opdat een GBx deze parameters kan gebruiken bij de HTTP-communicatie met en authenticatie van de ZIM.
Scope	GBZ/GBO
Karakter	Verplicht
Condities	-
Toelichting	De in het GBx ingestelde waarden komen overeen met de in het applicatieregister van de ZIM geregistreerde gegevens.
Verificatiewijze	Test
Voorheen	GBZ·AE·BZA·e01

GBX.FBH.e4070	
Binnen de organisatie moet er een speciale rol toegewezen (en geautoriseerd) worden om toegang te krijgen tot de diverse opgeslagen tokens (inschrijf- en mandaattoken).	
Functie	Beveiligen van tokens
Scope	GBZ/GBO
Karakter	Conditioneel
Condities	Deze eis geldt indien er gebruik wordt gemaakt van inschrijf- en mandaattokens.
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.
Verificatiewijze	Monitoring
Voorheen	

Bijlage A: Referenties

Referentie	Document	Versie
[Arch_AORTA]	Architectuur AORTA	8.2.0.0
[ISO27001]	Information technology - Security techniques - Information security management systems – Requirements	-
[IH Transport]	Implementatiehandleiding SOAP berichttransport	8.2.0.0
[NEN7510]	Medische informatica - Informatiebeveiliging in de zorg – Algemeen	2017
[PvE GZN]	Programma van eisen Goedbeheerd ZorgNetwerk (GZN)	8.2.0.0
[PvE GBP]	Programma van eisen organisatie goed beheerd patiëntenportaal (GBP)	8.2.0.0
[UZI-Register]	CA model pasmodel certificaatprofielen	https://www.zorgcsp.nl/ca-certificaten
[Besluit EGDZ]	Besluit elektronische gegevensverwerking door zorgaanbieders, 10 november 2017	https://zoek.officielebekendmakingen.nl/stb-2017-446.html