



Architectuur AORTA

Datum: 14 oktober 2025
Publicatie: v8.5.1

Table of Contents

1	Release-informatie.....	8
1.1	Wijzigingshistorie.....	8
1.1.1	Achtergrond.....	8
1.1.2	Reikwijdte	8
1.1.3	Samenhang met andere documenten	8
1.1.4	Uitgangspunten.....	9
1.1.5	Wijzigingsoverzicht t.o.v. de vorige release	9
2	Manifest VZVZ	12
3	Principes.....	15
3.1	Generieke Architectuurprincipes / Stelseloverstijgende principes.....	16
3.2	AORTA Principes.....	30
4	Architectuurvisie AORTA	33
4.1	Ontwikkelingen.....	33
4.2	Hybride (bimodal) besturingsvormen.....	33
4.3	Zorgservices.....	34
5	Juridische context	35
5.1	Wettelijk kader.....	35
5.1.1	Overzicht wetgevend kader	35
5.1.2	De Wet op de geneeskundige behandelovereenkomst (WGBO).....	36
5.1.3	Wet beroepen individuele gezondheidszorg (Wet BIG)	37
5.1.4	Wet kwaliteit, klachten en geschillen in de zorg (Wkkgz).....	38
5.1.5	Algemene verordening gegevensbescherming (AVG)	38
5.1.6	Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz).....	40
5.1.7	Wetsvoorstel elektronische gegevensuitwisseling in de zorg (Wegiz)	43
5.1.8	Kwaliteitswet zorginstellingen (KWZi).....	44
5.1.9	Wet klachtrecht cliënten zorgsector (WKCZ).....	44
6	Governance	46
6.1	Diensten.....	46
6.2	Releasebeleid	46

6.2.1	Releasecriteria en versiebeheer	46
6.2.2	Releasefrequentie	46
6.2.3	Externe koppelingen	47
7	Logische architectuur	48
7.1	Samenvatting	48
7.1.1	Primaire interacties.....	48
7.1.2	Ondersteunende interacties	48
7.1.3	Authenticatie en autorisatie	48
7.1.4	Informatiesystemen.....	49
7.1.5	Berichtafhandeling.....	51
7.1.6	Non-functionele aspecten en beveiliging	51
7.2	Inleiding en context.....	51
7.2.1	Achtergrond.....	51
7.3	Primaire interacties.....	53
7.3.1	Interacties.....	53
7.3.2	Primaire informatiesysteeminteracties – opvragen en sturen van gegevens	54
7.3.3	Actoren	58
7.3.4	Rollen toekennen aan actoren	60
7.3.5	Toegangsmodel	62
7.3.6	Identificatie en authenticatie.....	65
7.3.7	Patiëntgegevens	66
7.3.8	Het zoeken van gegevenshouders en gegevensontvangers.....	66
7.4	Ondersteunende interacties	67
7.4.1	Ondersteunende interacties.	68
7.4.2	Ondersteunende informatiesysteeminteracties	69
7.4.3	Actoren en rollen.....	87
7.4.4	Opvragen/verifiëren BSN en controleren omloopstatus WID	88
7.4.5	Aan- en afmelden van patiëntgegevens	89
7.4.6	Bijhouden van abonnementen en signaleren van gebeurtenissen	89
7.4.7	Selecteren van zorgaanbieders, zorgverleners en zorgaanbiederapplicaties.....	90
7.4.8	Raadplegen toegangslog.....	90
7.4.9	Vastleggen autorisatieprotocollen	91

7.4.10 Vastleggen determinatietabellen	91
7.4.11 Raadplegen verwijzindex	91
7.5 Informatiesystemen	91
7.5.1 AORTA on FHIR	95
7.5.2 Interacties tussen informatiesystemen	97
7.5.3 Applicatie-interacties voor beheer	100
7.5.4 Zorginformatiemakelaar (ZIM)	105
7.5.5 Goed beheerd informatiesysteem (GBx)	110
7.5.6 Zorginformatiesystemen (XIS) en het Goed beheerd zorgsysteem (GBZ)	110
7.5.7 Goed beheerd patiëntportaal (GBP)	111
7.5.8 Goed beheerd klantenloketsysteem (GBK)	112
7.5.9 Goed beheerde organisatie (GBO)	113
7.5.10 Dienstverlener Zorgaanbieder (DVZA)	113
7.5.11 Goed beheerde connector (GBC)	113
7.5.12 Basisregistraties en vertrouwensmiddelen	113
7.5.13 Resource Broker (RB)	116
7.5.14 Autorisatie Server (AS)	117
7.5.15 Resource Server (RS)	117
7.5.16 Berichtentransformatiedienst (BTD)	118
7.6 Beheerinteracties	118
7.6.1 Actoren en rollen	118
7.6.2 Toegang van GBZ-beheerders tot primaire en ondersteunende interacties	119
7.6.3 Beheer van aansluitingen	120
7.6.4 Beheer van de verwijzindex	120
7.6.5 Beheer van het zorgadresboek	121
7.6.6 Beheer van zorgtoepassingen	121
7.6.7 Beheer van selectie en determinatieserver	121
7.7 Overzicht van systeemrollen	122
7.8 Berichtafhandeling	123
7.8.1 Protocollen	123
7.8.2 Foutafhandeling	125
7.8.3 Afhandelen van berichtversies	126

7.8.4	Ondersteunen van bouwsteenversies	127
7.8.5	Berichtafhandeling door de ZIM	130
7.9	Infrastructurele aspecten	145
7.9.1	Conceptueel overzicht infrastructuur	145
7.9.2	Operationele aspecten.....	150
7.10	Beveiliging	152
8	Zorgtoepassingen.....	154
8.1	Acute Zorg	154
8.1.1	Opvragen professionele samenvatting RAV & SEH	154
8.1.2	Spoedverwijzing HAP-SEH	154
8.2	Huisartswaarneemgegevens	154
8.2.1	Vast Huisartssysteem	154
8.2.2	Waarnemend Huisartssysteem.....	155
8.3	Jeugdgezondheidszorg	155
8.4	LSP Ketenzorg.....	156
8.4.1	HIS Ketenzorg	156
8.4.2	KIS Ketenzorg.....	156
8.5	MedMij.....	157
8.5.1	MedMij Bronsysteem.....	157
8.5.2	MedMij HIS t.b.v. OPEN	218
8.6	Medicatieproces	285
9	Processen.....	286
9.1	Aansluiten Mitz	286
9.2	Contracttoken	286
9.3	Vereenvoudigd gebruik UZI-pas (VGU)	286
9.3.1	Inleiding	286
9.3.2	Vereenvoudigd proces UZI-pas.....	287
9.3.3	Generieke uitwerking vereenvoudigd gebruik van de UZI-pas (VGU)	289
9.3.4	UZI-middel gebruik.....	290
9.3.5	Aandachtspunten.....	294
9.3.6	Acceptatie	295
9.4	Abonnement- en signaalfunctie	296

9.4.1	Gebruik abonnement	296
9.4.2	Verwijderen Abonnement	298
9.4.3	Synchronisatie met Abonnementenregister.....	299
9.4.4	Lokaal abonnementenregister	300
9.4.5	Afhandelen signalen	300
9.4.6	Processen m.b.t. signaalfunctie	303
10	Aansluit- en Implementatiewijzer Kern.....	305
10.1	Berichttransport	305
10.1.1	AORTA_Trp_IH_Berichttransport	305
10.2	Toestemming	355
10.2.1	Mitz 3.8.0_1	355
10.3	Token specificaties.....	357
10.3.1	JSON Web tokens	359
10.3.2	AORTA SAML tokens	368
11	Bestandenlijst.....	611
12	VZVZ Registratie van OID en codesystemen	614
12.1	Registratie van URI's	618
13	AORTA Verklarende woordenlijst.....	620
13.1	Afkortingen.....	620
13.2	Begrippen	626
14	Referenties	641
15	Errata	644
16	Addenda	645

De AORTA-architectuur beschrijft een landelijke uitwisselingsstructuur voor veilige elektronische uitwisseling van medische gegevens tussen applicaties van zorgverleners. De uitwisseling van gegevens is gebaseerd op professionele afspraken die worden gemaakt tussen betrokken beroepsgroepen uit de zorg en vindt plaats met gestandaardiseerde berichten en uitwisselprotocollen. Hierbij gebruikt VZVZ (inter)nationaal breed geaccepteerde en open standaarden zodat voor de betrokken leveranciers maximale herbruikbaarheid bestaat en zorgaanbieders niet gebonden zijn aan leveranciersspecifieke oplossingen.

1 Release-informatie

De release- en versiebeschrijving duidt de positionering en status van deze publicatie. Wijzigingen ten opzichte van eerder gepubliceerde versies (en een historisch overzicht van wijzigingen) zijn hier te vinden.

1.1 Wijzigingshistorie

Versie	Datum	Omschrijving
8.5.1	8-10-2025	AORTA-infrastructuurdocumentatie v8.5.1
8.5.0	9-9-2025	AORTA-infrastructuurdocumentatie v8.5.0
8.4.0.0	15-10-2024	AORTA-infrastructuurdocumentatie v8.4.0.0

1.1.1 Achtergrond

VZVZ richt zich op de totstandkoming van een betere informatievoorziening rondom en voor de patiënt/cliënt met behulp van ICT. Het uiteindelijke doel is het bereiken van een hogere doelmatigheid en kwaliteit van ICT in de zorg. Ter ondersteuning van dit doel is een samenhangende set documentatie ontwikkeld: de zogenoemde AORTA-documentatierelease. De wijzigingshistorie ondersteunt de lezers met een beknopt overzicht van alle wijzigingen in de 'nieuwe' AORTA-documentatierelease ten opzichte van de vorige totaalrelease inclusief patches en errata.

1.1.2 Reikwijdte

De wijzigingshistorie is een handreiking voor softwareontwikkelaars van XIS-applicaties, bedoeld als informatief hulpmiddel en niet als een uitgebreid en volledig overzicht van issues.

1.1.3 Samenhang met andere documenten

In de wijzigingshistorie wordt aan diverse documenten van AORTA gerefereerd. De nadruk ligt echter op de volgende documenten die het 'koppelvlak' met de programmeurs vormen:

- De PvE's;
- De implementatiehandleidingen;
- Het XML-materiaal.

1.1.4 Uitgangspunten

1.1.4.1 Referenties

Zie hiervoor: [Referenties](#) (see page 641)

1.1.4.2 Begrippen

Zie hiervoor: [AORTA Verklarende woordenlijst](#) (see page 620)

1.1.4.3 Afkortingen

Zie hiervoor: [Afkortingen](#) (see page 620)

1.1.5 Wijzigingsoverzicht t.o.v. de vorige release

1.1.5.1 Vorm

1.1.5.1.1 Categorieën versiecompatibiliteit

Om te bepalen welke wijziging potentieel compatibiliteitsproblemen oplevert tussen systemen met verschillende operationele AORTA-versies, classificeert VZVZ elke voorgenomen wijziging. VZVZ hanteert daarbij de volgende categorieën:

- Categorie 0: geen wijziging voor systemen. Wijzigingen in de architectuurdocumentatie zonder impact op het programma van eisen. Geïnstalleerde onderdelen van de infrastructuur hoeven niet aangepast en niet opnieuw gekwalificeerd te worden. Een voorbeeld van deze wijzigingen zijn verduidelijkingen in de documentatie.
- Categorie 1: wijzigingen die lokaal doorgevoerd kunnen worden. Wijzigingen met impact op 1 partij of op meerdere partijen maar zonder onderlinge afhankelijkheden. Deze wijzigingen zijn binnen de verschillende onderdelen van de infrastructuur afzonderlijk door te voeren zonder dat daarbij verlies aan functionaliteit optreedt. Een voorbeeld van dit soort wijzigingen is een wijziging in de eis voor GBZ's inzake de bewaartermijn voor bepaalde gegevens. Dit heeft impact op elke GBZ, maar de wijziging hiervan binnen een GBZ heeft geen gevolgen voor overige onderdelen van de infrastructuur.
- Categorie 2: wijzigingen die compatibel zijn met de vorige versie. Wijzigingen die impact hebben op meerdere partijen met onderlinge afhankelijkheden maar die compatibel zijn. Deze wijzigingen worden zodanig ontworpen dat het doorvoeren van de wijzigingen geen afhankelijkheden met zich meebrengt voor overige onderdelen van de infrastructuur. Dat wil zeggen, zowel de uitwisseling tussen een oude zender en een nieuwe ontvanger blijft goed gaan, als de uitwisseling tussen een nieuwe zender en een oude ontvanger blijft goed gaan. Ook deze wijzigingen kunnen dus lokaal doorgevoerd worden (zonder dat men van elkaar weet welke versie geïnstalleerd is). Een voorbeeld van zo'n wijziging is wanneer op landelijk niveau wordt afgesproken dat een optioneel veld in een bepaald bericht voortaan gebruikt gaat worden. Een ander, iets complexer voorbeeld is wanneer een optioneel veld verplicht wordt. Een dergelijke

wijziging is niet 100% compatibel, maar kan wel als zodanig ontworpen worden door te specificeren dat de nieuwe ontvanger ook een leeg of ontbrekend veld kan verwerken. Een GBZ hoeft dan niet twee versies van één bericht te onderhouden, maar kan lokaal de nieuwe versie doorvoeren.

- **Categorie 3:** wijzigingen die centraal worden opgevangen. Wijzigingen met impact op meerdere partijen met onderlinge afhankelijkheden, die niet compatibel zijn, maar waarbij de ZIM verschillende versies ondersteunt zodat GBZ'en geen maatregelen hoeven te nemen. Deze categorie betreft wijzigingen die niet compatibel ontworpen kunnen worden, maar wel door het LSP afgevangen kunnen worden. Dat wil zeggen dat, indien er geen verdere maatregelen getroffen worden, de invoering van de wijziging leidt tot een verlies aan communicatiemogelijkheden en/of functionaliteit. In deze categorie wijzigingen zal de ZIM echter een faciliterende rol vervullen zodat het voor de verschillende decentrale onderdelen van de architectuur lijkt alsof er geen sprake is van verschillende versies. Een voorbeeld van deze categorie zijn wijzigingen in de buitenste wrappers van een bericht. Het LSP kan hierbij zowel een oude als een nieuwe versie ondersteunen zodat er geen compatibiliteitsproblemen ontstaan. Hierbij is de centrale registratie van de conformancetabel per GBZ uiteraard wel van belang.
- **Categorie 4:** wijzigingen die versiebeheer vergen bij een GBZ. Wijzigingen met impact op meerdere partijen met onderlinge afhankelijkheden, niet compatibel, niet te ondersteunen door de ZIM. Deze laatste categorie bestaat uit wijzigingen die niet compatibel te ontwerpen zijn en waarbij de ZIM ook niet kan faciliteren. Voor deze categorie zal VZVZ per wijziging, in overleg met de belanghebbenden, een aanpak opstellen om de wijziging door te voeren. Een voorbeeld van deze categorie is de inperking van de mogelijke doseerinstructies om de ontvangende applicatie te ontlasten (die hoeft dan niet alle theoretische combinaties aan te kunnen). Het probleem hierbij is dat een nieuwe ontvanger van een oude zender nog een oude doseerinstructie kan krijgen. Het eisen dat de nieuwe ontvanger deze nog even moet ondersteunen is juist niet de bedoeling van de wijziging.

1.1.5.2 Overzicht wijzigingen gepubliceerd in erratum

RfC	Beschrijving	Docs

1.1.5.3 Wijzigingen versie 8.5.1 t.o.v. 8.5.0

Wijziging	Beschrijving	Compatibiliteitscategorieg	Documentatie
VTAS-103	Ondersteuning van Zorg-ID Smartcard toegevoegd binnen AORTA-LSP.	1	Zie pagina "Basisregistraties en vertrouwensmiddelen"

VTAS-138	Alle verwijzingen naar verouderde of onveilige TLS-verbindingen en SHA-1 voorbeelden zijn aangepast of uit het afsprakenstelsel verwijderd.	0	-
VTAS-149	In het stelsel zijn diverse stijl-, grammatica- en schrijffouten vastgesteld en gecorrigeerd.	0	-

1.1.5.4 Wijzigingen versie 8.5.0 t.o.v. 8.4.0.0

Wijziging	Beschrijving	Compatibiliteitsc ategorie	Documentatie
VTAS-135	Releasebeleid voor het AORTA afsprakenstelsel.	0	Zie pagina "Releasebeleid"
VTAS-64	De volgorde van de inhoudsopgave in het linkermenu is aangepast.	0	-

2 Manifest VZVZ



1. Persoon op één

De burger, cliënt en patiënt in de zorg staan op de eerste plek in het denken, doen en laten. Deze personen zijn de klant van de zorg. Zorgprocessen veranderen en spelen steeds meer in op de wensen en behoeften van deze klant. Soms moeten ook andere personen de belangen van de klant behartigen. Denk hierbij aan mantelzorgers, ouders van een ziek kind, bewindvoerders en zorgverleners die vanuit hun rol bepaalde beslissingen moeten kunnen nemen of bepaalde handelingen moeten kunnen uitvoeren namens de klant. Het welzijn van deze andere betrokken personen ten aanzien van het gebruik van systemen is net zo goed belangrijk. Zij moeten op een eenvoudige efficiënte manier hun werk kunnen doen. Andere wijzen van werken en nieuwe oplossingen vereenvoudigen het werk voor de betrokken personen en ontlasten hen hierin. Al deze personen werken samen aan de gezondheid van de klant. Wij zullen daarom zowel de belangen behartigen van de kwetsbare medemens, die vanwege ziekte of een gebrek aan digitale vaardigheden maximaal gefaciliteerd wil worden vanuit het eigen zorgnetwerk, als van de zelfredzame patiënt, die maximale invloed en betrokkenheid wenst om zelf zijn of haar rechten uit te kunnen oefenen. Hierdoor krijgt de klant, los van wie hij of zij is als persoon, meer regie en daarmee een gelijkwaardigere rol in het zorgveld.



2. Zorgcentrisch

Goede zorgcommunicatie, tussen zorgverleners en hun klanten, tussen zorgverleners onderling en tussen zorgleverende instellingen onderling, is enorm belangrijk. Alleen oplossingen die de betrokken personen nader tot elkaar brengen zijn de moeite waard om te realiseren, ook al moeten onze bestaande inzichten en oplossingen daarvoor op de schop. Oplossingen sluiten zo goed mogelijk aan op zorgprocessen en op de beleavingswereld van patiënt, zorgverlener en andere betrokken personen. Oplossingen brengen goede en juiste informatievoorziening voor het zorgproces. Niet de zorgaanbieder, zorgverlener, leverancier of de patiënt staat hierin centraal, maar de zorg voor de persoon en zijn of haar processen als geheel.



3. Waarde gedreven

In de zoektocht naar oplossingen staat het leveren van meerwaarde voorop. Dit betekent dat de (ervaren) meerwaarde, voor patiënt, zorgverlener en andere betrokken personen, leidend is bij onze beslissingen. Het anticiperen op en het leveren van die meerwaarde is ons doel. Alle voorgenomen verbeteringen moeten hieraan bijdragen. Waarde is soms beter kwalitatief dan kwantitatief te expliciteren. Het interpreteren van informatie uit een zorgtraject ten behoeve van zorggebaseerde waardeparameters is een kunst apart, maar steeds beter mogelijk. De rol van de mens in het waarderen en ervaren van zorg blijft cruciaal. Onze oplossingen zijn daarom *waardevol* voor de betrokken personen.



4. In balans

In de werkelijkheid bestaan er meerdere waarheden en niet slechts één waarheid die koste wat het kost moet prevaleren. Het gaat ons om het bereiken van het doel, niet om de manier waarop of het middel waarmee dat doel wordt bereikt. Techniek is zo'n middel dat ons helpt doelen te verwezenlijken. Veel factoren zijn van invloed op het bereiken van ons doel en de keuzes die we maken ten aanzien van de middelen. Soms staan die factoren op gespannen voet met elkaar. Een beoogde oplossing kan misschien wel de gewenste meerwaarde leveren maar moet ook realiseerbaar en betaalbaar zijn. Zowel tijdens de bouw als tijdens de levenscyclus. Een beoogde oplossing kan misschien wel de meest veilige zijn maar burgers en zorgverleners moeten ook goed kunnen werken met de systemen die we bouwen. Wij streven daarom naar de optimale balans tussen al dit soort factoren die van toepassing zijn op de zorgcommunicatie. Het hogere doel leidend laten zijn in de zoektocht naar balans in de werkelijkheid werkt hierbij *verbindend*.



5. Samen

Om de juiste balans te vinden zoeken wij steeds meer de samenwerking met de patiënt, het zorgveld, de leveranciers de koepels, de financiers en de overheid. Wanneer het kan zoeken we de verbinding op en iedereen is welkom om met ons in gesprek te gaan. We staan daarbij open voor de aangereikte feedback. We nemen zoveel als mogelijk een neutrale positie in en vormen van daaruit een platform om de verschillende stakeholders bij elkaar te brengen en houden. Op deze basis willen we verder. In samenspraak stellen we onze missie en doelen vast. Samen, niet alleen, want alleen samen zijn we in staat om de juiste balans te vinden en vast te houden. Samen staan we sterk. Samen *inlevend* in elkaar.



6. Met liefde en lef

Vooruitstrevendheid vergt lef. We zien dat vooruitstrevendheid ook weerstand kan oproepen. De ene keer steken we de kop boven het maaiveld uit en is het betere de vijand van het goede, de andere keer lopen we voor de troepen uit en is het goede de vijand van het betere. Onze liefde voor de zorg en voor het doel dat wij nastreven helpen ons dan het hoofd niet te verliezen en de rug recht te houden in gesprek met alle betrokkenen. Het maakt ons *slagvaardig* in de missie die we met veel geduld en lange adem uitvoeren.



7. Op alle lagen

Wij geloven dat interoperabiliteit alleen gerealiseerd kan worden als alle lagen uit het [interoperabiliteitsmodel](https://www.nictiz.nl/standaardisatie/interoperabiliteit/)¹ worden betrokken. Wij geloven in open protocollen, normering, vrije en universeel implementeerbare standaarden en vindbare en toegankelijke data. Wij geloven in vrijheid van technologiekeuzes en daarbij horende technologie-agnostische oplossingen de zorginformatiebouwstenen, in het naast elkaar bestaan van verschillende componenten, uitwisselpatronen en topologieën in het ecosysteem, in open translaties om van de ene technische open standaard naar de andere over te kunnen gaan en in al die andere zaken die nodig zijn om hergebruik mogelijk te maken zodat de uitdagingen in de zorg efficiënt en effectief kunnen worden gepareerd. Wij realiseren ons dat de onderste lagen van het interoperabiliteitsmodel zich het best

1. <https://www.nictiz.nl/standaardisatie/interoperabiliteit/>

lenen voor internationale standaardisatie en er naar de bovenste lagen toe meer sprake is van standaardisatie op nationaal niveau. Samenwerking houdt daar rekening mee. Op alle lagen moet er interoperabiliteit zijn om de beoogde meerwaarde te kunnen leveren.



8. Keuzevrijheid

Aansluiten op of gebruik maken van onze diensten is een keuze. Alle partijen in de zorg mogen en kunnen er gebruik van maken. Het maken van zo'n keuze door de ene partij kan gevolgen hebben voor de andere partij. We maken hierover afspraken met elkaar en zien erop toe dat de belangen van de betrokken partijen hierin zorgvuldig worden afgewogen.



9. Transparant

Wij geloven in transparantie en verantwoording. We creëren transparantie voor alle betrokken personen en instanties en zijn transparant over ons handelen. Hierover leggen wij verantwoording af waar en wanneer dat nodig is. Transparantie en controle achteraf blijven sterke middelen om de privacy te waarborgen. Transparantie helpt ons om neutraal te blijven.



10. Veilig

Wij geloven dat zorgcommunicatie veilig moet zijn. Veilige zorgcommunicatie is beschikbaar, integer en vertrouwelijk. Zeker in de zorg is het erg belangrijk dat gegevens op de juiste plek en op het juiste moment beschikbaar zijn om de juiste zorg te kunnen leveren. Wij vinden veiligheid erg belangrijk, omdat gegevens onderweg niet aangepast mogen worden, omdat duidelijk moet zijn wie de communicerende partijen zijn en omdat de vertrouwelijkheid van het medisch dossier te allen tijde gegarandeerd moet zijn. Wij willen het beste voor de privacy van de patiënt. Privacybescherming en informatiebeveiliging behoren tot onze specialiteiten. Wij willen in vertrouwen met elkaar communiceren wanneer het over gevoelige onderwerpen gaat. Samenwerken doen we in vertrouwen. Wat ons in vertrouwen ter ore komt blijft vertrouwelijk. Hetzelfde verwachten wij van onze samenwerkingspartners. Wij geloven daarom in privacy- en security by design en by default. Wij laten ons extern certificeren. Wij hanteren de Plan-Do-Check-Act-cyclus en streven daardoor continu naar verbeteringen en optimalisaties die de veiligheid in de keten verhogen op die punten waar dat het meest relevant is. De keten is immers zo sterk als de zwakste schakel. Honderd procent veiligheid is door niemand te garanderen. Oplossingen moeten in balans zijn. Wij streven daarom maximale veiligheid na binnen de gestelde kaders waarbij het doel blijft: meerwaarde voor patiënt en zorgverlener.

Bovenstaande maakt dat wij vertrouwen kunnen hebben in elkaar. Het maakt ons samen *betrouwbaar*.

3 Principes



Wat zijn principes (Bron ZIRA)

Er zijn vele theoretische definities en interpretaties van architectuurprincipes. De rode draad is dat het regels zijn, afgeleid van organisatiedoelstellingen, -missie en -visie, die richting en structuur geven aan het ontwerp van organisatie, proces, informatie, applicatie en techniek, en daarmee dus restricties aan de ontwerpvrijheid vormen.

Architectuurprincipes zijn:

- - Richtinggevende afspraken binnen een organisatie, gebaseerd op overtuigingen hoe de ambities van de organisatie te realiseren.
 - Richtinggevende uitspraken over de inrichting en realisatie van de informatievoorziening, geven structuur aan de inrichting van proces, informatie, applicatie en techniek;
 - Richtinggevende uitspraken die gebruikt kunnen worden als leidraad en toetsinstrument bij veranderingen;

Architectuurprincipes zijn een kernonderdeel van enterprise-architectuur; ze richten zich op de essentie en bieden een stabiel handvat voor veranderingen in organisaties.



Proces (conform Handboek Architectuur)

Wanneer projecten of toepassingen willen afwijken van bestaande principes kan dit grote gevolgen hebben voor o.a.

- Afspraken en technieken die gebruikt worden in bestaande uitwisselingen
- Herbruikbaarheid
- Herstelwerkzaamheden (architectuurschuld, technologieschuld)
- Relatie met andere ontwikkelingen
- Volgordelijkheid van implementaties
- Doorlooptijd
- Conformance aan wet- en regelgeving

Principes worden toegepast conform pas-toe-of-leg-uit. Afwijkingen op de principes worden signaleerd, opgenomen in het architectuurlogboek en ter besluitvorming voorgedragen.

Met AORTA 8.3 zijn ook de AORTA principes herzien. Generieke (stelseloverstijgende) principes zijn geïntroduceerd met daarbij een (associatieve) referentie naar de DIZRA en de principes en uitgangspunten genoemd in de Visie op samenhang in zorginfrastructuren.



Uiteraard volgen we de vigerende wetgeving, regelgeving en normering in de zorg. Hiervoor zijn geen aparte principes opgenomen en zijn een paar oude AORTA principes vervallen omdat de implicaties inmiddels zijn opgenomen in de wet- en regelgeving.

- AORTA.ALG.p1020: voor toegang tot patiëntgegevens moeten zorgverleners persoonlijk worden geïdentificeerd en geauthentiseerd
- AORTA.ALG.p1030: de mate van toegang van zorgverleners tot patiëntgegevens wordt bepaald door de rol van de zorgverlener.
- AORTA.ALG.p1040.1: gegevens worden slechts beschikbaar gesteld door zorgaanbieders via AORTA na toestemming van de patiënt;

3.1 Generieke Architectuurprincipes / Stelseloverstijgende principes

Generieke architectuurprincipes zijn stelseloverstijgend.

ID	VZVZ.GEN.P100
Toepassingsgebied	Generiek
Stelling	Leveren van meerwaarde voor de persoon
Beschrijving	De systemen en voorzieningen die geleverd worden moeten een meerwaarde leveren ten aanzien van informatievoorziening aan de persoon (zorgverlener en cliënt/patiënt). Eisen die worden gesteld ondersteunen dat doel. Bij het maken van (architectuur)keuzes dient het VZVZ manifest (see page 12) als morele leidraad.
Rationale	Voor het leveren van meerwaarde t.b.v. het verlenen van goede zorg is het nodig dat: • Er wordt voorzien in de informatiebehoefte van de zorgverlener omdat de zorgverlener hierdoor in staat wordt gesteld om betere beslissingen te nemen in het behandeltraject van de patiënt. • Het tijdig mogelijk maken van nieuwe gegevensuitwisselingen ter ondersteuning van die informatiebehoefte biedt een belangrijke meerwaarde voor zowel client/patiënt als zorgverlener.

ID	VZVZ.GEN.P100
Implicaties	• Het leveren van meerwaarde vergt architectuurdenken dat nieuwe gegevensuitwisselingen tussen verschillende infrastructuren mogelijk maakt. • Het koppelen van verschillende vertrouwensdomeinen moet mogelijk gemaakt worden. Nieuwe gegevensuitwisselingen tussen systemen die al met elkaar communiceren binnen een bestaand vertrouwensdomein zijn vaak sneller te realiseren dan gegevensuitwisselingen die moeten worden opgezet tussen verschillende vertrouwensdomeinen. • Meerwaarde tijdig leveren vergt architectuurdenken in korte en lange termijn doelstellingen.
Mappings	<i>Onder de mappings wordt een relatie gelegd met het VZVZ Manifest, de DIZRA en de visie op samenhang. Een mapping is een (associatieve) relatie.</i>
Mapping VZVZ Manifest	• 1 Persoon op één • 2 Zorg-centrisch • 3 Waarde gedreven
Mapping DIZRA ²	• In het informatiestelsel hebben burgers regie op hun eigen gezondheidsdata en kunnen deze data meenemen en delen in hun reis door het zorglandschap en in het netwerk van zorgverleners en ondersteuners dat zich rondom hen vormt. • BP1 Mensgericht: "bij het verstrekken van gegevens over mij, aan mij, houden dienstverleners rekening met mijn wensen en kunnen." • AP1 Vanuit een gebruiksdoel: "onze bouwstenen zijn ontwikkeld vanuit de eindgebruikers van het informatiestelsel en zijn of haar gebruiksdoelen".
Mapping Visie samenhang ³	N.A.
Mapping AORTA oud	N.A.

ID	VZVZ.GEN.P110
Toepassingsgebied	Generiek

2. <https://dizra.gitbook.io/dizra/manifest>

3. <https://public.vzvv.nl/pages/worddav/preview.action?fileName=Visie+op+samenhang+in+zorginfrastructuren+3.0+schoon+.pdf&pagelId=24545583>

ID	VZVZ.GEN.P110
Stelling	Een stelsel of voorziening bevat een vertrouwensmodel
Beschrijving	Een stelsel of voorziening beschrijft hoe het vertrouwen tussen de deelnemers is geregeld met betrekking tot de aspecten: • Identificatie • Authenticatie • Toestemming • Logging • Transparantie • Beheer • Beveiliging • Beschikbaarheid
Rationale	Het vertrouwensmodel is het geheel van technische, organisatorische en juridische waarborgen voor het vertrouwen in de landelijke elektronische uitwisseling van medische gegevens. Het vertrouwensmodel ziet toe op het onderlinge vertrouwen tussen zorgaanbieders, zorgverleners en patiënten en borgt daarmee de vertrouwelijkheid van het medische dossier.
Implicaties	
Mapping VZVZ Manifest	• 10. Veilig
Mapping DIZRA	• In het informatiestelsel wordt federatief samengewerkt aan afspraken voor data en voor diensten. Iedereen implementeert deze afspraken en is aanspreekbaar op het nakomen van de afspraken en de kwaliteit van de implementatie.
Mapping Visie samenhang	• Dankzij afspraken, waaronder een gezamenlijk vertrouwensmodel, ontstaat een basis voor interoperabiliteit tussen de verschillende zorginfrastructuren;
Mapping AORTA oud	

ID	VZVZ.GEN.P120
Toepassingsgebied	Generiek
Stelling	Het koppelen van verschillende vertrouwensdomeinen vergt een overeengekomen groeipad
Beschrijving	Het koppelen van verschillende vertrouwensdomeinen vergt maatwerk doordat er in ieder domein andere afspraken zijn gemaakt over de omgang met de waarborgen uit het vertrouwensmodel. Een transitie gericht op het tijdig leveren van meerwaarde is waardevoller dan afwachten tot het moment waarop iedereen aan dezelfde eisen kan voldoen maar vergt wel een groeipad met duidelijke afspraken waarbinnen de vertrouwensdomeinen naar elkaar kunnen toegroeien.
Rationale	Voor het tijdig realiseren van gegevensuitwisselingen tussen verschillende vertrouwensdomeinen is het nodig dat: • De verschillen in afspraken over de te leveren waarborgen worden overbrugt. Deze verschillen in afspraken zijn vaak dermate groot dat de zoektocht naar een uniforme set aan eisen, waaraan ieder domein moet voldoen voordat er gekoppeld kan worden, het tijdig leveren van meerwaarde in de weg staat, • Het leveren van meerwaarde in de situatie waarin verschillende vertrouwensdomeinen aan elkaar worden gekoppeld moet daarom niet wachten tot zo'n beoogde toekomstige situatie volledig gerealiseerd is. • Een transitie gericht op het tijdig leveren van meerwaarde is waardevoller maar vergt een groeipad met duidelijke afspraken waarbinnen de vertrouwensdomeinen naar elkaar kunnen toegroeien.
Implicaties	• Gegevensuitwisselingen worden gerealiseerd onder behoefte van afspraken die worden gemaakt tussen (vertegenwoordigers van) de raadplegende en dossier houdende zorgaanbieders waarbij de raadplegende dossierhouder, conform wetgeving, gezien wordt als verantwoordelijke voor het al dan niet beschikbaar stellen van medische gegevens. De dossierhouder is derhalve verantwoordelijk voor de autorisatie en de daarbij horende identificatie, authenticatie en accounting.
Mapping VZVZ Manifest	• 4 In balans
Mapping DIZRA	• Het informatiestelsel is duurzaam doordat het relevant is en blijft. Het omarmt voor nu en in de toekomst de complexiteit van meerdere standaarden in een stelsel waarin verandering en innovatie welkom is. • AP3 Een gemodereerd ecosysteem: "we voldoen aan de gemeenschappelijke afspraken om mee te doen aan het informatiestelsel".

ID	VZVZ.GEN.P120
Mapping Visie samenhang	• Gebruikers (of hun vertegenwoordigers) zijn middels de governance medeverantwoordelijk voor de doorontwikkeling van de voorzieningen ;
Mapping AORTA oud	N.A.

ID	VZVZ.GEN.P130
Toepassingsgebied	Generiek
Stelling	Gegevens worden bij de bron opgevraagd
Beschrijving	Voor zover gegevens worden opgeslagen dient dit uitsluitend om: • de gegevensbronnen op efficiënte wijze te kunnen ontsluiten; • te kunnen voldoen aan wettelijke verplichtingen t.a.v. dataminimalisatie (AVG, WGB0); • vast te kunnen stellen wie welke gegevens mag uitwisselen; • vast te kunnen stellen wie op welk moment gegevens heeft uitgewisseld.
Rationale	Er zijn diverse argumenten om patiëntgegevens bij het bronsysteem op te vragen: • Omdat er steeds uitgegaan wordt van de oorspronkelijke gegevens en niet van gekopieerde gegevens, blijft de actualiteit van gegevens gewaarborgd. Eerder ontvangen gegevens (push en pull) verliezen voor een raadpleger snel hun waarde vanwege het verloop in actualiteit van deze gegevens. Door gegevens telkens bij de bron op te vragen wordt de datakwaliteit, en daarmee de patiëntveiligheid, beter doordat (foutieve)gegevens alleen bij de bron kunnen worden gecorrigeerd en dus alleen bij de bron recent blijven. • De dossier houdende zorgaanbieder, als eigenaar van het bronsysteem, houdt de controle over de gegevens. Deze eigenaar is conform wetgeving (m.n. AVG, WGB0, WABVPZ) verantwoordelijk voor de geheimhouding van deze gegevens en daarom verantwoordelijk voor de toegangsverlening tot die gegevens. • Er is minder kans op gebruik van de gegevens voor andere doeleinden dan de oorspronkelijke. De dossierhouder is verantwoordelijk voor de verwerkingen die op de gegevens mogen worden uitgevoerd doordat de dossierhouder de patiënt heeft moeten informeren over deze verwerkingen. Verwerkingen die buiten de scope van deze doelbinding vallen zijn primair niet toegestaan (AVG).

ID	VZVZ.GEN.P130
Implicaties	
Mapping VZVZ Manifest	N.A.
Mapping DIZRA	De data blijft bij de bron, onder de verantwoordelijkheid van de bronhouder, voor een veilig en vertrouwd informatiestelsel waarin het voor burgers transparant is welke bronhouders welke gezondheidsgegevens registreren en wie ze raadpleegt.
Mapping Visie samenhang	De verantwoordelijkheid voor de (inhoudelijke) kwaliteit van gegevens ligt bij de (oorspronkelijke) bron;
Mapping AORTA oud	AORTA.ALG.p1000: Patiëntgegevens worden steeds bij het bronsysteem opgevraagd.

ID	VZVZ.GEN.P140
Toepassingsgebied	Generiek

ID	VZVZ.GEN.P140
Stelling	We hanteren de FAIR data uitgangspunten binnen wettelijke kaders
Beschrijving	The FAIR Guiding Principles To be Findable: • F1. (meta)data are assigned a globally unique and persistent identifier • F2. data are described with rich metadata (defined by R1 below) • F3. metadata clearly and explicitly include the identifier of the data it describes • F4. (meta)data are registered or indexed in a searchable resource • Uiteraard rekening houdend met AVG, wet en regelgeving (conform toestemming e.d.) To be Accessible: • A1. (meta)data are retrievable by their identifier using a standardized communications protocol • A1.1 the protocol is open, free, and universally implementable • A1.2 the protocol allows for an authentication and authorization procedure, where necessary • A2. metadata are accessible, even when the data are no longer available • Uiteraard rekening houdend met WGBO het recht vergeten te worden. To be Interoperable: • I1. (meta)data use a formal, accessible, shared, and broadly applicable language for knowledge representation. • I2. (meta)data use vocabularies that follow FAIR principles • I3. (meta)data include qualified references to other (meta)data To be Reusable: • R1. meta(data) are richly described with a plurality of accurate and relevant attributes • R1.1. (meta)data are released with a clear and accessible data usage license • R1.2. (meta)data are associated with detailed provenance • R1.3. (meta)data meet domain-relevant community standards Bron: The FAIR Guiding Principles for scientific data management and stewardship⁴
Rationale	
Implicaties	

4. [https://openaccess.leidenuniv.nl/bitstream/handle/1887/46904/ScientificData3\(2016\)160018.pdf?sequence=1](https://openaccess.leidenuniv.nl/bitstream/handle/1887/46904/ScientificData3(2016)160018.pdf?sequence=1)

ID	VZVZ.GEN.P140
Mapping VZVZ Manifest	9 Transparant
Mapping DIZRA	• Data wordt enkelvoudig geregistreerd bij de bron en vervolgens beschikbaar gesteld voor meervoudig gebruik in verschillende toepassingen. Hiervoor hanteert het informatiestelsel de FAIR-data principes. • BP6 Vindbaar en toegankelijk: "mijn gegevens zijn eenvoudig te vinden en te hergebruiken."
Mapping Visie samenhang	• Informatie (zorginhoudelijk, administratief, kwaliteit en proces) is binnen wettelijke kaders beschikbaar voor alle betrokkenen en wordt daarmee zorgbreed (her)gebruikt;
Mapping AORTA oud	

ID	VZVZ.GEN.P150
Toepassingsgebied	Generiek
Stelling	Privacy by design & Zero Trust (never trust, always verify)
Beschrijving	

ID	VZVZ.GEN.P150
Rationale	Er wordt gewerkt conform de gebruikelijke principes van privacy en security by design. O.a: Privacy • Proactive not reactive – hier gaat om maatregelen om te voorkomen dat de privacy van mensen wordt geschonden. • Privacy as the default setting – individuen hoeven geen actie te ondernemen om hun privacy te beschermen, privacy is ingebouwd in de software. • Privacy embedded into design – privacy wordt een essentieel deel van de kernfunctionaliteiten. • Full functionality – valse tegenstelling zoals security vs. privacy of functionaliteit vs privacy vermijden. • Transparantie & recht op informatie – De applicaties waar een organisatie gebruik van maakt moet conform zijn aan het niveau van privacy en security dat door de organisatie wordt gehanteerd. • Respect for User Privacy – de privacy van het individu is overal in het ontwerp van de software op de voorgrond aanwezig. • End-to-end encryption • Autorisaties tot gegevensverzamelingen worden nauwlettend volgens de geldende privacy normen ingesteld. Beveiligingsprincipes • Minimaliseer het aanvalsoppervlak • Stel veilige standaardwaarden vast • Principe van het minste voorrecht • Verdedigingsprincipe • Veilig falen • Vertrouw geen services Scheiding van taken • Vermijd beveiliging door onduidelijkheid • Houd beveiliging eenvoudig • Beveiligingsproblemen correct oplossen Zero Trust • Devices mogen standaard niet worden vertrouwd, zelfs als ze zijn verbonden met een geautoriseerd netwerk zoals een bedrijfs-LAN en zelfs als ze eerder zijn geverifieerd • Continue verificatie. Controleer altijd de toegang tot alle bronnen. • Minimaliseer de impact als er een externe of interne inbreuk plaatsvindt. • Automatiseer het verzamelen en reageren van context. Neem gedragsgegevens op en haal context uit de hele IT-stack (identiteit, eindpunt, werklast, enz.) voor de meest nauwkeurige reactie
Implicaties	

ID	VZVZ.GEN.P150
Mapping VZVZ Manifest	• 10. Veilig
Mapping DIZRA	• BP4 Vertrouwen: “ik kan er op vertrouwen dat mijn gegevens de juiste zorg krijgen”. • AP7 Verantwoord gebruik: “we dragen zorg voor de bescherming van persoonsgegevens”.
Mapping Visie samenhang	• Er wordt gewerkt conform de principes van privacy en security by design, autorisaties tot gegevensverzamelingen worden nauwlettend volgens de geldende privacy normen ingesteld.
Mapping AORTA oud	

ID	VZVZ.GEN.P160
Toepassingsgebied	Generiek
Stelling	Stelsel en voorzieningen leggen alleen eisen op die noodzakelijk zijn voor veilige uitwisseling van gegevens op basis van gezamenlijk vastgestelde open standaarden,
Beschrijving	
Rationale	Zorgverleners werken met diverse zorginformatiesystemen die zij afnemen van verschillende marktpartijen. Stelsels zijn bedoeld om de uitwisseling van patiëntgegevens tussen deze systemen te faciliteren met behoud van marktwerking. Daarom moeten eisen aan de systemen waartussen gegevens worden uitgewisseld zoveel mogelijk worden beperkt tot het strikt noodzakelijke en gebaseerd op internationale standaarden om te komen tot: gestandaardiseerde uitwisseling van gegevens; • adequate beveiliging van de uitwisselingsinfrastructuur als geheel; • functioneren van de uitwisselingsinfrastructuur als geheel, bijvoorbeeld wat betreft beschikbaarheid.

ID	VZVZ.GEN.P160
Implicaties	We gebruiken zoveel mogelijk internationale standaarden, deze prefereren boven nationale standaarden maar erkennen dat nationale uitbreidingen of beperkingen soms nodig en nuttig kunnen zijn
Mapping VZVZ Manifest	• 7 Op alle lagen
Mapping DIZRA	• Het informatiestelsel hanteert een gelijk speelveld voor alle leveranciers. Afspraken worden gemaakt over het gebruik van standaarden, niet over het gebruik van een product of dienst. Iedere organisatie kiest haar eigen leveranciers voor het implementeren van de standaarden. • Semantische en technische interoperabiliteit wordt in het informatiestelsel gerealiseerd door te kiezen voor open internationale standaarden. Iedere deelnemer aan het stelsel moet voldoen aan de standaarden die zijn afgesproken. • AP21 Internationale standaarden: "we maken gebruik van open standaarden, internationaal boven nationaal".
Mapping Visie samenhang	De (zorg)informatiesystemen kunnen eenvoudig aansluiten op basis van gezamenlijk vastgestelde open standaarden en koppelvlakken. Er worden (nationale extensies van) internationale standaarden gebruikt. Data wordt onafhankelijk van applicaties opgeslagen en beheerd, met procesondersteuning gebaseerd op bij voorkeur (wettelijk) verplicht gestelde open standaarden. In een gelijkwaardig speelveld met open interfaces (eventueel op basis van open source) kunnen verschillende ICT-leveranciers en data-organisaties (versneld) diensten ontwikkelen, waardoor de belangen van betrokken partijen goed tot hun recht komen. Voor aangesloten partijen zijn alle mogelijkheden aanwezig om zelfstandig te innoveren en beschikbare kennis, expertise en technologieën te benutten. De markt kan haar werk doen; • Er wordt gebruik gemaakt van (nationale extensies van) internationale standaarden;
Mapping AORTA oud	AORTA.ALG.p1010: aan aangesloten zorgsystemen worden uitsluitend eisen gesteld die noodzakelijk zijn voor veilige gestandaardiseerde uitwisseling van gegevens.

ID	VZVZ.GEN.P170
Toepassingsgebied	Generiek
Stelling	Gebruikers (of hun vertegenwoordigers) zijn middels de governance medeverantwoordelijk voor het beheer en de doorontwikkeling van de voorzieningen
Beschrijving	
Rationale	om besluiten te nemen voor ontwikkeling en beheer
Implicaties	• Beheerspartijen en leveranciers van de in de gegevensuitwisseling betrokken informatiesystemen werken proactief samen om beheersproblemen te voorkomen en lossen de problemen primair onderling op maar kunnen problemen escaleren naar een regie-voerende partij. • Beheerpartijen van de in de gegevensuitwisseling betrokken informatiesystemen maken afspraken over de beschikbaarheid.
Mapping VZVZ Manifest	5 Samen
Mapping DIZRA	In het informatiestelsel wordt federatief samengewerkt aan afspraken voor data en voor diensten. Iedereen implementeert deze afspraken en is aanspreekbaar op het nakomen van de afspraken en de kwaliteit van de implementatie. AP4 Federatief: “we ontwikkelen en beheren het informatiestelsel gezamenlijk”.
Mapping Visie samenhang	Gebruikers (of hun vertegenwoordigers) zijn middels de governance medeverantwoordelijk voor de doorontwikkeling van de voorzieningen ;
Mapping AORTA oud	N.A.

ID	VZVZ.GEN.P180
Toepassingsgebied	Generiek

ID	VZVZ.GEN.P180
Stelling	Open speelveld en keuzevrijheid
Beschrijving	Afspraken worden gemaakt over het gebruik van standaarden, niet over het gebruik van een product of dienst. Iedere organisatie kiest haar eigen leveranciers voor het implementeren van de standaarden.
Rationale	
Implicaties	
Mapping VZVZ Manifest	8 Keuzevrijheid
Mapping DIZRA	Het informatiestelsel hanteert een gelijk speelveld voor alle leveranciers. Afspraken worden gemaakt over het gebruik van standaarden, niet over het gebruik van een product of dienst. Iedere organisatie kiest haar eigen leveranciers voor het implementeren van de standaarden
Mapping Visie samenhang	In een gelijkwaardig speelveld met open interfaces (eventueel op basis van open source) kunnen verschillende ICT-leveranciers en data-organisaties (versneld) diensten ontwikkelen, waardoor de belangen van betrokken partijen goed tot hun recht komen. Voor aangesloten partijen zijn alle mogelijkheden aanwezig om zelfstandig te innoveren en beschikbare kennis, expertise en technologieën te benutten. De markt kan haar werk doen;
Mapping AORTA oud	N.A.

ID	VZVZ.GEN.P190
Toepassingsgebied	Generiek

ID	VZVZ.GEN.P190
Stelling	Semantische vertalingen vallen onder de MDR (Medical Device Regulation) verordening, technische transformaties niet. VZVZ voert daarom geen semantische vertalingen uit.
Beschrijving	Technische transformaties zijn iets anders dan semantische transformatie. Er kan pas worden gesproken van semantische transformatie als de betekenis van de gegevens bij het interpreteren door een gebruiker (zorgverlener) anders is geworden door een uitgevoerde transformatie. Technische transformaties dienen het doel om gegevensuitwisseling mogelijk te maken tussen systemen die verschillende (versies van) standaarden hanteren. Bij een technische transformatie wordt de semantiek van de informatie niet geraakt. Er moet dus anders worden omgegaan met semantische transformaties dan met technische transformaties. Dit volgt uit o.a. Europese richtlijnen. Uit Qualification and classification of software - Regulation (EU) 2017/745 and Regulation (EU) 2017/746 m.b.t. de MDR volgt dat: De software medische informatie moet creëren of modificeren met een medisch doel anders dan de representatie van data aanpassen voor compatibiliteitsdoeleinden om de MDR van toepassing te kunnen verklaren. Software voor zoeken (dossier ophalen via match op metadata) en/of het ophalen/vragen van informatie niet onder de MDR verordening valt. Zie ook de NEN-7503-2022 m.b.t. MDR
Rationale	Semantische transformaties kunnen de betekenis bij interpretatie door de gebruiker van de opgevraagde gegevens veranderen. Bij technische transformatie verandert de betekenis van de opgevraagde gegevens niet.
Implicaties	Technische transformaties om de gegevensuitwisseling tot stand te brengen kennen een ander kader dan semantische transformaties, dat heeft gevolgen voor de technische omgang met die gegevens. Er is een tussenvorm waarin er door een technische vertaling informatie wegvalt doordat de standaard waar naar omgezet wordt geen ruimte biedt waarin die gegevens (al dan niet één-op-één) kunnen worden overgenomen. Daar moeten we zorgvuldig mee omgaan.
Mapping VZVZ Manifest	N.A.

ID	VZVZ.GEN.P190
Mapping DIZRA	Semantische en technische interoperabiliteit wordt in het informatiestelsel gerealiseerd door te kiezen voor open internationale standaarden. Iedere deelnemer aan het stelsel moet voldoen aan de standaarden die zijn afgesproken AP14 Een gemeenschappelijk vocabulaire: “onze gegevens zijn uitwisselbaar met een gemeenschappelijk vocabulaire zodat we elkaar kunnen begrijpen”. AP20 Taal los van transport: “we maken onderscheid tussen taal en transport en koppelen dat los van elkaar”.
Mapping Visie samenhang	N.A.
Mapping AORTA oud	N.A.

3.2 AORTA Principes

ID	VZVZ.AORTA.P1000
Toepassingsgebied	AORTA
Stelling	Het is voor de burger transparant welke gegevens tussen welke zorgaanbieders is uitgewisseld
Beschrijving	Burgers hebben achteraf inzicht in welke gegevens zijn uitgewisseld. Daarbij wordt inzichtelijk tussen welke zorgaanbieders de gegevens zijn uitgewisseld. Er wordt expliciet niet transparant welke zorgverlener(s) betrokken was (waren) bij de uitwisseling. Het is de verantwoordelijkheid van de zorgaanbieder om een patiënt inzage te geven in de loggegevens van de betrokken zorgverleners.
Rationale	
Implicaties	

ID	VZVZ.AORTA.P1000
Mapping VZVZ Manifest	9 Transparant
Mapping DIZRA	In het informatiestelsel hebben burgers regie op hun eigen gezondheidsdata en kunnen deze data meenemen en delen in hun reis door het zorglandschap en in het netwerk van zorgverleners en ondersteuners dat zich rondom hen vormt. AP12 Regie over gegevens: “we stellen patiënten, cliënten en burgers in staat om controle en regie te nemen over hun gegevens”
Mapping Visie samenhang	Informatie (zorginhoudelijk, administratief, kwaliteit en proces) is binnen wettelijke kaders beschikbaar voor alle betrokkenen en wordt daarmee zorgbreed (her)gebruikt;
Mapping AORTA oud	AORTA.ALG.p1050: patiënten hebben via AORTA toegang tot hun eigen gegevens. AORTA.ALG.p1060: toegang tot patiëntgegevens wordt vastgelegd en is hierdoor traceerbaar.

ID	VZVZ.AORTA.P1100
Toepassingsgebied	AORTA
Stelling	AORTA kent een modulaire architectuur
Beschrijving	Gebruik van voor-gedefinieerde, herbruikbare bouwstenen
Rationale	Gebruik van voor-gedefinieerde, herbruikbare bouwstenen vereenvoudigt het ontwerpen van uitwisselingen voor nieuwe zorgtoepassingen. Het bespaart (ontwikkel-) inspanning en –kosten en verkort de doorlooptijd van nieuwe toepassingen. De complexiteit voor XIS-leveranciers die meerdere zorgtoepassingen implementeren in hun software wordt hiermee gereduceerd.
Implicaties	
Mapping VZVZ Manifest	

ID	VZVZ.AORTA.P1100
Mapping DIZRA	Het informatiestelsel is duurzaam doordat het relevant is en blijft. Het omarmt voor nu en in de toekomst de complexiteit van meerdere standaarden in een stelsel waarin verandering en innovatie welkom is.
Mapping Visie samenhang	Het stelsel van zorginfrastructuren omvat (ook) voorzieningen en gegevensdiensten, welke voor algemeen gebruik beschikbaar zijn en op basis van keuzevrijheid kunnen worden gebruikt.
Mapping AORTA oud	AORTA.ALG.p1070: De AORTA architectuur ondersteunt informatie-uitwisseling via berichten met informatie opgenomen in voorgedefinieerde, herbruikbare bouwstenen

4 Architectuurvisie AORTA

4.1 Ontwikkelingen

- Opkomst/ontwikkeling van meerdere landelijke/regionale/leverancier specifieke zorginfrastructuren in Nederland, naast AORTA. Informatie die uitgewisseld wordt in/binnen de ene zorginfrastructuur kan relevant zijn voor toepassingen die in een andere zorginfrastructuur. Daarom ziet VZVZ de noodzaak om AORTA te kunnen koppelen op andere zorginfrastructuren, bij voorkeur via het Twiin afsprakenstelsel. Een uitdaging hierbij is dat het verschil in (implementatie van het) beveiligings-/vertrouwensniveau met AORTA overbrugt dient te worden.
- Ontwikkelingen in de AORTA-architectuur duren vaak lang omdat de lat voor veilige uitwisseling in het stelsel hoog is gelegd. Naast dit bestaande 'spoor' moet AORTA ook een spoor kunnen bieden waar ontwikkelingen kort cyclisch gedaan kunnen worden en er sneller meerwaarde aan de eindgebruiker geboden kan worden.
- Landelijke normeringen op verschillende aspecten gaan deels dicteren hoe AORTA moet werken en/of geïmplementeerd moet worden:
 - Duurzaam Informatiestelsel in de Zorg Referentie Architectuur (DIZRA). Afsprakenstelsels en andere bouwstenen die onderdeel willen zijn van het duurzame informatiestelsel in de zorg dienen te voldoen aan DIZRA.
 - Vanuit de [Wet elektronische gegevensuitwisseling in de zorg \(Wegiz\)](#) worden er [verschillende NEN-normen opgesteld waaraan bepaalde informatie-uitwisselingen in de zorg aan moeten voldoen](#). Onder andere zal dit gaan gelden voor toestemming, identificatie & authenticatie en lokalisatie van patiëntgegevens.
- Verandering van het IT-landschap van meer monolithische systemen naar een open IT-platform

Om de ontwikkelingen te kunnen volgen dient AORTA het volgende te gaan ondersteunen:

4.2 Hybride (bimodal) besturingsvormen

- Hybride besturingsvormen [kunnen](#) elke op hun eigen manier [informatie- en technologie-intensieve diensten leveren](#):
 - Modus 1 is traditioneel en legt de nadruk op veiligheid en nauwkeurigheid
 - Modus 2 is verkennend en legt de nadruk op wendbaarheid en snelheid

Modus 1		Modus 2
Betrouwbaarheid	Doel	Wendbaarheid
Goede prijs, hoge performance	Klantwaarde	Optimale klantbeleving, nieuwe features

Waterval, projectmanagement, Lean	Aanpak	Agile, Lean, Scrum, DevOps
Plan- en mandaat gedreven	Governance	Empirisch, continue proces georiënteerd
Lange termijn contracten, grote leveranciers, structurele financiering	Sourcing	Innovatieve leveranciers, nieuwe toetreders, korte termijn contracten, stimuleren met tijdelijke subsidies
Gericht op standaardisatie, project gedreven, zekerheidzoekend	Competentie medewerkers	Gericht op vernieuwing, kunnen omgaan met onzekerheden
IT centraal, klant op afstand	Cultuur kenmerk	Klant centraal, gericht op functionaliteit en klantwaarde
Lang, maanden	Cyclustijd	Kort, dagen, weken

- Deze hybride besturing vraagt om een verbindend afsprakenstelsel waarmee beide modi naast elkaar kunnen werken (en samenwerken). Hierin moet komen te staan
 - Hoe modus 2 met modus 1 kan communiceren
 - Hoe in modus 2 ontwikkelde toepassing naar modus 1 kan worden overgebracht
 - Hoe beide modi tegelijk kunnen werken en ieder een eigen governance hebben
 - Hoe modus 1 zich toch ook toekomstvast kan blijven vernieuwen
- Het koppelen van andere zorginfrastructuren aan AORTA moet via modus 2
 - Dit vraagt om de introductie van zorgservices; generieke functionaliteit die los van het LSP te gebruiken is

4.3 Zorgservices

Een 'zorgservice' levert generieke functionaliteit, gerealiseerd door software, die locatie onafhankelijk is (in het XIS of hierbuiten). Voorbeelden van zorgservices zouden bijvoorbeeld kunnen zijn: lokaliseren van patiëntgegevens, autoriseren, het beheren van toestemming of adressering. Het idee is dat wanneer dit soort generiek functionaliteit los gebruikt / aangeboden kan worden, projecten in modus 2 makkelijker bediend en versneld kunnen worden zonder dat men aan alle implementatie-eisen hoeft te voldoen die nu een samenhangend geheel vormen voor de aansluiting op het LSP/de ZIM. Daarnaast biedt het de mogelijkheid om degelijke generieke diensten los(ser) van elkaar verder te ontwikkelen en implementeren of aan te passen op specifieke behoeftes voor een bepaald project. Mogelijke nadelen van losse generieke functies kunnen zijn de algehele beschikbaarheid en een verhoogde complexiteit van het systeem.

5 Juridische context

In dit hoofdstuk wordt het wettelijk kader besproken; de wetten en normen die voor AORTA relevant zijn. Het wettelijk kader is niet altijd heel concreet, eenduidig en/of compleet. Daarom is er ook een zogenaamd 'vertrouwensmodel' opgesteld. Hierin wordt beschreven hoe invulling gegeven wordt aan de verplichtingen die voortkomen uit het wettelijk kader, waardoor patiënten, zorgaanbieders en andere betrokken partijen vertrouwen kunnen hebben in een veilige en betrouwbare uitwisseling van patiëntgegevens via AORTA. Dit wordt gedaan door afspraken te maken over technische, organisatorische en juridische waarborgen.

De wet- en regelgeving, het vertrouwensmodel tezamen met de missie, visie en de organisatiedoelstellingen van AORTA leiden vervolgens weer tot architectuurprincipes. Architectuurprincipes zijn regels en richtlijnen die richting en structuur geven aan alles aspecten van het ontwerp van AORTA (organisatie, proces, informatie, applicatie en techniek), en daarmee dus restricties aan de ontwerpvrijheid vormen.

5.1 Wettelijk kader

Dit hoofdstuk geeft een overzicht van het wettelijk kader. Uit wet- en regelgeving volgt het kader voor het elektronisch delen van gegevens tussen zorgaanbieders, zorgverleners en met de patiënt. AORTA is in lijn met alle toepasselijke wet- en regelgeving en met alle relevante normen. In dit hoofdstuk is allereerst een overzicht opgenomen van de relevante wet- en regelgeving en normen. Vervolgens wordt de inhoud daarvan kort beschreven.

5.1.1 Overzicht wetgevend kader

De wet- en regelgeving die van toepassing is op gegevensuitwisseling in de zorg is voortdurend in beweging. Tabel 2.1 geeft een overzicht van de wet- en regelgeving die relevant is voor het AORTA Afsprakenstelsel. Deze versie behandelt de wet- en regelgeving die geldt op 1 december 2021. Dit zijn de belangrijkste wetten op het gebied van zorginformatie-uitwisseling:

Wet op de geneeskundige behandelingsovereenkomst https://wetten.overheid.nl/BWBR0005290/2021-07-01#Boek7_Titeldeel7_Afdeling5	WGB O
Wet beroepen individuele gezondheidszorg https://wetten.overheid.nl/BWBR0006251/2021-07-01	Wet BIG
Wet kwaliteit, klachten en geschillen zorg De wet vervangt de wetten Kwaliteitswet Zorginstellingen en de Wet klachtrecht cliënten zorgsector https://wetten.overheid.nl/BWBR0037173/2021-07-01	Wkk gz

Algemene verordening gegevensbescherming Deze Europese verordening vervangt sinds 25 mei 2018 de Richtlijn bescherming persoonsgegevens en de Wet bescherming persoonsgegevens (Wbp) en bevat onder meer de meldplicht datalekken (voorheen de Wet meldplicht datalekken) https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=celex%3A32016R0679	AVG
Uitvoeringswet Algemene verordening gegevensbescherming Implementatiewetgeving die de normen in de AVG voor Nederland nader invult https://wetten.overheid.nl/BWBR0040940/2020-01-01	UAV G
Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg Deze wet vervangt sinds 1 juli 2017 de Wbsn-z (Wet gebruik Burgerservicenummer in de zorg). De Wet Cliëntenrechten is opgenomen in hoofdstuk 3a van de Wabvpz. https://wetten.overheid.nl/BWBR0023864/2020-07-01	Wab vpz
Besluit elektronische gegevensverwerking door zorgaanbieders Dit besluit van 10 november 2017, beschrijft nadere regels over functionele, technische en organisatorische maatregelen bij elektronische gegevensverwerking door en tussen zorgaanbieders https://wetten.overheid.nl/BWBR0040238/2020-10-01	Begz

5.1.2 De Wet op de geneeskundige behandelovereenkomst (WGBO)

Deze wet bevat onder andere het recht van de patiënt op inzage in en afschrift van het eigen dossier, een verklaring aan het dossier toe te voegen en gegevens uit het dossier te laten vernietigen. Deze wet verplicht de zorgverlener zich te houden aan de professionele standaard en de kwaliteitsstandaarden, te voldoen aan de informatieplicht richting de patiënt en aan de dossierplicht. Ook bevat deze wet regels over de vertegenwoordiging van de patiënt.

De zorgverlener is op basis van deze wet gebonden aan het medische beroepsgeheim. Uit het beroepsgeheim volgt onder andere dat aan anderen dan de patiënt geen inlichtingen over de patiënt dan wel inzage in of afschrift van de gegevens uit het dossier worden verstrekt dan met toestemming van de patiënt. Een uitzondering geldt voor degenen die rechtstreeks betrokken zijn bij de uitvoering van de behandelingsovereenkomst en degene die optreedt als vervanger van de zorgverlener, tenminste voor zover noodzakelijk voor de door hen in dat kader te verrichten werkzaamheden.

De zorgverlener is verplicht de patiënt naar redelijkheid te informeren en toestemming voor een behandeling te vragen. De patiënt is verplicht de zorgverlener correct en zo volledig mogelijk te informeren.

Voor iedere geneeskundige behandeling is mondelinge of schriftelijke toestemming van de patiënt vereist (informed consent). Zonder deze toestemming kan de hulpverlener geen behandeling starten, voortzetten en mag hij medische informatie niet met een andere zorgverlener delen. Deze toestemming kan ook impliciet of stilzwijgend plaatsvinden. Bij een minder ingrijpende of noodzakelijke verrichting zal dit eerder zo zijn dan bij een ingrijpende, riskante of electieve behandeling. In dat laatste geval moet de patiënt in ieder geval expliciet instemmen met de behandeling en wordt dit ook door de arts in het dossier vastgelegd. In bepaalde situaties moet acuut worden ingegrepen en kan op toestemming van de patiënt of zijn vertegenwoordiger niet worden

gewacht. Ook hiervoor geeft de WGBO een basis. Behandeling zonder toestemming is mogelijk indien 'onverwijld uitvoering van de verrichting nodig is teneinde ernstig nadeel voor de patiënt te voorkomen'.

5.1.3 Wet beroepen individuele gezondheidszorg (Wet BIG)

De Wet BIG heeft als doel om de kwaliteit van de beroepsuitoefening te bevorderen en te bewaken en de patiënt te beschermen tegen ondeskundig en onzorgvuldig handelen door beroepsbeoefenaren.⁴³ De wet spitst zich toe op de individuele gezondheidszorg, dat wil zeggen zorg die rechtstreeks is gericht op een persoon.

Beroepsbeoefenaren

De Wet BIG bevat een systeem van titelbescherming voor een beperkt aantal beroepsgroepen. Wie een wettelijk geregeld beroep uitoefent, mag een publiekrechtelijk beschermde beroeps- of opleidingstitel voeren. Om te worden aangemerkt als een beroepsbeoefenaar in de zin van de Wet BIG moet worden voldaan aan een aantal wettelijke eisen. De belangrijkste daarvan hebben betrekking op de opleiding. Door een beschermde titel te voeren is voor derden duidelijk op welk gebied een bepaalde beroepsbeoefenaar deskundig is.

Het systeem van titelbescherming in de Wet BIG is voor de landelijke infrastructuur van belang omdat alleen beroepsbeoefenaars en door hen gemandateerde medewerkers hiertoe toegang kunnen krijgen.

Een beroep kan op twee manieren wettelijk worden geregeld. Er is een 'zware' regeling bij wet (artikel 3 Wet BIG) en een 'lichte' regeling bij algemene maatregel van bestuur (artikel 34 Wet BIG). Bij wet worden acht beroepen geregeld, te weten: arts, tandarts, apotheker, gezondheidszorgpsycholoog, psychotherapeut, fysiotherapeut, verloskundige en verpleegkundige.

Voor elk van de genoemde beroepen stelt de rijksoverheid registers in. Het gaat hier om een zogeheten constitutieve registratie. Die komt erop neer dat alleen geregistreerde personen de beroepstitel mogen voeren en dat alleen zij vallen onder het tuchtrecht.

Ook derden kunnen op verzoek informatie krijgen uit het register. Zij kunnen dus nagaan of een beroepsbeoefenaar met recht een beschermde beroepstitel voert en of er mogelijk sprake is van beperkende voorwaarden op het punt van de beroepsuitoefening.

De 'lichte' regeling bij algemene maatregel van bestuur is voornamelijk bedoeld voor de paramedische beroepen. Voorbeelden zijn: de diëtist, de logopedist en de mondhygiënist. In de algemene maatregel van bestuur wordt het deskundigheidsgebied omschreven en de opleiding geregeld. Wie aan de gestelde eisen voldoet heeft het recht een opleidingstitel te voeren. De overheid houdt voor deze beroepsgroepen geen register bij. In de praktijk worden dergelijke registers veelal wel bijgehouden door de beroepsgroepen.

Tuchtrecht

Voor de acht bij wet geregelde beroepen voorziet de Wet BIG in tuchtrechtspraak.

Deze dient voor het bevorderen en bewaken van de kwaliteit van de beroepsuitoefening.

De Wet BIG geeft twee tuchtnormen.⁴⁴ De eerste heeft betrekking op zorgvuldigheid bij het verlenen van zorg van de geregistreerde beroepsbeoefenaar ten opzichte van de patiënt. De tweede norm geldt voor alle andere gedragingen die strijdig zijn met het belang van een goede uitoefening van de

individuele gezondheidszorg, waaronder mede enig handelen of nalaten in strijd met hetgeen bij of krachtens de artikelen 13h en 13hb van de Kaderwet is bepaald.⁴⁵ Tuchtrect, strafrect en burgerlijk rect kunnen overigens tegelijkertijd worden toegepast.

Als een tuchtcollege een klacht gegrond acht, volgt er altijd een maatregel. Schuldigverklaring zonder strafoplegging is niet mogelijk. Op grond van artikel 48 Wet BIG kunnen verschillende tuchtrechtelijke maatregelen worden opgelegd. Opklimmend naar zwaarte zijn dat:

- waarschuwing;
- berisping;
- geldboete van ten hoogste € 4500;
- schorsing van de inschrijving in het register voor ten hoogste één jaar;
- gedeeltelijke ontzegging van de bevoegdheid het beroep uit te oefenen onder het voeren van de titel;
- doorhaling van de inschrijving in het register.

Wie zijn of haar inschrijving heeft verloren bij wijze van tuchtrechtelijke maatregel, kan niet opnieuw in het register worden opgenomen en niet meer de wettelijk beschermde titel voeren. Voor artsen, tandartsen en verloskundigen betekent dit tevens dat zij niet langer bevoegd zijn om zelfstandig voorbehouden handelingen te verrichten. De waarschuwing, berisping en geldboete leiden niet tot een beperking van de beroepsuitoefening.

Strafbepalingen

De Wet BIG kent naast tuchtrechtelijke maatregelen ook strafbepalingen.⁴⁶ Die bepalingen gelden voor iedereen die bepaalde in de wet opgenomen verboden of verplichtingen niet nakomt. Dat kunnen behalve beoefenaren van wettelijk geregelde beroepen ook anderen zijn die beroepsmatig handelen. Er worden drie straffen genoemd, te weten: hechtenis, geldboete en ontzetting uit het beroep.

5.1.4 Wet kwaliteit, klachten en geschillen in de zorg (Wkkgz)

De Wkkgz legt vast wat goede zorg precies inhoudt. Op basis van deze wet is de zorgaanbieder als instelling gehouden om te zorgen voor “zodanige toedeling van verantwoordelijkheden, bevoegdheden alsmede afstemmings- en verantwoordingsplichten, dat een en ander redelijkerwijs moet leiden tot het verlenen van goede zorg.”

Ook bepaalt de Wkkgz wat er moet gebeuren als patiënten een klacht hebben over de zorg. Op basis van de Wkkgz kunnen patiënten terecht bij de klachtenfunctionaris van de zorgaanbieder. Daarnaast biedt de wet ook een laagdrempelig alternatief: de onafhankelijke geschilleninstantie. Die doet een uitspraak waar beide partijen zich aan moeten houden. De geschilleninstantie kan ook een schadevergoeding toekennen tot EUR 25.000,-.

De Wkkgz bepaalt dat zorgaanbieders een interne werkwijze moeten hebben zodat medewerkers veilig incidenten kunnen melden.

5.1.5 Algemene verordening gegevensbescherming (AVG)

De AVG is een Europese wet die rechtstreekse werking heeft in de hele Europese Unie. De AVG regelt onder welke voorwaarden persoonsgegevens verwerkt mogen worden binnen de EU.

Persoonsgegevens ziet op alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Deze wordt in de AVG de 'betrokkene' genoemd. Onder 'verwerking van gegevens', valt: verzamelen, vastleggen, ordenen, bewaren, bewerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, evenals het afschermen, uitwissen of vernietigen van gegevens.

In de oude wet, de Wbp was sprake van een 'bewerker' en een 'bewerkersovereenkomst'. Onder de AVG is dat 'verwerker' en 'verwerkersovereenkomst' geworden.

5.1.5.1 Grondslag en doel

De AVG bepaalt dat dit slechts is toegestaan als sprake is van een rechtmatige grondslag. De AVG noemt zes grondslagen voor verwerking:

1. toestemming van de betrokkene
2. uitvoeren van een overeenkomst
3. wettelijke verplichting
4. vitaal belang van de betrokkene of een andere natuurlijke persoon
5. uitvoeren van een publiekrechtelijke taak
6. gerechtvaardigd belang van de verwerkingsverantwoordelijke of van een derde

De grondslag voor de verwerking kan verschillen per zorgtoepassing en per gegevensuitwisseling.

Bovendien mogen persoonsgegevens op basis van het proportionaliteitsbeginsel enkel worden verwerkt voor zover dat nodig is voor welbepaalde doeleinden.

Daarbij geldt een verbod om bijzondere categorieën van persoonsgegevens te verwerken, waaronder gegevens over gezondheid, genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon en gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid. Op dit verbod zijn een beperkt aantal uitzonderingen van toepassing. Eén van die uitzonderingen is dat de verwerking noodzakelijk is voor het verstrekken van gezondheidszorg.

De verwerkingsverantwoordelijke is verplicht om betrokkenen goed te informeren over de verwerking van hun gegevens en over hun privacy-rechten op basis van de AVG, waaronder het recht op inzage, rectificatie, vergetelheid, beperking, dataportabiliteit en bezwaar. Uit deze rechten volgt dat de verwerkingsverantwoordelijke inzichtelijk moet hebben welke persoonsgegevens hij verwerkt, waar deze zich bevinden en hoe deze definitief verwijderd kunnen worden.

5.1.5.2 Verwerkersovereenkomst

De AVG verplicht de verwerkingsverantwoordelijke een verwerkersovereenkomst te sluiten met iedere verwerker. De AVG bepaalt ook dat de verwerkersovereenkomst aan een aantal eisen moet voldoen. In die overeenkomst moet onder andere worden bepaald wat de aard en het doel is van de verwerking, de duur van de verwerking en het soort persoonsgegevens en de categorieën van betrokkenen. Een verwerker is niet zelfstandig verantwoordelijk voor de verwerking van de persoonsgegevens, maar heeft wel een aantal afgeleide verplichtingen voor onder meer beveiliging en geheimhouding van de gegevens. De verwerkersovereenkomst moet er onder andere voor zorgen dat verwerker voldoende waarborgen biedt ten aanzien van de technische- en organisatorische beveiligingsmaatregelen met

betrekking tot de verwerking van de aan hem ter beschikking gestelde persoonsgegevens. De Brancheorganisaties Zorg hebben een model verwerkersovereenkomst opgesteld die voldoet aan de eisen van de AVG, te vinden via: https://www.brancheorganisatieszorg.nl/nieuws_list/modelverwerkersovereenkomst-voor-de-zorgsector/

5.1.5.3 Data protection impact assessment (DPIA)

De AVG verplicht om een data protection impact assessment (DPIA) uit te voeren als een gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert voor de mensen van wie de organisatie gegevens verwerkt. Een DPIA is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen. En om daarna maatregelen te kunnen nemen om de risico's te verkleinen.

Zie voor actuele informatie <https://www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia?qa=PIA>

5.1.5.4 UAVG - Uitvoeringswet Algemene verordening gegevensbescherming

De UAVG geeft een nadere invulling voor de toepassing van de AVG binnen Nederland. Daar waar de AVG ruimte laat voor nationale regelingen of soms opdraagt tot het treffen van een regeling, komt de UAVG in beeld.

De UAVG bepaalt dat de uitzondering op het verwerkingsverbod van gezondheidsgegevens voor het verstrekken van gezondheidszorg enkel geldt voor hulpverleners, instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening en enkel voor zover de verwerking noodzakelijk is met het oog op een goede behandeling of verzorging van de betrokkene dan wel het beheer van de betreffende instelling of beroepspraktijk (artikel 30 lid 3 UAVG).

De Uitvoeringswet AVG regelt dat het BSN alleen mag worden gebruikt bij de verwerking van persoonsgegevens ter uitvoering van de desbetreffende wet dan wel voor doeleinden bij de wet bepaald (art 46 UAVG).

In de UAVG is uitgewerkt dat minderjarigen vanaf 16 jaar zelfstandig beslissen over de verwerking van hun persoonsgegevens (artikel 5 UAVG).

De UAVG wijst de Autoriteit Persoonsgegevens aan als de toezichthouder voor de AVG die handhavend kan optreden.

5.1.6 Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz)

5.1.6.1 Het gebruik van het BSN

De Wabvpz bevat verplichtingen over het gebruik van het BSN. Om patiënten in de zorg op een betrouwbare manier te kunnen identificeren, moeten zorgaanbieders, indicatieorganen en zorgverzekeraars het BSN verplicht gebruiken in hun administratie en bij de onderlinge communicatie over patiënten. Om geen twijfel te laten bestaan over de correctheid van het BSN worden er twee acties uitgevoerd: BSN-verificatie en BSN-validatie.

5.1.6.1.1 BSN-verificatie

Bij de BSN-verificatie verifieert de zorgaanbieder dat bepaalde persoonskenmerken, waaronder naam, geslacht en geboortedatum), bij een BSN horen. Als persoonskenmerken en BSN bij elkaar horen, spreken we van een 'geverifieerd BSN'.

Voor de verificatie gebruikt de zorgaanbieder de interfaces van de SBV-Z (Sectorale Berichten Voorziening in de Zorg) die zorgen voor de ontsluiting van het BSN register en het Registratie Niet-ingezetenen.

5.1.6.1.2 BSN-validatie

Zodra de nieuwe patiënt voor het eerst in het ziekenhuis komt, wordt aan de hand van een geldig Wettig Identiteits Document (WID: paspoort, rijbewijs, ID-kaart) gecontroleerd of de persoon voor de balie inderdaad degene is die is- of wordt ingeschreven in het EPD. Hierdoor is vanaf dat moment sprake van een 'gevalideerd BSN'.

Optioneel is het ook mogelijk de geldigheid van het identiteitsbewijs elektronisch te laten controleren m.b.v. een (tweede) koppeling met het SVB-Z voor de WID-controle. Dit kan men bijvoorbeeld doen als er twijfels zijn aan de geldigheid van het identiteitsbewijs. Om een BSN te valideren is deze controle stap echter niet vereist en niet alle zorgaanbieders hebben de koppeling in gebruik.

Het kan voorkomen dat het BSN van een patiënt wel bekend is binnen een ziekenhuis-informatiesysteem, maar dat deze nog niet is gevalideerd. Bijvoorbeeld als een patiënt zich nog niet heeft geïdentificeerd met een identiteitsbewijs.

5.1.6.1.3 Gebruik BSN in de praktijk

Voor gebruik van het BSN bij uitwisseling van gegevens tussen verschillende zorgaanbieders, moeten zorgaanbieders aan de volgende regels voldoen:

- Voordat de zorgverlener/zorgaanbieder gegevens van een patiënt mag delen met een andere zorgaanbieder, moet de brondossierhouder een gevalideerd BSN van de patiënt hebben. Dat wil dus zeggen dat de patiënt fysiek in de zorginstelling is geweest en dat de identiteit van de patiënt is vastgesteld aan de hand van een wettig identiteitsdocument. (NB dit staat los van het feit dat de patiënt daarnaast toestemming moet hebben gegeven voor het delen van zijn gegevens).
- Voor het raadplegen en overhalen van gedeelde patiëntgegevens van een andere zorgaanbieder, is het voldoende dat de patiënt in de eigen organisatie bekend is met een geverifieerd BSN. De patiënt hoeft hiervoor dus nog niet fysiek aanwezig geweest te zijn.

In sommige gevallen, zoals bij een spoedverwijzing of een intercollegiaal consult, kan het voorkomen dat de patiënt nog niet bekend is in de zorginstelling die een gegevensopvraging doet. Uitgangspunt is in deze gevallen dat men erop kan vertrouwen dat de zorginstelling die de medische gegevens heeft vastgelegd en aangemeld voor delen buiten de zorginstelling, het BSN heeft geverifieerd.

Het proces van validatie van het BSN in de opvragende zorginstelling blijft bestaan. De eerste keer dat een patiënt daar fysiek aanwezig is, geldt de reguliere validatieprocedure.

5.1.6.2 Elektronisch uitwisselingssysteem

De Wabvpz regelt de voorwaarden voor het gebruik van een elektronisch uitwisselingssysteem. Dit is een systeem waarmee zorgaanbieders op elektronische wijze, dossiers, gedeelten van dossiers of gegevens uit dossiers voor andere zorgaanbieders raadpleegbaar kunnen maken.

De belangrijkste rechten van de patiënt die in de Wabvpz geregeld worden, zijn:

- Het recht op (kosteloos) elektronische inzage in zijn dossier;
- Het recht op een (kosteloos) elektronisch afschrift van zijn dossier;
- Sinds juli 2020: het recht op een (kosteloos) elektronisch overzicht wie bepaalde informatie in een elektronisch uitwisselingssysteem beschikbaar heeft gesteld en op welke datum en wie informatie heeft ingezien of opgevraagd en op welke datum.

De Wabvpz doet geen afbreuk aan de privacy-rechten van betrokken op basis van de AVG.

De belangrijkste plichten van een zorgaanbieder bij (elektronische) gegevensuitwisseling zijn:

- De plicht de patiënt te informeren over zijn rechten bij elektronische gegevensuitwisseling, de wijze waarop hij zijn rechten kan uitoefenen, de werking van het elektronisch uitwisselingssysteem en welke zorgaanbieders zijn aangesloten op het systeem;
- De plicht om zijn patiënt uitdrukkelijke toestemming te vragen voor het beschikbaar stellen van de patiëntgegevens via een elektronisch uitwisselingssysteem;
- De patiënt te informeren als nieuwe categorieën zorgverleners aansluiten bij het elektronisch uitwisselingssysteem;

5.1.6.3 Besluit elektronische gegevensverwerking door zorgaanbieders (Begdz)

De Begdz bepaalt onder andere dat een zorgaanbieder moet zorgen voor een veilig en zorgvuldig gebruik van het zorginformatiesysteem en van het elektronisch uitwisselingssysteem waarop hij is aangesloten, conform NEN 7510 en NEN 7512 en dat de logging voldoet aan NEN 7513.

De Begdz verplicht de verantwoordelijke voor een elektronisch uitwisselingssysteem om te werken met een zorgserviceprovider die is geautoriseerd op basis van overeenkomstig NEN 7512 vastgestelde criteria. Een zorgserviceprovider is een netwerkleverancier van een beveiligde netwerkverbinding tussen een zorginformatiesysteem en een elektronisch uitwisselingssysteem.

Ook verplicht de Begdz de rechtspersoon die een elektronisch uitwisselingssysteem beheert en in stand houdt, om eens in de vijf jaar door middel van een audit te laten vaststellen dat het systeem voldoet aan NEN 7510 en NEN 7512 en daarnaast om te borgen dat de logging van het systeem voldoet aan NEN 7513.

Overigens is de Begdz niet de enige wet die naleving van een NEN norm vereist. De Regeling gebruik burgerservicenummer in de zorg verplicht dat gegevensverwerking van het BSN voldoet aan NEN7510.

5.1.6.4 Normen – NEN 7510, 7512, 7513

Om veilig met elektronische medische gegevens om te gaan heeft het Nederlands Normalisatie-instituut (NEN) een aantal normen ontwikkeld. De eerste norm die is ontwikkeld is de NEN 7510, de norm voor Informatiebeveiliging in de zorg. Deze norm is gebaseerd op de Code voor Informatiebeveiliging, de ISO- 27000-serie. Voor de zorgsector is een aangepaste versie van deze norm opgesteld. De reden hiervoor is dat er zorg-specifieke aandachtspunten zijn, met name het belang van de vertrouwelijkheid en integriteit van persoonlijke gezondheidsinformatie. De NEN 7510 is voor de zorg aangevuld met NEN 7512 vertrouwensbasis voor gegevensuitwisseling en de NEN 7513 logging. Zorgaanbieders zijn verplicht om NEN 7510 toe te passen bij de verwerking van BSN en alledrie de normen bij gebruik van een elektronisch uitwisselingssysteem.

5.1.6.4.1 NEN 7510, informatiebeveiliging in de zorg (NEN 7510:2017)

De NEN 7510 bestaat uit twee onderdelen. NEN 7510-1 beschrijft de eisen voor het vaststellen, implementeren, bijhouden en continu verbeteren van een managementsysteem voor informatiebeveiliging. NEN 7510-2 voorziet in richtlijnen voor zorginstellingen en andere beheerders van persoonlijke gezondheidsinformatie over hoe met het beste de beschikbaarheid, integriteit en vertrouwelijkheid van dergelijke informatie kan beschermen.

5.1.6.4.2 NEN 7512, Vertrouwensbasis voor gegevensuitwisseling (NEN 7512:2015)

In de NEN 7510 is een risicoclassificatie uitgewerkt. In de NEN 7512 zijn voor de verschillende risicoklassen minimale eisen opgesteld ten aanzien van authenticatie en identificatie. De eisen hebben betrekking op:

- De zender (entiteit: persoon, organisatie of de informatiesystemen waarmee de informatie wordt verzonden);
- Het medium;
- De ontvanger.

Het beveiligingsniveau van de gehele keten is bepalend voor de veiligheid waarmee de informatie uitgewisseld wordt.

5.1.6.4.3 NEN 7513, logging (NEN 7513:2018)

Deze norm bepaalt welke gegevens in de logging aanwezig moeten zijn, welke gebeurtenissen moeten worden gelogd, welke gegevens van die gebeurtenissen moeten worden vastgelegd en aan welke kwaliteitseisen het loggen en de logbestanden moeten voldoen. Ook bepaalt de norm hoe lang de logbestanden moeten worden bewaard. Verder biedt de norm houvast aan zorginstellingen en andere beheerders van persoonlijke gezondheidsinformatie over het verstrekken van informatie over wie toegang heeft gehad tot haar of zijn elektronisch patiëntdossier.

}

5.1.7 Wetsvoorstel elektronische gegevensuitwisseling in de zorg (Wegiz)

Dit wetsvoorstel is op 30 april 2021 ingediend bij de Tweede Kamer en is nog in behandeling. Als dit wetsvoorstel wordt aangenomen, zal de wet verplicht stellen om gebruik te maken van een

elektronische infrastructuur voor bij AMvB aangewezen gegevensuitwisselingen. De Wegiz is enkel van toepassing op het uitwisselen van patiëntgegevens tussen zorgaanbieders. De Wegiz is opgezet als een kaderwet. In onderliggende AMvB's zal per gegevensuitwisseling worden vastgelegd aan welke eisen moet worden voldaan. Het gaat primair om eisen ten aanzien van taal en techniek. Deze eisen zullen in NEN-normen worden vastgelegd. De minister zal een meerjarenagenda opstellen voor de Wegiz met daarin een lijst met gegevensuitwisselingen die aangewezen kunnen worden.

5.1.8 Kwaliteitswet zorginstellingen (KWZi)

Zorginstellingen zijn verplicht verantwoorde zorg aan te bieden. Normen hiervoor zijn opgenomen in de Kwaliteitswet zorginstellingen (KWZi). Deze wet is van toepassing op alle instellingen waar in georganiseerd verband zorg wordt aangeboden.⁴⁷

De KWZi bevat een aantal globale normen:

- De zorginstelling moet verantwoorde zorg bieden;
- De zorginstelling moet zorgdragen voor een op die zorg gerichte adequate organisatie;
- De zorginstelling moet zorgdragen voor een systematisch kwaliteitssysteem;
- De zorginstelling dient een kwaliteitsjaarverslag te publiceren;⁴⁸

De Minister van VWS en in dringende gevallen de Inspectie voor de Gezondheidszorg (IGZ) zien toe op de naleving van deze normen.

Het gebruik van de landelijke infrastructuur kan worden beschouwd als onderdeel van het verlenen van verantwoorde zorg in de zin van de KWZi. Bij het gebruik van de landelijke infrastructuur kunnen de normen in de KWZi op uiteenlopende manieren relevant zijn.

5.1.9 Wet klachtrecht cliënten zorgsector (WKCZ)

De Wet klachtrecht cliënten zorgsector (WKCZ) voorziet in de mogelijkheid om klachten in te dienen wegens onheuse behandeling of manco's in het hulpverleningsproces. De WKCZ stelt randvoorwaarden voor het klachtrecht om de rechtspositie van de patiënt te versterken. Het uitoefenen van dit recht staat aan het gebruik van andere juridische middelen, zoals een beroep op civielrechtelijke, tuchtrechtelijke en strafrechtelijke normen, overigens niet in de weg.

Voorbeelden van gedragingen waarover via de WKCZ zou kunnen worden geklaagd zijn: het niet meewerken aan de uitoefening van patiëntenrechten, zoals een verzoek om inzage, en het invoeren van onjuiste of onvolledige gegevens.

De WKCZ bevat geen algemene norm voor de beoordeling van een klacht. Als uitgangspunt kan echter worden genomen dat de zorgaanbieder zich behoort te gedragen zoals een goede zorgaanbieder, individuele beroepsbeoefenaar of voor een zorgaanbieder werkzame persoon zou doen.

Klachtenprocedure WKCZ

Op grond van de WKCZ dient iedere zorgaanbieder een regeling te treffen voor de behandeling van klachten over een gedraging van hem of van voor hem werkzame personen jegens een cliënt. Deze regeling dient bovendien op passende wijze onder de aandacht van zijn cliënten te worden gebracht.⁴⁹ De klachtenprocedure staat open voor cliënten en oud-clieñten. Ook kan een klacht worden ingediend namens een cliënt die inmiddels is overleden.⁵⁰

De klachtencommissie kan geen sancties opleggen. De uitspraak van de klachtencommissie heeft de status van een advies aan de zorgaanbieder en is dus niet bindend. Zo kan de klachtencommissie adviseren tot het geven van een waarschuwing aan een persoon die een fout heeft gemaakt, het nemen van rechtspositionele maatregelen, het wijzigingen van bepaald beleid, bepaalde regels of procedures, en het beter bekendmaken van een bepaald beleid of bepaalde regels.

De zorgaanbieder dient binnen een maand nadat hij de uitspraak heeft ontvangen te laten weten wat hij met het oordeel van de klachtencommissie doet.⁵¹ Is sprake van een ernstige situatie met een structureel karakter, waaromtrent de zorgaanbieder geen maatregelen neemt, dan is de klachtencommissie verplicht de Inspectie voor de Gezondheidszorg (IGZ) hiervan in kennis te stellen.

6 Governance

Onder governance verstaan we de inrichting van de rollen, taken, verantwoordelijkheden en spelregels die nodig zijn voor een goed functioneren van een afsprakenstelsel.

6.1 Diensten

6.2 Releasebeleid

Het AORTA releasebeleid beschrijft aan welke eisen het releaseproces (het doorvoeren en publiceren van vernieuwingen) moet voldoen. Ook stelt dit releasebeleid eisen aan de termijn binnen welke marktpartijen hun implementatie(s) moeten aanpassen, nadat een nieuwe major-versie van het afsprakenstelsel is gepubliceerd.

Deze beschrijving loopt vooruit op een verdere uitwerking van het AORTA releasebeleid en het voortbrengingsproces, die in volgende releases van het AORTA-afsprakenstelsel zullen worden aangescherpt.

6.2.1 Releasecriteria en versiebeheer

Releases van het AORTA-afsprakenstelsel worden ingedeeld volgens de principes van Semantic Versioning (SemVer, versie 2.0.0), waarbij de versie nummers worden opgebouwd uit drie onderdelen: major.minor.patch (x.y.z):

- **Major release:** wijzigingen met impact op functionaliteit die niet terugwaarts compatibel zijn.
- **Minor release:** wijzigingen met impact op functionaliteit die wel terugwaarts compatibel zijn.
- **Patch release:** wijzigingen zonder impact op functionaliteit die altijd terugwaarts compatibel zijn.

Deze eenduidige classificatie biedt helderheid en maakt het versiebeheer voorspelbaar en beheersbaar.

6.2.2 Releasefrequentie

Voor het AORTA afsprakenstelsel gelden de volgende eisen:

- Maandelijks is er een publicatiemoment;
- Publicatiemomenten worden per jaar gepland en met de marktpartijen gecommuniceerd;
- Maximaal twee keer per jaar wordt een major release uitgebracht;
- Tussen twee major-release zit minimaal een periode van zes maanden;
- Minors en patches kunnen iedere maand uitgebracht worden;
- Dringende patches, bijvoorbeeld ter oplossing van kritieke fouten of beveiligingsissues, kunnen op elk tussentijds moment worden uitgebracht;

6.2.3 Externe koppelingen

- Voor de externe koppeling volgen wij de releases en eisen van bijbehorende afsprakenstelsels. Externe koppelingen binnen het AORTA afsprakenstelsel zijn:
 - Implementatie van de rol Dientverlener aanbieder (DVA) uit het MedMij afsprakenstelsel;
 - Implementatie van de rollen GtK Leverancier en GtK Beheerder uit het Twiin afsprakenstelsel;

7 Logische architectuur

7.1 Samenvatting

AORTA is **de landelijk beschikbare infrastructuur voor gegevensuitwisseling in de zorg in Nederland**, met behulp waarvan zorgverleners onderling patiëntgegevens kunnen uitwisselen en patiënten hun eigen gegevens kunnen raadplegen.

7.1.1 Primaire interacties

AORTA ondersteunt als primaire interacties ⁽¹⁾ het opvragen van patiëntgegevens en het versturen van patiëntgegevens. Hierbij maakt AORTA gebruik van een intermediair, het Landelijk Schakelpunt (LSP); het LSP houdt een verwijzindex bij, waarbij de gegevenshouders kunnen aanmelden dat zij over patiëntgegevens beschikken. Vervolgens kunnen zorgverleners en patiënten via het LSP gegevens opvragen zonder dat zij elke afzonderlijke gegevenshouder apart hoeven te benaderen. Ook bij het versturen van gegevens treedt het LSP op als intermediair en ondersteunt hierbij de adressering van gegevens.

⁽¹⁾ Een interactie is een wisselwerking tussen organisaties, personen en/of systemen, waarbij gegevens kunnen worden uitgewisseld.

7.1.2 Ondersteunende interacties

AORTA ondersteunt het opvragen en versturen van gegevens met de volgende interacties:

- het aan- en afmelden van gegevens bij de verwijzindex;
- het nemen van een abonnement op wijzigingen in patiëntgegevens of op verzonden berichten omtrent een specifieke patiënt;
- het raadplegen van een toegangslog waarin alle gegevensuitwisselingen zijn vastgelegd voor controle achteraf op de toegangsregels, in aanvulling op de beveiligingsmaatregelen vooraf.

Daarnaast worden er externe services aangeboden voor op de AORTA aangesloten systemen. Het gaat hier specifiek over:

- het opzoeken van gegevens over zorgaanbieders, zorgverleners en het opzoeken van adresseringsinformatie van een op AORTA aangesloten zorginformatiesysteem

7.1.3 Authenticatie en autorisatie

AORTA authenticceert zorgverleners en patiënten die via AORTA gegevens uitwisselen. Zorgverleners moeten hiertoe beschikken over een UZI-pas, die hun unieke zorgverlener identificatie bevat. Patiënten moeten beschikken over een DigiD met sms verificatie.

AORTA regelt ook de autorisatie van betrokken zorgverleners en patiënten. De autorisatie houdt rekening met diverse aspecten, namelijk actieve instemming door de patiënt met het ter beschikking stellen van gegevens door de zorgaanbieder (voor niet gemigreerde systemen door middel van een lokaal geregistreerde opt-in, via gemigreerde systemen wordt de opt-in via Mitz geregeld), het bestaan

van een behandelrelatie tussen zorgverlener en patiënt, het beroep van de zorgverlener en eventueel bezwaar van de patiënt tegen uitwisseling van gegevens. Ook is er de mogelijkheid voor de zorgverlener om andere medewerkers direct of indirect (op basis van een set aan autorisatieregels) te mandateren, waarbij de medewerker gegevens kan uitwisselen onder verantwoordelijkheid van de zorgverlener.

Patiënten die niet zelf over de mogelijkheden beschikken om toegang tot AORTA te verkrijgen, kunnen zich wenden tot een Klantenloketorganisatie. Klantenloketmedewerkers kunnen hierbij enkele gegevens namens de patiënt opvragen. Klantenloketmedewerkers identificeren zich met een PKIO-pas.

7.1.4 Informatiesystemen

De standaard voor informatie-uitwisseling verschuift bij AORTA van HL7v3 richting HL7 FHIR, waar het communicatie met de patiënt betreft, maar ook waar met apps gewerkt wordt en de behoefte aan FHIR voor uitwisseling tussen zorgaanbieders is.

Aorta zal zowel HL7v3 als FHIR gaan ondersteunen als platform/stelsel voor uitwisseling. Een belangrijke innovatie bij AORTA richting HL7 FHIR, is de ontwikkeling van API-gebaseerde interacties, en met name het samenspel tussen de Resource Broker ([HL7-FHIR standaard](#)⁵) en de Autorisatie Server ([OAuth-protocol](#)⁶) die in deze informatie-uitwisseling van belang zijn.

Het LSP maakt gebruik van een centraal bericht uitwisselingsplatform, de Zorginformatiemakelaar (ZIM). De ZIM is verantwoordelijk voor de HL7v3 berichtuitwisseling tussen initiërende systemen en reagerende systemen.

LSP+ is een uitbreiding of extensie voor HL7 FHIR, omdat het AORTA-netwerk niet alleen o.b.v. HL7v3 aan het MedMij-netwerk wordt gekoppeld, maar ook o.b.v. HL7-FHIR, waardoor alle (op FHIR-gebaseerde) MedMij-gegevensdiensten via LSP+ geboden kunnen worden.

Alle informatiesystemen die op de ZIM worden aangesloten moeten aan een stelsel van implementatie- en exploitatie-eisen voldoen, waarna ze worden aangeduid als 'goed beheerd' informatiesysteem, aangeduid met de afkorting GBx.

Tot de groep van GBx'en behoren:

- goed beheerde zorgsystemen (GBZ), informatiesystemen die door zorgverleners worden gebruikt om een patiëntdossier in te richten;
- goed beheerde patiëntportalen (GBP), portalen die patiënten toegang geven tot hun eigen gegevens⁽¹⁾;
- VZVZ-portaal, specialisatie van een GBP onder beheer van VZVZ.
- een goed beheerd klantenloketsysteem (GBK), het toegangssysteem van de klantenloketorganisatie;
- goed beheerde organisaties (GBO), informatiesystemen die door zorgverleners worden gebruikt, maar die geen uzi abonnee kunnen worden;

5. <https://www.hl7.org/fhir/index.html>

6. <https://tools.ietf.org/html/rfc6749>

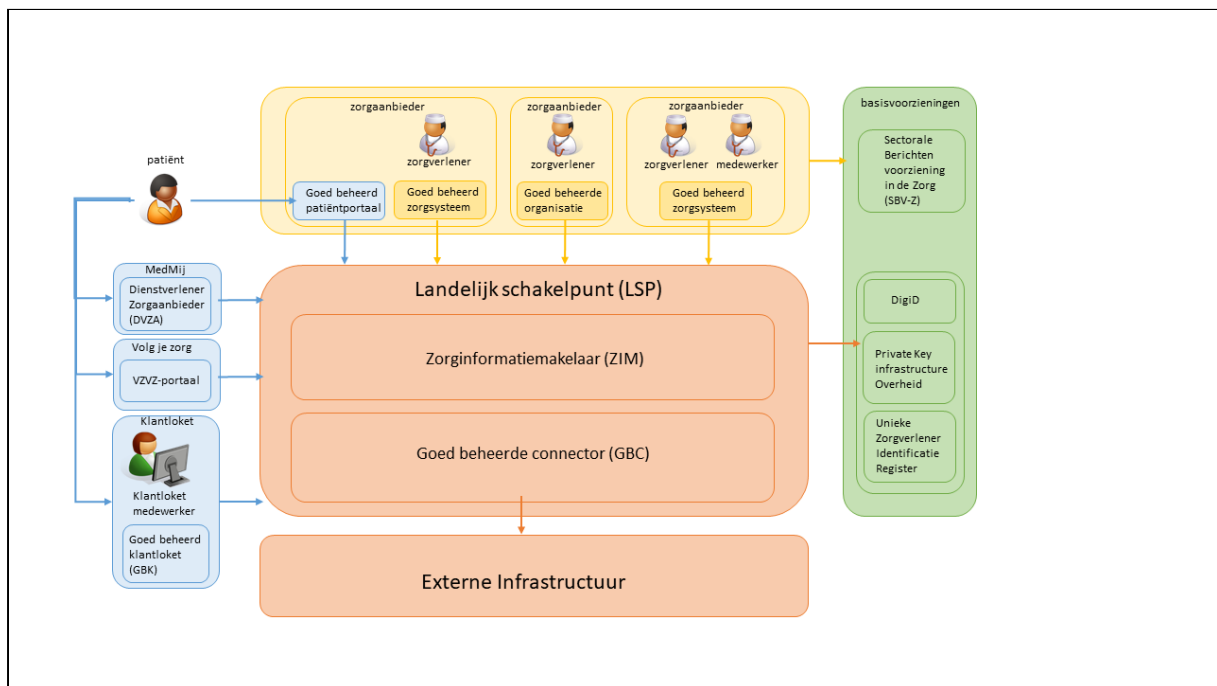
- goed beheerde connector (GBC), connector die patiëntgegevens ontsluit van externe infrastructuur aan de AORTA-infrastructuur;
- dienstverlener zorgaanbieder (DVZA), connector die patiëntgegevens uit de AORTA-infrastructuur ontsluit aan het MedMij-netwerk.

Het LSP en LSP+ zullen samen de Resource Broker gaan vormen voor het HL7 FHIR verkeer, waarbij er tevens van één Autorisatie Server gebruik gemaakt gaat worden, die op termijn opgeschaald wordt naar een gemeenschappelijke dienst en op Mitz aangesloten wordt. Om systemen van zorgaanbieders te kunnen vinden en adresseren, wordt gebruik gemaakt van de gemeenschappelijke dienst ZORG-AB. Om de interoperabiliteit te bevorderen, zal gebruik gemaakt worden van Zorg Informatie Bouwstenen (ZIB's) die tussen zorgaanbieders onderling, als ook tussen zorgaanbieders en burgers worden uitgewisseld.

Informatie uitwisseling tussen zorgaanbieders mag ook direct plaatsvinden, zonder tussenkomst van de Resource Broker, zodat voor iedere use case, de optimale informatiestroom kan worden ingeregeld. Met behulp van een vertaal (of translatie) services van de Resource Broker wordt het zorgaanbieders mogelijk gemaakt tussen HL7v3- en HL7 FHIR systemen te communiceren.

Voor systeemaan authenticatie moeten systemen beschikken over een UZI-servercertificaat (GBZ) of een servercertificaat van PKI-overheid (partijen die geen UZI abonnee kunnen worden, zoals ZIM, GBP, GBK, GBO).

Zowel de GBx'en als de ZIM hebben toegang tot de services van een aantal basisregistraties.



(1) Hoewel de ZIM is voorbereid op berichten vanuit een GBP, is op het moment van publicatie nog geen concreet GBP gerealiseerd, waardoor daadwerkelijke patiënttoegang tot AORTA via een GBP nog niet mogelijk is.

7.1.5 Berichtafhandeling

Om de interacties tussen zorgverleners onderling en tussen patiënt en zorgverlener te ondersteunen, is een reeks van interfaces gedefinieerd op de ZIM. Er wordt onderscheid gemaakt tussen de interfaces voor GBZ'en, GBO's, GBP'en en GBK'en en de DVZA. Via de GBC kan een externe infrastructuur bevraagd worden. Er worden (nog) geen interfaces aangeboden specifiek voor externe infrastructuren.

Voor berichtuitwisseling tussen GBx en ZIM wordt gebruik gemaakt van berichten die gebaseerd zijn op de internationale medische berichtenstandaard HL7v3. HL7-berichten worden verstuurd over SOAP over HTTPS. GBx en ZIM worden gekoppeld via datacommunicatienetwerken (DCN's) op basis van TCP/IP. De leveranciers van deze DCN's moeten aan speciale eisen voldoen om zich te kwalificeren als Goedbeheerd ZorgNetwerk (GZN, voorheen Zorg Service Provider).

Voor berichtuitwisseling tussen GBx onderling of tussen PGO en LSP+ kan van FHIR REST API's gebruik gemaakt worden, die gebaseerd zijn op FHIR profielen. FHIR profielen zijn specifieke en uitgebreide FHIR resources die voor specifieke toepassingen gemaakt zijn. Door de manier waarop profielen worden toegepast binnen FHIR kunnen er voor een bepaalde (FHIR) basis resource verschillende profielen bestaan, bijvoorbeeld afhankelijk van zorgdomein, land, instelling of leverancier. Om interoperabiliteit te borgen is het van belang dat binnen een bepaalde use case dezelfde profielen gebruikt worden. Een register met FHIR profielen is te vinden op www.simplifier.net⁷(in samenwerking met HL7 Nederland).

De kern van de relatie tussen bouwstenen op basis van ZIB's (Zorg Informatie Bouwstenen) en FHIR is dat de bouwstenen op modelniveau via mapping "omgezet" moeten worden in FHIR resources en vice versa. Daarvoor zijn er specifieke profielen door Nictiz en andere partijen ontwikkeld en in beheer gegeven bij HL7 Nederland. De gepubliceerde ZIB profielen zijn terug te vinden op [Nictiz STU3 Zib 2017](http://Nictiz.STU3.Zib.2017)⁸(zie ook [ZIB Publicatie 2017 NL](http://ZIB.Publicatie.2017.NL)⁹). Het onderhanden werk bij Nictiz is terug te vinden op <https://simplifier.net/organization/nictiz/~projects>.

7.1.6 Non-functionele aspecten en beveiliging

De ZIM is ten behoeve van beschikbaarheid en continuïteit redundant en op gescheiden locaties geïmplementeerd. Voor beschikbaarheid, responstijden, capaciteit en schaalbaarheid zijn richtlijnen opgesteld die zijn vastgelegd in een programma van eisen (zie [PvE ZIM]) en in beheerafspraken.

Beveiliging van AORTA is een centraal aspect van de architectuur en is gebaseerd op een [vertrouwensmodel](#) (see page 642), dat een geheel vormt van technische, organisatorische en juridische waarborgen. In de architectuur komen vooral de technische waarborgen aan de orde.

7.2 Inleiding en context

7.2.1 Achtergrond

Zorgverleners in Nederland zijn op grond van de [WGB¹⁰] verplicht tot het inrichten van een dossier waarin alle gegevens omtrent de behandeling en de gezondheid van de patiënt worden opgenomen.

7. <http://www.simplifier.net>

8. <https://simplifier.net/nictizstu3-zib2017>

9. [https://zibs.nl/wiki/ZIB_Publicatie_2017\(NL\)](https://zibs.nl/wiki/ZIB_Publicatie_2017(NL))

Zorgverleners maken hiertoe niet alleen gebruik van papieren dossiers, maar ook van verschillende gespecialiseerde informatiesystemen zoals huisartsinformatiesystemen (HIS) en ziekenhuisinformatiesystemen (ZIS).

Vaak worden gegevens over dezelfde patiënt opgenomen in meerdere informatiesystemen, doordat de patiënt behandeld wordt door meerdere zorgverleners, bijvoorbeeld de huisarts, de vervangende huisarts, de apotheker en de medisch specialist. De verschillende behandelaars hebben hierbij niet altijd direct inzicht in elkaars gegevens. Dit kan ertoe leiden dat behandelaars niet beschikken over voor hen relevante informatie over eerdere of gelijktijdige behandelingen of medicatie.

Uitwisseling van patiëntgegevens tussen zorgverleners is in het belang van zowel patiënt als behandelaar. In veel situaties is voor de behandelaar belangrijke informatie namelijk al bij andere zorgverleners aanwezig; inzicht in de actuele medicatiestatus bij huisartswaarneming of in spoedgevallen is een klassiek voorbeeld. Indien deze uitwisseling elektronisch kan plaatsvinden kan dit de snelheid, doelmatigheid en betrouwbaarheid van gegevensuitwisseling bevorderen.

Elektronische uitwisseling van gegevens is echter complex om een aantal redenen:

- Er is een grote diversiteit aan bronsystemen waarin patiëntgegevens zijn opgeslagen; om desondanks efficiënt informatie te kunnen uitwisselen is standaardisatie nodig van de wijze waarop gegevensuitwisseling plaatsvindt.
- Zorgverleners weten niet in alle gevallen in welke informatiesystemen van andere zorgverleners gegevens over hun patiënten zijn opgeslagen. Er is dus een mechanisme nodig om relevante bronsystemen te achterhalen.
- Patiënten en zorgverleners moeten erop kunnen vertrouwen dat patiëntgegevens slechts worden geraadpleegd door personen die daartoe bevoegd zijn. Dit stelt speciale eisen aan de informatie-uitwisseling.

Elk initiatief tot informatie-uitwisseling in de zorg wordt geconfronteerd met deze aspecten. Vanuit het oogpunt van doelmatigheid is het zinvol om te komen tot een gezamenlijke aanpak tussen meerdere zorgpartijen, waaronder zorgverleners, koepelorganisaties, patiëntenorganisaties en leveranciers van ICT-systemen, waarbij gedeelde en toekomstvastе oplossingen worden gezocht. AORTA, de infrastructuur voor berichtenuitwisseling in de zorg, is tot stand gekomen in samenwerking met vertegenwoordigers van elk van deze partijen in het zorgveld.

AORTA adresseert de bovengenoemde uitdagingen door een aantal belangrijke uitgangspunten te kiezen ten aanzien van de architectuur:

- De berichtenuitwisseling binnen AORTA maakt gebruik van internationaal en/of nationaal geaccepteerde standaarden, zowel op technisch als medisch inhoudelijk niveau.
- AORTA bevat een verwijzindex waardoor kan worden bijgehouden in welke zorginformatiesystemen patiëntgegevens aanwezig zijn. Een verzoek om gegevens kan hierdoor efficiënt worden gerouteerd, terwijl de gegevens bij de bron blijven, niet onnodig worden gedupliceerd en actueel zijn op het moment van opvragen.
- AORTA is gebaseerd op het [Vertrouwensmodel] waarbinnen gebruikers eenduidig worden geïdentificeerd, geauthenticeerd en geautoriseerd voor gegevensuitwisselingen. Alle uitwisselingen vinden plaats over beveiligde verbindingen tussen geïdentificeerde systemen en

10. <https://vzvz.atlassian.net/wiki/x/hwERBQ>

worden gelogd. De patiënt kan volledig inzicht krijgen tussen wie en welke gegevens uitgewisseld worden.

- AORTA stelt eisen aan alle bij de informatie-uitwisseling betrokken organisaties en informatiesystemen, zowel op het gebied van techniek als op het gebied van beveiliging en beheer.

7.3 Primaire interacties

In dit hoofdstuk worden de primaire interacties en de gerelateerde onderdelen beschreven.

7.3.1 Interacties

Het primaire doel van AORTA is het ondersteunen van informatie-uitwisseling tussen zorgverleners. Hiertoe ondersteunt AORTA een tweetal primaire interacties^{(1 (see page 54))}, zoals weergegeven in diagram AORTA.ALG.d1010:

1. Het opvragen van patiëntgegevens. Hierbij vraagt een gegevensraadpleger patiëntgegevens op bij de gegevenshouder(s).
2. Het sturen van patiëntgegevens. Hierbij stuurt een gegevenszender patiëntgegevens naar een gegevensontvanger.

In dit hoofdstuk wordt een aantal algemene aspecten van deze primaire interacties besproken, los van de implicaties op informatiesysteemniveau.

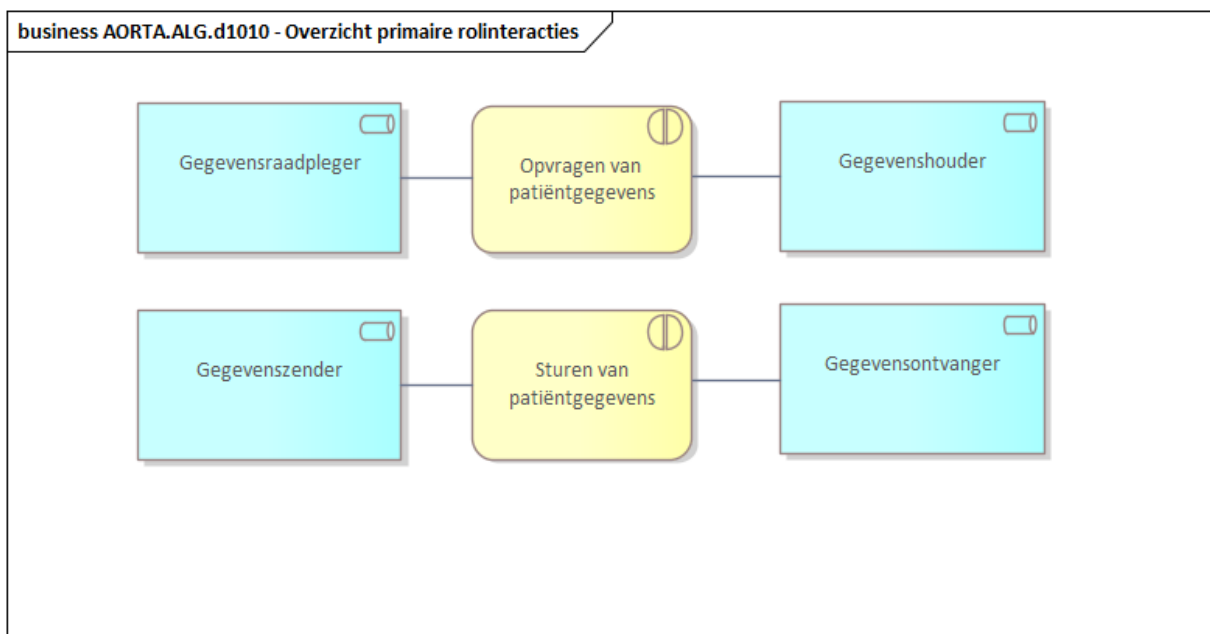


Diagram AORTA.ALG.d1010 - primaire interacties van AORTA

Gegevenshouder, gegevensraadpleger, gegevenszender en gegevensontvanger zijn algemene rollen en worden geconcretiseerd door aan te geven welke actoren deze rollen kunnen vervullen. Hiertoe is het noodzakelijk eerst een aantal actoren te introduceren die binnen de context van AORTA van belang zijn.

(1) Een 'interactie' is een wisselwerking tussen organisaties, personen en/of systemen, waarbij gegevens kunnen worden uitgewisseld.

7.3.2 Primaire informatiesysteeminteracties – opvragen en sturen van gegevens

Op deze pagina wordt uitgewerkt hoe de [primaire interacties](#)¹¹ worden uitgewerkt op informatiesysteemniveau.

7.3.2.1 Opvragen van patiëntgegevens

AORTA koppelt patiëntgegevens raadplegende systemen via de ZIM aan bronsystemen voor patiëntgegevens. Zorgverleners zijn zo in staat om via hun eigen GBZ gegevens over hun patiënten uit de GBZ'en van andere zorgverleners op te vragen. Hiertoe moet hun informatiesysteem gekoppeld zijn aan de ZIM. De zorgverlener hoeft niet zelf te weten in welke andere informatiesystemen gegevens over zijn patiënten zijn opgeslagen. Dit wordt voor niet naar Mitz gemigreerde systemen bijgehouden in de Verwijsindex (VWI), die onderdeel is van de ZIM. Bij naar Mitz gemigreerde systemen kan dit via Mitz worden opgevraagd.

In het geval een raadplegend systeem een specifieke bron wil bevragen, is het ook mogelijk om een gerichte bevraging te doen. De VWI zal in dat geval niet geraadpleegd worden.^[1] Indien het bevroegde systeem gemigreerd is naar Mitz, wordt wel Mitz bevraagd om te kijken of er toestemming is om de bron te bevragen.

De ZIM biedt voor het opvragen twee interfaces aan patiëntgegevens raadplegende systemen:

- LSP.OPV.i1010: Opvragen van patiëntgegevens;
- LSP.OPV.i1020: Opvragen van patiëntgegevens binnen context.

Patiënten kunnen hun eigen patiëntgegevens opvragen, voor zover deze bij de VWI zijn aangemeld. Dit kan via een GBP, met gebruikmaking van de interface LSP.OPV.i1010^[2]¹². Deze functionaliteit is niet actief. Een patiënt kan zijn eigen patiëntgegevens opvragen via een zogenaamde Persoonlijke Gezondheidsomgeving (PGO). Voor meer informatie hierover wordt verwezen naar het afsprakenstelsel van MedMij.

Deze situatie is weergegeven in diagram AORTA.OPV.d1050.

11. <https://vzvz.atlassian.net/wiki/x/8gIRBQ>

12. http://vzvz.atlassian.net/#_ftn2

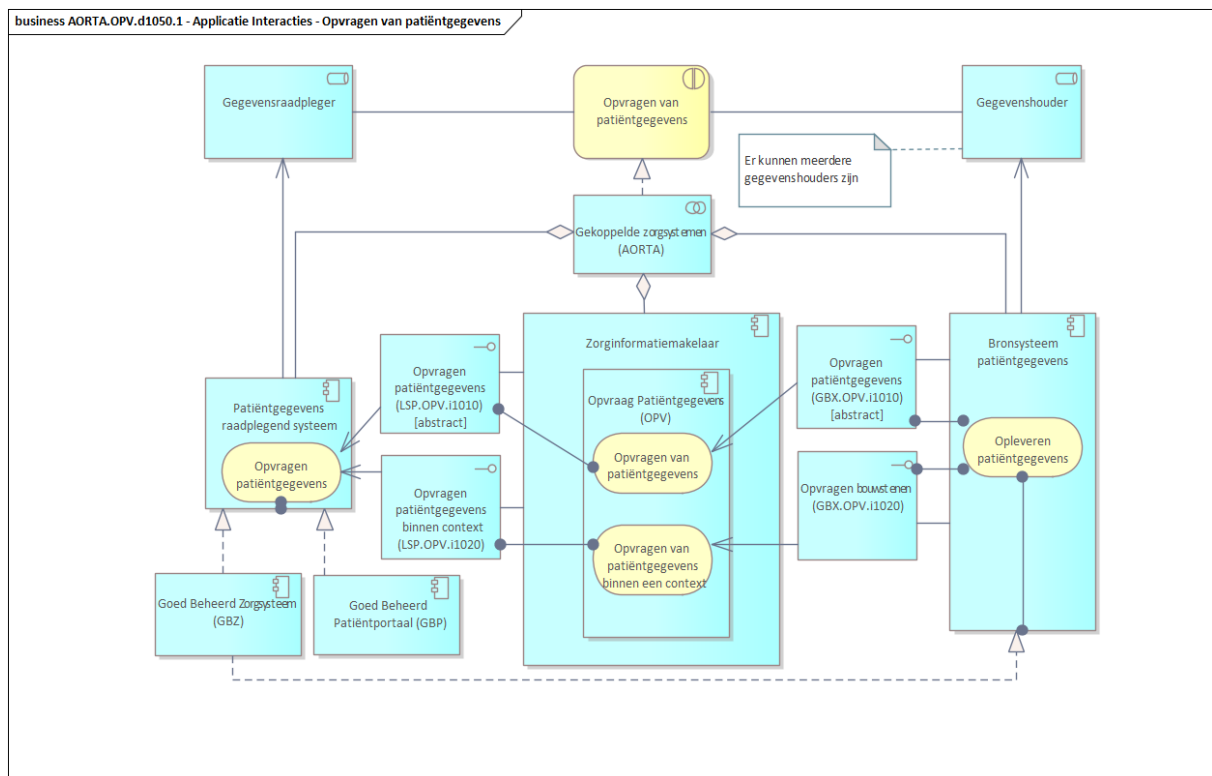


Diagram AORTA.OPV.d1050.1 - informatiesysteeminteracties voor het opvragen van patiëntgegevens

De interfaces 'opvragen van patiëntgegevens' en 'opvragen bouwstenen' zijn abstracte interfaces; er bestaat dus geen concreet geïmplementeerde interface met deze naam. De abstracte interface bestaat enkel op ontwerpniveau om het beschrijven van een aantal generieke aspecten van deze interface mogelijk te maken, zodat de ZIM verschillende concrete opvraagberichten op een generieke wijze behandelt. In de uitwerking van concrete zorgtoepassingen (bijvoorbeeld medicatieproces, huisartswaarneminggegevens) worden concrete implementaties ontworpen van de interface 'opvragen patiëntgegevens' (bijvoorbeeld 'opvragen medicatievoorschriften'). De interface 'opvragen bouwstenen' wordt ingevuld door specifieke bouwsteen bevestigingen (bijvoorbeeld 'opvragen medicatieverstrekkingen'). Waar sprake is van abstracte interfaces wordt dit expliciet benoemd.

7.3.2.1.1 Interface LSP.OPV.i1010: opvragen van patiëntgegevens

Het opvragen van patiëntgegevens kan vanuit een op de ZIM aangesloten patiëntgegevens raadplegend systeem worden geïnitieerd. Deze interface wordt gebruikt om de inhoudelijke gegevens van een patiënt op te vragen zoals die in andere op de ZIM aangesloten informatiesystemen aanwezig zijn. Wanneer patiëntgegevens via de ZIM worden opgevraagd, stuurt de ZIM-component 'Opvraag patiëntgegevens' (OPV) de opvraag door naar alleen die GBZ'en die volgens de Verwijsindex over de gevraagde gegevens beschikken.^[1] De OPV component verzamelt vervolgens de resultaten en beantwoordt het oorspronkelijke verzoek.^[2]

Om het doorsturen van opvraagverzoeken mogelijk te maken moet een op de ZIM aangesloten informatiesysteem de benodigde interface implementeren, GBX.OPV.i1010; deze is structureel gelijk aan LSP.OPV.i1010, maar het doorgestuurde opvraagverzoek bevat nu de ZIM als afzender.

Zie voor een verdere uitwerking van de aspecten van deze interface het ontwerp van de component 'Opvraag patiëntgegevens' (OPV) (zie [Ontw OPV]).

7.3.2.1.2 Interface LSP.OPV.i1020: opvragen van patiëntgegevens binnen context

Het opvragen van patiëntgegevens binnen een context kan vanuit een op de ZIM aangesloten patiëntgegevens raadplegend systeem worden geïnitieerd. Deze interface wordt gebruikt om de inhoudelijke gegevens van een patiënt op te vragen zoals die in andere op de ZIM aangesloten informatiesystemen aanwezig zijn. Wanneer patiëntgegevens via de ZIM worden opgevraagd, zal door de SDS component worden bepaald welke specifieke bouwstenen moeten worden opgevraagd en met welke eventuele beperkingen.

Er wordt binnen deze interface onderscheid gemaakt tussen een gerichte en een ongerichte bevraging. Bij een gerichte opvraag heeft het patiëntraadplegend systeem de te bevragen GBZ(en) opgenomen in de bevraging en zal de Verwijsindex niet geraadpleegd worden. In het geval van een ongerichte bevraging zal de OPV component per bouwsteen de specifieke bouwsteenvraag versturen naar de bronsystemen die volgens de VWI over de bouwsteen zouden kunnen beschikken.[\[3\]](#)

Zie voor een precieze uitwerking van de aspecten van deze interface het ontwerp van de component 'Opvraag patiëntgegevens' (OPV) (zie [Ontw OPV]).

7.3.2.2 Versturen van patiëntgegevens

AORTA stelt zorgverleners in staat om via hun eigen informatiesysteem gegevens over de door hen behandelde patiënten op te sturen naar de informatiesystemen van andere zorgverleners.

Hiertoe moeten de informatiesystemen van zender en ontvanger gekoppeld zijn aan de ZIM. Voorafgaand aan het verzenden heeft de zender de mogelijkheid om via de ZIM de voor het adresseren benodigde informatie op te zoeken over de ontvanger (zie hiervoor pagina '[Raadplegen van de verwijsindex \(see page 75\)](#)').

De ZIM biedt voor het sturen één interface:

- LSP.STU.i1010: Versturen van patiëntgegevens

Een systeem dat deze interface implementeert heeft de systeemrol 'gegevens versturend systeem'. Deze situatie is weergegeven in diagram AORTA.STU.d1050.

7.3.2.2.1 Interface LSP.STU.i1010: sturen van patiëntgegevens

Het sturen van patiëntgegevens kan vanuit een op de ZIM aangesloten informatiesysteem worden geïnitieerd. Deze interface biedt de mogelijkheid om de inhoudelijke gegevens van een patiënt te versturen naar een op de ZIM aangesloten informatiesysteem dat toebehoort aan een andere zorgaanbieder. Wanneer patiëntgegevens via de ZIM worden verstuurd, stuurt de ZIM-component 'Sturen patiëntgegevens' (STU) de verzonden gegevens door naar het informatiesysteem dat in de adressering van het bericht is gespecificeerd. Om dit doorsturen mogelijk te maken moeten de aangesloten informatiesystemen de benodigde interface implementeren, GBX.STU.i1010; deze is structureel gelijk aan LSP.STU.i1010; ook inhoudelijk wordt de boodschap niet aangepast. De ZIM acteert dus alleen als intermediair.

Zie voor een verdere uitwerking van de aspecten van deze interface het ontwerp van de component 'Sturen patiëntgegevens' (STU) (zie [Ontw STU]).

N.B. De 'sturen van patiëntgegevens' interface is een abstracte interface; er bestaat dus geen concreet geïmplementeerde interface met deze naam. De abstracte interface bestaat enkel op ontwerpniveau om het beschrijven van een aantal generieke aspecten van deze interface mogelijk te maken, zodat de ZIM verschillende concrete opvraagberichten op een generieke wijze behandelt. In de uitwerking van concrete zorgtoepassingen (bijvoorbeeld medicatieproces, huisartswaarneminggegevens) worden concrete implementaties ontworpen van deze interface (bijvoorbeeld 'versturen medicatievoorschrift').

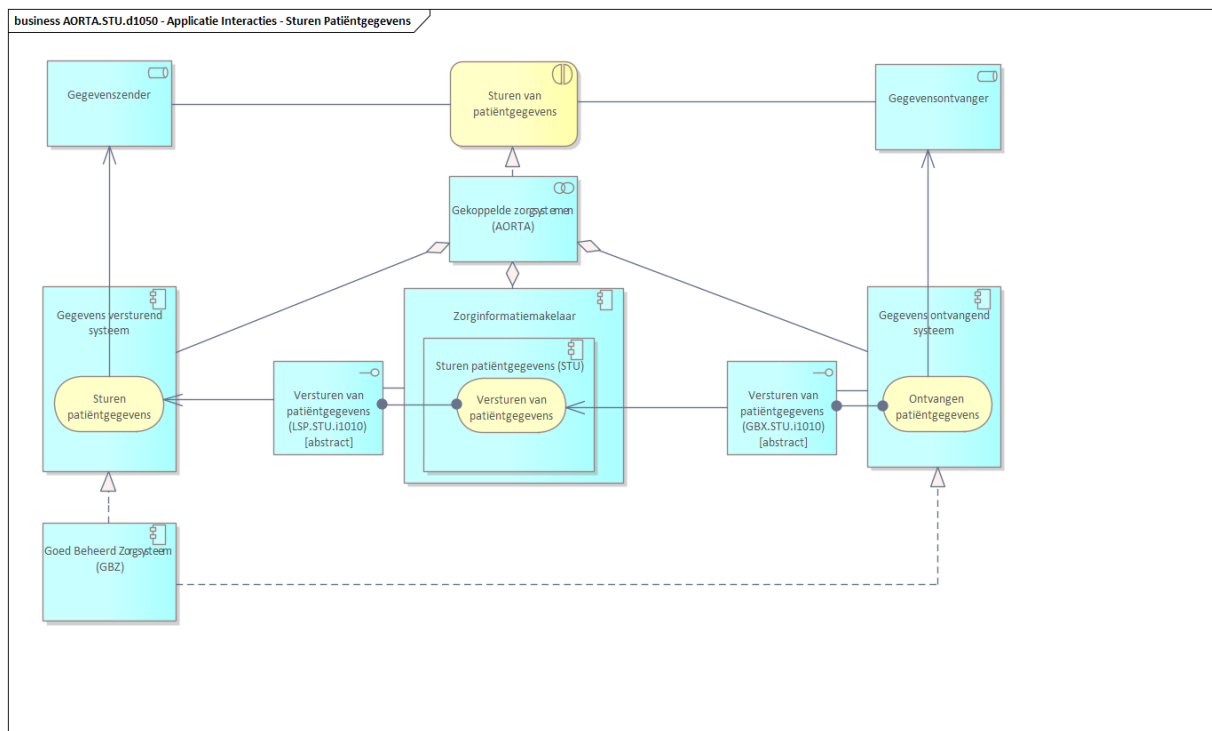


Diagram AORTA.STU.d1050 - informatiesysteeminteracties voor het sturen van patiëntgegevens

- [1] Omdat de ZIM hierbij de vraag afkomstig van één applicatie uitzet naar meerdere applicaties wordt gesproken van 'divergeren' van een verzoek.
- [2] Omdat hierbij de antwoorden afkomstig van meerdere applicaties weer worden gebundeld, wordt gesproken van 'convergeren' van antwoorden.
- [3] De VWI bepaalt de juiste verwijzingen door te bepalen welke gegevenssoorten specifieke bouwsteentypen bevatten. Bronnen die een verwijzing van een relevant bouwsteentype of gegevenssoort hebben aangemeld zullen worden bevestigd.

[2]

Deze functionaliteit wordt alleen geboden via de interface LSP.OPV.i1020. Hier wordt bedoeld dat in principe zowel een GBZ als een GBP kan optreden als patiëntgegevens-raadplegend systeem. Op het moment van publicatie zijn nog geen GBP's gerealiseerd die deze functionaliteit bieden.

7.3.3 Actoren

Binnen de context van AORTA zijn de volgende actoren van belang, namelijk:

- zorgverlener;
- zorgaanbieder;
- medewerker van een zorgaanbieder;
- patient;
- goed beheerde organisatie.

7.3.3.1 Zorgverlener

In AORTA een 'zorgverlener' gedefinieerd als een individuele uitoefenaar van een medisch beroep zoals bedoeld in artikel 3 of 34 van de Wet op de beroepen in de individuele gezondheidszorg. Een zorgverlener kan uniek worden geïdentificeerd en beschikt over één of meer wettelijk beschermde beroepstitels.

7.3.3.2 Zorgaanbieder

In AORTA wordt verstaan onder een 'zorgaanbieder':

- een zorginstelling zoals bedoeld in de Kwaliteitswet zorginstellingen, of;
- een individuele zorgverlener, die niet werkt binnen een zorginstelling, of;
- een instelling die een belangrijke rol speelt in een specifiek zorgproces.

Een individuele zorgverlener kan dus ook een zorgaanbieder zijn, bijvoorbeeld in het geval van een huisarts met een eigen praktijk. Zorgaanbieder en zorgverlener kunnen dan dezelfde persoon zijn.

Een zorgaanbieder kan zorgverleners in dienst hebben en medewerkers die geen zorgverlener zijn. Dit geldt ook als de zorgaanbieder een individuele zorgverlener is: een huisarts kan bijvoorbeeld een verpleegkundige in dienst hebben en een huisartsassistente.

Deze relaties worden geïllustreerd in diagram AORTA.ALG.d1020. Dit toont dat een zorgaanbieder 'gerealiseerd' kan worden door een zorgverlener of een zorginstelling en dat zorgaanbieders (zowel zorginstellingen als zorgverleners) zorgverleners en medewerkers in dienst kunnen hebben.

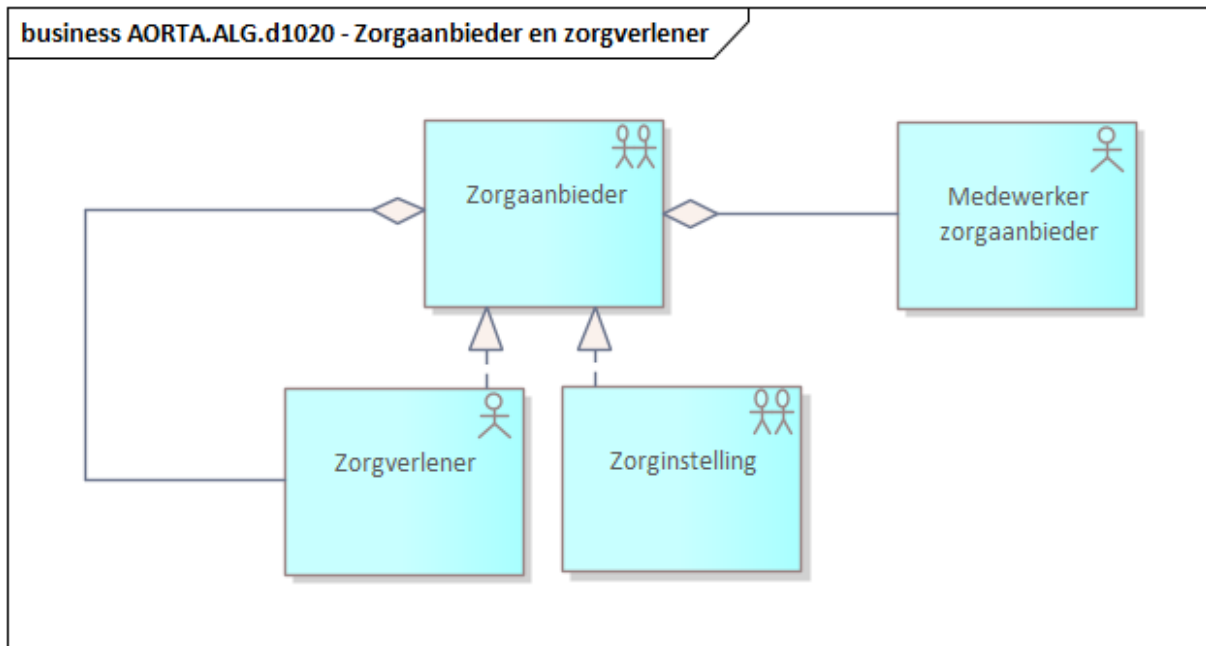


Diagram AORTA.ALG.d1020 - illustratie van het begrip zorgaanbieder

7.3.3.3 Medewerker van een zorgaanbieder

In AORTA wordt bedoeld met een 'medewerker van een zorgaanbieder' een persoon die werkt voor een zorgaanbieder en zelf geen zorgverlener is. Een medewerker is uniek identificeerbaar en er kan worden vastgesteld voor welke zorgaanbieder de medewerker werkt.

7.3.3.4 Patiënt

Het begrip 'patiënt' wordt in AORTA niet beperkt tot personen die behandeld worden voor een aandoening, maar wordt meer algemeen opgevat. De patiënt is een uniek-identificeerbare natuurlijke persoon over wie informatie kan worden uitgewisseld. Omdat in de Wbsn-z is vastgelegd dat bij alle berichtgevingen tussen zorgaanbieders onderling het burger servicenummer aanwezig moet zijn, kan de patiënt in de praktijk elke persoon zijn aan wie een burger servicenummer is toegekend. Dat desondanks gesproken wordt over de patiënt en niet over 'de burger' heeft te maken met het feit dat in het kader van zorgprocessen de term 'patiënt' meer herkenning oproept.

7.3.3.5 Goed Beheerde Organisatie

Goed beheerde organisaties (GBO) zijn instellingen die niet beschreven staan in de Kwaliteitswet zorginstellingen. Deze instellingen kunnen als gevolg niet beschikken over UZI authenticatiemiddelen. Om toch gebruik te kunnen maken van de AORTA infrastructuur dient de instelling voorzien te worden van een PKI-overheid servercertificaat. In geval een instelling is voorzien van een PKI-overheid servercertificaat gelden dezelfde uitgangspunten als voor een zorgaanbieder.

Alleen zorgverleners kunnen gegevens uitwisselen via de AORTA infrastructuur. Binnen een GBO dienen dus wel zorgverleners werkzaam te zijn om patiëntgegevens op te kunnen vragen.

7.3.4 Rollen toekennen aan actoren

Nu de actoren 'zorgaanbieder', 'zorgverlener' en 'patiënt' zijn geïntroduceerd, kunnen de rollen behorend bij de primaire interacties worden geconcretiseerd. Hierbij geldt voor de actor GBO hetzelfde als voor de actor 'zorgaanbieder'.

7.3.4.1 Opvragen van patiëntgegevens

De rollen behorend bij de interactie 'opvragen van patiëntgegevens' worden getoond in diagram AORTA.OPV.d1010.

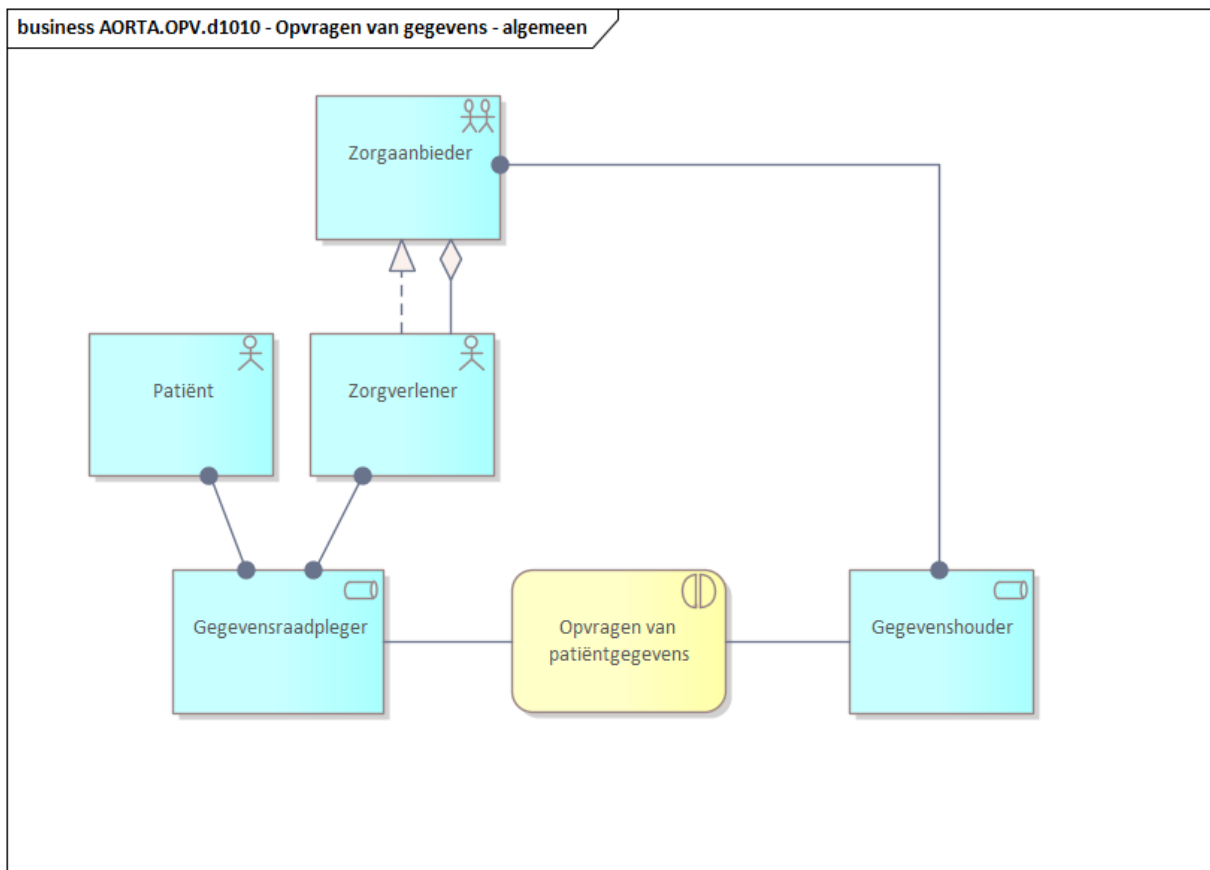


Diagram AORTA.OPV.d1010 - opvragen van patiëntgegevens

Gegevenshouder

Bij het opvragen van patiëntgegevens heeft een *zorgaanbieder* de rol van gegevenshouder. De opslag van dossiergegevens is namelijk in het algemeen gemeenschappelijk georganiseerd door de zorgaanbieder voor (groepen van) zorgverleners die bij de zorgaanbieder werkzaam zijn; toegang tot de dossiergegevens moet daarom op het niveau van de zorgaanbieder worden geregeld. Meerdere zorgaanbieders kunnen gegevenshouder zijn van gegevens van een bepaalde patiënt.

Gegevensraadpleger

Een individuele zorgverlener behorend bij een zorgaanbieder (in het algemeen een andere zorgaanbieder dan de gegevenshouder) heeft de rol van gegevensraadpleger. Het is mogelijk dat een zorgverlener een systeem mandateert om voor hem gegevens op te vragen. Er zal echter altijd een zorgverlener zijn, die verantwoordelijk is voor een opvraag. Ook de patiënt kan optreden als gegevensraadpleger van zijn eigen gegevens.

7.3.4.2 Sturen van patiëntgegevens

De rollen behorend bij de interactie 'sturen van patiëntgegevens' worden getoond in diagram AORTA.STU.d1010.

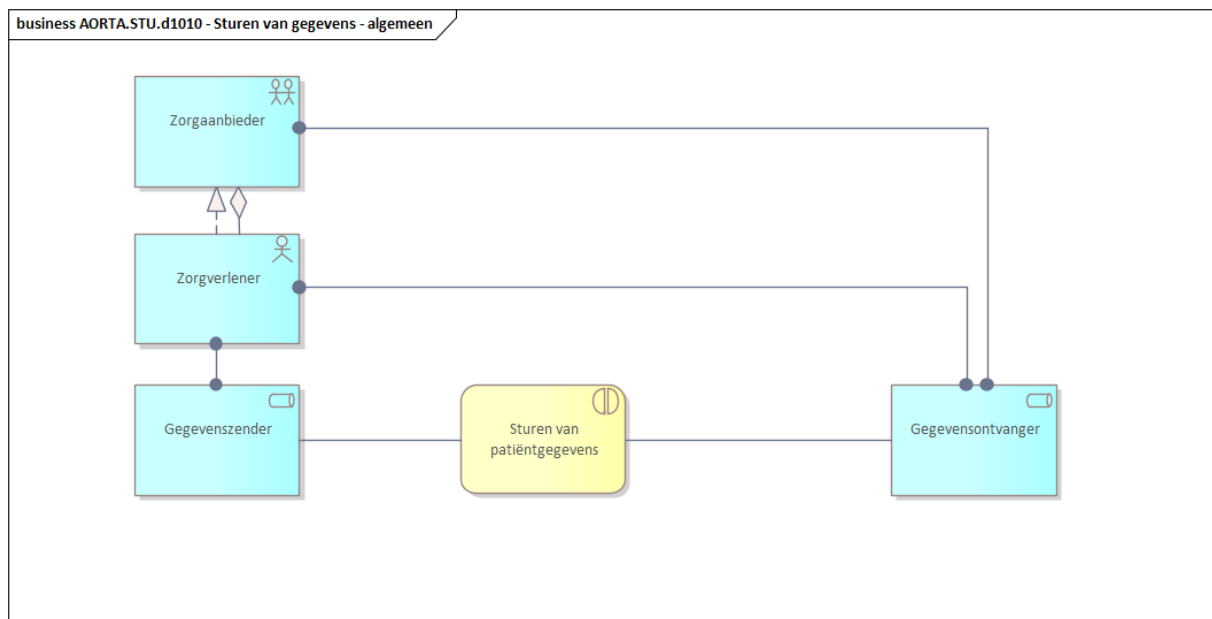


Diagram AORTA.STU.d1010 - Sturen van patiëntgegevens

Gegevenszender

Bij het sturen van patiëntgegevens heeft een zorgverlener die hoort bij een zorgaanbieder de rol van gegevenszender.

Gegevensontvanger

De gegevensontvanger kan een individuele zorgverlener zijn die hoort bij een zorgaanbieder (in het algemeen een andere zorgaanbieder dan de zorgaanbieder waartoe de gegevenszender behoort). Het is echter ook mogelijk dat de gegevenszender op het moment van verzenden nog niet kan vaststellen welke zorgverlener bij de ontvangende zorgaanbieder de behandeling van de patiënt zal uitvoeren en daartoe de gegevens zal raadplegen. In dit geval is de gegevensontvanger de zorgaanbieder, waarbij het aan de zorgaanbieder is om de gegevens beschikbaar te maken aan de individuele zorgverlener die de patiënt zal behandelen.

7.3.4.3 Toegangsbeperkingen

De modellen die op deze pagina beschreven staan houden niet in dat een zorgverlener die optreedt als gegevensraadpleger automatisch toegang kan hebben tot alle patiëntgegevens van alle patiënten waarover de gegevenshouder beschikt, of dat iedere zorgverlener die optreedt als gegevenszender de gegevens van elke willekeurige patiënt kan versturen. Een nadere inperking door een model van toegangsregels is vereist in de vorm van een toegangsmodel.

}

7.3.5 Toegangsmodel

Het model van toegangsregels is het toegangsmodel. Hiervoor worden enkele aanvullende begrippen geïntroduceerd:

- opt-in van de patiënt;
- behandelrelatie;
- bevoegdheid op grond van BIG-titel van de zorgverlener;
- mandatering;
- vertegenwoordiging;
- samenwerkingsverband.

7.3.5.1 Opt-in van de patiënt

De [AVG], [WGB0] en [WABVPZ] van de bieden het wettelijk kader voor het uitwisselen van gegevens in de zorg. Op grond van deze wetgeving geldt voor uitwisseling van medische gegevens onder dat uitdrukkelijke toestemming nodig is van de patiënt voor het beschikbaar stellen van gegevens door een gegevenshouder aan een gegevensraadpleger. Deze toestemmingen worden voor een systeem, dat zijn toestemmingen nog niet naar Mitz heeft gemigreerd, lokaal opgeslagen. Voor een systeem dat zijn toestemmingen wel heeft gemigreerd naar Mitz zijn deze toestemmingen geregistreerd in het (externe) Mitz systeem, dat door AORTA bevestigd wordt.

Hierbij zijn de volgende uitgangspunten gehanteerd:

- De opt-in-vraag is nodig voor het *beschikbaar stellen* van gegevens aan andere zorgaanbieders.
- De opt-in-vraag wordt gesteld door *elke* zorgaanbieder die patiëntgegevens beschikbaar wil stellen.
- Het vooraf vastleggen van de toestemming van de patiënt is bedoeld voor het beschikbaar stellen van patiëntgegevens door gegevenshouders voor opvragen door gegevensraadplegers; de gegevenshouder kan hierbij namelijk geen toestemming vragen op het moment van opvragen. Bij *sturen van patiëntgegevens* kan per geval toestemming worden gevraagd en is vastlegging van toestemming vooraf niet nodig.
- De zorgaanbieder stelt gegevens van de cliënt slechts beschikbaar via een elektronisch uitwisselingssysteem, voor zover bij het raadplegen van die gegevens door een andere zorgaanbieder, de persoonlijke levenssfeer van een ander dan de cliënt niet wordt geschaad.

7.3.5.2 Behandelrelatie

Het bestaan van een behandelrelatie tussen de zorgverlener en de patiënt is een voorwaarde voor toegang van de zorgverlener tot patiëntgegevens.

De volgende zorgaanbieders[2] of zorgverleners hebben een behandelrelatie volgens de [WGBO]:

- degene die een behandelingsovereenkomst[3] heeft met de patiënt;
- degene die rechtstreeks betrokken is bij de uitvoering van de behandelingsovereenkomst;
- degene die optreedt als vervanger van degene die een behandelingsovereenkomst heeft met de patiënt.

Bij het opvragen van gegevens moet de zorgverlener die de rol heeft van gegevensraadpleger een behandelrelatie hebben. Bij het verzenden van gegevens geldt dit voor de zorgverlener die de gegevens verstuurt én voor de zorgverlener of zorgaanbieder die de ontvangen gegevens raadpleegt.

7.3.5.3 Bevoegdheid op basis van BIG-titel

Zoals vastgelegd in de definitie van het begrip zorgverlener oefent de zorgverlener een beroep uit zoals bedoeld in de wet BIG. Niet alle patiëntgegevens zijn voor iedere zorgverlener relevant. Bij het uitwisselen van patiëntgegevens kunnen daarom gegevens worden afgestemd op het beroep en specialisme[4] van de betrokken zorgverleners. Het resultaat van deze afstemming wordt vastgelegd in een autorisatieprotocol en in determinatietabellen.

7.3.5.4 Mandatering

Zoals uitgelegd op pagina 'Rollen toekennen aan actoren'¹³ kan een zorgverlener patiëntgegevens opvragen bij een zorgaanbieder.

In de praktijk van de zorg komt het regelmatig voor dat een medewerker van de zorgaanbieder onder verantwoordelijkheid van de zorgverlener patiëntgegevens moet opvragen of verzenden. Voorbeelden zijn vervangingssituaties, opleidingssituaties en gevallen waarin medewerkers zonder BIG-titel gegevens moeten opzoeken voor een arts. Hierbij is het mogelijk dat de zorgverlener andere zorgverleners, medewerkers of systemen van de zorgaanbieder *mandateert* om onder zijn verantwoordelijkheid gegevens op te vragen of te verzenden. De zorgverlener die verantwoordelijkheden overdraagt is de *mandaterende*, de andere zorgverleners, medewerkers of systemen zijn de *gemandateerden*. Mandaten gelden binnen de context van de zorgaanbieder waaronder de mandaten zijn verstrekt.

Bij opvragen van gegevens door een gemandateerde moet duidelijk zijn:

- wie de *gemandateerde* is en
- wie de *mandaterende* zorgverlener is onder wiens verantwoordelijkheid de gemandateerde handelt.

13. <https://vzvz.atlassian.net/wiki/x/MwARBQ>

De controle van de autorisatie moet hierbij worden toegepast alsof de mandaterende zorgverlener *zelf* de opvraag uitvoert.

7.3.5.5 Vertegenwoordiging

Zoals beschreven op pagina '[Rollen toekennen aan actoren](#)¹⁴' kan een patiënt de eigen patiëntgegevens opvragen bij een zorgaanbieder.

Hierbij moet rekening worden gehouden met enkele uitzonderingen, waarbij:

- *In plaats van* de patiënt een vertegenwoordiger (bijvoorbeeld een ouder) namens de patiënt optreedt;
- *Naast* de patiënt ook een vertegenwoordiger namens de patiënt op kan treden.

Zie de tekst van de [WGB0] voor een precieze beschrijving van deze uitzonderingssituaties. Bij de bespreking van de informatiesystemen voor patiënttoegang op pagina '[Goed beheerd patiëntportaal \(GBP\)](#)¹⁵' en '[Goed beheerd klantenloketsysteem \(GBK\)](#)¹⁶' wordt aangegeven in hoeverre deze uitzonderingen in de architectuur een rol spelen.

7.3.5.6 Samenwerkingsverband

Zoals uitgelegd op pagina '[Rollen toekennen aan actoren](#)¹⁷' kan een zorgverlener patiëntgegevens opvragen bij een zorgaanbieder.

Hierbij moet rekening worden gehouden dat opvragingen gelimiteerd kunnen zijn tot bronsystemen waarmee het opvragende systeem een samenwerkingsverband heeft. Alle samenwerkingsverbanden zijn in het applicatieregister vastgelegd. Bij elke opvraging wordt gecontroleerd of de organisatie, behorend bij het initiërende systeem, voorkomt in een (of één van de) samenwerkingsverband(en) die aan het te bevragen bronsysteem gekoppeld is. Een zorgaanbieder kan in meerdere samenwerkingsverbanden voorkomen of er voor kiezen om zijn patiëntgegevens landelijk beschikbaar te stellen. Voor het sturen van patiëntgegevens wordt niet gekeken naar de samenwerkingsverbanden.

[1] Zie voor een uitgebreide interpretatie van de wettelijke condities de [Zienswijze CBP].

[2] De WGB0 spreekt eigenlijk over 'hulpverlener'; de hulpverlener is een natuurlijke of rechtspersoon die een geneeskundig beroep of bedrijf uitoefent. Omdat sprake kan zijn van een natuurlijke of rechtspersoon spelen in AORTA-terminologie zowel de zorgverlener als de zorgaanbieder een rol in de behandelingsovereenkomst. De behandelingsovereenkomst komt van rechtswege tot stand zodra medische handelingen worden verricht of hierover afspraken worden gemaakt, ook als de partijen zich hiervan niet bewust zijn.

[3] Zie [WGB0] (artikel 7:446 BW)

14. <https://vzvz.atlassian.net/wiki/x/MwARBQ>

15. <https://vzvz.atlassian.net/wiki/x/mwARBQ>

16. <https://vzvz.atlassian.net/wiki/x/IQARBQ>

17. <https://vzvz.atlassian.net/wiki/x/MwARBQ>

[4] Hiermee wordt een beroep en specialisme bedoeld uit de officiële lijst van beroepen zoals bedoeld in artikel 3 en 34 van de wet BIG. Een voorbeeld van een beroep is arts, een voorbeeld van een specialisme is huisarts.

7.3.6 Identificatie en authenticatie

Alle actoren die betrokken zijn bij het opvragen en sturen van gegevens moeten geïdentificeerd kunnen worden om de volgende redenen:

- Om fouten te voorkomen, moet onomstotelijk vaststaan over welke patiëntgegevens worden uitgewisseld.
- Om autorisatieregels te kunnen controleren, moet onomstotelijk vaststaan welke zorgverleners en zorgaanbieders (en in het geval van patiënttoegang welke patiënten en eventuele vertegenwoordigers) optreden als gegevensraadpleger of gegevenszender.
- Om het uitwisselen van gegevens traceerbaar te maken, moet onomstotelijk vaststaan welke zorgverleners en zorgaanbieders (en in het geval van patiënttoegang welke patiënten en eventuele vertegenwoordigers) optreden als gegevensraadpleger of gegevenszender.

De betrokken actoren kunnen op de volgende wijze kunnen worden geïdentificeerd:

- Patiënten worden geïdentificeerd aan de hand van hun Burgerservicenummer (BSN). Het BSN is een uniek persoonsnummer. Iedereen die zich inschrijft bij een Nederlandse gemeente krijgt een BSN. Het BSN is bedoeld om persoonsverwisselingen te voorkomen. Er is wettelijk geregeld welke instanties of organisaties het BSN mogen gebruiken. De Wet Aanvullende Bepalingen Verwerking Persoonsgegevens in de Zorg (Wabvpz) regelt het gebruik van het BSN in de zorg.
- Zorgverleners worden geïdentificeerd aan de hand van hun 'unieke zorgverlener identificatie (UZI)'. Het Unieke Zorgverlener Identificatie-register (UZI-register) is een overheidsregister onder beheer van het Ministerie van VWS waarin iedere zorgverlener zich kan laten registreren, waarbij tevens een koppeling wordt gelegd met het beroep van de zorgverlener zoals vastgelegd in het BIG-register. Zorgverleners krijgen een UZI-pas om hun identiteit mee aan te tonen. Overigens is het mogelijk dat een zorgverlener die werkzaam is bij meerdere zorgaanbieders slechts één UZI-pas heeft die bij meerdere zorgaanbieders kan worden gebruikt; dit wordt 'gastgebruik' genoemd (zie ook pagina '[Authenticatie van de gebruiker / pashouder](#)' (see page 132)).
- Zorgverleners kunnen ook geïdentificeerd worden met de ZORG-ID Smartcard. De ZORG-ID Smartcard wordt beheerd door zorgaanbieders en uitgegeven op basis van een actieve UZI-pas op naam van de zorgmedewerker. Het Landelijk Schakelpunt (LSP) zal deze smartcards accepteren voor de ondertekening van inschrijftokens en transactietokens.
- Medewerkers van zorgaanbieders (niet-zorgverleners) worden eveneens geïdentificeerd aan de hand van hun 'Unieke Zorgverlener Identificatie' (UZI). Ze krijgen een door het UZI-register uitgegeven medewerker pas op naam om hun identiteit mee aan te tonen.
- Systemen worden geïdentificeerd aan de hand van hun unieke applicatieID. Ze krijgen een door het LSP-organisatie uitgegeven applicatieID om hun identiteit mee aan te tonen.
- Zorgaanbieders worden geïdentificeerd aan de hand van hun UZI-registerabonneenummer (URA). Dit is een identificatie die wordt verstrekt aan de zorgaanbieder of zorgverlener die UZI-

passen heeft aangevraagd. Als een zorgaanbieder UZI-passen aanvraagt voor haar zorgverleners en medewerkers, krijgt de organisatie een unieke URA en worden de zorgverleners en medewerkers van de zorgaanbieder aan dit URA gekoppeld. Daardoor kunnen zorgverleners worden gerelateerd aan zorgaanbieders. Aangezien de organisatie die UZI-passen aanvraagt een grote organisatie kan zijn (bv. een zorggroep met meerdere huisartsenpraktijken) is de organisatienaam die gerelateerd is aan de URA niet noodzakelijk herleidbaar tot één vestiging locatie of organisatieonderdeel van die zorgaanbieder.

- Niet UZI-abonnees (GBO) worden geïdentificeerd aan de hand van hun PKI-overheid servercertificaatnummer.

7.3.7 Patiëntgegevens

In de praktijk gebruiken gegevenshouders voor het bewaren van patiëntgegevens verschillende informatiesystemen die elk een andere systematiek kunnen hanteren bij de keuze voor de gegevensopslagstructuur.

Bij het opvragen en versturen van patiëntgegevens is het echter van belang dat overeenstemming bestaat over de structuur en betekenis van de uitgewisselde gegevens.

In de praktijk bestaan diverse gestandaardiseerde methoden om medische gegevens te modelleren maar zijn voor concrete uitwisselingssituaties nadere afspraken nodig tussen partijen welke van deze gestandaardiseerde methoden zullen worden ingezet en op welke wijze.

Binnen de architectuur van AORTA is er voor gekozen om gegevensberichten te baseren op HL7v3 of HL7 FHIR, een internationaal geaccepteerde open standaard voor uitwisseling van medische informatie.

7.3.8 Het zoeken van gegevenshouders en gegevensontvangers

Bij het opvragen van patiëntgegevens door een gegevensraadpleger kan er sprake zijn van meerdere gegevenshouders en hoeven de gegevenshouders in de praktijk niet bekend te zijn bij de gegevensraadpleger.

AORTA adresseert dit probleem door het introduceren van een intermediair, het Landelijk Schakelpunt (LSP).

Het Landelijk Schakelpunt is een intermediaire organisatie die diensten verleend aan zorgaanbieders die zorginformatie willen uitwisselen en waarbij de gegevenshouders de beschikbaarheid van gegevens over patiënten kunnen aanmelden.

Door het aanmelden worden deze locatie gegevens opgenomen in een Verwijsindex.

De Verwijsindex (VWI) is een register waarin vastligt welke gegevenshouders over patiëntgegevens van specifieke patiënten beschikken.

Vervolgens kunnen gegevensraadplegers via de intermediair de beschikbare gegevens opvragen, zonder dat de gegevensraadpleger elke gegevenshouder afzonderlijk hoeft te benaderen.

Overigens is voor het aanmelden van gegevens bij de verwijsindex het verkrijgen van toestemming vooraf van de patiënt (opt-in) vereist.

De gegevensraadplegers en de gegevenshouders maken bij dit mechanisme één set van afspraken met de intermediair over uitwisselingsformaten, beveiligingsaspecten en dergelijke.

De voordelen van deze oplossing zijn:

- Gegevenshouders en gegevensraadplegers hoeven elkaar niet te kennen; het bijhouden van gegevenslocaties en het verzamelen van gegevens afkomstig van verschillende locaties wordt door de intermediair voor de gegevensraadpleger opgelost;
- Alleen gegevenshouders die over informatie beschikken worden om informatie gevraagd;
- Gegevenshouders en gegevensraadplegers hoeven slechts één set van afspraken te maken over de randvoorwaarden van gegevensuitwisseling.

Indien een gegevensraadpleger een specifieke gegevenshouder(s) wil bevragen, dan wordt de VWI niet geraadpleegd. Als dit systeem gemigreerd is naar Mitz, wordt Mitz wel bevraagd met een **gesloten** vraag [[MITZ-IHOG \(see page 643\)](#)] om te kijken of er toestemming gegeven is voor het bevragen van dit systeem.

Om te kunnen bepalen aan welke gegevensbronnen toestemming is verleend door de patiënt voor opvraging, wordt er eerst een **open** vraag uitgezet bij Mitz. Hiermee worden alle systemen gevonden die de patiënttoestemmingen gemigreerd hebben naar Mitz. De systemen die nog niet gemigreerd zijn worden gevonden door de VWI te bevragen.

Bij het versturen van gegevens is het minder waarschijnlijk dat de gegevenszender de gegevensontvanger niet kent, maar er doen zich wel soortgelijke vraagstukken voor:

- De manier waarop verschillende gegevensontvangers kunnen worden geadresseerd kan verschillen.
- Er moeten ook in dit geval afspraken worden gemaakt over diverse technische aspecten van de uitwisseling.

Door ook bij het verzenden van gegevens gebruik te maken van het LSP als intermediair, kunnen de wijze van adressering en de technische aspecten van gegevensuitwisseling worden gestandaardiseerd.

Daarnaast biedt een adresboek een mogelijkheid om identificerende zorgaanbieder- en zorgverlener gegevens op te zoeken met de bijbehorende (technische) adressering. Hiervoor is aangesloten op ZORG-AB, is een database waarin diverse zorgaanbidersgegevens en zorgverlenersgegevens zijn opgeslagen en raadpleegbaar worden gemaakt voor derden.

Bij de bespreking van de informatiesysteem aspecten van de architectuur (vanaf hoofdstuk 6) worden de concepten van gegevensuitwisseling via een intermediair en verwijzindex verder uitgewerkt.

7.4 Ondersteunende interacties

In dit hoofdstuk worden de ondersteunende interacties en de gerelateerde onderdelen beschreven.

7.4.1 Ondersteunende interacties.

Naast de primaire interacties van opvragen en sturen van patiëntgegevens, biedt AORTA een aantal ondersteunende ('secundaire') interacties. Een overzicht van de ondersteunende interacties wordt gegeven in diagram AORTA.ALG.d1030.5.

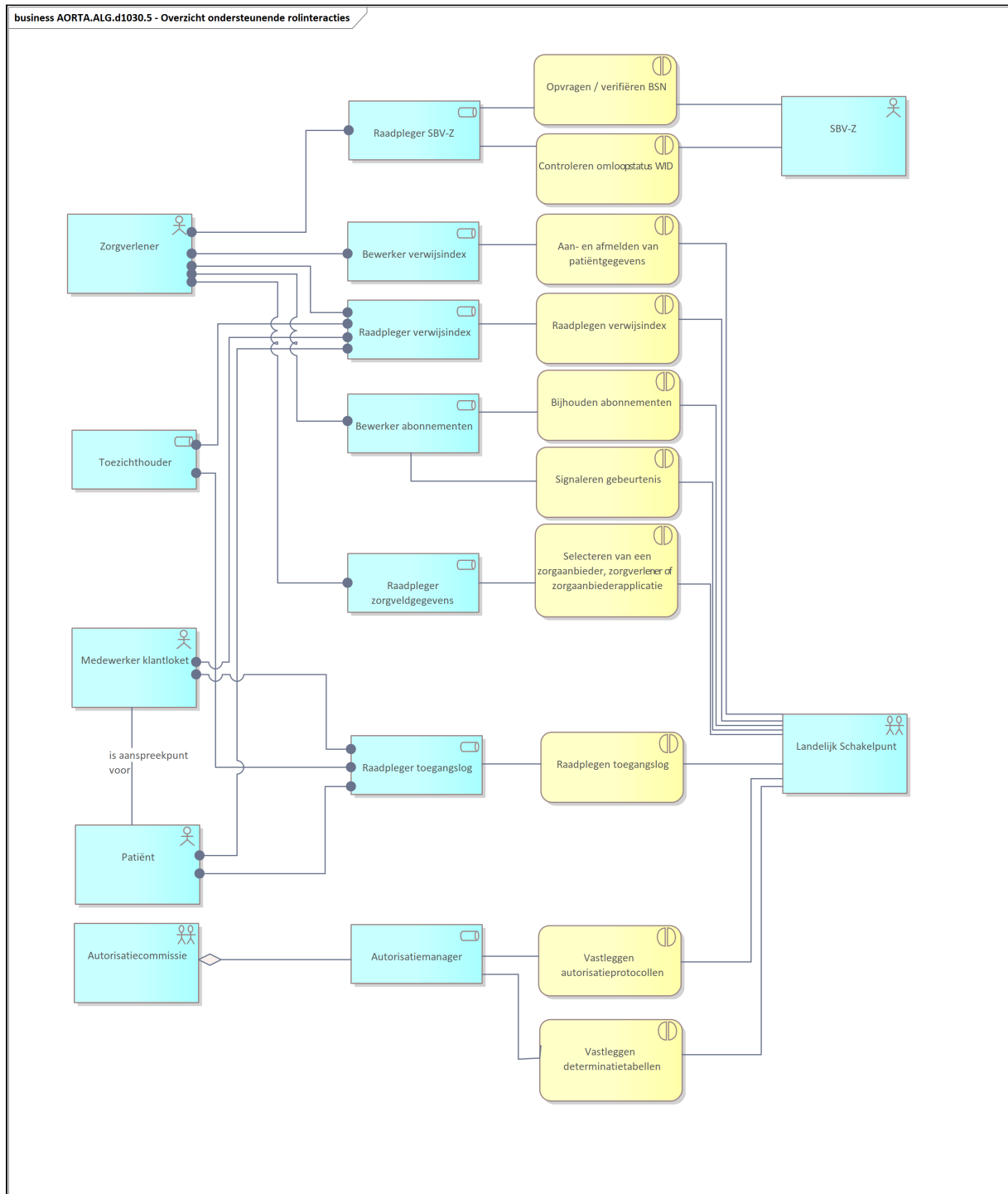


Diagram AORTA.ALG.d1030.5 - overzicht van ondersteunende interacties

Bij de volgende ondersteunende interactie wisselen eindgebruikers gegevens uit met de Sectorale Berichten Voorziening in de Zorg (SBV-Z) (zie pagina [Actoren en rollen](#)¹⁸):

- Opvragen/verifiëren BSN;
- Controleren omloopstatus WID.

Bij de volgende ondersteunende interacties wisselen eindgebruikers gegevens uit met het LSP, in plaats van met een andere eindgebruiker:

- aan- en afmelden van patiëntgegevens;
- raadplegen van de verwijsindex;
- bijhouden van abonnementen op specifieke gebeurtenissen, zoals wijzigingen in patiëntgegevens;
- selecteren van zorgaanbieders, zorgverleners en zorgaanbiederapplicaties;
- raadplegen van een toegangsllog;
- vastleggen van autorisatieprotocollen;
- vastleggen van determinatietabellen.

De bovenstaande interacties worden vanaf [zie pagina [Opvragen/verifiëren BSN en controleren omloopstatus WID](#)¹⁹] besproken.

7.4.2 Ondersteunende informatiesysteeminteracties

Op deze pagina worden de [ondersteunende interacties](#)²⁰ op informatiesysteemniveau uitgewerkt.

7.4.2.1 Opvragen/verifiëren BSN en controleren omloopstatus WID

De [SBV-Z](#) (see [page 115](#)) biedt interfaces voor:

- Opvragen/verifiëren BSN – deze interface maakt het mogelijk om op basis van een aantal persoonsgegevens het Burgerservicenummer van een persoon op te vragen, of te controleren of bepaalde persoonsgegevens en een bekend BSN daadwerkelijk bij elkaar horen;
- Opvragen persoonsgegevens – deze interface maakt het mogelijk om persoonsgegevens te verkrijgen op basis van het BSN;
- WID-controle – deze interface maakt het mogelijk om de omloopstatus van een Nederlands identiteitsdocument te controleren.

18. <https://vzvz.atlassian.net/wiki/x/-wARBQ>

19. <https://vzvz.atlassian.net/wiki/x/JgIRBQ>

20. <https://vzvz.atlassian.net/wiki/x/ewQRBQ>

De systeemrol die deze interfaces gebruikt wordt aangeduid als 'patiënt administrerend systeem'. Omdat binnen AORTA bij communicatie over patiënten een correct BSN nodig is, moet een GBZ geaccepteerd zijn voor een 'patiënt administrerend systeem'.

Deze interfaces vallen buiten de specificaties van AORTA, aangezien de specificaties worden beheerd door de SBV-Z (zie [SBV-Z]). Voor AORTA is nog relevant dat van deze interfaces twee implementatievarianten bestaan, waarvan één gebaseerd op HL7v3-berichten. Het GBZ zou de interface gebaseerd op HL7v3 niet moeten gebruiken. Deze is niet meer actueel.

7.4.2.2 Aan- en afmelden van patiëntgegevens

Om een ongerichte opvraag van patiëntgegevens via AORTA door andere zorgverleners mogelijk te maken, moet een zorgaanbieder het bestaan van patiëntgegevens in zijn eigen informatiesysteem aanmelden bij het Landelijk Schakelpunt. In het geval er geen gebruik wordt gemaakt van Mitz, zullen er alleen patiëntgegevens worden aangemeld van die patiënten die ook daadwerkelijk toestemming hebben gegeven.

Deze aanmelding leidt tot het opnemen van een nieuwe verwijzing in de Verwijsindex (VWI) of het Actualiteitenregister (AR) die onderdeel zijn van de ZIM. Deze verwijzing bevat geen medisch inhoudelijke informatie, maar bevat metagegevens over de informatie die in het systeem van de aanmeldende zorgverlener aanwezig is, waaronder het patiëntnummer (BSN) en bouwsteentype. Het (mogelijke) onderscheid in bouwsteentypen wordt onder meer gebruikt om toegang van zorgverleners te kunnen beperken tot specifieke delen van het medische dossier van een patiënt.

De aanmelding bij de VWI gebeurt per bouwsteentype. Er komt per bouwsteentype per bronsysteem per patiënt één verwijzing in de VWI.

De ZIM biedt voor de aanmelding een aantal interfaces die zijn toegekend aan services van de Verwijsindex:

- LSP.VWI.i1025: Publiceren gegevens;
- LSP.VWI.i1035: Afmelden verwijzing.
- LSP.VWI.i1090: Synchroniseren indexgegevens met vergelijking.

Deze situatie is weergegeven in diagram AORTA.VWI.d1010. De interfaces worden hier kort behandeld, zie [Ontw VWI] voor details.

Indien het aanmeldende systeem is gemigreerd naar Mitz, word er gekeken of er voor deze BSN/ applicatie-ID combinatie al een toestemming abonnement genomen is. Indien dit niet het geval is, wordt het proces Toestemming Abonnement opgestart.

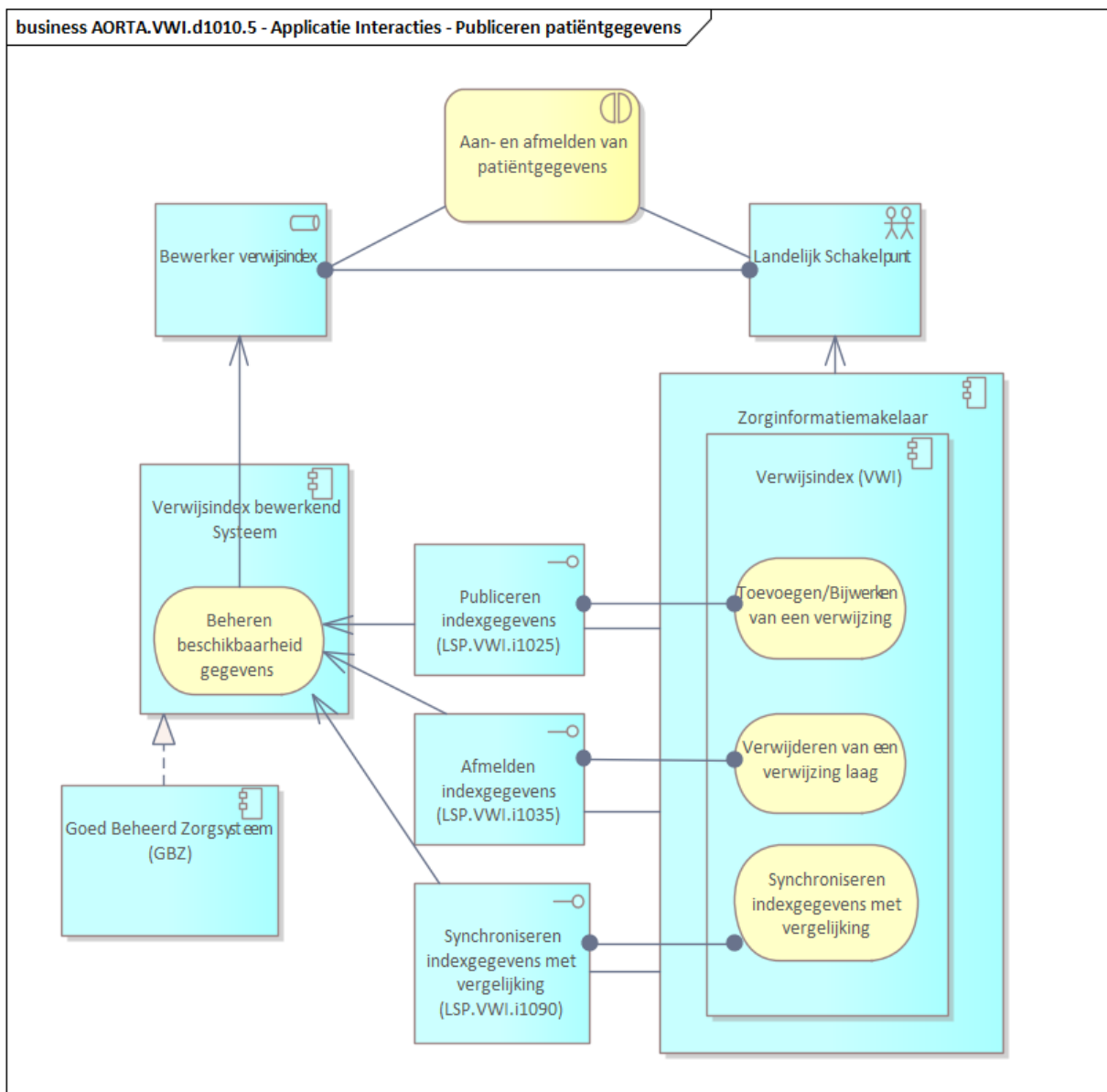


Diagram AORTA.VWI.d1010 - informatiesysteeminteracties voor het beschikbaar maken van patiëntgegevens

7.4.2.2.1 Interface LSP.VWI.i1025: Publiceren gegevens

Een (her)aanmelding wordt geïnitieerd vanuit het informatiesysteem van de zorgverlener. De (her)aanmelding leidt tot toevoegen of bijwerken van een verwijzing in de Verwijsindex (VWI). Een van de voorwaarden voor aanmelden is dat de zorgverlener de identiteit en Burgerservicenummer van de patiënt heeft geverifieerd. Deze interface wordt aangesproken op vertrouwensniveau laag.

7.4.2.2.2 Interface LSP.VWI.i2035: Afmelden verwijzing

Een zorgverlener of het systeem heeft de mogelijkheid om eerder aangemelde gegevens weer af te melden. Hierbij wordt de desbetreffende verwijzing uit de VWI verwijderd. Deze interface wordt aangesproken op vertrouwensniveau laag.

7.4.2.2.3 Interface LSP.VWI.i1090: Synchroniseren indexgegevens met vergelijking

Het synchronisatieproces wordt gestart door een GBZ-beheerder. Door gebruik te maken van deze interface worden de geregistreerde verwijzingen in de VWI gesynchroniseerd met de lokale administratie van verwijzingen in het GBZ. De 'synchroniseren indexgegevens met vergelijking'-interface levert slechts een vergelijkingsresultaat op. In combinatie met de interfaces LSP.VWI.i1025 Publiceren gegevens en LSP.VWI.i1035 Afmelden indexgegevens laag kunnen de verwijzingen in de VWI worden aangepast.

7.4.2.2.4 Controle op opt-in bij het aanmelden van patiëntgegevens

Bij het aanmelden/publiceren van patiëntgegevens voor uitwisseling via AORTA is het van belang dat vooraf door de gegevenshouder toestemming ('opt-in') is verkregen van de patiënt voor het beschikbaar maken van zijn gegevens. Daarom wordt bij het (her)aanmelden door de gegevenshouder gecontroleerd of de vereiste opt-in van de patiënt is verkregen. Dit moet gebeuren in het GBx dat een (her)aanmelding verricht.

Diagram AORTA.VWI.d1060 beschrijft globaal het proces en de controles die van toepassing zijn bij het aanmelden van patiëntgegevens. Een nadere uitwerking hiervan op systeemniveau is opgenomen in het [Ontw VWI].

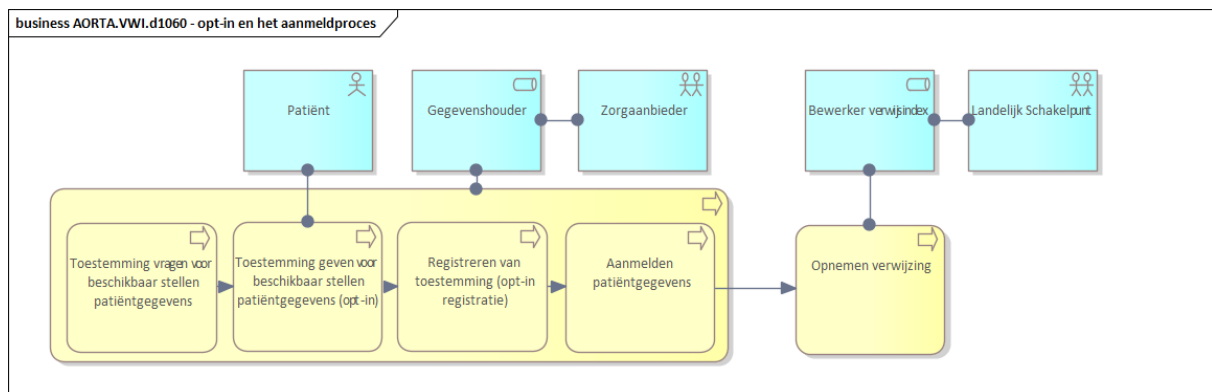
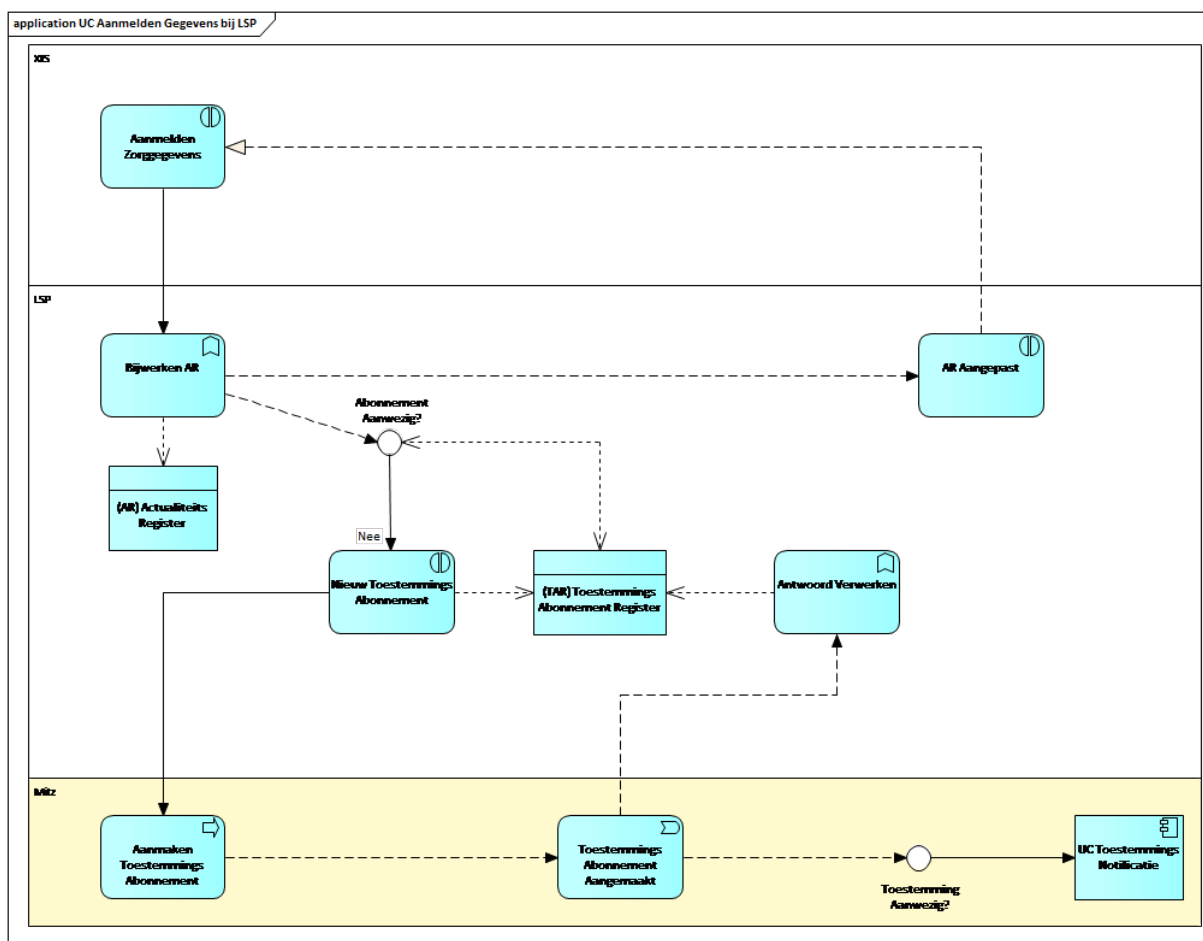


Diagram AORTA.VWI.d1060 - Opt-in en het aanmeldproces

1. Elke zorgverlener die als gegevenshouder verantwoordelijk is voor het beschikbaar stellen van gegevens via het Landelijk Schakelpunt vraagt (eenmalig voor een bepaalde toepassing) toestemming aan de patiënt voor het beschikbaar stellen van diens patiëntgegevens.
2. De patiënt geeft (eenmalig per zorgverlener) toestemming voor het beschikbaar stellen van patiëntgegevens. Uiteraard kan de patiënt ook besluiten hiervoor geen toestemming te geven of deze later in te trekken.

3. De gegevenshouder registreert het geven van toestemming (of het niet geven van toestemming) door de patiënt.
4. De gegevenshouder meldt de gegevens van de patiënt aan bij het Landelijk Schakelpunt, dat optreedt als bewerker van de verwijzingsindex. [1] Aanmelden mag alleen indien toestemming verkregen is en dit uit de eigen registratie blijkt. De verantwoordelijkheid voor het correct aanmelden ligt bij de gegevenshouder. De gegevenshouder kan ervoor kiezen om aanmeldingen automatisch te laten uitvoeren door het eigen informatiesysteem (XIS), mits dit alleen aanmeldingen uitvoert voor patiënten waarvoor een opt-in in de registratie is opgenomen.
5. De bewerker van de verwijzingsindex neemt de verwijzing op.

7.4.2.3 Toestemming abonnement



Processtappen

Binnen deze processtappen wordt er vanuit gegaan dat de XIS geïmigreerd is naar Mitz. Indien dit niet het geval is blijft de oude situatie van kracht.

Aanmelden patiëntgegevens (XIS)

Het proces begint op de XIS, waar patiënt gegevens zijn veranderd. Zonder te hoeven kijken naar toestemmingen, worden deze gegevens aangemeld bij het LSP. Hierbij kunnen de gegevens zowel in bouwstenen als in gegevens soorten verdeeld zijn. Alles wordt aangemeld. (Zie [Aan- en afmelden van patiëntgegevens](#)²¹⁾)

Abonnement aanwezig? (LSP)

Na dit aanmelden gaat het LSP kijken of er wel een toestemming abonnement is afgenomen voor deze zorgapplicatie voor deze BSN. Deze abonnementen worden voor het LSP door Mitz bijgehouden in het toestemming abonnement register.

Als een toestemmingsabonnement geregistreerd is, wordt er aan het XIS gemeld dat het Actualiteitsregister (ACT) is aangepast en zijn er verder geen acties nodig.

Nieuw Toestemming Abonnement (LSP)

Indien er nog geen toestemming abonnement is genomen, dan neemt het LSP deze automatisch, hiervoor hoeft de XIS niets te doen of bij te houden.

In het Toestemming Abonnement Register wordt nu de Applicatie Id, huidige datum/tijd en BSN genoteerd. Dit wordt op deze plaats gedaan, zodat je bij meerdere aanmeldingen geen meerdere aanvragen krijgt. Meerdere aanvragen zou later tot een probleem kunnen leiden.

Voor de interface naar Mitz voor het aanmaken van een nieuw toestemming abonnement zie [\[MitzToe \(see page 286\)\]](#)

Aanmaken Toestemming Abonnement (Mitz)

Deze en de volgende stap wordt uitgevoerd door Mitz. Hier heeft het LSP verder geen invloed op. Ze zijn hier opgenomen om het proces duidelijker te maken.

In deze stap maakt Mitz een toestemming abonnement.

Toestemming Aanmaken (Mitz)

De volgende stap is dat Mitz kijkt of er al toestemming staan voor de combinatie van applicatie_id en BSN. Indien dit het geval is, wordt er een notificatie verstuurd naar het LSP.

Antwoord Verwerkt (LSP)

21. <https://vzvz.atlassian.net/wiki/spaces/AORTA84/pages/879592561/Ondersteunende+informatiesysteeminteracties#Ondersteunendeinformatiesysteeminteracties-Aan-enafmeldenvanpatiëntgegevens>

Ondersteunende+informatiesysteeminteracties#Ondersteunendeinformatiesysteeminteracties-Aan-enafmeldenvanpatiëntgegevens

Aan het LSP wordt gemeld dat er een abonnement is aangemaakt en met welk ID dat het is opgeslagen. Deze wordt door het LSP in het toestemming abonnement register bijgewerkt, door deze gegevens in het record erbij te zetten, dat eerder in de stap "Nieuw Toestemming Abonnement" is aangemaakt.

Indien het niet mogelijk was om dit abonnement te maken, wordt het in de stap "Nieuw Toestemming Abonnement" aangemaakte record gemarkeerd als "incomplete".

7.4.2.4 Raadplegen van de verwijfsindex

De Verwijsindex (VWI), die onderdeel is van de ZIM, houdt bij in welke informatiesystemen gegevens over patiënten zijn opgeslagen.

De ZIM biedt de volgende interface voor de bevraging van de verwijfsindex:

- LSP.VWI.i1060: Actualiteit controle;
- LSP.VWI.i1080: Opvragen indexgegevens midden.

Deze situatie is weergegeven in diagram AORTA.VWI.d1020.3 .

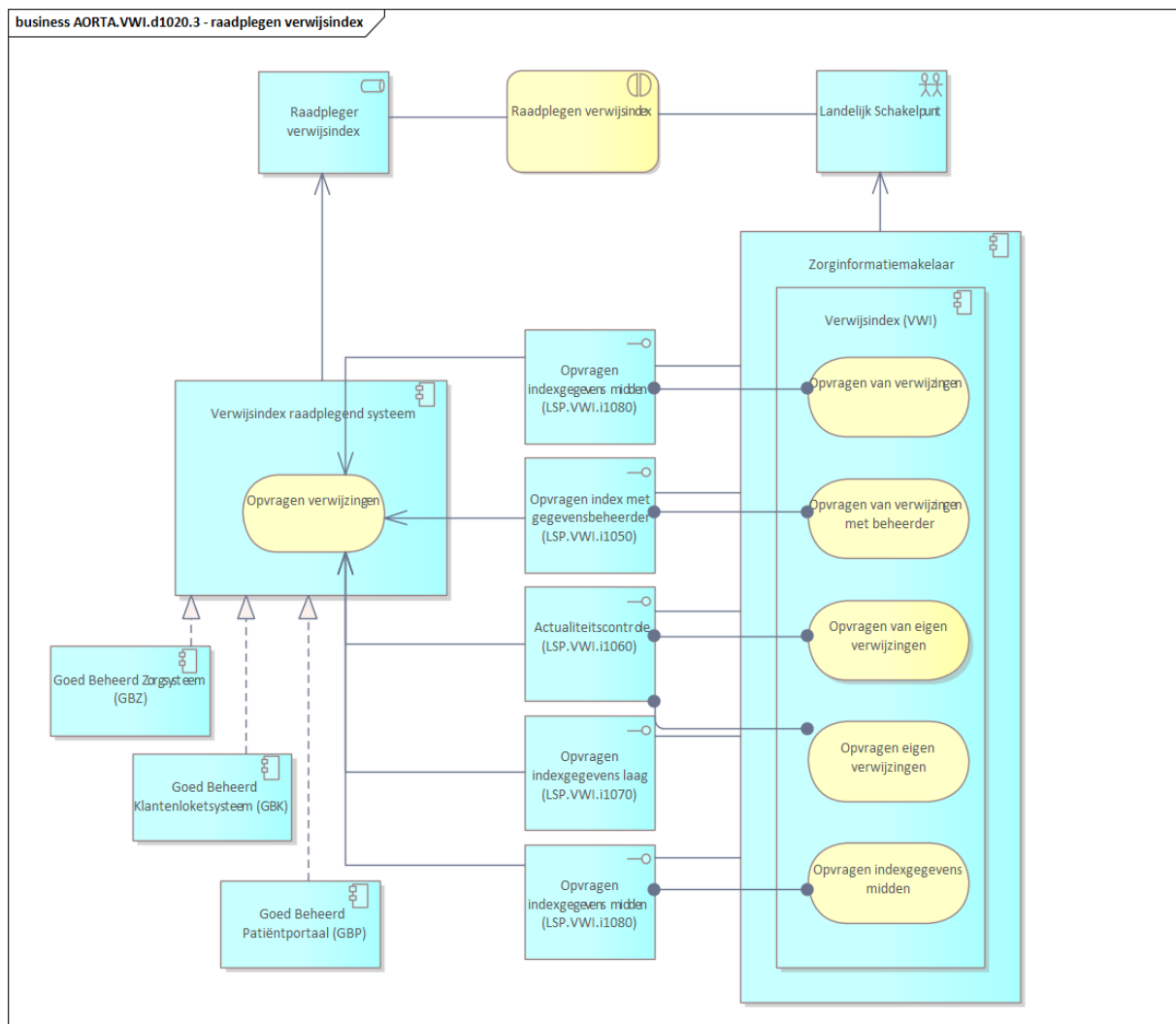


Diagram AORTA.VWI.d1020.3 - informatiesysteeminteracties voor het raadplegen van de verwijfsindex

7.4.2.4.1 Interface LSP.VWI.i1060: Actualiteit controle

Om te bepalen of er nieuwe gegevens beschikbaar zijn gekomen sinds een bepaalde datum kan een GBZ via de service 'Opvragen actualiteit' een actualiteit controle verzoek doen aan de ZIM. De ZIM kijkt of er na de opgenomen tijd een VWI bijwerking is geweest voor de in het bericht opgenomen queryparameters. Als antwoord op het verzoek komt er een bevestiging of ontkening terug. Voor het opvragen van de actualiteit wordt het opvragen Actualiteit-bericht verstuurd op autorisatie-niveau laag door het Verwijsindex Raadplegend Systeem.

7.4.2.4.2 Interface LSP.VWI.i1080: opvragen index midden

De 'opvragen index' interface biedt de mogelijkheid om een overzicht op te vragen van de verwijfsindex zoals die aanwezig zijn in de VWI van de ZIM voor een specifieke patiënt. Het opvragen van de index kan vanuit een op de ZIM aangesloten informatiesysteem (GBZ, GBK, GBO) plaatsvinden. Een verwijfsindex bevat onder meer de gegevenssoort of het bouwsteentype, de zorgaanbieder die de

gegevens heeft aangemeld en een tijdsinterval waarover gegevens beschikbaar zijn (zie [Ontw VWI] voor details).

Nadat het GBx heeft vastgesteld welke verwijzingen in de VWI aanwezig zijn, kan het GBx meer gericht naar inhoudelijke gegevens vragen. Deze interface wordt aangesproken op vertrouwensniveau midden.

7.4.2.5 Toestemming Abonnement Register

In het toestemming Abonnement register wordt bijgehouden of een applicatie voor een BSN een abonnement heeft genomen.

Dit is van belang om binnen het LSP bij te houden, omdat bij het **afmelden** van een abonnement een ID moet worden meegegeven. Dit ID wordt bepaald door Mitz en wordt na het aanmaken van het abonnement teruggegeven.

Het register bevat de volgende velden:

Veld	Omschrijving
Applicatie ID	
BSN	
Aanmaak Datum/Tijd	
Abonnement ID	Komt van Mitz
Error Indicatie	Geeft aan dat er wel wat is aangevraagd, maar dat er een fout antwoord is terug gekomen. Staat initieel op false

7.4.2.6 Verwijderen Toestemming Abonnement

<Dit wordt pas in de volgende versie ondersteund>

7.4.2.7 Bijhouden van abonnementen en signaleren van gebeurtenissen

Zorgverleners kunnen zich abonneren op het optreden van specifieke gebeurtenissen in de ZIM, zoals bijvoorbeeld het optreden van wijzigingen in de verwijsindex voor een bepaalde patiënt. Daarnaast is het voor de patiënt mogelijk om zich te abonneren op verzonden berichten over het LSP met zijn persoon als onderwerp en op mogelijke aanmeldingen in de verwijsindex. De ZIM stuurt dan automatisch een abonnement signaal indien de gebeurtenis optreedt. Bij het aangaan van het abonnement kan het abonnerend systeem het informatiesysteem opgeven (binnen dezelfde zorgaanbieder) waarvoor het signaal bedoeld is. Het informatiesysteem dat het signaal ontvangt moet

hiertoe beschikken over een module die wordt aangeduid als ‘abonnement signaal ontvangend systeem’.

De systeemrollen ‘abonnerend systeem’ en ‘abonnement signaal ontvangend systeem’ kunnen door hetzelfde informatiesysteem worden gerealiseerd, maar dit hoeft niet, zolang de informatiesystemen maar onder dezelfde zorgaanbieder vallen.

De ZIM biedt de volgende interfaces voor het bijhouden van abonnementen:

- LSP.ABR.i1010: Registreren abonnement
- LSP.ABR.i1020: Beëindigen abonnement
- LSP.ABR.i1030: Opvragen abonnementen

De ZIM beschikt over een abonnement signaleringsafhandelaar die zorgt voor het sturen van berichten in het geval een gebeurtenis zich voordoet (zie voor details het [Ontw Sgl GBV]).

Om signaleringen van opgetreden gebeurtenissen te kunnen ontvangen moet het abonnement signaal ontvangend systeem in staat zijn om abonnement signaal-berichten te verwerken. Hiervoor moet het de volgende interface aanbieden:

- GBX.SGL.i1050: Verwerken abonnement signaal

Deze situatie is weergegeven in diagram AORTA.ABR.d1010.

7.4.2.7.1 Interface LSP.ABR.i1010: Registreren abonnement

De ‘registreren abonnement’ interface biedt de mogelijkheid om een abonnement te registreren voor een specifieke gebeurtenis in de ZIM, zoals het optreden van een nieuwe aanmelding van gegevens van een patiënt. Het registreren van een abonnement vindt plaats vanuit een abonnerend systeem.

7.4.2.7.2 Interface LSP.ABR.i1020: Beëindigen abonnement

De ‘beëindigen abonnement’ interface biedt de mogelijkheid om een eerder geregistreerd abonnement te beëindigen. Eventueel kan het abonnerend systeem vooraf de geregistreerde abonnementen opvragen via LSP.ABR.i1030.

7.4.2.7.3 Interface LSP.ABR.i1030: Opvragen abonnementen

De ‘opvragen abonnementen’ interface biedt de mogelijkheid om een lijst op te vragen van de gebeurtenissen per patiënt waarop het abonnerend systeem een abonnement heeft genomen. Een abonnerend systeem kan via deze interface de eigen abonnementen van een zorgverlener opvragen.

7.4.2.7.4 Interface GBX.SGL.i1050: Verwerken abonnement signaal

De interface 'verwerken abonnement signaal' moet door een abonnement signaal-ontvangend systeem geïmplementeerd worden zodat het signalen kan ontvangen indien één van de gebeurtenissen optreedt waarop via het abonnerend systeem een abonnement is genomen. Een abonnement signaalbericht bevat geen medisch inhoudelijke informatie. Het ontvangen van een abonnement signaalbericht kan eventueel aanleiding zijn om vervolgens medisch inhoudelijke informatie via de ZIM op te vragen.

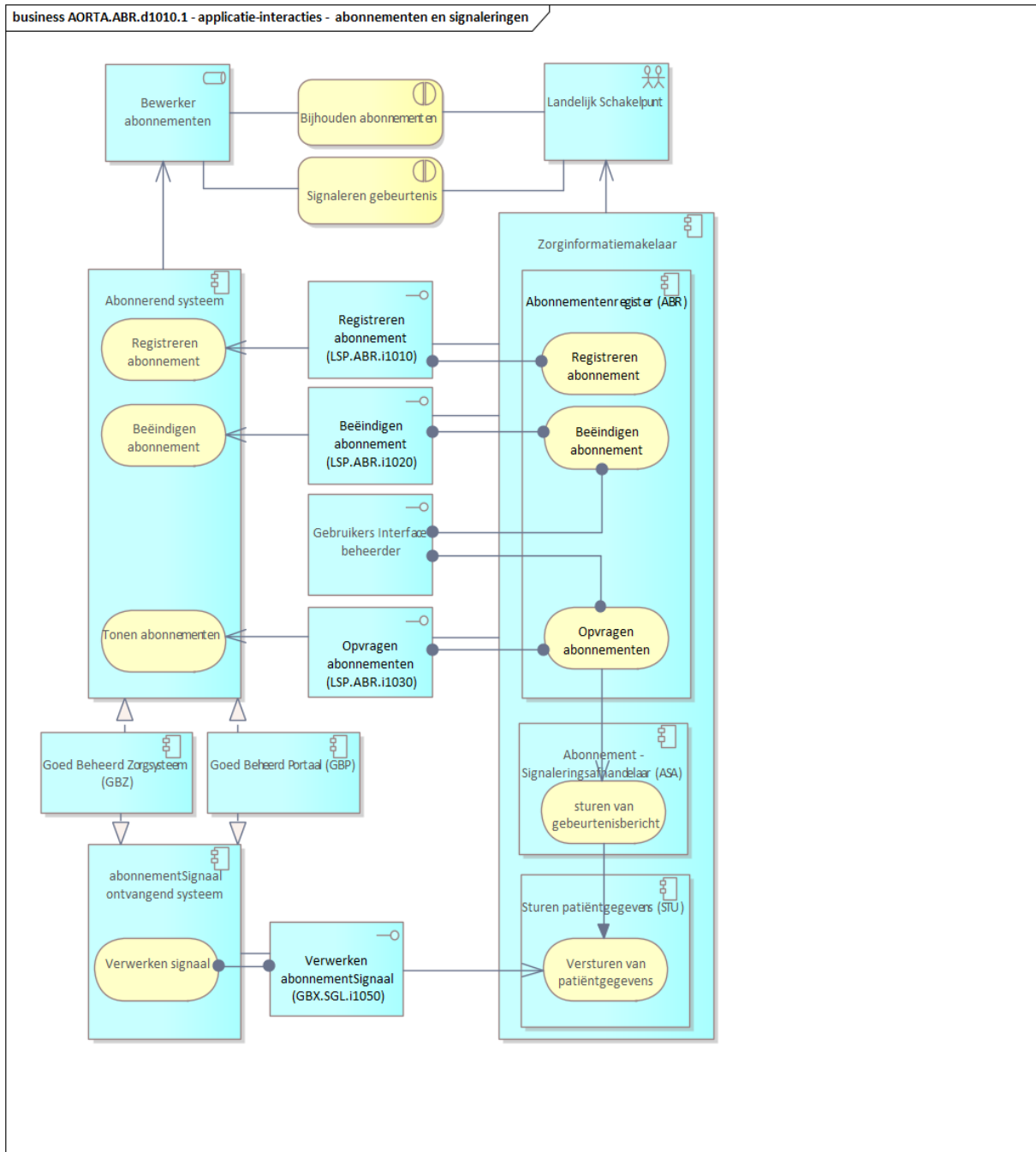


Diagram AORTA.ABR.d1010 – informatiesysteeminteracties – abonnementen en signaleringen

Zie voor een verdere behandeling van het abonnementenregister en de signaleringsafhandelaar de ontwerpen [Ontw Sgl ABR] en [Ontw Sgl GBV].

7.4.2.8 Selecteren van zorgaanbieders, zorgverleners en zorgaanbiederapplicaties

De ZAB stelt aangesloten informatiesystemen in staat om beschrijvende gegevens te achterhalen over de zorgaanbieder of zorgverlener, bijvoorbeeld de naam van een zorgaanbieder voor presentatie aan de eindgebruiker. Ook kunnen gegevens van aangesloten GBZ'en worden opgevraagd.

Deze functionaliteit is onder meer nodig bij het versturen van informatie via de ZIM naar het informatiesysteem van een andere zorgaanbieder. Hiervoor heeft de zendende partij het unieke applicatielD nodig van het informatiesysteem van de ontvanger.

De ZAB stelt hiertoe interfaces beschikbaar die toegang geven tot informatie uit twee ondersteunende componenten van het LSP, het ZAB en het Applicatieregister (APR). De ZAB heeft een koppeling met het APR om daar de benodigde informatie op te halen.

De ZAB biedt interfaces om gegevens op te vragen, aan te vullen, bij te werken en te verwijderen. De diverse interfaces zijn beschreven in het [Ontwerp ZAB].

Binnen het goed beheerd zorgsysteem van de opvragende zorgverlener moeten hiertoe modules aanwezig zijn die het gebruik van deze interface ondersteunen. Deze modules zijn hier aangeduid als 'zorgadresboek raadplegend systeem' en 'zorgadresboek bewerkend systeem'.

7.4.2.9 Raadplegen van de toegangslog

De toegangslog (TLG), die onderdeel is van de ZIM, houdt bij welke toegangsgebeurtenissen hebben plaatsgevonden waarbij berichten met de ZIM zijn uitgewisseld door op de ZIM aangesloten informatiesystemen.

De ZIM biedt één interface voor het *raadplegen* van de toegangslog:

- LSP.TLG.i1010: Raadplegen toegangslog.

Deze interface is toegankelijk voor de patiënt via een GBP[2] en voor medewerkers van het Klantenloket via het GBK. Deze informatiesystemen moeten hiertoe een module implementeren die aangemerkt wordt als 'toegangslog raadplegend systeem'.

De ZIM stelt aan informatiesystemen die op de ZIM zijn aangesloten geen externe interface beschikbaar om rechtstreeks te communiceren met de daadwerkelijke logging service van de toegangslog. In plaats daarvan wordt de logging service aangeroepen als onderdeel van het afhandelen van andere berichtuitwisselingen tussen ZIM en aangesloten informatiesystemen, zoals het opvragen van patiëntgegevens. Hiertoe biedt de logging component één service aan andere componenten binnen de ZIM aan:

- Registreren toegangsgebeurtenis.

Deze situatie is weergegeven in een diagram AORTA.TLG.d1010. De interfaces worden hier kort behandeld. Zie voor meer detail het [Ontw TLG].

7.4.2.9.1 Interface LSP.TLG.i1010: raadplegen toegangslog

De interface 'raadplegen toegangslog' biedt de mogelijkheid om op te vragen welke berichten met de ZIM zijn uitgewisseld door aangesloten informatiesystemen over een specifieke patiënt. Het opvragen van het toegangslog kan vanuit een op de ZIM aangesloten GBP of GBK plaatsvinden.

7.4.2.9.2 ZIM-interne service: registreren toegangsgebeurtenis

De toegangslog biedt deze service aan andere componenten binnen de ZIM om gegevens over het uitwisselen van berichten met informatiesystemen te registreren. De ZIM gebruikt deze service tijdens elke berichtafhandeling waarbij een informatiesysteem betrokken is. Dit legt de basis voor inzicht in de traceerbaarheid van gegevensuitwisseling via AORTA.

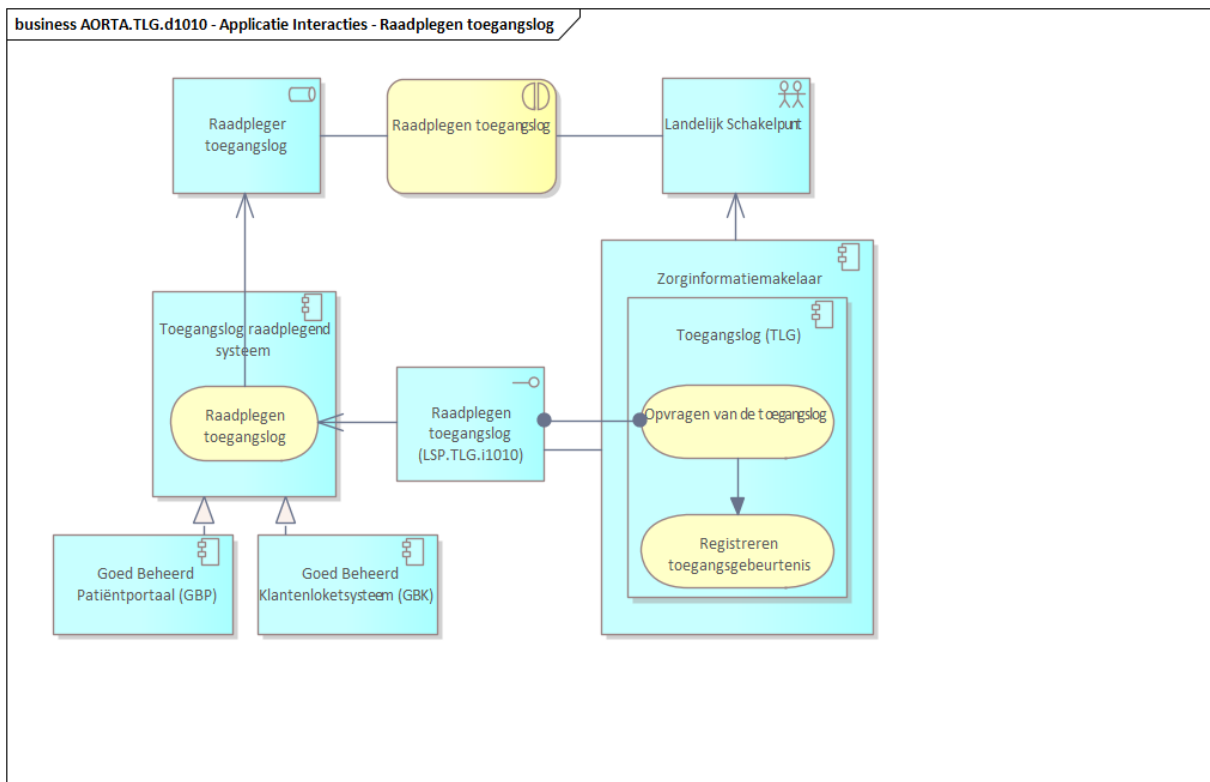


Diagram AORTA.TLG.d1010 - informatiesysteeminteracties voor raadplegen van de toegangsllog

7.4.2.10 Vastleggen autorisatieprotocollen

Het autorisatieprotocol (APT) is een component van de ZIM die:

- voor alle beroepen en specialisaties van zorgverleners vastlegt per gegevenssoort of per context welke berichtuitwisselingen via AORTA zijn toegestaan; voor de combinatie van beroep en specialisatie wordt hierbij een rolcode gebruikt;
- voor rolcodes van niet-zorgverleners (bijvoorbeeld patiënt, ouder, voogd) vastlegt per gegevenssoort of per context welke berichtuitwisselingen via AORTA zijn toegestaan.

Daarnaast legt de ZIM in het Applicatieregister (APR) vast voor welke interacties de op de ZIM aangesloten informatiesystemen zijn geautoriseerd, door een aangesloten informatiesysteem te koppelen aan een zogenaamde 'HL7v3 conformancetabel'. Deze tabel wordt bij autorisatie gebruikt om te controleren of een applicatie een bepaald bericht mag verzenden en/of mag ontvangen.

De gewenste instellingen voor het autorisatieprotocol worden vastgesteld door een autorisatiecommissie waarin medische beroepsverenigingen en patiëntenverenigingen vertegenwoordigd zijn. Deze instellingen worden op last van de autorisatiemanager in het systeem aangebracht door een medewerker van het landelijk schakelpunt in de rol van autorisatiebeheerder van de ZIM.

Hiertoe is een beheerderinterface op de ZIM beschikbaar die toegang geeft tot een beheerservice voor autorisatieprotocol. Deze beheerservice ondersteunt twee functies, namelijk:

- raadplegen autorisatieprotocol;
- aanpassen autorisatieprotocol.

De ZIM stelt vooralsnog geen externe interface beschikbaar aan op de ZIM aangesloten informatiesystemen om direct te communiceren met de services van het autorisatieprotocol. In plaats daarvan wordt het autorisatieprotocol gecontroleerd als onderdeel van het afhandelen van berichtuitwisselingen tussen ZIM en aangesloten informatiesystemen, zoals het opvragen van patiëntgegevens. Hiertoe biedt het autorisatieprotocol twee services aan andere componenten binnen de ZIM aan:

- autoriseren van rol voor interactie;
- autoriseren van applicatie voor interactie.

Deze situatie is weergegeven in diagram AORTA.APT.d1010.1.

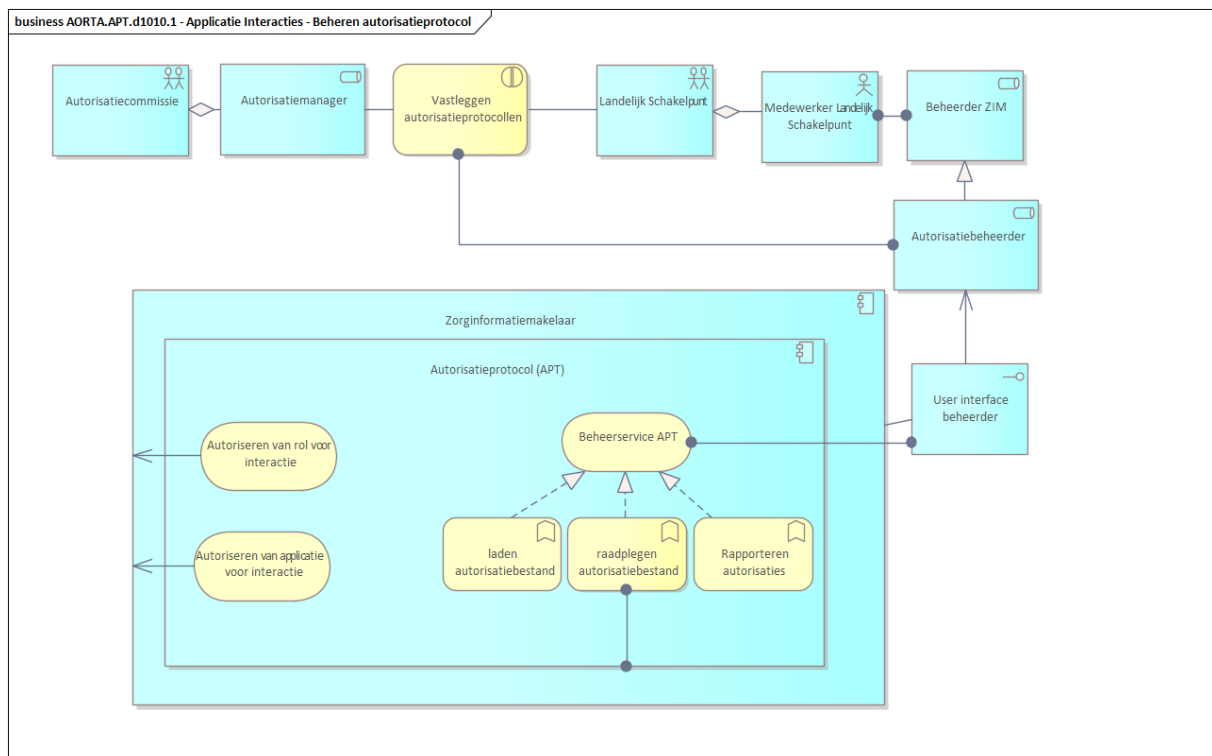


Diagram AORTA.APT.d1010.1 - informatiesysteeminteracties voor het beheer van het autorisatieprotocol

7.4.2.10.1 ZIM-interne service: autoriseren van rol voor interactie

De autorisatieprotocolcomponent biedt aan andere componenten binnen de ZIM een service 'autoriseren van rol voor interactie' om te bepalen of een inkomend bericht is toegestaan voor de rolcode van de afzender van het bericht. De ZIM gebruikt deze service tijdens elke berichtafhandeling (behoudens enkele uitzonderingssituaties, zie [Ontw APT]). Deze controle veroorzaakt een foutbericht indien het te controleren bericht een onbekende zorgverlenerfunctie of rolcode bevat of indien de rolcode niet is geautoriseerd voor het berichttype.

7.4.2.10.2 ZIM-interne service: autoriseren van applicatie voor interactie

De autorisatieprotocolcomponent biedt aan andere componenten binnen de ZIM een service 'autoriseren van applicatie voor interactie' om te bepalen of een inkomend bericht is toegestaan voor de applicatie die het bericht heeft ingestuurd. De ZIM gebruikt deze service tijdens elke berichtafhandeling (behoudens enkele uitzonderingssituaties, zie [Ontw APT]). Deze controle veroorzaakt een foutbericht indien de verzendende applicatie niet is geautoriseerd voor het desbetreffende berichttype.

7.4.2.10.3 Beheerfunctie 'raadplegen autorisatiebestand'

Met de functie 'raadplegen autorisatiebestand' kan de autorisatiebeheerder de instellingen van het autorisatieprotocol raadplegen. Hierbij is de ingangsdatum vast te stellen van elke autorisatie van een specifieke rolcode voor een specifiek berichttype.

7.4.2.10.4 Beheerfunctie 'laden autorisatiebestand'

Met de functie 'laden autorisatiebestand' kan de autorisatiebeheerder (op last van de autorisatiemanager namens de autorisatiecommissie) de instellingen van het autorisatieprotocol wijzigen. Hiermee kunnen specifieke rolcodes geautoriseerd worden voor specifieke berichttypes, of kan deze autorisatie juist worden ingetrokken.

7.4.2.10.5 Beheerfunctie 'rapporteren autorisaties'

Met de functie 'rapporteren autorisaties' kan de autorisatiebeheerder de instellingen van het actuele autorisatiebestand rapporteren.

-

N.B. De geautoriseerde interactiesoorten kunnen per informatiesysteem worden aangepast via een interface van de ZIM die toegang geeft tot de instellingen van het applicatieregister (zie '[Applicatieregister](#)²²').

De functionaliteit van het autorisatieprotocol wordt verder uitgewerkt in [Ontw APT].

7.4.2.11 Vastleggen determinatietabellen

De Selectie en Determinatie Service (SDS) is een component van de ZIM die:

- voor alle beroepen en specialisaties van zorgverleners vastlegt per context welke bouwsteentypen via AORTA opvraagbaar zijn en welke beperkingen daarop gelden. Voor de combinatie van beroep en specialisatie wordt hierbij een rolcode gebruikt;
- vastlegt uit welke bouwstenen een gegevenssoort bestaat.

De gewenste instellingen voor de SDS worden vastgesteld door een autorisatiecommissie waarin medische beroepsverenigingen en patiëntenverenigingen vertegenwoordigd zijn. Deze instellingen worden op last van de autorisatiemanager in het systeem aangebracht door een medewerker van het landelijk schakelpunt in de rol van autorisatiebeheerder van de ZIM.

Hiertoe is een beheerderinterface op de ZIM beschikbaar die toegang geeft tot een beheerservice voor de SDS. Deze beheerservice ondersteunt drie functies, namelijk:

- Raadplegen SDS;
- Aanpassen SDS;
- Rapporteren SDS configuratie.

De ZIM stelt vooralsnog geen externe interface beschikbaar aan op de ZIM aangesloten informatiesystemen om direct te communiceren met de services van de SDS. In plaats daarvan wordt

22. <https://vzvz.atlassian.net/wiki/display/A8/Applicatieregister>

de SDS door de ZIM gebruikt als onderdeel van het afhandelen van opvragingen binnen een context. Hiertoe biedt de SDS twee services aan andere componenten binnen de ZIM aan:

- Bepalen bouwsteentypen;
- Bepalen gegevenssoorten.

Deze situatie is weergegeven in diagram AORTA.SDS.d1010.

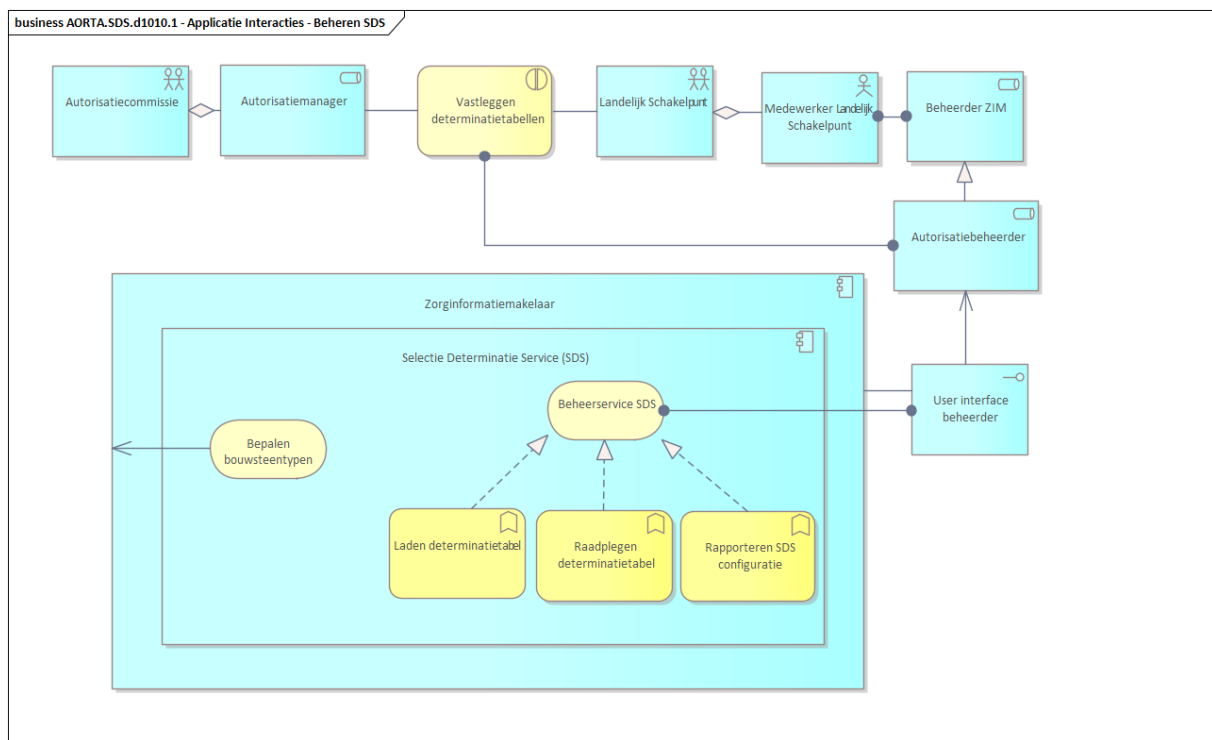


Diagram AORTA.SDS.d1010 - informatiesysteeminteracties voor het beheer van de Selectie en Determinatie Service

7.4.2.11.1 ZIM-interne service: Bepalen bouwsteentypen en selectieparameters

De SDS component biedt aan de OPV component binnen de ZIM een service 'Bepalen bouwsteentypen en selectieparameters'. Deze service bepaalt welke bouwsteentypen er opgevraagd dienen te worden binnen de context van een bepaalde opvraag, en welke selectieparameters daarbij gehanteerd moeten worden. Hierbij wordt rekening gehouden met de rolcode van de opvrager. De rolcode kan bepaalde beperkingen met zich mee brengen met betrekking tot de op te leveren bouwsteen instantiaties.

De service Bepalen Bouwsteentypen gebruikt intern in het SDS component twee andere services:

- Bepalen interactieIDs;

- Bepalen selectieparameters.

De service Bepalen van interactieIDs bepaalt welke interactieIDs zijn gekoppeld aan de bouwsteentypen behorende bij de context en rolcode zoals bepaald door de service Bepalen Bouwsteentypen. Het kan hier maximaal gaan om twee verschillende versies van een bouwsteeninteractie.

De service Bepalen selectieparameters bepaalt de beperkingen die gesteld worden aan de inhoud van een bepaalde bouwsteen. Deze beperkingen worden bepaald door de context in combinatie met de rolcode van de opvrager.

De OPV component gebruikt deze service tijdens elke generieke opvraag van patiëntgegevens binnen een specifieke context.

7.4.2.11.2 ZIM-interne service: Bepalen gegevenssoorten

De service Bepalen gegevenssoorten bepaalt aan de hand van een bouwsteentype in welke gegevenssoort(en) dit bouwsteentype voorkomt. Op basis van de gevonden gegevenssoort(en) en de al eerder bepaalde bouwsteentypen kan worden bepaald welke bronnen bevraagd dienen te worden aan de hand van de verwijzingen in de verwijzindex.

7.4.2.11.3 Beheerfunctie 'raadplegen determinatietabel'

Met de functie 'raadplegen determinatietabel' kan de autorisatiebeheerder de instellingen van de SDS raadplegen. Daarnaast is het ook mogelijk om eerdere versies van de SDS te raadplegen.

Elke wijziging in een determinatietabel heeft een nieuwe versie van de tabel als gevolg. Iedere vorige versie zal worden gelogd voor mogelijke reconstrueren van door de ZIM verstuurde opvraagberichten.

7.4.2.11.4 Beheerfunctie 'laden determinatietabel'

Met de functie 'laden determinatietabel' kan de autorisatiebeheerder (op last van de autorisatiemanager namens de autorisatiecommissie) de instellingen van de determinatietabel wijzigen.

7.4.2.11.5 Beheerfunctie 'rapporteren SDS configuratie'

Met de functie 'rapporteren SDS configuratie' kan de autorisatiebeheerder de instellingen van de actuele SDS rapporteren. Deze rapportage kan ter verificatie dienen van de ingeladen determinatietabel.

[1] Ook indien een eenmalige 'opt-in' is verkregen, geeft de gegevenshouder de patiënt nog steeds bij elk contact de mogelijkheid om specifieke gegevens niet beschikbaar te maken (dus niet aan te melden).

[2] Hier wordt bedoeld dat een GBP de systeemrol van toegangslog-raadplegend systeem kan implementeren. Op het moment van publicatie zijn nog geen GBP's gerealiseerd die deze functionaliteit bieden.

7.4.3 Actoren en rollen

De actoren 'zorgverlener' en 'patiënt' zijn geïntroduceerd op pagina 'Actoren'²³. Aanvullende actoren worden hier besproken.

7.4.3.1 SBV-Z

De Sectorale Berichtenvoorziening in de Zorg (SBV-Z) is een onderdeel van het agentschap CIBG, uitvoeringsorganisatie van het ministerie van VWS. De SBV-Z vormt voor de zorgsector de toegangspoort tot de Beheervoorziening BSN (BVBSN), de organisatie die primair verantwoordelijk is voor de uitgifte en het beheer van het Burgerservicenummer (BSN). Bij deze instantie kunnen Burgerservicenummers van patiënten opgevraagd en geverifieerd worden. Ook biedt de SBV-Z een dienst om de omloopstatus van een wettelijk identificatiedocument (WID) te controleren.

7.4.3.1.1 Landelijk schakelpunt

Het Landelijk Schakelpunt (LSP) (geïntroduceerd op pagina 'Het zoeken van gegevenshouders en gegevensontvangers'²⁴) is een intermediaire organisatie die diensten verleend aan zorgaanbieders die zorginformatie willen uitwisselen en waarbij de gegevenshouders de beschikbaarheid van gegevens over patiënten kunnen aanmelden. Het LSP treedt op als intermediair tussen gegevensraadplegers en gegevenshouders, en tussen gegevenszender en gegevensontvanger.

7.4.3.1.2 Klantenloket en Medewerker klantenloket

Een uitgangspunt van AORTA is dat de patiënt volledig inzicht moet kunnen krijgen in de uitwisseling van de eigen patiëntgegevens. Er is voorzien dat patiënten, die zelf geen toegang hebben tot de daarvoor benodigde technische voorzieningen, toch een aanspreekpunt hebben dat dit inzicht kan verschaffen; dit aanspreekpunt is het klantenloket. Een medewerker van het klantenloket kan de patiënt van informatie voorzien over de uitwisseling van zijn patiëntgegevens via AORTA, overigens zonder dat de klantenloketmedewerker de uitgewisselde patiëntgegevens zelf kan inzien (de klantenloketmedewerker heeft uitsluitend toegang tot verwijzingsindexgegevens en toegangsloggegevens, zie pagina 'Raadplegen verwijzingsindex'²⁵ en 'Raadplegen toegangslog'²⁶). Klantenloketmedewerkers worden geïdentificeerd aan de hand van een PKI-overheidscertificaat (zie pagina 'PKIO (see page 114)').

7.4.3.1.3 Mitz

Mitz is een landelijk voorziening waarin de toestemmingen van burgers worden opgeslagen. Mitz is een onafhankelijk uitwisselingssysteem en kan worden gebruikt als een locatieservice (waar staan er gegevens van deze burger en waar heeft de patiënt toestemming gegeven voor gegevensuitwisseling)

23. <https://vzvz.atlassian.net/wiki/x/OQARBQ>

24. <https://vzvz.atlassian.net/wiki/x/6QERBQ>

25. <https://vzvz.atlassian.net/wiki/x/VwERBQ>

26. <https://vzvz.atlassian.net/wiki/x/iwIRBQ>

en als toestemmingsregister (is er wel toestemming om deze opvraging bij deze zorgaanbieder te doen).

7.4.3.1.4 Autorisatiecommissie

De autorisatiecommissie is een commissie met diverse vertegenwoordigers uit het zorgveld die per beroep en specialisatie van zorgverleners vaststelt wie welke gegevens mag raadplegen, versturen en/of ontvangen via AORTA. Deze commissie stelt dus het autorisatieprotocol en de determinatietabellen vast die zijn beschreven op pagina '[Bevoegdheid op basis van BIG-titel](#)'. De autorisatiemanager is een rol van de voorzitter van de autorisatiecommissie. De autorisatiemanager zorgt ervoor dat de afgesproken autorisatieprotocollen worden vastgelegd bij het landelijk schakelpunt.

7.4.3.1.5 Toezichthouder

De toezichthouder op het correct gebruik van AORTA:

- behandelt klachten over mogelijk onterechte toegang tot patiëntgegevens;
- kan zorgverleners om verantwoording vragen ten aanzien van het geconstateerd gebruik van AORTA;
- kan gepaste maatregelen nemen in geval van geconstateerd misbruik.

De rol van toezichthouder wordt vervuld door het College Bescherming Persoonsgegevens (CBP) en de Inspectie voor de Gezondheidszorg (IGZ).

7.4.3.1.6 Rollen

In het overzichtsdiagram AORTA.ALG.d1030.5 worden diverse rollen geïntroduceerd, zoals 'bewerker verwijsindex' en 'raadpleger verwijsindex'. Deze rollen worden geïntroduceerd om modeltechnische redenen (om het telkens herhalen van alle betrokken actoren te voorkomen) en impliceren niet dat voor iedere actor die een bepaalde rol vervult exact dezelfde autorisatie-eisen gelden; voor de rol van 'raadpleger verwijsindex' geldt bijvoorbeeld dat een zorgverlener toegang krijgt tot andere indexgegevens dan een patiënt.

7.4.3.1.7 Mandatering

De mogelijkheid van mandatering die is geïntroduceerd op pagina '[Mandatering](#)' voor de interacties 'opvragen van patiëntgegevens' en 'sturen van patiëntgegevens' strekt zich ook uit tot de ondersteunende interacties die een zorgverlener mag uitvoeren. Waar sprake is van 'zorgverlener' kan dit, tenzij anders vermeld, dus worden geïnterpreteerd als 'zorgverlener' of een door de zorgverlener gemandateerde zorgverlener, medewerker of systeem.

7.4.4 Opvragen/verifiëren BSN en controleren omloopstatus WID

De Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz) regelt dat in alle berichtgeving tussen zorgaanbieders het burgerservicenummer (BSN) aanwezig moet zijn, om persoonsverwisseling en daardoor (mogelijke) medische fouten te voorkomen. Verder regelt de Wbsn-z dat de zorgaanbieder bij het eerste patiëntcontact de identiteit van de patiënt moet vaststellen aan de hand van een wettelijk identificatiedocument.

Een zorgverlener kan aan de hand van een aantal persoonsgegevens bij de SBV-Z controleren dat een BSN bij een bepaalde persoon hoort.^[1] Ook kan een zorgverlener de omloopstatus van een aan hem aangeboden identificatiedocument bij de SBV-Z controleren.

^[1] Wanneer de zorgverlener het BSN van een patiënt die in zijn eigen administratie voorkomt, heeft gecontroleerd via de SBV-Z, dan wordt binnen AORTA gesproken van ‘gekoppelde’ patiëntgegevens (het lokale administratienummer van de patiënt is als het ware ‘gekoppeld’ aan het BSN). Als de patiënt zich nog niet heeft gelegitimeerd met een geldig wettelijk identificatiedocument, is sprake van ‘voorlopig gekoppelde’ patiëntgegevens; na legitimatie is sprake van ‘definitief gekoppelde’ patiëntgegevens.

7.4.5 Aan- en afmelden van patiëntgegevens

Opvragen van patiëntgegevens vindt plaats via het LSP, zodat de zorgverlener niet op de hoogte hoeft te zijn welke zorgaanbieders gegevens hebben over de patiënt. Om het opvragen van patiëntgegevens via AORTA door andere zorgverleners mogelijk te maken, moet een zorgverlener de aanwezigheid van patiëntgegevens (in het informatiesysteem van de zorgaanbieder waartoe hij behoort) aanmelden bij het Landelijk Schakelpunt.

Aanmelding leidt tot het opnemen van een nieuwe verwijzing in een verwijsindex. Deze verwijzing kan later geactualiseerd worden door middel van een zogenaamde ‘bijwerking’. De aanwezigheid van gegevens moet overigens ook weer afgemeld kunnen worden.

De zorgverlener die patiëntgegevens bijwerkt of afmeldt heeft hierbij de rol van ‘bewerker verwijsindex’.

Voordat patiëntgegevens daadwerkelijk worden geregistreerd bij het LSP moet aan de voorwaarde worden voldaan dat toestemming van de patiënt is verkregen voor het beschikbaar stellen van de medische gegevens (opt-in); dit moet blijken uit een registratie bij de zorgverlener.

7.4.6 Bijhouden van abonnementen en signaleren van gebeurtenissen

Voor een behandelend zorgverlener kan het van belang zijn om zo snel mogelijk op de hoogte te zijn van patiëntgegevens die door een andere zorgverlener over een patiënt worden vastgelegd. Daarom kan een zorgverlener, in de rol van ‘bewerker abonnementen’, zich abonneren op specifieke gebeurtenissen die in het LSP plaatsvinden, zoals bijvoorbeeld het aanmelden van nieuwe gegevens over een patiënt bij de verwijsindex. De abbonementhouder ontvangt dan een abonnementssignaal indien de gebeurtenis optreedt, en kan vervolgens actie ondernemen naar aanleiding van het abonnementssignaal, bijvoorbeeld opnieuw patiëntgegevens opvragen via het LSP.

Naast de zorgverlener als abonneehouder is het mogelijk voor een patiënt om een abonnement af te sluiten met betrekking tot gegevensuitwisseling omtrent zijn persoon. Bij elk nieuw logevent met betrekking tot de patiënt wordt, in geval van een geldig abonnement, een signaal verstuurd naar het GBP waar het abonnement is afgesloten. Het GBP is vervolgens verantwoordelijk voor het op de juiste manier versturen van een notificatie aan de patiënt.

In AORTA is een niet abonneerbaar signaal een signaal dat door het LSP wordt verstrekt aan een actor zonder dat deze actor een abonnement heeft op de specifieke gebeurtenis (denk bijvoorbeeld aan het

verlopen van een abonnement). Een abonnement signaal, is een signaal dat door het LSP wordt verstrekt aan een actor die een abonnement heeft genomen op dergelijke signalen. In het geval de actor een patiënt betreft, dan wordt gesproken over een notificatie in plaats van over een abonnement signaal.

7.4.7 Selecteren van zorgaanbieders, zorgverleners en zorgaanbiederapplicaties

Bij het versturen van gegevens moet de gegevenszender patiëntgegevens kunnen adresseren aan een gegevensontvanger.

Aangezien ook bij het versturen van gegevens het LSP als intermediair optreedt, biedt het LSP aan de gegevenszender de mogelijkheid om voorafgaand aan het sturen van gegevens de gewenste ontvanger op te zoeken in een zorgadresboek (ZORG-AB). De zorgverlener die het zorgadresboek raadpleegt neemt de rol aan van 'raadpleger zorgveldgegevens'.

Aangezien de beoogde ontvanger van de te versturen patiëntgegevens zowel een zorgaanbieder als een individuele zorgverlener kan zijn (zie pagina '[Sturen van patiëntgegevens](#)²⁷⁾') zijn zowel zorgaanbieders als zorgverleners opgenomen in dit adresboek. De laatsten moeten wel door de werkgever (zorgaanbieder) met toestemming van het individu worden opgenomen.

De gegevenszender moet ook de zorgaanbiederapplicatie (het informatiesysteem^[1] van een zorgaanbieder) waarnaar de gegevens daadwerkelijk worden gestuurd kunnen opzoeken.

[1] De termen 'informatiesysteem' en 'applicatie' worden in dit document beide gebruikt voor het aanduiden van een systeem voor gegevensverwerking.

7.4.8 Raadplegen toegangslog

Patiëntgegevens zijn privacygevoelige gegevens die alleen toegankelijk zijn voor de behandelende zorgverleners en de patiënt zelf. Daarom is het van belang dat precies kan worden vastgesteld wie patiëntgegevens heeft geraadpleegd, opgevraagd of verstuurd. Omdat het LSP optreedt als intermediair bij het opvragen en sturen van patiëntgegevens, kan het LSP nauwkeurig bijhouden in een log wie bij opvragen en sturen van gegevens betrokken is geweest. Deze log-informatie wordt vervolgens beschikbaar gemaakt aan de volgende actoren in de rol van 'raadpleger toegangslog':

- De patiënt, voor zover het de eigen gegevens betreft; de patiënt heeft recht om te weten welke zorgverleners zijn gegevens hebben opgevraagd. VZVZ stelt deze gegevens niet beschikbaar, maar verwijst door naar de desbetreffende zorgaanbieder.
- De patiënt, voor zover het de eigen gegevens betreft; de patiënt heeft recht om te weten welke zorgaanbieders zijn gegevens hebben opgevraagd.
- Een medewerker van het klantenloket, als aanspreekpunt voor de patiënt die niet in staat is om zelfstandig de loggegevens te raadplegen.
- De toezichthouder op het correct gebruik van AORTA.

27. <https://vzvz.atlassian.net/wiki/display/A8/Rollen+toekennen+aan+actoren#Rollentoekennenaanactoren-Sturenvanpatiëntgegevens>

7.4.9 Vastleggen autorisatieprotocollen

Zoals beschreven op pagina '[Bevoegdheid op basis van BIG-titel](#)' wordt een autorisatieprotocol vastgesteld waarin wordt vastgelegd per beroepsgroep en specialisatie welke berichten kunnen worden verstuurd via AORTA. Een autorisatiecommissie stelt deze autorisatieprotocollen vast en laat deze via de autorisatiemanager vastleggen door het LSP.

7.4.10 Vastleggen determinatietabellen

Zoals beschreven op pagina '[Bevoegdheid op basis van BIG-titel \(see page 63\)](#)' wordt een determinatietabel vastgesteld waarin wordt vastgelegd per beroepsgroep en specialisatie welke gegevens kunnen worden uitgewisseld via AORTA. Een determinatietabel geeft aan welke bouwsteentypen aan een zorgverlenerrol binnen welke context mogen worden opgeleverd en welke aanvullende beperkingen ten aanzien van de bouwsteeninstantiaties van die typen gesteld zijn. Een autorisatiecommissie stelt deze determinatietabellen vast en laat deze via de autorisatiemanager vastleggen in het LSP.

7.4.11 Raadplegen verwijzindex

Het raadplegen van de verwijzindex is nodig om vast te stellen welke zorgaanbieders hebben aangegeven over patiëntgegevens voor een specifieke patiënt te beschikken, zodat deze gegevens kunnen worden opgevraagd. Het betreft hier metagegevens, dus de medisch inhoudelijke informatie is niet in de verwijzindex terug te vinden.

De rol van 'raadpleger verwijzindex' kan worden vervuld door:

- zorgverleners die willen vaststellen welke zorgaanbieders over patiëntgegevens van een bepaalde patiënt beschikken;
- zorgverleners die willen controleren welke patiëntgegevens vanuit hun eigen informatiesysteem bij de verwijzindex zijn aangemeld;
- de patiënt, voor zo ver het de eigen gegevens betreft; de patiënt heeft recht om te weten welke zorgaanbieders gegevens over de patiënt hebben aangemeld;
- een medewerker van het klantenloket, als aanspreekpunt voor de patiënt die niet in staat is om zelfstandig de verwijzindexgegevens te raadplegen;
- de toezichthouder op het correct gebruik van AORTA.

Note: Deze functie is na overgang naar Mitz niet meer aanwezig

7.5 Informatiesystemen

De standaard voor informatie-uitwisseling verschuift bij AORTA richting HL7 FHIR.

AORTA zal zowel HL7v3 als FHIR gaan ondersteunen als platform/stelsel voor uitwisseling. Een belangrijke innovatie bij AORTA richting HL7 FHIR, is de ontwikkeling van API-gebaseerde interacties, en met name het samenspel tussen de Resource Broker (HL7-FHIR standaard²⁸) en de Autorisatie Server ([OAuth-protocol](#)²⁹) die in deze informatie-uitwisseling van belang zijn.

28. <https://www.hl7.org/fhir/index.html>

Vooralsnog worden hieronder de ontwikkelingen met betrekking tot FHIR en de architectuurlijke en infrastructurele wijzigingen nog niet beschreven.

AORTA.INF.d1020 geeft in een vereenvoudigd infrastructuurdiagram^[1] een overzicht van de (HL7v3) informatiesystemen die elk afzonderlijk in dit hoofdstuk worden besproken.

29. <https://tools.ietf.org/html/rfc6749>

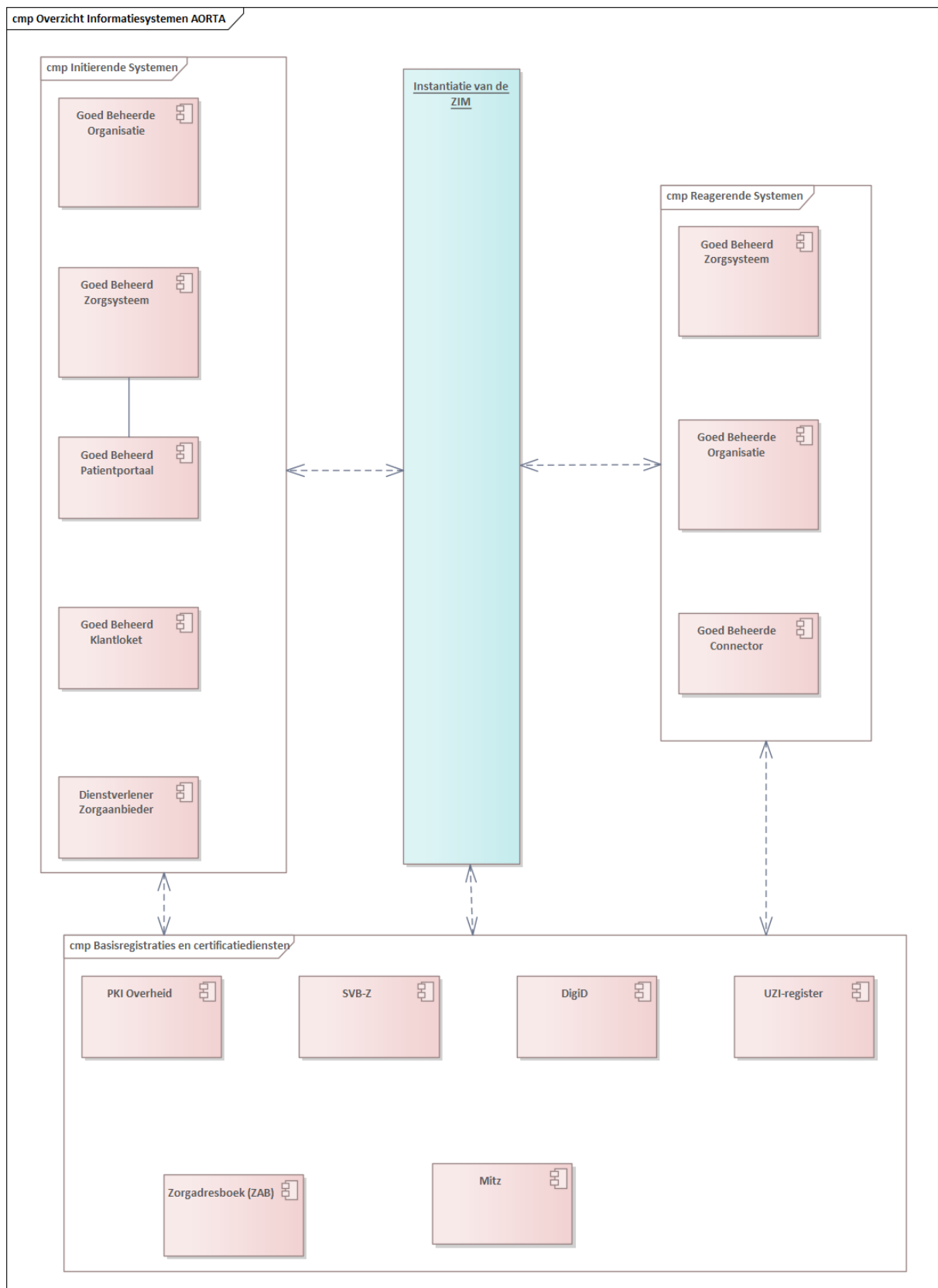


Diagram AORTA.INF.d1020 – overzicht informatiesystemen (HL7v3) AORTA

Centraal in AORTA staat de Zorginformatiemakelaar (ZIM) (zie pagina '[Zorginformatiemakelaar \(ZIM\)](#)³⁰⁾'), die verantwoordelijk is voor de berichtuitwisseling tussen opvragende systemen en bronsystemen (en tussen sturende en ontvangende systemen).

Alle informatiesystemen die op de ZIM worden aangesloten moeten aan een set implementatie- en exploitatie-eisen voldoen, waarna ze worden aangeduid als 'goed beheerd' informatiesysteem, aangeduid met de afkorting GBx (zie pagina '[Goed beheerd informatiesysteem \(GBx\)](#)³¹⁾).

Tot de groep van GBx'en behoren:

- een goed beheerd zorgsysteem (zie pagina '[Zorginformatiesystemen \(XIS\) en het Goed beheerd zorgsysteem \(GBZ\)](#)³²⁾'), een informatiesysteem dat door een zorgverlener of een medewerker wordt gebruikt om patiëntdossiers in te richten en te onderhouden;
- een goed beheerd patiëntportaal (zie pagina '[Goed beheerd patiëntportaal \(GBP\)](#)³³⁾'), een portaal dat patiënten toegang geeft tot hun eigen gegevens;
- het goed beheerd klantenloketsysteem (zie pagina '[Goed beheerd klantenloketsysteem \(GBK\)](#)³⁴⁾'), het toegangssysteem van de klantenloketorganisatie.
- een goed beheerde organisatie (zie pagina '[Goed beheerde organisatie \(GBO\)](#)³⁵⁾'), een informatiesysteem (zoals een goed beheerd zorgsysteem) dat door zorgverleners wordt gebruikt, maar dat geen UZI-abonnee kan worden.

Naast informatiesystemen zijn er connectoren die patiëntgegevens uit of aan informatiesystemen in de AORTA-infrastructuur ontsluiten:

- de Dienstverlener Zorgaanbieder (zie pagina '[Dienstverlener Zorgaanbieder \(DVZA\)](#)³⁶⁾'), connector die patiëntgegevens uit de AORTA-infrastructuur ontsluit aan informatiesystemen in het MedMij-netwerk.
- de goed beheerde connector (zie pagina '[Goed beheerd connector \(GBC\)](#)³⁷⁾'), connector die patiëntgegevens ontsluit van externe infrastructuren aan informatiesystemen binnen de AORTA-infrastructuur.

Daarnaast hebben zowel de GBx'en als de ZIM toegang tot de services van een aantal basisregistraties en certificatediensten, namelijk:

- het [UZI-register](#) (see page 113), dat unieke zorgverlener identificaties van zorgverleners en zorgaanbieders bevat;
- [PKIoverheid](#), een infrastructuur voor het uitgeven en beheren van digitale certificaten;
- [DigiD](#) (see page 115), een register van persoonsidentiteiten voor burgers.
- [Mitz](#) (see page 116), een register van patiënttoestemmingen.
- ZORG-AB, een gemeenschappelijke adresinformatievoorziening

30. <https://vzvz.atlassian.net/wiki/x/eQARBQ>

31. <https://vzvz.atlassian.net/wiki/x/fgARBQ>

32. <https://vzvz.atlassian.net/wiki/x/iQARBQ>

33. <https://vzvz.atlassian.net/wiki/x/mwARBQ>

34. <https://vzvz.atlassian.net/wiki/x/lQARBQ>

35. <https://vzvz.atlassian.net/wiki/x/QwARBQ>

36. <https://vzvz.atlassian.net/wiki/x/VwARBQ>

37. <https://vzvz.atlassian.net/wiki/x/UQARBQ>

- Sectorale Berichten Voorziening in de Zorg (SBV-Z, reeds geïntroduceerd, zie pagina 'SBV-Z'³⁸ ; en pagina 'Basisregistraties en vertrouwensmiddelen SBV-Z (see page 115)' voor de systeemdiensten van SBV-Z).

[1] Zie voor een meer uitgebreide bespreking van de infrastructuur de pagina 'Infrastructurele aspecten'³⁹.

7.5.1 AORTA on FHIR

Met AORTA-on-FHIR worden enkele nieuwe informatiesystemen geïntroduceerd.

- Het AORTA-netwerk wordt niet langer slechts o.b.v. HL7-v3 aan het MedMij-netwerk gekoppeld, maar nu ook o.b.v. HL7-FHIR, waardoor alle (op FHIR-gebaseerde) MedMij-gegevensdiensten via LSP+ aangeboden kunnen worden;
- HL7-FHIR koppelvlakken die t.b.v. MedMij zijn ontwikkeld kunnen ook worden toegepast voor uitwisseling tussen zorgaanbieders.
- LSP+ en LSP versmelten (functioneel) tot één Resource Broker die (in de toekomst ook) kan gaan fungeren als een Koppelpunt binnen TWIIN en ook kan worden gekoppeld aan een Europees netwerk;
- De Resource Broker maakt gebruik van één Autorisatie Server, die op termijn kan worden opgeschaald naar een gemeenschappelijke dienst en ook zal worden aangesloten op Mitz;
- Om systemen van zorgaanbieders te kunnen vinden en adresseren, wordt gebruik gemaakt van de gemeenschappelijke dienst Adresseringsservice in combinatie met ZORG-AB.

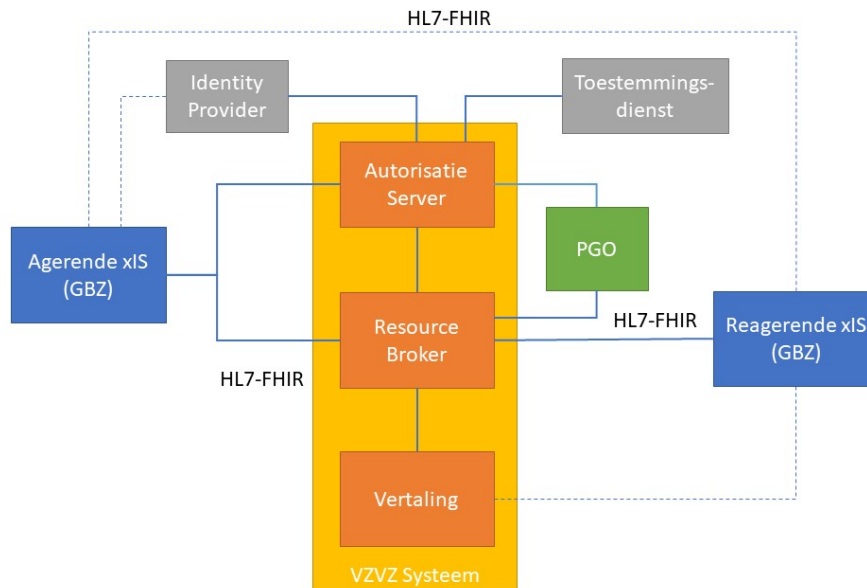
Tevens worden door deze AORTA-on-FHIR uitbreiding, de positie en de mogelijkheden van AORTA significant versterkt, en wordt voorkomen dat AORTA verwordt tot een "legacy" infrastructuur. Zo wordt het mogelijk om:

- Bouwstenen (ZIB's) zowel tussen zorgaanbieders onderling uit te wisselen, als ook tussen zorgaanbieders en burgers;
- Uitwisseling niet slechts te laten plaatsvinden via de VZVZ Resource Broker, maar ook (meer decentraal ingestoken) direct tussen systemen onderling, zodat voor iedere use case, de optimale informatiestroom kan worden ingeregeld;
- Dankzij vertaalservices van de VZVZ Resource Broker ook uitwisseling mogelijk te maken tussen HL7-v3 systemen en HL7-FHIR systemen.

Onderstaande figuur toont een overzicht van het beoogde systeemlandschap.

38. <https://vzvz.atlassian.net/wiki/spaces/ACM/pages/1797390478/8.5.0+Actoren+en+rollen#id-8.5.0Actorenenrollen-SBV-Z>

39. <https://vzvz.atlassian.net/wiki/x/XQMRBQ>



In bovenstaande opzet kunnen gegevens worden uitgewisseld tussen:

- PGO's (Persoons Gebonden Omgeving) en XIS'en (reagerend)
- XIS'en onderling;

Er wordt hierbij een architectuurscheiding aangebracht tussen autorisatie en uitwisseling. Autorisatie wordt afgehandeld in de Autorisatie Server. Uitwisseling verloopt (o.b.v. verkregen autorisatie- of toegangstokens) ofwel via de Resource Broker, ofwel direct tussen XIS'en onderling. Autorisatie omvat hierbij niet alleen de toepassing van autorisatieregels, zoals het MAP, maar ook de toestemming van de burger (zie Toestemmingsdienst). Om een geleidelijke overgang van bestaande HL7v3 naar HL7 FHIR mogelijk te maken, zal AORTA beide standaarden gelijktijdig ondersteunen. Via een vertaalservice wordt het mogelijk gemaakt om agerende XIS'en die nog op de HL7v3-standaard zitten, te laten communiceren met reagerende XIS'en die op HL7 FHIR standaard zitten. Dit zorgt voor een hybride ontwikkelijn voor leveranciers en creëert een geleidelijke migratiestrategie.

Voor authenticatie van gebruikers wordt gebruik gemaakt van bestaande Identity Providers, zoals het UZI-register, DigiD, ZorgID, etc. Dit kan worden uitgebreid naar andere Identity Providers. Agerende XIS'en van zorgaanbieders kunnen een eigen aansluiting hebben op deze Identity Providers (IdP), maar indien gewenst kan deze aansluiting ook verlopen via de autorisatieserver.

7.5.2 Interacties tussen informatiesystemen

De volgende pagina's '[Primaire informatiesysteem interacties](#)⁴⁰', '[Ondersteunende informatiesysteem interacties](#)⁴¹' en '[Applicatie-interacties voor beheer](#)⁴²' beschrijven hoe binnen AORTA de interacties uit de pagina's '[Primaire Interacties](#)⁴³', '[Ondersteunende Interacties](#)⁴⁴' en '[Beheer interacties](#)⁴⁵' worden gerealiseerd door de informatiesystemen van de pagina [Informatiesystemen](#)⁴⁶. Hierbij ligt de nadruk op de generieke interfaces die de ZIM aanbiedt aan aangesloten informatiesystemen.

7.5.2.1 Algemene beschrijving van interacties

Diagram AORTA.ALG.d1060.1 is een algemene weergave van een berichtinteractie tussen een "initieërend systeem" (bijvoorbeeld een GBZ) en de ZIM, waarbij het initiërend systeem via de ZIM communiceert met een reagerend systeem (bijvoorbeeld een ander GBZ). Het diagram illustreert tevens de in de volgende hoofdstukken gebruikte notatie.

De ZIM biedt een interface ("door ZIM aangeboden interface") aan het initiërend systeem. Dit systeem heeft een service om deze interface te gebruiken ("gebruiken van door ZIM geboden interface").

De verantwoordelijkheid voor de afhandeling van de interface door de ZIM is toegekend aan de orkestratie service van de ZIM. De orkestratie service volgt hierbij ten dele een vast patroon, omdat een aantal taken bij elke berichtuitwisseling moet plaatsvinden. Hierbij maakt de orchestratieservice gebruik van de componenten Applicatieregister, Authenticatie, Autorisatieprotocol, Toegangslog en de Selectie Determinatie Service. Dit vaste verwerkingspatroon wordt verder uitgewerkt op pagina '[Berichtafhandeling door de ZIM](#)⁴⁷'

40. <https://vzvz.atlassian.net/wiki/x/2wMRBQ>

41. <https://vzvz.atlassian.net/wiki/x/FgMRBQ>

42. <https://vzvz.atlassian.net/wiki/x/JQMRBQ>

43. <https://vzvz.atlassian.net/wiki/x/8gIRBQ>

44. <https://vzvz.atlassian.net/wiki/x/wQERBQ>

45. <https://vzvz.atlassian.net/wiki/x/6gMRBQ>

46. <https://vzvz.atlassian.net/wiki/x/twIRBQ>

47. <https://vzvz.atlassian.net/wiki/x/xQIRBQ>

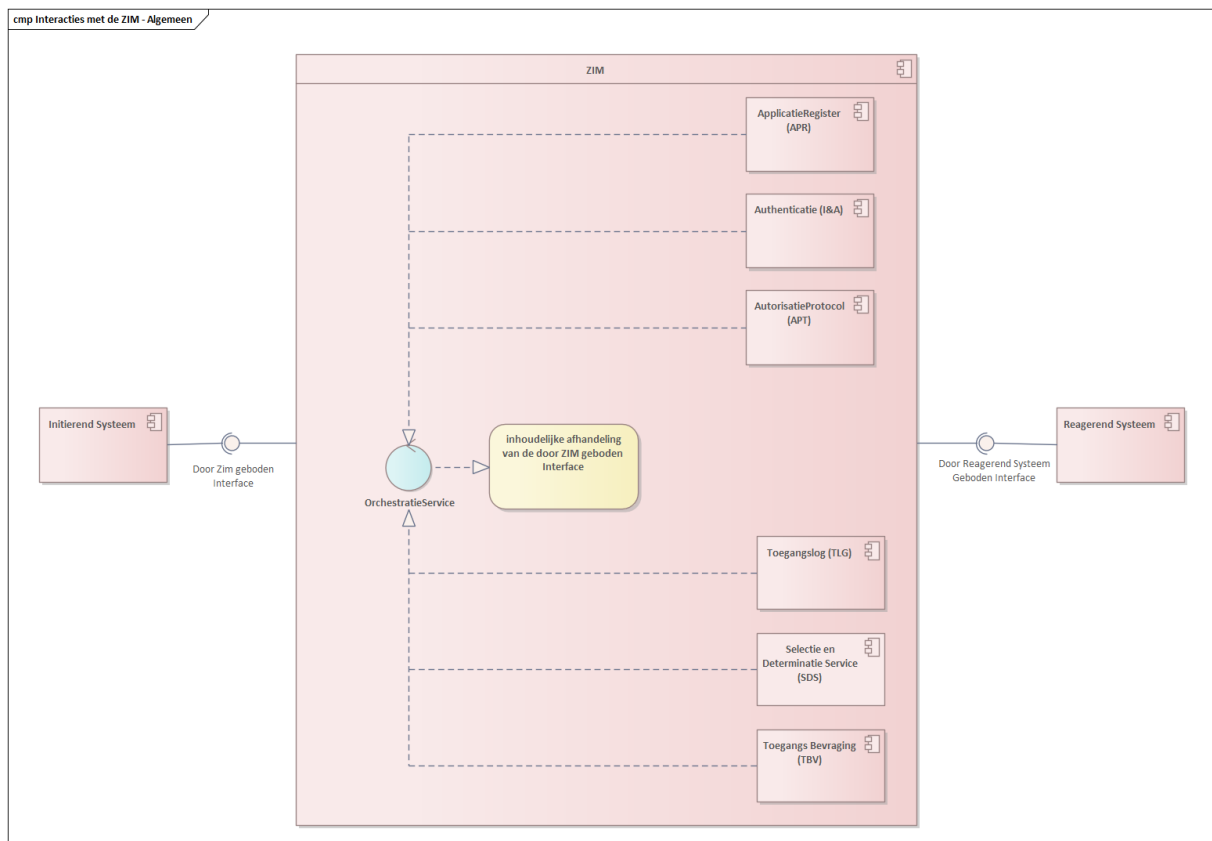


Diagram AORTA.ALG.d1060.1 – algemene beschrijving van interacties met de ZIM

Een deel van de berichtafhandeling is echter per interactietype verschillend en is in het diagram aangegeven met de service “inhoudelijk afhandelen van door ZIM geboden interface”. Deze inhoudelijke afhandeling wordt uitgevoerd door wisselende componenten van de ZIM, afhankelijk van het type bericht. In de volgende hoofdstukken zal per type interactie worden aangegeven welke component van de ZIM verantwoordelijk is voor de inhoudelijke afhandeling. Tijdens deze inhoudelijke verwerking kunnen ook reagerende systemen buiten de ZIM (bijvoorbeeld andere aangesloten GBZ'en) worden aangeroepen, die hiertoe dan ook een interface moeten implementeren (in het diagram aangegeven met “door reagerend systeem geboden interface”).

De volgende hoofdstukken concentreren zich op de door de ZIM aangeboden interfaces en de componenten die binnen de ZIM verantwoordelijk zijn voor de inhoudelijke afhandeling. Daarom worden de orchestratieservice en het vaste patroon van aanroepen van componenten niet steeds opnieuw getoond. Het diagram AORTA.ALG.d1060.1 kan versimpeld worden weergegeven zoals getoond in diagram AORTA.ALG.d1070. Hierbij zijn de orchestratieservice en overige componenten weggelaten en wordt de service van de component die verantwoordelijk is voor de *inhoudelijke* afhandeling van de door de ZIM geboden interface direct toegekend aan de door de ZIM geboden interface. Dit is de notatieconventie die verder in de tekst wordt gevolgd.



Diagram AORTA.ALG.d1070 – vereenvoudigde weergave van AORTA.ALG.d1060.1

7.5.2.2 Systeemrollen

De ZIM ondersteunt diverse soorten berichten, onder meer voor het opvragen en sturen van patiëntgegevens. Niet voor elk op de ZIM aangesloten GBx zijn alle berichten relevant, zo kunnen niet bij ieder GBx patiëntgegevens worden opgevraagd.

Een “systeemrol” binnen AORTA is een deelverzameling van berichtuitwisselingen die functioneel verwant zijn. Een voorbeeld van een dergelijke systeemrol is ‘verwijsindex raadplegend systeem’; hieronder vallen uitsluitend berichtuitwisselingen die te maken hebben met het raadplegen van de verwijsindex. Voor softwareleveranciers (bv. XIS-leveranciers) is het mogelijk om voor hun software product (bv. een XIS) een acceptatie te behalen voor specifieke combinaties van systeemrollen.

In hoofdstukken Primaire informatiesysteem interacties, Ondersteunende Informatiesysteem interacties en Beheer interacties worden de verschillende berichtuitwisselingen besproken die behoren bij de AORTA-basisinfrastructuur. Hierbij worden ook de bijbehorende systeemrollen benoemd. Een totaaloverzicht van systeemrollen wordt tenslotte gegeven in hoofdstuk Overzicht van systeemrollen.

7.5.2.3 Zorgtoepassingen

De ZIM biedt een basisinfrastructuur voor berichtuitwisseling in de zorg. Over deze basisinfrastructuur kunnen berichten worden uitgewisseld die relevant zijn binnen bepaalde ketenprocessen in de zorg, bijvoorbeeld het medicatieproces, waarbij o.a. huisartsen en apotheken zijn betrokken. De groep van berichten die relevant is voor een bepaald ketenproces in de zorg, wordt samen een *zorgtoepassing* genoemd; een voorbeeld is de groep van berichten die bedoeld is voor communicatie tussen huisartsen en apotheken voor de uitwisseling van medicatiegegevens.

Bij deze zorgtoepassingen horen specifieke systeemrollen. Een voorbeeld van een dergelijke systeemrol is ‘medicatie-voorschrijvend-systeem’; hieronder vallen uitsluitend berichtuitwisselingen die behoren bij de zorgtoepassing medicatiegegevens en die relevant zijn voor de informatiesystemen van medicatievoorschrijvers (bijvoorbeeld huisartsen). Aan een XIS kan een kwalificatie worden toegekend voor één of meer van dergelijke systeemrollen. Specifieke zorgtoepassingen worden

behandeld in aparte ontwerpdocumenten; aan zorgtoepassingen gerelateerde systeemrollen worden daarom niet in dit document behandeld.

Voor verdere uitwerking wordt verwezen naar de pagina [Zorgtoepassingen](#) (see page 154).

7.5.3 Applicatie-interacties voor beheer

Op deze pagina wordt uitgewerkt hoe de beheersmatige interacties, zoals besproken bij 'Beheerinteracties'⁴⁸, worden uitgewerkt op informatiesysteemniveau.

7.5.3.1 Raadplegen en bewerken van het applicatieregister

De ZIM bewaart de informatie over aangesloten informatiesystemen ('applicaties') in een applicatieregister. Opname in het applicatieregister is een voorwaarde voor berichtenuitwisseling met de ZIM. Hiertoe bevat het applicatieregister kerngegevens van het GBx, waaronder één zorgaanbiederidentificatie, één of meer unieke applicatie-identificatienummers en - per applicatie - een URI^[1] waarop de applicatie bereikbaar is.

De ZIM biedt, om het APR te raadplegen en te bewerken, de volgende interfaces, die worden afgehandeld door het APR:

- Interface LSP.APR.i1010: verifiëren communicatiekoppeling (tick-tock)^[2]
- Interface LSP.APR.i1020: verifiëren applicatiekoppeling (ping-pong)
- Interface LSP.APR.i1075: Beheren TKID

Voor het gebruik van deze interfaces moeten binnen een op de ZIM aangesloten informatiesysteem modules aanwezig zijn die het gebruik van deze interfaces ondersteunen. Deze modules zijn hier aangeduid als:

- applicatieregister bewerkend systeem; dit gebruikt interface LSP.APR.i1075
- koppeling verifiërend systeem; dit gebruikt interfaces APR.i1010 en LSP.APR.i1020.

Omdat de ZIM op kan treden als intermediair voor koppeling verificatie tussen een koppeling verifiërend systeem en een koppeling bevestigend systeem, moet een GBx om te kunnen optreden als koppeling bevestigend systeem de volgende interfaces implementeren. Deze zijn functioneel gelijk aan LSP.APR.i1010 en LSP.APR.i1020 maar hebben de ZIM als afzender:

- Interface GBX.APR.i1010: verifiëren communicatiekoppeling (tick-tock)
- Interface GBX.APR.i1020: verifiëren applicatiekoppeling (ping-pong)

Deze situatie is weergegeven in diagram AORTA.APR.d1010.

48. <https://vzvz.atlassian.net/wiki/x/6gMRBQ>

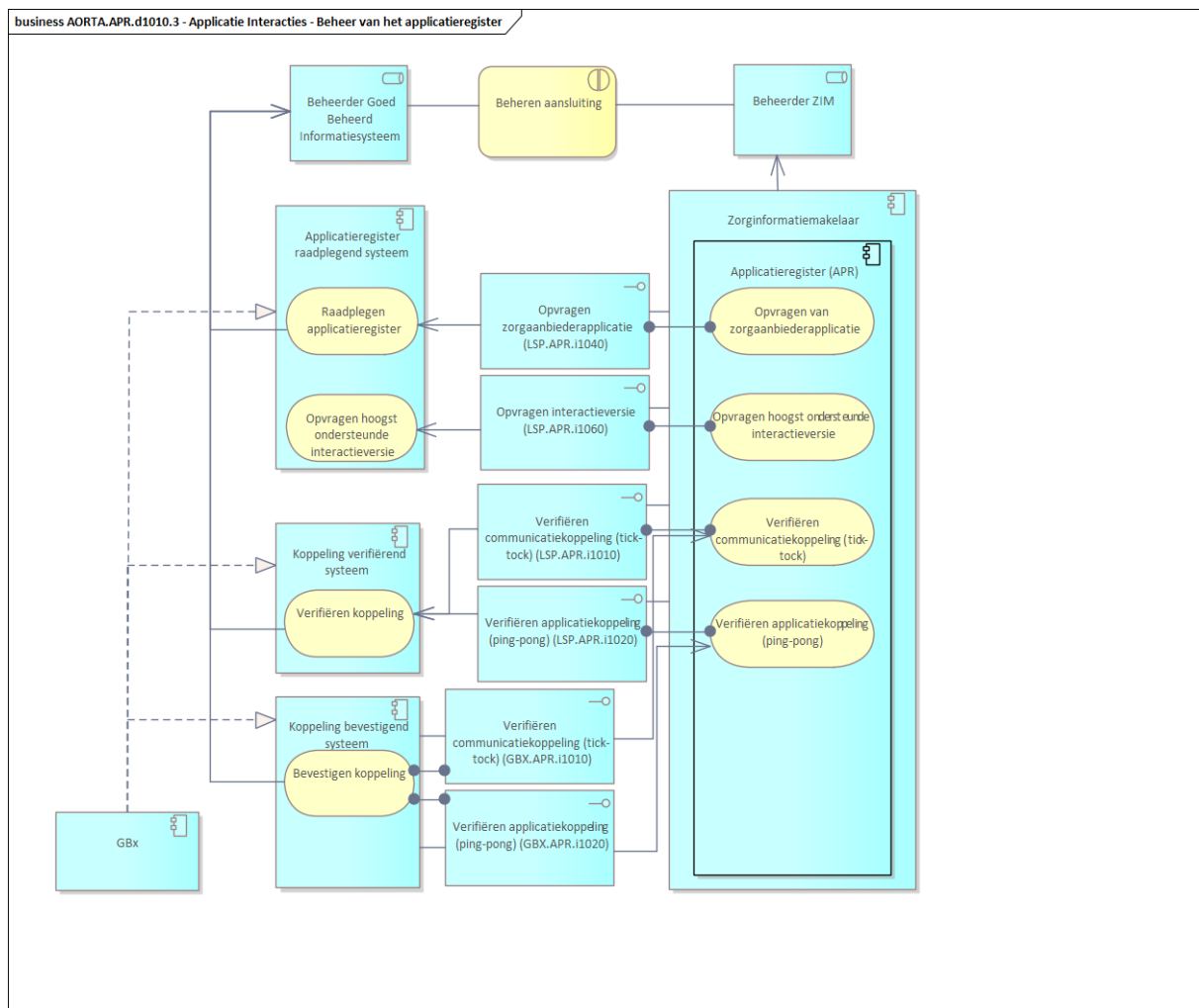


Diagram AORTA.APR.d1010.3 - applicatie-interacties voor het beheer van het applicatieregister

7.5.3.1.1 Interface LSP.APR.i1010: verifiëren communicatiekoppeling (tick-tock)

De interface 'verifiëren communicatiekoppeling' wordt aangeroepen vanuit de module 'koppeling verifiërend systeem' van een GBx en dient om het bestaan van een communicatiekoppeling met de ZIM of een reagerend GBx te controleren. Een 'tick'-bericht test of het 'koppeling bevestigend systeem' in staat is om HL7-berichten te ontvangen.

7.5.3.1.2 Interface LSP.APR.i1020: verifiëren applicatiekoppeling (ping-pong)

De interface 'verifiëren applicatiekoppeling' wordt aangeroepen vanuit de module 'koppeling verifiërend systeem' van een GBx en dient om het bestaan van een applicatiekoppeling met de ZIM of een reagerend GBx te controleren. Een 'ping'-bericht test of het 'koppeling bevestigend systeem' in staat is om HL7-berichten inhoudelijk te verwerken.

7.5.3.1.3 Interface LSP.APR.i1075: Beheren TKID

De interface 'Beheren TKID' wordt aangeroepen vanuit de module 'koppeling bewerkend systeem' van een GBx. Deze interface biedt de mogelijkheid om vanuit een GBx een bericht te versturen met de te gebruiken TKID's.

7.5.3.1.4 Rol van het APR bij beperking van het opleveren van gegevens tot een beperkte groep van zorgverleners (regionale beperking)

Het APR biedt een faciliteit om per organisatie een expliciete lijst bij te houden van zorgaanbieders die gegevens kunnen opvragen bij de desbetreffende organisatie. Een lijst voor een samenwerkingsverband bestaat uit een naam van het samenwerkingsverband, de gegevenssoort(en)/context die betrekking hebben op het samenwerkingsverband en een lijst met zorgaanbieders die het samenwerkingsverband vormen. Op deze lijst worden zorgaanbieders geplaatst, geïdentificeerd met hun UZI-registerabonneenummer (URA). Indien een dergelijke lijst is opgenomen worden opvraagberichten alleen gehonoreerd indien ze afkomstig zijn van de zorgaanbieders op de lijst en als het de gegevenssoort/context betreft die bij het samenwerkingsverband is opgenomen. Dit is een mechanisme dat bijvoorbeeld kan worden toegepast om uitwisseling regionaal te beperken. Een organisatie kan een uitzondering maken op regionale beperking door kenbaar te maken dat landelijke bevraging mogelijk is. Hiervoor dient wel in het APR ingesteld te worden dat het landelijke uitwisselingsvinkje op actief staat en dus wordt meegenomen bij de autorisatie van een opvraagbericht.

Voor het beheren van de samenwerkingsverbandlijsten worden geen speciale (bericht-) interfaces voor beheerders of andere gebruikers beschikbaar gesteld, maar zijn wel beheerfaciliteiten vereist op het niveau van de ZIM. Zie voor verdere uitwerking van dit aspect het [Ontw APR].

7.5.3.2 Beheer van de verwijfsindex

In de VWI van de ZIM staan alle aanmeldingen afkomstig uit GBZ-applicaties. Om te controleren of het beeld van de aangemelde gegevens dat bij de GBZ-beheerder bestaat overeenkomt met de werkelijke situatie in de VWI, kan de GBZ-beheerder gebruik maken van de VWI synchronisatiefunctie (Interface LSP.VWI.i1090: Synchroniseren indexgegevens met vergelijking). Het is verplicht om de verwijfsindex synchroon te houden met de lokale administratie.

Daarnaast kent de VWI, evenals andere componenten van de ZIM (zie '[Beheer van overige aspecten van de ZIM](#)⁴⁹'), een beheerservice die toegankelijk is voor een beheerder van de ZIM via een beheerder user interface. Deze geeft de beheerder de mogelijkheid om onderhoud te plegen op de verwijfsindex (zie [Ontw VWI]).

Deze situatie is weergegeven in diagram AORTA.VWI.d1040.2.

49. <https://vzvz.atlassian.net/wiki/x/6gMRBQ>

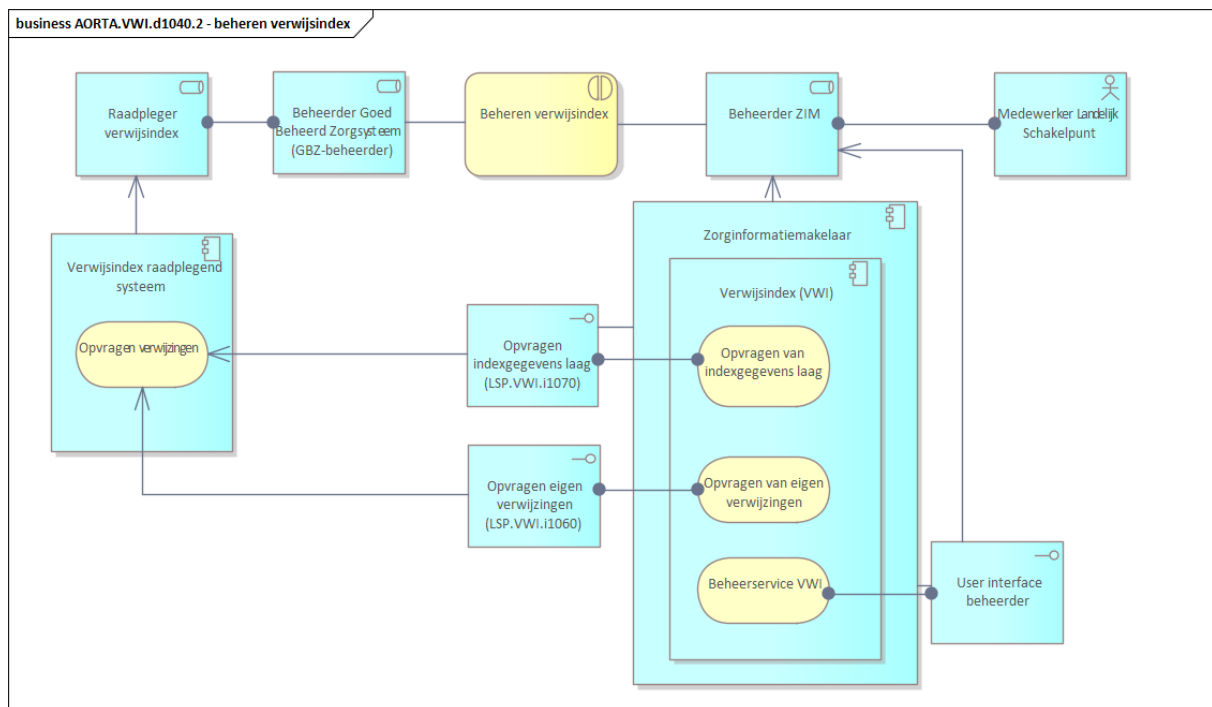


Diagram AORTA.VWI.d1040.2 – beheren verwijfsindex

7.5.3.2.1 Beheer van het zorgadresboek

De gegevens over zorgaanbieders en zorgverleners in het zorgadresboek (ZORG-AB) worden deels overgenomen uit een centraal zorgaanbieder/zorgverlener register (het UZI-register) en de VZVZ-administratie. Wijzigingen in het UZI-register en in de VZVZ-administratie moeten periodiek worden verwerkt in het ZORG-AB. Hiermee wordt voorkomen dat er gewerkt wordt met obsoleete gegevens.

Daarnaast moet er een beheerderinterface zijn om ZORG-AB-gegevens te kunnen verwijderen voor een zorgaanbieder die niet meer de mogelijkheid (bijvoorbeeld geen geldig servercertificaat) heeft om zelf wijzigingen aan het ZORG-AB toe te brengen.

ZORG-AB is een component die los staat van het LSP en wordt aangeboden als een generieke voorziening. Zie voor de betreffende documentatie de VZVZ internetpagina met betrekking tot ZORG-AB.

7.5.3.2.2 Beheer van overige aspecten van de ZIM

Diagram LSP.ZIM.d1020. toont op conceptueel niveau de beheerfaciliteiten van de ZIM. De ZIM beschikt over een gebruikersinterface die toegang geeft aan een beheerder voor het uitvoeren van beheeracties op elk van de componenten binnen de ZIM. Deze gebruikersinterface geeft de mogelijkheid om de toegang tot specifieke beheeracties te beperken tot beheerders in een meer specifieke rol. Weliswaar is op logisch niveau sprake van één beheerderinterface, op fysiek niveau kan sprake zijn van afzonderlijke interfaces voor deelcomponenten van de ZIM.

Elke component binnen de ZIM biedt een beheerservice die het voor een beheerder mogelijk maakt om configuratieparameters van de component in te stellen en eventuele storingen op te sporen en op te lossen. Per component kunnen in ontwerpdocumenten configuratieparameters en beheeracties worden geïdentificeerd.

Beheeracties worden gelogd in een beheerlog, met vastlegging van beheerderidentificatie, tijdstip en aanduiding van de beheergebeurtenis. Per component kunnen in ontwerpdocumenten beheergebeurtenissen worden geïdentificeerd die in de beheerlog moeten worden vastgelegd. Op basis van de beheerlog kan inzicht worden verkregen in de beheergebeurtenissen die hebben plaatsgevonden. De beheerlog dient als basis voor rapportages over beheergebeurtenissen, waarbij selecties mogelijk zijn per periode, gebeurtenistype of beheerder. In logische zin is sprake van één log, in technische zin kan sprake zijn van diverse aparte logs, die echter wel als één (eventueel virtueel) log benaderbaar zijn.

Analoog aan de beheerlog kent de ZIM een systeemlog, waarin alle foutsituaties worden gelogd die binnen de ZIM worden gedetecteerd. zie de pagina '[Foutafhandeling](#)⁵⁰'. Ook overschrijdingen van ingestelde grenswaarden van kritische systeemvariabelen worden in de systeemlog opgeslagen.

Op basis van het systeemlog kan inzicht worden verkregen in de foutgebeurtenissen die hebben plaatsgevonden. Het systeemlog dient als basis voor rapportages over foutgebeurtenissen, waarbij selecties mogelijk zijn tenminste per periode en gebeurtenistype.

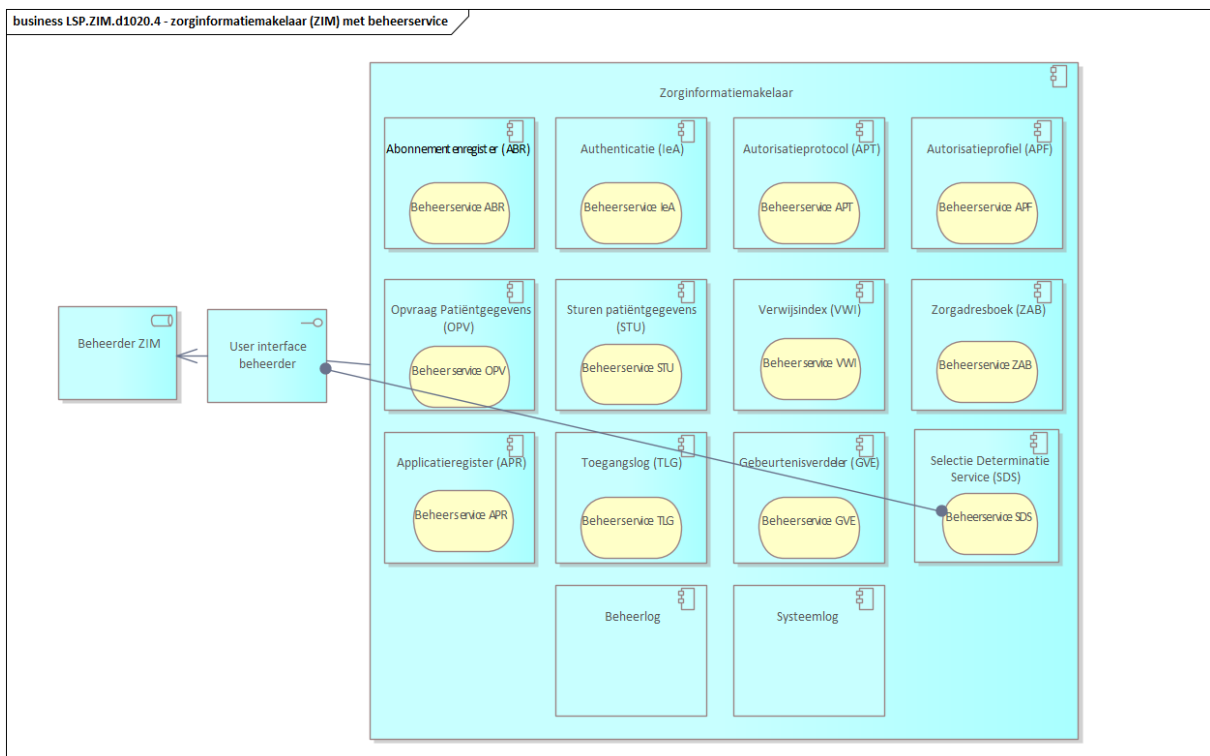


Diagram LSP.ZIM.d1020.4– beheer services, beheerlog en systeemlog

50. <https://vzvz.atlassian.net/wiki/x/ggMRBQ>

[1] Uniform Resource Identifier, in dit geval het webadres waaronder de applicatie bereikbaar is

[2] Deze interface zal langzaam uitgefaseerd worden. Voor XIS-leveranciers is deze interface geen verplichting meer zijn.

7.5.4 Zorginformatiemakelaar (ZIM)

De 'Zorginformatiemakelaar' (ZIM), volledig op HL7v3 (SOAP services) gebaseerd, is een centraal bericht uitwisselingsplatform, waarop de informatiesystemen van zorgaanbieders kunnen worden aangesloten. De ZIM wordt gebruikt door het LSP om invulling te geven aan de functie van intermediair tussen gegevenshouders en gegevensraadplegers die op HL7v3 gebaseerd zijn. De term 'informatiemakelaar' is van toepassing omdat het platform in feite optreedt als een 'makelaar'[1] van informatie.

Notitie: Naast de ZIM (Message Broker) is er ook een Resource Broker, deze wordt echter ingezet voor FHIR RESTful berichten, die op [FHIR Resources](#)⁵¹ en [REST APIs](#)⁵² zijn gebaseerd.

De ZIM heeft binnen AORTA de volgende taken:

- het bijhouden per patiënt in welke informatiesystemen van zorgaanbieders gegevens over de patiënt aanwezig zijn;
- het bijhouden van relevante gegevens over op de ZIM aangesloten informatiesystemen, waaronder bereikbaarheidsinformatie;
- het aannemen van verzoeken om patiëntinformatie van raadplegende informatiesystemen en het afhandelen hiervan door het opvragen van de gewenste informatie uit de systemen die volgens de verwijzindex over deze informatie beschikken;
- het bepalen van bouwsteentypen met de daarbij behorende selectieparameters op basis van context en rolcode;
- het bieden van een abonnementsfunctie aan raadplegende informatiesystemen zodat deze systemen een abonnement signaal kunnen krijgen indien bepaalde gebeurtenissen optreden;
- het zorgdragen voor beveiliging, door het authenticeren van de indiener van informatie-uitwisselingsverzoeken en het controleren van diens autorisatie om de gevraagde gegevens te raadplegen;
- het traceerbaar maken van informatie-uitwisseling door het registreren van alle berichtuitwisselingen tussen de ZIM en op de ZIM aangesloten informatiesystemen.

Naast de hierboven genoemde taken is er ook een taak die wordt aangeboden door het ZORG-AB:

- het faciliteren van het verzenden van patiëntinformatie door het bieden van de mogelijkheid om de informatiesystemen van aangesloten zorgaanbieders op te zoeken en te adresseren.

Het ZORG-AB is naast de ZIM gepositioneerd, maar voor het overzicht wordt de ZORG-AB-functionaliteit ook meegenomen in de beschrijving binnen dit hoofdstuk (zie pagina '[Zorgadresboek](#)⁵³').

51. <https://www.hl7.org/fhir/resourcelist.html>

52. <https://www.hl7.org/fhir/http.html>

53. <https://vzvz.atlassian.net/wiki/x/PQERBQ>

De ZIM is hiertoe samengesteld uit een aantal logische componenten waaraan deelverantwoordelijkheden zijn toegekend. Diagram LSP.ZIM.d1010.5 geeft hiervan een overzicht. Deze componenten worden hier kort behandeld. Meer informatie wordt gegeven op pagina 'Beheerinteracties'⁵⁴ en in de ontwerpdocumenten van de individuele componenten.

De ZIM beschikt naast de logische componenten over een orkestratieservice^[1]. Deze zorgt ervoor dat een bericht dat binnenkomt bij de ZIM in een aantal logische stappen wordt afgehandeld, waarbij de verschillende deelcomponenten in de juiste volgorde een bijdrage leveren aan de afhandeling van het bericht. Deze orkestratie wordt in detail behandeld op de pagina 'Berichtafhandeling door de ZIM'⁵⁵.



Diagram LSP.ZIM.d1010.5 - systeemcomponenten binnen de Zorginformatiemakelaar

Zowel de componenten en orkestratiedienst worden op logisch niveau beschreven. Over de fysieke implementatievorm van componenten en orkestratiedienst worden geen uitspraken gedaan.

[1] Parallel aan de Engelse term 'Message Broker'.

7.5.4.1 Opvraag patiëntgegevens

Deze component is verantwoordelijk voor het afhandelen van verzoeken van gegevensraadplegers. Het verzamelt daartoe per verzoek de gevraagde gegevens uit de informatiesystemen waarin volgens de verwijsindex gegevens aanwezig zijn. In het geval er door een gegevensraadpleger een gerichte vraag wordt verstuurd, wordt de verwijsindex niet geraadpleegd.

54. <https://vzvz.atlassian.net/wiki/x/6gMRBQ>

55. <https://vzvz.atlassian.net/wiki/x/xQIRBQ>

7.5.4.2 Sturen patiëntgegevens

Deze component is verantwoordelijk voor het doorsturen van patiëntgegevens van een aangesloten gegevenszender naar de juiste aangesloten gegevensontvanger.

7.5.4.3 Verwijsindex

Deze component houdt per patiënt bij in welke bij de ZIM aangesloten informatiesystemen patiëntgegevens aanwezig zijn. De verwijsindex houdt geen medische informatie bij, deze blijft in het aangesloten zorgsysteem.

7.5.4.4 Zorgadresboek

Het ZORG-AB is gepositioneerd naast de ZIM, maar is wel opgenomen in de LSP-omgeving. Het ZORG-AB houdt informatie bij over zorgaanbieders en zorgverleners die betrokken kunnen zijn bij uitwisseling van informatie via de ZIM. Deze informatie is afkomstig uit het UZI-register en uit de lokale VZVZ-administratie.

7.5.4.5 Applicatieregister

Deze component houdt relevante gegevens bij over de informatiesystemen van zorgaanbieders die op de ZIM zijn aangesloten.

7.5.4.6 Abonnementenregister

Het abonnementenregister houdt bij welke zorgverleners en patiënten abonnementen hebben geregistreerd op bepaalde gebeurtenissen in de ZIM. Deze component maakt het mogelijk voor zorgverleners en patiënten om vanuit op de ZIM aangesloten informatiesystemen abonnementen te registreren, op te vragen en te beëindigen.

7.5.4.7 ToestemmingsAbonnementenregister

Het toestemmingsabonnementenregister houdt bij welke applicaties voor welke patiënten abonnementen hebben geregistreerd bij Mitz. Dit component is nodig, om geen onnodige abonnementen af te sluiten en de ID te bepalen bij afmelden van het toestemmingsabonnement.

7.5.4.8 Authenticatie

Dit component is betrokken bij de afhandeling van elk bericht dat bij de ZIM binnenkomt vanuit een op de ZIM aangesloten informatiesysteem, zoals bij het opvragen en versturen van patiëntgegevens. De component identificeert en authentificeert hierbij de initiator van het bericht, aan de hand van informatie die in het bericht is meegegeven waarbij de authenticiteit met voldoende waarborg moet worden vastgesteld.

Hiertoe heeft de gebruiker een vertrouwensmiddel aan de hand waarvan de gebruiker kan worden geauthentificeerd (zie pagina '[Basisregistraties en vertrouwensmiddelen](#)'⁵⁶).

56. <https://vzvz.atlassian.net/wiki/x/MoWObg>

- Een zorgverlener maakt hiertoe gebruik van een UZI-pas.
- Een klantenloketmedewerker maakt gebruik van een PKI-overheidspas.
- De patiënt kan zich authenticeren door middel van DigiD.

A.d.h.v. een vertrouwensmiddel wordt een authenticatie token aangemaakt die via een beveiligde verbinding tussen de GBx en ZIM wordt uitgewisseld, op basis van het servercertificaat van het GBx en het servercertificaat van de ZIM. Op basis van het servercertificaat van het GBx wordt vastgesteld vanuit welke organisatie de berichtuitwisseling is geïnitieerd.

Het doel van de authenticatietoken is:

1. de gebruiker te identificeren en authenticeren
2. de authenticiteit van het verstuurd bericht (deels) te borgen. Hierbij worden elementen uit het verstuurd bericht in het authenticatietoken geplaatst.
3. de gebruiker onweerlegbaar aan het verstuurd bericht te koppelen.

Daarnaast kan t.b.v. authenticatie van de gebruiker in het bericht meerdere tokens opgenomen zijn:

- Transactietoken (T); een token dat gekoppeld is aan een uniek bericht; Dit token is getekend door een servercertificaat van het versturende systeem of door het persoonlijke UZI- certificaat van de gebruiker. Zie IH Berichtauthenticatie Transactietoken voor een complete afhandeling en beschrijving van het transactietoken;
- PKIO-token (P); een token dat gekoppeld is aan een uniek bericht; Dit token is getekend door het persoonlijke PKIO-certificaat van de gebruiker. Zie IH Berichtauthenticatie PKIO voor een complete afhandeling en beschrijving van het PKIO-token;
- Mandaattoken (M); een token dat AORTA-autorisaties overdraagt van de mandaterende naar een gemandateerde. Zie IH Mandaattoken voor een complete afhandeling en beschrijving van het mandaattoken;
- Inschrijftoken (I); een token dat de koppeling legt tussen een patiënt en de behandelende organisatie. Zie IH Inschrijftoken voor een complete afhandeling en beschrijving van het Inschrijftoken.

Het voorkomen van een token is afhankelijk van het vertrouwensniveau waarop een bericht wordt verstuurd, of er sprake is van een mandaat en welk specifiek uitwisselingsmechanisme wordt gebruikt.

7.5.4.8.1 SAML2 tokens

Alle XIS-systemen hebben nu voor de authenticatietoken de SAML2 standaard gebruikt. Voor de authenticatie van burgers (patiënten) zijn we afhankelijk van DigiD, die ook op SAML2 is gebaseerd. Voor de FHIR REST interfaces worden SAML2 (authenticatie) ook ondersteund. Het SAML2 (authenticatie) token wordt in XML-vorm opgenomen in de SOAP header van het bericht. De hele SOAP envelop verdwijnt bij het gebruik van een (FHIR) REST service, omdat dit op HTTP gebaseerd is. Hierbij zullen de SAML2 (authenticatie) tokens verplaatst worden naar de HTTP "authorization" header in Base64 gecodeerd. Dit heeft de volgende praktische beperkingen:

1. de ontvanger van het bericht moet de HTTP "authorization" header eerst decoderen. Het LSP doet de SAML2 (authenticatie) token validatie en controleert of elementen uit het token corresponderen met elementen uit het bericht.

2. in de HTTP standaard is er geen beperking aan de grootte van headers, maar in de praktijk hebben verschillende web servers helaas wel een limiet op de de grootte van headers.
3. Het SAML2 token verwijst naar bepaalde HL7v3 elementen (zoals triggerEventID). Niet al deze elementen uit HL7v3 hebben een gelijksoortig element in FHIR. De specificaties/ implementatiehandleiding van de tokens zal voor FHIR/REST uitwisseling daarom sowieso aangepast moeten worden.

In de huidige opzet zou het meesturen van 1 of meerdere SAML2 "assertions" (beweringen) tokens in de HTTP header van het FHIR verzoek mogelijk zijn. HTTP-headers kennen een beperkte grootte. Bij grotere en meerdere tokens zullen we moeten overgaan op een ander protocol. Web servers kunnen bij een te grootte datavolume de informatie in de HTTP headers niet verwerken. De combinatie van SAML2 en REST is voor de XIS-leveranciers mogelijk ook een blokkerend punt, omdat SAML2 gezien kan worden als een legacy-protocol.

}

7.5.4.9 Autorisatieprotocol

Deze component is betrokken bij de afhandeling van elk bericht dat bij de ZIM binnenkomt vanuit een op de ZIM aangesloten informatiesysteem en controleert of het beroep en specialisatie of de rol van de initiator van het bericht in overeenstemming is met de gegevens die door middel van het bericht worden gevraagd of uitgewisseld.

7.5.4.10 Toegangslog

Deze component is betrokken bij de afhandeling van elk bericht dat bij de ZIM binnenkomt vanuit een op de ZIM aangesloten informatiesysteem en registreert enkele kerngegevens (conform de NEN7513) waardoor elk uitwisseling achteraf controleerbaar is.

7.5.4.11 Gebeurtenisverdeler en gebeurtenisafhandelaars

De gebeurtenisverdeler is het centrale meldpunt voor gebeurtenissen voor de overige componenten van de ZIM. De gebeurtenisverdeler zorgt ervoor dat gebeurtenissen worden doorgegeven aan alle gebeurtenisafhandelaren die in een bepaalde gebeurtenis geïnteresseerd zijn. Gebeurtenisafhandelaren zijn technische componenten die specifieke acties kunnen ondernemen, zoals het sturen van signaleringen. Concrete gebeurtenisafhandelaren zijn de Signaleringsafhandelaar en de Afhandelaar Bezwaar Patiënt.

De Signaleringsafhandelaar is een gebeurtenisafhandelaar die signalen stuurt naar een op de ZIM aangesloten informatiesysteem als een gebeurtenis plaatsvindt waarvoor het aangesloten systeem een abonnement heeft geregistreerd. De signaleringsafhandelaar gebruikt hierbij het [abonnementenregister](https://vzvz.atlassian.net/wiki/x/QwERBQ)⁵⁷ om te controleren welke systemen een abonnement hebben voor een bepaalde gebeurtenis.

57. <https://vzvz.atlassian.net/wiki/x/QwERBQ>

7.5.4.12 Selectie Determinatie Service

Deze component is betrokken bij het bepalen van de op te leveren bouwstenen en de specifieke invulling van deze bouwstenen op basis van de determinatietabellen. De op te leveren bouwstenen en de specifieke invulling hiervan worden bepaald aan de hand van de context van de opvraag en de rolcode^{[2]⁵⁸} van de zorgverlener die de opvraag doet.

^{[2]⁵⁹} In het geval er sprake is van een mandaat, zal de rolcode van de mandaterende zorgverlener bepalend zijn.

7.5.5 Goed beheerd informatiesysteem (GBx)

Een goed beheerd informatiesysteem (GBx) binnen AORTA is een concrete implementatie van een softwareproduct die voldoet aan een set van eisen voor de aansluiting op de ZIM. Deze eisen raken zowel het gebruikte softwareproduct als het beheer en exploitatie van de concrete implementatie van het softwareproduct.

GBx wordt gebruikt als een groeperende term voor alle concrete installaties van systemen van verschillende aard, dus niet uitsluitend zorgsystemen, die aan de eisen voor aansluiting op de ZIM voldoen.

7.5.6 Zorginformatiesystemen (XIS) en het Goed beheerd zorgsysteem (GBZ)

Een 'XIS' is een verzamelterm voor informatiesystemen in het zorgveld, zoals bijvoorbeeld Huisartsinformatiesystemen (HIS) en Apotheekinformatiesystemen (AIS). In de praktijk beschikken zorgaanbieders, afhankelijk van hun werkzaamheden, over verschillende typen informatiesystemen. Dit zijn veelal implementaties van commercieel verkrijgbare informatiesystemen gebouwd door gespecialiseerde softwareleveranciers, maar kunnen ook in eigen beheer zijn ontwikkeld.

Een Goed Beheerd Zorgsysteem (GBZ) is een concrete installatie van een XIS of verzameling XIS'en, elk met een XIS-typekwalificatie (zie verderop in deze paragraaf), in gebruik bij één zorgaanbieder, die voldoet aan de implementatie- en exploitatie-eisen voor aansluiting op de ZIM^[1]. Het begrip GBZ is een deelverzameling van het begrip GBx en is in feite een goed beheerd informatiesysteem (GBx) dat gebruikt wordt door een zorgaanbieder.

Om een XIS in te zetten als GBZ moet aan twee soorten eisen worden voldaan:

- Voorwaarden die in algemene zin aan het XIS als *softwareproduct* moeten worden gesteld. In de eerste plaats zijn dit functionele eisen, bijvoorbeeld ten aanzien van de berichtuitwisseling die door een XIS moet worden ondersteund. Ook gelden non-functionele eisen die leiden tot eisen aan het XIS als softwareproduct, bijvoorbeeld wat betreft ondersteuning van twee-factor-authenticatie door het softwareproduct. Producenten van XIS'en kunnen een XIS-typekwalificatie behalen waarbij gecontroleerd wordt of het product aan deze eisen voldoet.
- Voorwaarden die gelden voor een specifieke implementatie van een XIS voor een bepaalde zorgaanbieder. Dit zijn bijvoorbeeld eisen aan de beheersorganisatie of de

58. https://vzvz.atlassian.net/wiki/display/A8/6.2%09Zorginformatiemakelaar#_ftn2

59. https://vzvz.atlassian.net/wiki/display/A8/6.2%09Zorginformatiemakelaar#_ftnref2

gebruikersvoorzieningen, zoals de beschikbaarheid van authenticatie-middelen. Deze aanvullende eisen zijn dus implementatieafhankelijk en maken geen deel uit van een XIS-typekwalificatie.

Het GBZ heeft in het kader van berichtenuitwisseling via AORTA enkele belangrijke verantwoordelijkheden[2]:

- Het GBZ legt de basis voor authenticatie van de gegevensraadpleger of gegevenszender. Allereerst authenticceert het GBZ zelf de eindgebruiker als deze aanlogt bij het GBZ. Ook verstrekt het GBZ in berichten aan de ZIM verifieerbare identiteitsinformatie van de eindgebruiker. Het GBZ legt de basis voor de identificatie van de patiënt, door het burgerservicenummer van de patiënt vast te leggen; hierbij registreert het GBZ ook of de identiteit van de patiënt is geverifieerd door de controle van een wettelijk identiteitsdocument (WID) als genoemd in de Wbsn-z.
- In het GBZ wordt, indien het GBZ dient als bronsysteem van patiëntgegevens, vastgelegd of de patiënt heeft ingestemd (opt-in) met het beschikbaar maken van gegevens via AORTA. Het is mogelijk om deze opt-in in plaats van in het bronsysteem te laten vastleggen in Mitz.
- In het GBZ wordt het bestaan van een behandelrelatie tussen zorgverlener en patiënt vastgelegd; aangezien de behandelrelatie in het contact tussen zorgverlener en patiënt tot stand komt, is het zorgsysteem van de zorgverlener de aangewezen plaats om de behandelrelatie te bevestigen.
- In het GBZ wordt bijgehouden op basis van welke autorisatieregels een zorgverlener gebruik kan maken van een mandaat.

[1] Het voldoen aan de implementatie- en exploitatie-eisen wordt getoetst door een eigen verklaring van de beheerorganisatie en uitvoering van steekproefsgewijze schouwingen.

[2] Deze lijst van verantwoordelijkheden is niet limitatief. Hier worden enkele kernverantwoordelijkheden genoemd die bij het GBZ worden belegd in tegenstelling tot de ZIM.

7.5.7 Goed beheerd patiëntportaal (GBP)

Een Goed Beheerd Patiëntportaal (GBP) is een (web)portaal voor patiënten die voldoet aan software-specifieke eisen om berichten uit te wisselen met de ZIM én aan implementatie- en exploitatie-eisen die voorwaardelijk zijn voor aansluiting op de ZIM.

Zoals besproken in '[Rollen toekennen aan actoren](#)' (see page 60) kan de patiënt optreden als gegevensraadpleger en heeft de patiënt hierbij toegang tot de eigen gegevens zoals die bij AORTA door zorgverleners zijn aangemeld. De patiënt krijgt toegang via een GBP.

Een inhoudelijke uitwerking van de architectuur van een GBP valt buiten de scope van AORTA. Wel is voor AORTA van belang dat voor een GBP verschillende implementatievormen mogelijk zijn:[1]

- Een GBP kan als zelfstandig systeem worden geïmplementeerd met een eigen aansluiting op de ZIM.
- Daarnaast kan een XIS-leverancier een patiëntportaalmodule implementeren als aanvullend onderdeel van een XIS. Als een dergelijk XIS wordt ingezet als GBZ, dan mag de patiëntportaalmodule echter niet via het GBZ gegevens ophalen uit AORTA. Om als GBP te

worden toegepast moet de patiëntportaalmodule van het XIS worden geïmplementeerd met een eigen aansluiting op de ZIM en mag alleen via deze route communiceren met AORTA. De patiënt kan verder pas via een dergelijke patiëntportaalmodule gegevens uitwisselen via de ZIM indien de module voldoet aan een aantal GBP-eisen, onder meer op het punt van patiëntauthenticatie. De patiëntportaalmodule krijgt een eigen vermelding als GBP in het applicatieregister.

Op dit moment biedt de ZIM nog geen ondersteuning voor vertegenwoordiging van patiënten door andere personen (zie [Toegangsmodel \(see page 64\)](#)). Eventuele vertegenwoordigers zijn daarom aangewezen op het klantenloket.

7.5.7.1 Volgjezorg

Volgjezorg (VZVZ-portaal) is een specifieke invulling van een GBP onder verantwoordelijkheid van VZVZ. Binnen Volgjezorg is het mogelijk om te bevragen welke zorgverleners er gegevens beschikbaar stellen van een specifieke patiënt. Daarnaast is het mogelijk om de logging te bevragen met betrekking tot de gegevensuitwisseling (gegevens over zijn eigen persoon) over de AORTA infrastructuur. Hierbij wordt getoond welke soort informatie is uitgewisseld en welke organisaties bij die uitwisseling betrokken zijn geweest. Er wordt expliciet niet getoond welke zorgverleners er betrokken zijn geweest bij het bevragen of het versturen van gegevens (deze gegevens worden uiteraard wel conform de NEN7513 gelogd). Indien een patiënt wil weten welke zorgverlener verantwoordelijk was voor initiatie van de berichtuitwisseling, dan dient de patiënt deze informatie te verkrijgen bij de verantwoordelijke zorgaanbieder. VZVZ verstrekt deze informatie niet aan de patiënt.

[1] Op het moment van publicatie bestaan nog geen concrete GBP-implementaties.

7.5.8 Goed beheerd klantenloketsysteem (GBK)

Een goed beheerd klantenloketsysteem (GBK) is een informatiesysteem voor klantenloketmedewerkers, dat voldoet aan software-specifieke eisen én aan beheereisen die voorwaardelijk zijn voor aansluiting op de ZIM.

Hiermee kan een medewerker van het klantenloket namens een patiënt een beperkte set van (niet medisch inhoudelijke) gegevens opvragen, zoals besproken in '[Actoren en rollen- Klantenloket en Medewerker klantenloket](#)'⁶⁰.

In plaats van de patiënt kan ook een wettelijk vertegenwoordiger van de patiënt contact opnemen met het klantenloket. De regels uit de [WGBO] worden dan procedureel gecontroleerd door de klantenloketmedewerker, eventueel daarin ondersteund door applicatiefunctionaliteit in het GBK. De ZIM voert geen controles uit op vertegenwoordigingsrelaties, het GBK vraagt de ZIM immers om gegevens van de patiënt, niet om gegevens van diens vertegenwoordiger.

Een inhoudelijke uitwerking van de architectuur van een GBK valt buiten de scope van AORTA.

60. <https://vzvz.atlassian.net/wiki/spaces/ACM/pages/1797390478/8.5.0+Actoren+en+rollen#id-8.5.0Actorenenrollen-KlantenloketenMedewerkerklantenloket>

7.5.9 Goed beheerde organisatie (GBO)

Een goed beheerde organisatie (GBO) is een informatiesysteem voor organisaties die geen UZI-abonnee kunnen worden. Een GBO moet voldoen aan software-specifieke eisen én aan beheereisen die voorwaardelijk zijn voor aansluiting op de ZIM.

Of een organisatie mag communiceren over de AORTA infrastructuur met alleen een PKIO-certificaat (anders dan UZI-certificaat), wordt voor elke organisatie apart bepaald. Een organisatie kan alleen worden aangesloten als er ook daadwerkelijk een businesscase is.

7.5.10 Dienstverlener Zorgaanbieder (DVZA)

Een Dienstverlener Zorgaanbieder (DVZA) betreft een rol in het MedMij Afsprakenstelsel. Het levert Diensten aan de Zorgaanbieder gerelateerd aan de uitwisseling tussen patiënt en zorgaanbieder en committeert zich hiervoor aan de naleving van de afspraken van het MedMij Afsprakenstelsel.

De AORTA-infrastructuur heeft een specifieke DVZA ten behoeve van ontsluiting van patiëntgegevens uit op de AORTA-infrastructuur aangesloten GBx-en. De AORTA DVZA is aangesloten op het LSP. Communicatie tussen de AORTA DVZA en een GBx zal dan ook altijd verlopen met het LSP als intermediair.

Naast de naleving van de afspraken van het MedMij Afsprakenstelsel dient de AORTA DVZA ook te voldoen aan specifieke eisen voor aansluiting op de AORTA-infrastructuur. De DVZA is tevens verantwoordelijk voor de vertaling van de verschillende (bericht)standaarden tussen het MedMij Afsprakenstelsel en de AORTA standaard.

7.5.11 Goed beheerde connector (GBC)

Een goed beheerde connector (GBC) is een connector die een externe infrastructuur koppelt aan de AORTA-infrastructuur. Hiermee is het mogelijk om patiëntgegevens van een informatiesysteem uit een externe infrastructuur te ontsluiten richting op AORTA aangesloten GBx-en.

De GBC treedt op als koppelvlak tussen de AORTA-infrastructuur en een externe infrastructuur. Het is (vooralsnog) alleen maar mogelijk om patiëntgegevens te ontsluiten vanuit een externe infrastructuur aan informatiesystemen binnen de AORTA-infrastructuur. AORTA stelt (vooralsnog) geen interfaces beschikbaar voor bevraging van patiëntgegevens ten behoeve van niet op AORTA aangesloten informatiesystemen.

7.5.12 Basisregistraties en vertrouwensmiddelen

7.5.12.1 UZI-register

Het Unieke Zorgverlener Identificatie register (kortweg UZI-register) is het door de Minister van VWS aangewezen register van zorgaanbieders zoals vermeld in artikel 14 van de Wbsn-z. Het UZI-register wordt beheerd door het CIBG, een uitvoeringsorganisatie van het ministerie van VWS.

Het UZI-register is de certificatedienstverlener (ook wel Certificate Service Provider of CSP) die certificaten uitgeeft voor de unieke identificatie en authenticatie van zorgaanbieders en indicatieorganen in de zorg.

Tevens geeft het UZI-register certificaten uit voor de unieke identificatie en authenticatie van zorgverleners. Het UZI-register koppelt hiertoe uniek de fysieke identiteit aan een elektronische identiteit en legt deze vast in certificaten. De certificaten en de hierbij behorende cryptografische sleutels bevinden zich op een smartcard, de UZI-pas.

Het UZI-register geeft UZI-passen uit voor door de minister van VWS bij wet en regelgeving aangewezen partijen. Zorgverleners en medewerkers worden door het UZI-register voorzien van een UZI-pas, informatiesystemen van een UZI-servercertificaat. De UZI-pas is binnen AORTA nodig voor authenticatie van zorgverleners en medewerkers van zorgaanbieders, het UZI-servercertificaat is nodig voor authenticatie van GBZ'en.

Een UZI-pas is een vertrouwensmiddel op basis van PKIO-certificaten (Private Key Infrastructure Overheid, zie [PKIO]). Er zijn aparte passen voor zorgverleners, medewerkers en medewerkers-niet-op-naam. De pas faciliteert bij elektronisch verkeer authenticatie, versleuteling en het plaatsen van een elektronische handtekening (dit laatste alleen met passen op naam). De pas bevat een apart certificaat voor elk van deze drie functies.

Een UZI-pas bevat o.a. het UZI-nummer, beroep en specialisatie van de pashouder. Ook bevat de pas het nummer van de zorgaanbieder die de pas heeft aangevraagd, het UZI-register abonneenummer (URA).

Een UZI-servercertificaat is eveneens een vertrouwensmiddel op basis van de PKIO. Het is nodig voor het identificeren van een informatiesysteem en het opzetten van een beveiligde elektronische verbinding. Het servercertificaat bevat eveneens het URA van de zorgaanbieder.

7.5.12.2 PKIO

De Public Key Infrastructure Overheid (PKIO) is een infrastructuur voor het uitgeven en beheren van digitale certificaten. PKIO-overheid heeft een hiërarchische structuur van certificaten. Het ankerpunt van vertrouwen binnen PKIO-overheid, het stamcertificaat Staat der Nederlanden, valt onder verantwoordelijkheid van de Nederlandse overheid.

PKIO verstrekt zowel persoonlijke vertrouwensmiddelen op naam (PKIO-passen), als systeemvertrouwensmiddelen (servercertificaten).

PKIO-passen worden gebruikt voor de identificatie van medewerkers van het klantenloket.

PKIO-servercertificaten worden gebruikt door de ZIM, door het GBK, door GBP'en en door niet UZI-abonnees (GBO). Ze zijn nodig voor het identificeren van het informatiesysteem en het opzetten van een beveiligde elektronische verbinding.

7.5.12.3 ZORG-ID

ZORG-ID is een door VZVZ beheerde voorziening voor identificatie en authenticatie van zorgprofessionals en ondersteunend personeel binnen AORTA.

Het fungeert als een modern vertrouwensmiddel in aanvulling op de al bestaande middelen (zoals UZI, PKIO-overheid en DigiD) en sluit aan bij de wettelijke kaders en beveiligingsstandaarden die gelden in de zorg.

ZORG-ID voorziet zorgverleners en medewerkers van een elektronische identiteit die gebruikt kan worden voor:

- **Authenticatie** – sterke en multifactor authenticatie op basis van moderne standaarden.

- **Identificatie** – koppeling van de elektronische identiteit aan een fysieke identiteit door middel van een betrouwbaar registratieproces (RA-proces).
- **Digitale handtekening** – ondersteuning van geavanceerde of gekwalificeerde elektronische handtekeningen, afhankelijk van het gebruikte middel.

Het ZORG-ID platform ondersteunt zowel bestaande middelen (zoals de UZI-pas) als nieuwe vormen van identificatie en authenticatie die aansluiten bij de digitalisering van de zorg. Voorbeelden hiervan zijn:

- **ZORG-ID Mobile App** – een mobiele oplossing die fungeert als toegangsmiddel tot de ZORG-ID wallet, met ondersteuning voor twee-factorauthenticatie, digitale ondertekening en het scannen van een WID-document.
- **ZORG-ID Smartcard** – een fysieke kaart die toegang biedt tot de wallet en inlogfunctionaliteit ondersteunt.

Deze middelen faciliteren de drie rollen binnen het verifiable-credentials-model:

- **Issuer** – de partij die vertrouwelijke gegevens of attributen uitgeeft (bijvoorbeeld een UZI-register).
- **Holder** – de zorgprofessional die deze gegevens in de wallet beheert.
- **Verifier** – de partij die de gegevens en authenticatie controleert (bijvoorbeeld het LSP).

ZORG-ID zelf geeft X.509-certificaten uit en functioneert daarmee als zelfstandige Certificate Authority (CA).

7.5.12.4 DigiD

Het DigiD-register (zie [DigiD]) is een ICT-voorziening onder beheer van 'Logius', de dienst digitale overheid van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. In het DigiD-register worden personen geregistreerd die door het DigiD-register zijn voorzien van een vertrouwensmiddel. Personen die vervolgens hun DigiD gebruiken om zich te identificeren, kunnen door het DigiD-register worden geauthenticeerd. Hierbij geeft het DigiD-register een elektronisch ondertekende bewering af over de mate waarin het de authenticiteit van de gebruiker waarborgt. DigiD treedt hierbij dus op als 'identity provider'.

Authenticatie met behulp van DigiD is van toepassing voor patiënten die gebruikmaken van een GBP (zie ook '[Berichtafhandeling door de ZIM: Authenticatie van de gebruiker / pashouder](#)' (see page 132)).

7.5.12.5 SBV-Z

De SBV-Z biedt toegang tot de volgende BSN-diensten die voor AORTA relevant zijn:

- het opvragen en verifiëren van het BSN;
- het opvragen van persoonsgegevens op basis van het BSN;
- het verifiëren van de geldigheid van het Nederlands identiteitsdocument.

Deze diensten kunnen worden aangeroepen vanuit een GBZ wanneer de zorgverlener de identiteit van de patiënt verifieert (zie ook [Zorginformatiesystemen \(XIS\) en het Goed beheerd zorgsysteem \(GBZ\)](#) (see page 110)).

7.5.12.6 Mitz

- Mitz is een centrale toestemmingsregistratie en biedt de volgende services: Locatieservice; welke zorgaanbieder heeft welke gegevens van welke patiënt waarvoor tevens toestemming is gegeven voor gegevensdeling?
- Toestemmingservice; welke toestemmingen heeft een patiënt vastgelegd voor een zorgaanbieder?

7.5.13 Resource Broker (RB)

De Resource Broker (RB) is de vervanging van het LSP die naast HL7-v3 ook HL7-FHIR RESTful interacties ondersteund. Hierdoor worden tevens de zorgtoepassingen gebaseerd op de HL7-FHIR standaard ondersteund. De Resource Broker maakt gebruik van een Autorisatie Server (AS), waar autorisatie verzoeken heen kunnen worden gestuurd en indien het verzoek wordt goedgekeurd een toegangstoken wordt afgegeven voor een HL7-FHIR RESTful interactie. Verder biedt de Resource Broker een Verzending en Consolidatie dienst aan die HL7-v3 berichten naar HL7-FHIR transformeert. Voor het kunnen verzenden en consolideren wordt gebruik gemaakt van de Applicatie Register interface (APR). Om systemen van zorgaanbieders te kunnen vinden via de Resource Broker, wordt gebruik gemaakt van de Adresseringservice in combinatie met de gemeenschappelijke dienst ZORG-AB.

7.5.13.1 Resource Broker MedMij (RB MedMij)

De Resource Broker MedMij biedt de (HL7-FHIR) resource interface, zoals gespecificeerd in het MedMij afsprakenstelsel, zoals het delen van meetwaarden, antwoorden op vragenlijsten en het verzamelen van documenten, meetwaarden, basisgegevens (zorg en GGZ), verwijzingen naar vragenlijsten en afspraken. Verder biedt de Resource Broker op verzoek van een resource client (PGO Server) een CapabilityStatement op, met daarin de capabilities, zoals te vinden in de *Implementation Guides* van de informatiestandaarden die horen bij de door LSP+ geboden MedMij gegevensdiensten.

7.5.13.2 Resource Broker Zorgaanbieder-Zorgaanbieder (RB ZA-ZA)

De Resource Broker (ZA-ZA) vervult meerdere functies voor een resource client (xIS) en maakt gebruik van de Autorisatie Server ZA en eventueel de RB VnC (Verzending & Consolidatie).

De services zijn toegankelijk via een aangeboden interface en worden beschreven in de vorm van use cases. Responses die in een succes- of uitzonderingssituaties moeten worden geretourneerd zijn [voor iedere situatie beschreven](#)⁶¹.

7.5.13.3 Resource Broker Verzenden en Consolideren (RB VnC)

De Resource Broker VnC zijn toegankelijk via een geboden interface en worden beschreven in de vorm van use cases. Responses die in een succes- of uitzonderingssituaties moeten worden geretourneerd zijn [voor iedere situatie beschreven](#)⁶². De Resource Broker VnC kan FHIR-search interacties versturen naar meerdere resource servers en de antwoorden *consolideren* in de benodigde response interactie.

61. <https://vzvz.atlassian.net/wiki/x/loIpBQ>

62. <https://vzvz.atlassian.net/wiki/x/loIpBQ>

Het consolidatieproces consolideert ontvangen HL7v3-responses naar FHIR-responses middels een Transformatie Server (BTD).

7.5.14 Autorisatie Server (AS)

De Autorisatie Server (AS) implementeert specificaties van OAuth2 om toepassingen toegang te geven tot de interfaces van de Resource Broker (RB) of Resource Server (RS). Dit in overeenstemming met de toegangsregels zoals opgenomen in de diverse autorisatierichtlijnen van de op AORTA geïmplementeerde zorgtoepassingen en indien van toepassing de patiënttoestemming zoals opgenomen in Mitz.

De metadata, dat benaderbaar is via het publieke internet, van de Autorisatie Server kan, conform [RFC 8414](#)⁶³, worden opgehaald op een well-known URL die kan worden geconstrueerd m.b.v. de <iss> claim uit het token (zie ook [section-3.1 van RFC8414](#)⁶⁴).

7.5.14.1 Autorisatie Server MedMij (AS MedMij)

- De Autorisatie Server van MedMij ondersteunt het verkrijgen of uitgeven van een MedMij access token (toegangstoken)
- De Autorisatie Server van MedMij ondersteunt het inwisselen van een MedMij access token voor een AORTA access (JWT) token (benodigd bij de Resource Broker MedMij).
- De AORTA Token Interface is gebaseerd op [OAuth token exchange](#)⁶⁵.

7.5.14.2 Autorisatie Server Zorgaanbieder (AS ZA)

- De Autorisatie Server van Zorgaanbieder ondersteunt het verkrijgen of uitgeven van een AORTA access token (toegangstoken)
- De Autorisatie Server Zorgaanbieder ondersteunt het inwisselen van een Zorgaanbieder token (combinatie van transactie-, inschrijf- en eventueel mandaat token) voor een AORTA (JWT) access token (benodigd bij de Resource Broker Zorgaanbieder). Deze dienst zal slechts worden aangeroepen via de ZA-in component van de resource broker.
- De AORTA Token Interface is gebaseerd op [OAuth token exchange](#)⁶⁶

7.5.15 Resource Server (RS)

De Resource Server (XIS) verleent alleen toegang tot patiëntgegevens, indien een vraag tot patiëntgegevens wordt begeleid met een geldig access (JWT) token met de juiste scope.

Naast het access token kan conditioneel ook door een initiërende partij een consent token meegestuurd worden. Een token dat wordt meegezonden is in sommige gevallen een XML SAMLv2 Assertion, en in andere situaties een JSON Web Token (JWT). In het token, dat wordt ontvangen in een

63. <https://tools.ietf.org/html/rfc8414>

64. <https://datatracker.ietf.org/doc/html/rfc8414#section-3.1>

65. <https://tools.ietf.org/html/rfc8693>

66. <https://tools.ietf.org/html/rfc8693>

"Authorization" HTTP header, is informatie opgenomen over welke type inhoudelijk token het betreft en welke versie, dus bijvoorbeeld dat het gaat om een AORTA access (JWT) token.

De Resource Server ondersteunt de standaard FHIR interacties zoals Read, Search, Create, Update, Batch, Transaction en een aangepaste FHIR operatie \$is-allowed waarmee een resource client kan achterhalen of een zorgaanbieder bepaalde gegevens beschikbaar stelt of ontvankelijk is voor bepaalde gegevens.

Veder biedt de Resource Server een HL7v3 interface aan.

7.5.16 Berichtentransformatiedienst (BTD)

De Berichtentransformatiedienst (BTD wordt via de VnC (de [Verzending en Consolidatie Resource Broker](#)) aangeroepen en transformeert HL7v3 berichten van en naar HL7-FHIR. [De BTD bestaat uit een aantal endpoints. Ieder endpoint biedt een specifiek type transformatie.](#)

7.6 Beheerinteracties

Bij de pagina '[Ondersteunende interacties](#)⁶⁷' werden de ondersteunende interacties geïntroduceerd, die nodig zijn om de primaire interacties (het sturen en opvragen van patiëntgegevens) te ondersteunen. Enkele ondersteunende interacties tussen de partijen die betrokken zijn bij AORTA hebben betrekking op beheerwerkzaamheden voor informatiesystemen.

Nu de [informatiesystemen](#)⁶⁸ zijn geïntroduceerd, kunnen ook de beheerinteracties kort worden geïntroduceerd. Deze worden echter alleen behandeld voor zover zij leiden tot eisen aan de functionaliteit van de ZIM of GBx. Een uitgebreide analyse van beheerprocessen valt buiten de reikwijdte van dit document. Hiervoor wordt verwezen naar de operationele uitwerking van beheerprocedures zoals vastgelegd in [AORTA DAP].

7.6.1 Actoren en rollen

Ten behoeve van beheer worden de volgende aanvullende rollen onderscheiden.

7.6.1.1 GBx-beheerder en GBZ-beheerder^[1]

De 'GBx-beheerder' draagt de verantwoordelijkheid voor het zorgvuldig beheren van een GBx dat op de ZIM wordt aangesloten en is contactpersoon voor de beheerder van de ZIM op het gebied van systeemtechnische zaken die de communicatie tussen aangesloten informatiesysteem en de ZIM beïnvloeden. In het geval van een goed beheerd zorgsysteem (GBZ) spreken we van een GBZ-beheerder. De rol van GBZ-beheerder wordt uitgevoerd onder de verantwoordelijkheid van de zorgaanbieder die eigenaar is van het GBZ en kan zo nodig worden uitbesteed aan een externe beheerpartij, mits nog steeds aan de eisen wordt voldaan die worden gesteld aan een GBZ.

Vooralsnog is voor GBZ-beheerders geen eigen identificatiemiddel ontwikkeld.

67. <https://vzvz.atlassian.net/wiki/x/ewQRBQ>

68. <https://vzvz.atlassian.net/wiki/x/twIRBQ>

7.6.1.2 Beheerder ZIM

De 'beheerder ZIM' draagt de verantwoordelijkheid voor het zorgvuldig beheren van de ZIM en de connecties met de daarop aangesloten informatiesystemen. De beheerder ZIM draagt daarmee zorg voor het dagelijks functioneren van AORTA als geheel. Aan de rol van beheerder ZIM kunnen nadere eisen worden gesteld die de rol verder onderverdelen in deelrollen. De rol van beheerder ZIM valt onder de eindverantwoordelijkheid van de LSP-organisatie (zie pagina '[Actoren en rollen - Landelijk schakelpunt](#)⁶⁹⁾').

7.6.2 Toegang van GBZ-beheerders tot primaire en ondersteunende interacties

De [primaire](#)⁷⁰- en [ondersteunende](#)⁷¹interacties zijn besproken die ondersteund worden door AORTA.

Ter ondersteuning van het functioneren van AORTA moeten GBZ-beheerders ook in staat zijn om primaire en ondersteunende interacties uit te voeren die normaal gesproken door zorgverleners worden uitgevoerd, bijvoorbeeld om problemen te onderzoeken. GBZ-beheerders mogen echter geen toegang krijgen tot medische gegevens. Om deze reden is een reeks van niet werkelijk bestaande patiënten gedefinieerd met een speciale reeks burgerservicenummers, die "fictieve BSN's" worden genoemd. Interacties met betrekking tot patiëntgegevens mogen door GBZ-beheerders alleen worden uitgevoerd in relatie tot fictieve BSN's.

De volgende reeds behandelde interacties zijn toegankelijk voor GBZ-beheerders onder gebruik van fictieve BSN's:

- opvragen van patiëntgegevens;
- sturen van patiëntgegevens;
- aan- en afmelden van patiëntgegevens;
- raadplegen verwijsindex;
- bijhouden van abonnementen.

NB: vanwege het feit dat vooralsnog geen identificatiemiddel voor GBZ-beheerders voorhanden is, kan de beheerder in de praktijk nog niet zelfstandig van deze functionaliteit gebruik maken; het gebruik van fictieve BSN's is al wel toegankelijk met een UZI-zorgverlener pas, waardoor deze BSN's wel voor testdoeleinden bruikbaar zijn.

De volgende reeds behandelde interacties zijn niet gerelateerd aan patiëntgegevens en zijn toegankelijk voor GBZ-beheerders:

- selecteren van zorgaanbieders, zorgverleners en zorgaanbiederapplicaties.

69. <https://vzvz.atlassian.net/wiki/spaces/ACM/pages/1797390478/8.5.0+Actoren+en+rollen#id-8.5.0Actorenenrollen-Landelijkschakelpunt>

70. <https://vzvz.atlassian.net/wiki/x/8gIRBQ>

71. <https://vzvz.atlassian.net/wiki/x/ewQRBQ>

7.6.3 Beheer van aansluitingen

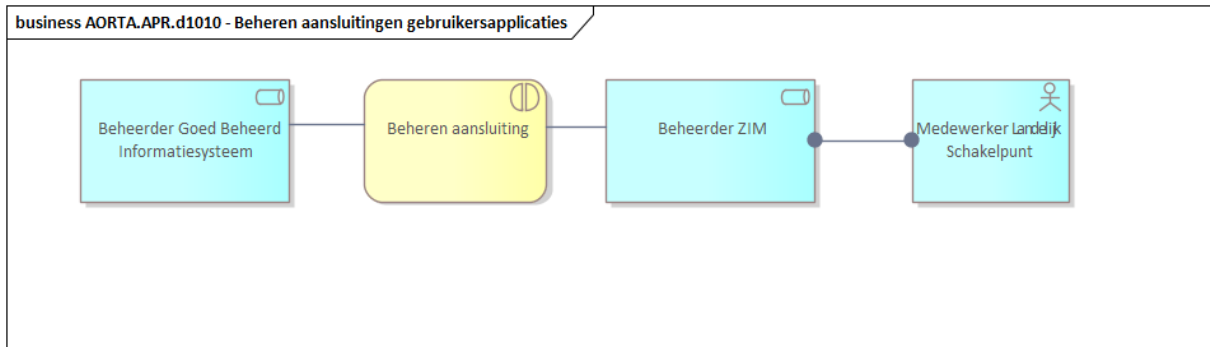


Diagram AORTA.APR.d1010 - interactie voor het beheren van aansluitingen

De ZIM bewaart informatie over aangesloten informatiesystemen in het APR. Opname in het APR is een voorwaarde voor berichtenuitwisseling met de ZIM. De beheerder van een aangesloten GBx moet gegevens uitwisselen met de beheerder van de ZIM om aansluitgegevens van het systeem actueel te houden.

Daarnaast is er een interface met het LSP waarmee een GBX een bericht kan versturen met configuratieparameters m.b.t. de functionaliteiten die de applicatie ondersteunt.

7.6.4 Beheer van de verwijzindex

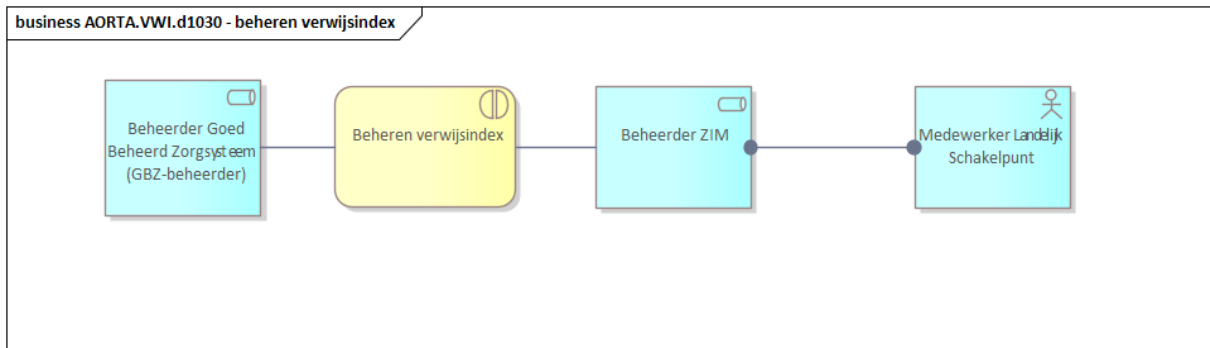


Diagram AORTA.VWI.d1030 – beheren van de verwijzindex

In de VWI van de ZIM staan alle **aanmeldingen van alle patiënten die bevraagd kunnen worden via AORTA**. Wanneer een GBZ-beheerder vermoedt dat de in de VWI opgenomen verwijzingen uit de pas lopen met het beeld dat men vanuit het eigen informatiesysteem van meldingen heeft, kan de GBZ-beheerder dit controleren door de verwijzingen uit het informatiesysteem van het GBZ te vergelijken met de verwijzingen die zijn opgenomen in de VWI. Hiervoor wordt een interface op de ZIM beschikbaar gesteld. Aan de hand van het resultaat van deze vergelijking kan de GBZ-beheerder nieuwe (her)aanmeldingen en/of afmeldingen initiëren.

7.6.5 Beheer van het zorgadresboek

De gegevens over zorgaanbieders en zorgverleners in het [ZORG-AB](#)⁷² worden overgenomen uit een centraal zorgaanbieder/zorgverlener register (het [UZI-register](#)⁷³) en de VZVZ-administratie.

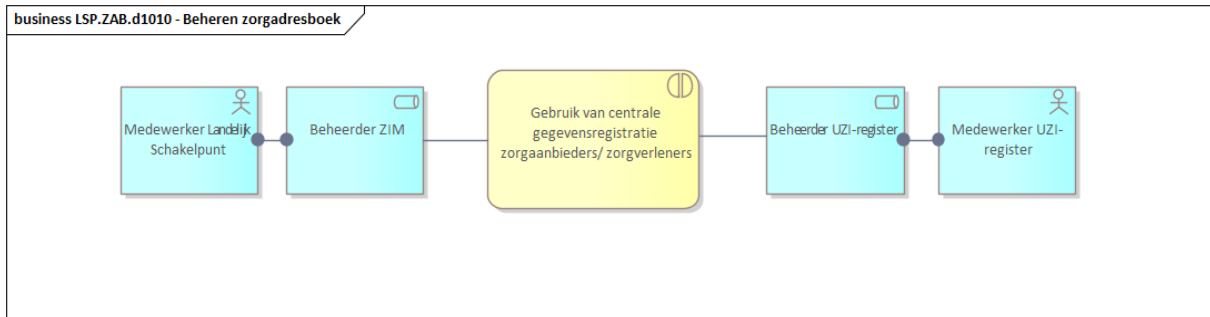


Diagram LSP.ZAB.d1010 - interactie voor het beheer van het adresboek

Wijzigingen in het UZI-register en de VZVZ-administratie moeten regelmatig worden verwerkt in het ZORG-AB. Dit om te voorkomen dat er niet-actuele gegevens worden gebruikt.

7.6.6 Beheer van zorgtoepassingen

De gegevens met betrekking tot zorgtoepassingen kunnen configureerbaar worden verwerkt door de beheerder ZIM. De configuratie-items worden aangeleverd door de LSP-opdrachtgever. De configuratie-items dienen door de beheerder ZIM ingelezen te worden.

Een configureerbare zorgtoepassing (CZT) geeft invulling aan de [primaire interacties](#)⁷⁴: het opvragen en sturen van patiëntgegevens.

7.6.7 Beheer van selectie en determinatieserver

De gegevens met betrekking tot de op te vragen bouwstenen, vraag- en filterparameters worden aangeleverd door de LSP-opdrachtgever. De betreffende gegevens worden ingelezen door de beheerder ZIM.

[1] In operationele zin wordt de beheerderrol per betrokken organisatie verder uitgewerkt in [AORTA DAP].

{}

72. <https://vzvz.atlassian.net/wiki/x/OQIRBQ>

73. <https://vzvz.atlassian.net/wiki/x/LwMRBQ>

74. <https://vzvz.atlassian.net/wiki/x/LwARBQ>

7.7 Overzicht van systeemrollen

Diagram GBX.ALG.d1010.4 geeft een samenvattend overzicht van de systeemrollen die zijn geïntroduceerd in de hoofdstukken “primaire informatiesysteeminteracties”, “ondersteunende informatiesysteeminteracties” en “beheerinteracties”. Samen representeren deze systeemrollen de set van mogelijke interacties tussen GBx'en en de ZIM die vallen binnen de basisinfrastructuur van AORTA. Het diagram geeft tevens aan welke systeemrollen kunnen worden gerealiseerd door alle GBx'en en welke zijn voorbehouden aan GBZ'en, GBP en GBK.

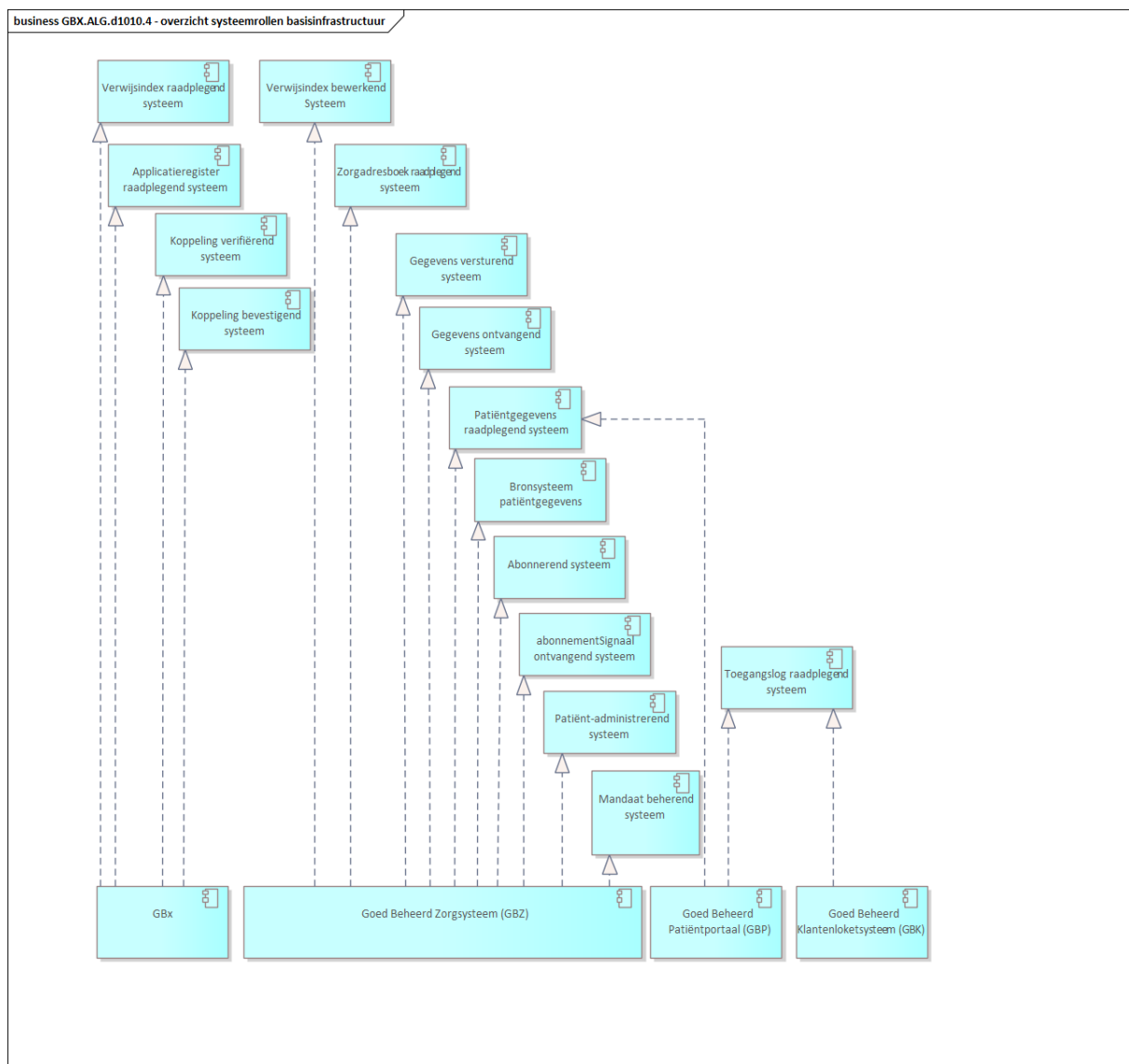


Diagram GBX.ALG.d1010.4 – overzicht systeemrollen basisinfrastructuur AORTA

}

7.8 Berichtafhandeling

In dit hoofdstuk worden de berichtafhandeling en de gerelateerde onderdelen beschreven.

7.8.1 Protocollen

De applicatie-interacties worden gerealiseerd door uitwisseling van berichten tussen de applicaties. Voor uitwisseling van (medische) gegevens wordt binnen AORTA gebruik gemaakt van de internationale HL7v3 en/of HL7 FHIR standaard. Voor het transport van HL7v3 en HL7 FHIR interacties/berichten/documenten over internetprotocollen zijn aanvullende keuzen nodig ten aanzien van transport- en beveiligingsprotocollen.

Voor HL7v3 worden de aanbevelingen gevolgd uit het [WS-I basic profile] en [WS-I basic security profile]. WS-I(nteroperability) basic profile is een richtlijn voor de toepassing van SOAP 1.1 en WSDL 1.1. WS-I basic security profile is een richtlijn voor het toepassen van onder meer de standaarden WS-security, XML-signature en XML-encryption.

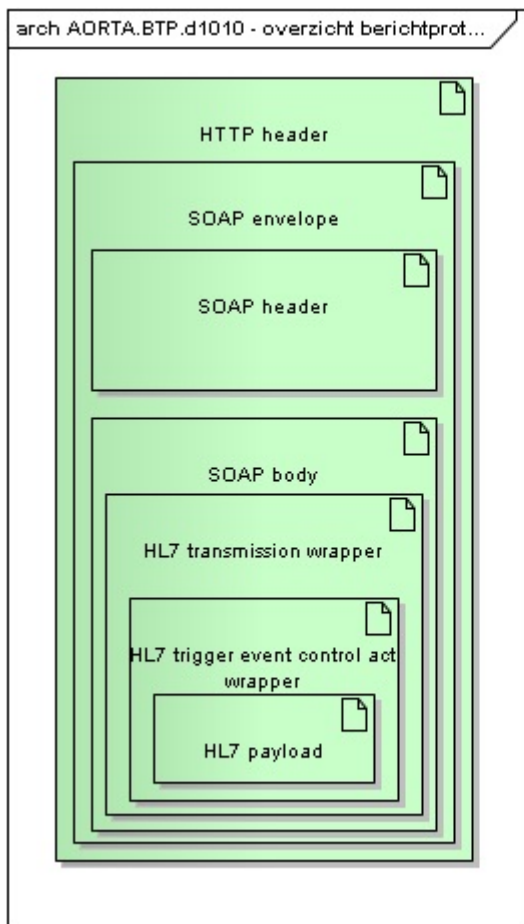


Diagram AORTA.BTP.d1010 - overzicht berichtprotocol-'stack'

Bovenstaand diagram AORTA.BTP.d1010 geeft een overzicht van de protocollen die gebruikt worden voor berichtuitwisseling op de applicatie laag.

Tussen applicatie laag en transport laag (van het TCP/IP model) wordt gebruik gemaakt van Transport Layer Security (TLS).

De HL7 payload is de eigenlijke berichtinhoud en bevat de medische gegevens die tussen de betrokkenen wordt uitgewisseld. De structuur van de medische gegevens is sterk afhankelijk van het soort gegevens dat wordt uitgewisseld. Hiertoe worden binnen HL7v3 verschillende informatiemodellen gebruikt, aangeduid met de term RMIM (Refined Message Information Model) die zijn toegespitst op de medische context van de gegevensuitwisseling. Daarnaast is het ook mogelijk om in de HL7 payload een CDA-document op te nemen.

De HL7v3 Trigger Event Control Act (TECA) wrapper bevat gegevens over de gebeurtenis die aanleiding was het bericht te versturen. Een belangrijk aspect van deze wrapper in het geval van verzoeken is dat deze wrapper aangeeft wie het verzoek heeft verzonden (de 'auteur') en wie verantwoordelijk is voor het zenden van het verzoek (de 'eindverantwoordelijke')^[1]; dit legt de basis voor autorisatie, inclusief mandateringsaspecten. Zie het ontwerp autorisatie [Ontw APT] voor details.

De HL7v3 TECA wrapper en payload worden opgenomen in een HL7v3 transmission wrapper, die gegevens bevat over het berichttransport. Overigens kunnen meerdere HL7v3 transmission wrappers worden gecombineerd in een HL7v3 batch wrapper (niet getoond in het diagram).

Het HL7v3 bericht als geheel bevindt zich in de SOAP-body. Deze bevindt zich samen met de SOAP-header in de SOAP envelope. De SOAP-header bevat instructies over de wijze waarop het bericht moet worden afgehandeld, onder meer op het gebied van beveiliging. De SOAP-envelope als geheel is opgenomen in een HTTP-header.

Bovenstaand diagram AORTA.BTP.d1010 gaat niet in op de gebruikte SOAP-headerprotocollen. Hiervoor wordt verwezen naar de implementatiehandleiding [IH Transport].

Meer gedetailleerde informatie over de protocollen en de samenstelling van HL7-berichten is opgenomen in de implementatiehandleidingen [IH Transport] en [Decor].

^[1] Auteur en eindverantwoordelijke kunnen dezelfde personen zijn.

Voor HL7 FHIR worden de security en privacy aanbevelingen gevolgd uit [HL7 FHIR Security and Privacy] en voor de uitwisseling van informatie de [HL7 FHIR Exchange] richtlijnen bij gebruik van HTTP 1.1 en FHIR Profiles (zie Simplifier.NET). Verder:

- Leveranciers en uitvoerders moeten ervoor zorgen dat ze bekend zijn met OAuth 2.0 threat model en alle beveiligingsoverwegingen, die in [\[RFC-6819⁷⁵\]](https://datatracker.ietf.org/doc/html/rfc6819) worden behandeld.
- Leveranciers en uitvoerders worden aanbevolen op de hoogte te zijn van de laatste OAuth 2.0 best practices die in [\[OAuth2-SBP⁷⁶\]](https://tools.ietf.org/wg/oauth/draft-ietf-oauth-security-topics/) worden behandeld.
- Leveranciers en uitvoerders worden aanbevolen op de hoogte te zijn van de laatste JWT best practices die in [\[RFC-8725⁷⁷\]](https://datatracker.ietf.org/doc/html/rfc8725) worden behandeld.

75. <https://datatracker.ietf.org/doc/html/rfc6819>

76. <https://tools.ietf.org/wg/oauth/draft-ietf-oauth-security-topics/>

77. <https://datatracker.ietf.org/doc/html/rfc8725>

- OpenID Connect 1.0 is een eenvoudige identiteit laag bovenop het OAuth 2.0-protocol. Het stelt klanten in staat om de identiteit van de eindgebruiker te verifiëren op basis van de authenticatie uitgevoerd door een Identity Provider, en om basisprofielinformatie over de eindgebruiker te verkrijgen op een interoperabele en REST-achtige manier. Deze specificatie definieert de kernfunctionaliteit van OpenID Connect: authenticatie bovenop OAuth 2.0 en het gebruik van claims om informatie over de eindgebruiker te communiceren. Het beschrijft ook de veiligheids- en privacyoverwegingen voor het gebruik van [\[OpenID Connect⁷⁸\]](#).
- ICT-beveiligingsrichtlijnen voor webapplicaties (zie Nationaal Cyber Security Centrum)

7.8.2 Foutafhandeling

In de berichtafhandeling zoals beschreven in '[Berichtafhandeling door de ZIM⁷⁹](#)' is aangegeven dat op meerdere momenten in de berichtafhandeling fouten kunnen optreden. Een fout is een gebeurtenis die afwijkt van de verwachte of gewenste wijze van afhandeling van het bericht. Dergelijke fouten worden zoveel mogelijk teruggemeld aan het initiërend systeem.

Indien een bericht de ZIM bereikt (zie diagram AORTA.ZIM.d1050.2), kan een fout plaatsvinden tijdens de berichtvalidatie, de controle van het applicatieregister, de authenticatie of de autorisatie. Deze fouten gaan vooraf aan de inhoudelijke afhandeling van het bericht en leiden tot het staken van de verdere berichtafhandeling. De fout wordt opgenomen in een systeemlog en het initiërend systeem ontvangt een foutmelding, zo mogelijk op HL7v3 niveau.

Indien de ZIM overgaat tot inhoudelijke afhandeling van het bericht, zijn voor de meeste berichten interacties nodig met reagerende systemen (zie diagram AORTA.ZIM.d1060).

Interacties met meerdere reagerende systemen vinden parallel plaats. In deze gevallen ontvangt de ZIM *per reagerend systeem* een resultaat of een foutmelding. Bij fouten in reagerende systemen zet de ZIM de uitwisseling met de andere systemen voort totdat ook de communicatie met deze systemen is afgehandeld. De ZIM combineert de deelresultaten tot een samengesteld antwoord, dat dus voor een deel uit foutmeldingen kan bestaan. Het samengestelde antwoord wordt teruggemeld aan het initiërend systeem. Omdat de uitwisseling met andere systemen parallel verloopt, is in het geval van meerdere foutmeldingen in de reagerende systemen de volgorde van foutmeldingen in het samengestelde antwoord aan het initiërend systeem willekeurig.

Voor de foutafhandeling in situaties waarbij de ZIM optreedt als intermediair tussen initiërend en reagerend systeem gelden de volgende regels:

- Indien de ZIM bij de communicatie met een reagerend systeem een fout ontvangt op HL7-v3-niveau^[1] wordt deze fout opgenomen in het antwoord aan het initiërend systeem.^[2] Ook de fouten die de ZIM zelf intern detecteert worden op HL7-v3-niveau gerapporteerd aan het initiërend systeem.
- Indien de ZIM bij de communicatie met één reagerend GBZ, waarbij sprake is van het versturen van patiëntgegevens, een SOAP fout ontvangt, retourneert de ZIM deze fout eveneens als

78. http://openid.net/specs/openid-connect-core-1_0.html

79. <https://vzvz.atlassian.net/wiki/x/xQIRBQ>

zodanig aan het initiërend systeem. Bij fouten op lager gelegen protocollen interpreteert de ZIM de fout en rapporteert de ZIM deze op HL7-v3-niveau aan het initiërend systeem.

- Indien de ZIM in overige communicatie met reagerende systemen een fout ontvangt op een lager protocolniveau dan HL7-v3 (SOAP, HTTP, TCP/IP) interpreteert de ZIM deze fout en rapporteert de ZIM deze op HL7-v3-niveau aan het initiërend systeem. Hierbij is de ZIM niet verplicht om de details van de oorspronkelijke foutmelding van het reagerend systeem in het bericht op te nemen, tenzij anders aangegeven in de [Foutentabel]. Dit kan namelijk vanuit beveiligingsoogpunt ongewenst zijn.

De [Foutentabel] geeft een lijst van mogelijke foutcondities per berichttype. De [Foutentabel] geeft per foutconditie:

- het type fout;
- de gewenste reactie bij detectie van de fout;
- meldingscode;
- verplichte op te nemen details;
- voorgestelde meldingstekst;
- mogelijke herstelacties.

[1] Er is een lijst van HL7-v3 meldingscodes gedefinieerd die is opgenomen in de foutentabel.

[2] Het initiërend systeem is vrij om de ontvangen meldcode te verrijken met een zelfgekozen tekst voor presentatie aan de eindgebruiker.

7.8.3 Afhandelen van berichtversies

De specificaties van de AORTA-infrastructuur en bijbehorende zorgtoepassingen vallen onder versiebeheerprocedures[1]; met regelmaat worden nieuwe versies gepubliceerd. Door het toevoegen van nieuwe functionaliteit aan AORTA kunnen meerdere versies van een interactietype ontstaan, waarbij verschillen kunnen optreden in de interface-definitie. Omdat aangesloten informatiesystemen een kwalificatietraject moeten doorlopen voor nieuwe AORTA-functies (zie '[Zorginformatiesystemen \(XIS\) en het Goed beheerd zorgsysteem \(GBZ\)](#)⁸⁰⁾'), worden nieuwe berichtversies niet in gelijk tempo door alle aangesloten informatiesystemen geadopteerd.

De ZIM ondersteunt steeds de berichtversies die horen bij twee opeenvolgende versies van een zorgtoepassing. Bij het versturen van patiëntgegevens moet een GBZ rekening houden met de interactieversie die de ontvanger ondersteunt. De interactieversie van de ontvanger kan achterhaald worden door middel van een bevraging van het ZAB.

Details van het omgaan met berichtversies zijn beschreven in het [Ontw OPV], het [Ontw STU] en het [Ontw APR].

80. <https://vzvz.atlassian.net/wiki/x/iQARBQ>

[1] Een beschrijving van deze versiebeheerprocedures valt buiten de reikwijdte van dit architectuurdokument.

7.8.4 Ondersteunen van bouwsteenversies

In AORTA 8 wordt er uitgewisseld op basis van bouwstenen. Binnen AORTA worden diverse bouwstenen gebruikt. Deze bouwstenen kunnen binnen diverse zorgtoepassingen gebruikt worden. Het kan echter zo zijn dat er binnen een bepaalde zorgtoepassing een wijziging in een bouwsteen gewenst is, maar die wijziging is niet (erg) relevant voor andere zorgtoepassingen. Een wijziging in een bouwsteen, betekent dat er een nieuwe versie van de bouwsteen ontstaat.

Om ervoor te zorgen dat er nieuwe versies van bouwstenen geïntroduceerd kunnen worden zonder dat dit impact heeft op andere zorgtoepassingen zijn er binnen AORTA regels omtrent versiebeheer.

Het mechanisme wordt in de paragraaf hieronder toegelicht. In de opvolgende paragrafen worden er voorbeelden gegeven om het mechanisme toe te lichten.

Versiebeheer binnen AORTA is gebaseerd op een stabiele minimum versie(baseline) en een mogelijk van meerdere opvolgende maar niet vereiste opvolgende versies.

Door ervoor te zorgen dat er binnen AORTA voor ieder systeem altijd een minimum versie is waarmee informatie uitgewisseld kan worden, wordt ervoor gezorgd dat er een manier is waarop ieder systeem binnen AORTA informatie kan uitwisselen. Daarnaast bestaat er een mogelijkheid om nieuwe en opvolgende versies te definiëren. In deze nieuwe versies kunnen zaken zijn toegevoegd die gewenst zijn binnen een bepaalde toepassing. Het is echter zo dat niet alle zaken zomaar ketenbreed uitgerold kunnen worden. Vandaar dat er een mogelijkheid is toegevoegd zodat zorgaanbieders informatie kunnen uitwisselen zonder dat daarvoor iedere partij binnen AORTA dit moet kunnen ondersteunen.

Het versiebeheer wordt zo toegepast, dat versies die in productie zijn niet te veel en te vaak veranderen om te voorkomen dat leveranciers van bronsystemen vaak aanpassingen moeten maken om nieuwe versies van bouwstenen te ondersteunen.

Binnen tests of POC's is het juist wel gewenst om wijzigingen in bouwstenen te kunnen testen en wil je juist flexibel zijn met wijzigingen.

Om een mechanisme te creëren dat juist stabiel is in productie en flexibel in andere omgevingen, zijn er naast technische eisen ook procedurele eisen nodig en is er een mechanisme nodig dat meerdere versies van een bouwsteen ondersteund. Om dit te kunnen faciliteren stelt VZVZ voor om gebruik te maken van baselines.

Baselines zijn versies die in de loop der tijd ontstaan en waarvan we gezamenlijk binnen de infrastructuur afspreken dat deze erg belangrijk zijn en dat die specifieke versie van een bouwsteen-type altijd opgeleverd moet kunnen worden. Het gaat hier om een in de gehele keten geïmplementeerde versie van een bouwsteen/type. Naast de baseline kan een leverancier meerdere andere versies ondersteunen afhankelijk van de programma's en POC's waarin wordt deelgenomen.

De functie van een baseline is om één versie van een bouwsteen/type te definiëren dat ieder systeem minimaal ondersteund. Op deze manier kan je er altijd op vertrouwen dat er met een systeem gecommuniceerd kan worden.

Een baseline is een versie van een bouwsteen die volgens een werkplan afspraak altijd minimaal ondersteund moet worden. Dit is dus een minimale versie die op basis van afspraken wordt geëist.

Een baseline is echter een versie waarvan we afspreken dat iedereen deze moet kunnen uitwisselen. Het is praktisch als de versies die daarna worden gepubliceerd backwards compatible zijn met deze baseline versie, want dan kan ook de nieuwe versie worden verstuurd terwijl deze ook nog door oude systemen kunnen worden verwerkt. Dit is echter geen eis bij het vaststellen van de baseline.

Systemen zijn daarnaast vrij om bouwsteen versies te implementeren die (ver) vooruitlopen op de baseline versie van de bouwsteen-types. Zij kunnen deze nieuwe versies ook uitwisselen met systemen die deze nieuwe versies al ondersteunen. Wil er echter een systeem zonder de ondersteuning van de laatste versie van een bouwsteen communiceren met systemen die al een veel nieuwere versie ondersteund? Dan kan er altijd worden teruggevallen op de baseline versie.

Vanwege de ontwikkelingen die in de versies van de bouwsteen-types uit de verschillende programma's plaats vinden, kan het wenselijk zijn om een nieuwe baseline vast te stellen. Er is dan een nieuwe (minimale) invulling van een bouwsteentype gewenst in de hele keten. Om deze overgang te kunnen faciliteren, zal er een situatie ontstaan waarin de bestaande baseline en de beoogde nieuwe baseline ondersteund dient te worden door de bronsystemen. Ieder bronsysteem kan in eigen tempo, maar voor een bepaalde deadline, de nieuwe beoogde baseline implementeren en uitrollen. In deze situatie dienen er twee versies ondersteund te worden. Op het moment dat alle bronsystemen zijn uitgerold met ondersteuning voor de nieuwe beoogde baseline, zal deze beoogde baseline de nieuwe baseline worden en kan de eerdere baseline in de gehele keten worden uitgefaseerd.

Om het versiebeheermechanisme toe te lichten zijn hieronder een aantal voorbeeld situaties geschetst.

Voorbeeld 1: 2 Systemen met een hoge mutatiegraad

In dit voorbeeld zijn er 2 systemen met een hoge mutatiegraad, systeem H1 en H2, die allebei snel ondersteuning van de nieuwe publicaties inbouwen. De baseline is in dit voorbeeld in het werkplan vastgesteld op versie 1.0 van de medicatieafpraak. Er bestaat nog geen nieuwe beoogde baseline van de medicatie afspraak bouwsteen.

In de nieuwste Medicatieproces publicatie wordt echter versie 2.4 al gebruikt.

Wanneer systeem H1 en H2 beide ondersteuning voor versie 2.4 inbouwen, dan kunnen zij onderling al versie 2.4 uitwisselen. Versie 2.4 is backwards compatibel met 2.1, 2.2 en 2.3 dus alle systemen die versie 2.x ondersteunen kunnen een 2.x uitwisselen.

Daarnaast dienen systeem H1 en H2 versie 1.0 van de medicatieafpraak nog te ondersteunen, omdat dit nog de bestaande baseline is.

In dit voorbeeld implementeren systemen H1 en H2 beide versie 1.0 en 2.4.

Voorbeeld 2: Systeem met een lage mutatiegraad

In dit voorbeeld is er een extra systeem tov voorbeeld 1, systeem L1. L1 is een systeem dat nog niet de laatste versie(2.4) heeft ingebouwd voor Medicatieproces vanwege andere prioriteiten en wordt geclassificeerd als een systeem met een lage mutatiegraad. Volgens de afspraken binnen het werkplan moeten alle systemen die medicatieafspraken uitwisselen wel de baseline ondersteunen. De baseline versie is 1.0. Daarom zal systeem L1 minimaal versie 1.0 geïmplementeerd moeten hebben.

Voorbeeld 3: Systeem met een matige mutatiegraad

In dit voorbeeld is er nog een systeem, systeem M1. Systeem M1 is sneller met ontwikkelen dan systeem L1, maar niet zo snel als systeem H1 en H2. Systeem M1 heeft de vereiste baseline versie van medicatieafspraken ingebouwd, versie 1.0. Daarnaast ondersteund dit systeem ook al versie 2.1. Dit is niet de laatste versie van de medicatieafpraak, maar een redelijk recente versie. Het systeem wordt daarom geclassificeerd als een systeem met een matige mutatiegraad.

Voorbeeld 4: Verandering van baseline

In voorbeeld 4 treedt er een verandering op. Er wordt nu namelijk bepaald in het werkplan dat er over moet worden gegaan naar een nieuwe baseline voor medicatieafspraken. Het plan is om versie 2.1 de baseline van medicatieafspraken te maken.

Er wordt afgesproken dat alle systemen die medicatieafspraken uitwisselen vanaf 1 oktober 2019 ook versie 2.1 moeten kunnen uitwisselen. Als alle systemen vanaf 1 oktober 2019 de beoogde baseline ondersteunen, kan dit de nieuwe baseline worden en kan er worden besloten om versie 1.0 als baseline te verwijderen. Alle partijen kunnen nu nog succesvol met elkaar communiceren, iedereen heeft namelijk versie 2.1 ingebouwd. Versie 1.0 wordt niet meer ondersteund en uitwisseling ervan wordt op het LSP gedeactiveerd. Vervolgens kan er in het werkplan een nieuwe afspraak worden gemaakt voor een nieuwe baseline.

Voor de verandering van baseline van versie 1.0 naar 2.1, zal alleen het systeem met een lage mutatiegraad, L1 uit het voorbeeld hierboven, extra moeite in de ontwikkeling van de medicatieafpraak bouwsteen moeten steken. De systemen met een matige en hoge mutatiegraad (H1, H2 en M1) moeten door de ophoging van de baseline geen extra energie in het ondersteunen van de nieuwe baseline besteden aangezien zij al versie 2.1 ondersteunen.

Voorbeeld 5: Doorontwikkeling bij systemen met een hoge mutatiegraad

In de tijd tussen nu en 1 oktober 2019 zou er ook een nieuwe medicatieproces publicatie kunnen komen waarin een nieuwe versie van medicatieafspraken, versie 3.0, wordt gepubliceerd. De systemen H1 en H2 met een hoge mutatiegraad zouden deze versie in de tussentijd ook willen gaan ondersteunen. Als zij dit ondersteunen, dan kunnen ze deze onderling uitwisselen zoals geschetst in voorbeeld 1.

Om ook nog met systemen met een matige en lage mutatiegraad te kunnen uitwisselen dienen de systemen H1 en H2 nog wel de op dat moment bestaande baseline en mogelijk beoogde baseline te ondersteunen.

Voorbeeld 6: Gebruik maken van de bouwsteen binnen een POC

Binnen een POC van eSpoed wordt een nieuwe versie van de medicatieafpraak getest. Dit wordt versie 3.1 van de medicatieafpraak.

Versie 3.1 kan geen baseline worden zolang deze alleen wordt gebruikt binnen de POC. Versie 3.1 wordt nu alleen ingebouwd door de leveranciers die meedoen met de POC. Het invoeren van deze versie heeft geen impact op wat er in productie wordt uitgewisseld.

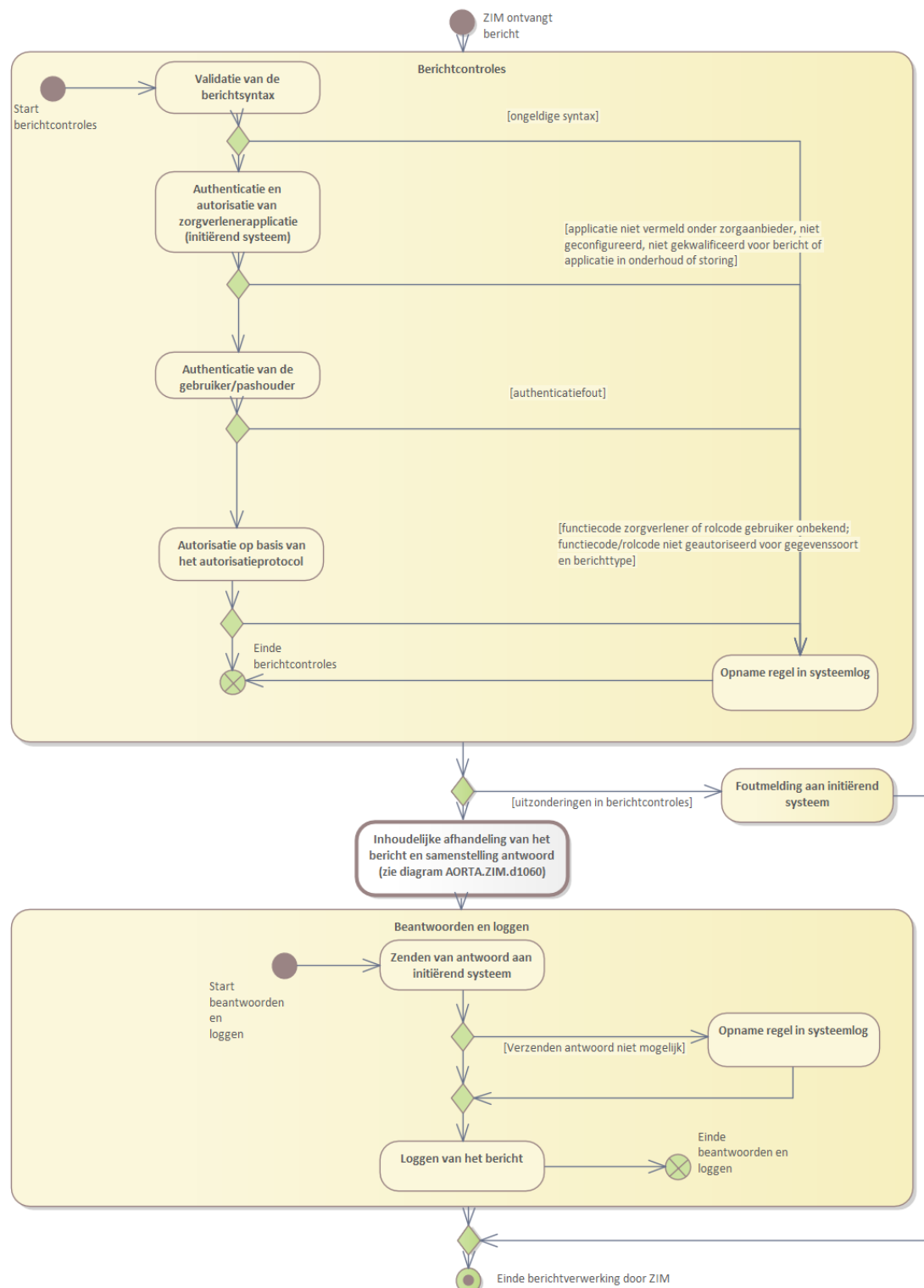
Eisen aan systemen

Om het bovenstaande versiebeheermechanisme succesvol te laten werken binnen AORTA zijn er eisen gedefinieerd waaraan GBX'en zich dienen te houden. Deze eisen zijn uitgewerkt in [PvE Infra Systeemrollen].

7.8.5 Berichtafhandeling door de ZIM

Bij het afhandelen van de berichten afkomstig van aangesloten GBx'en door de ZIM wordt een vast patroon gevolgd waarbij verschillende componenten binnen de ZIM betrokken zijn. Dit patroon is weergegeven in diagram AORTA.ZIM.d1050.3

act AORTA.ZIM.d1050.3 - standaard berichtafhandeling door ZIM



Het GBx dat de berichtuitwisseling initieert met een bericht naar de ZIM wordt in deze beschrijving aangemerkt als 'initieërend systeem'.

Een (eventueel) systeem dat tijdens de berichtafhandeling door de ZIM wordt geraadpleegd, wordt in deze beschrijving aangemerkt als 'reagerend systeem'.

7.8.5.1 Validatie van de berichtsyntax

De ZIM controleert (een gedeelte van) het bericht op geldigheid ten opzichte van XML schema's^[1]. Indien het ontvangen bericht syntactisch ongeldig is, retourneert de ZIM een foutmelding en breekt de afhandeling af. Berichten bestemd voor volledige afhandeling binnen de ZIM, worden geheel gevalideerd. Berichten die door de ZIM worden doorgestuurd naar een reagerend GBZ worden alleen gevalideerd voor zover nodig voor de verdere berichtverwerking; deze validatie strekt zich niet uit tot de HL7-payload (zie 'Protocollen'⁸¹) van het bericht.

7.8.5.2 Authenticatie en autorisatie van de zorgverlener applicatie

De ZIM controleert dat het applicatie-id, genoemd als afzender van het bericht, in het applicatieregister is geregistreerd onder de organisatie die opgenomen is in servercertificaat^[2]. Indien dit niet het geval is of indien de applicatie volgens het applicatieregister niet gekwalificeerd of geconfigureerd is voor het interactie-id, retourneert de ZIM een foutmelding en breekt de afhandeling af.

Indien de applicatie een status 'onderhoud' of 'storing' heeft in het applicatieregister, retourneert de ZIM een foutmelding, breekt de afhandeling af en neemt een gebeurtenis op in het systeemlog.^[3]

[1] Deze schema's zijn gebaseerd op normatieve beschrijvingen in implementatiehandleidingen.

[2] Voor een GBZ wordt deze organisatie afgeleid uit het UZI-abonneenummer op het servercertificaat van het GBZ waarmee de TLS-verbinding tot stand kwam, voor een GBP, GBK of een niet UZI-abonnee (GBO) de organisatie genoemd op het PKIO-servercertificaat.

[3] Berichten met betrekking tot het applicatieregister en de VWI-synchronisatiefunctie zijn hierop een uitzondering.

7.8.5.3 Authenticatie van de gebruiker / pashouder

Bij uitwisseling van gegevens met of via de ZIM moet de authenticiteit van de gebruiker of de verantwoordelijke voor de gegevensuitwisseling met voldoende waarborg worden vastgesteld. Hiertoe heeft de gebruiker een vertrouwensmiddel aan de hand waarvan de gebruiker kan worden geauthentiseerd (zie 'Basisregistraties en vertrouwensmiddelen'⁸²). Een zorgverlener maakt hiertoe gebruik van een UZI-pas, ZORG-ID Smartcard of ZORG-ID Mobile App. Een klantenloketmedewerker maakt gebruik van een PKI-overheidpas. De patiënt kan zich authenticeren door middel van DigiD.

81. <https://vzvz.atlassian.net/wiki/x/TAMRBQ>

82. <https://vzvz.atlassian.net/wiki/x/YQARBQ>

act AORTA.ZIM.d1050.3 - standaard berichtafhandeling door ZIM

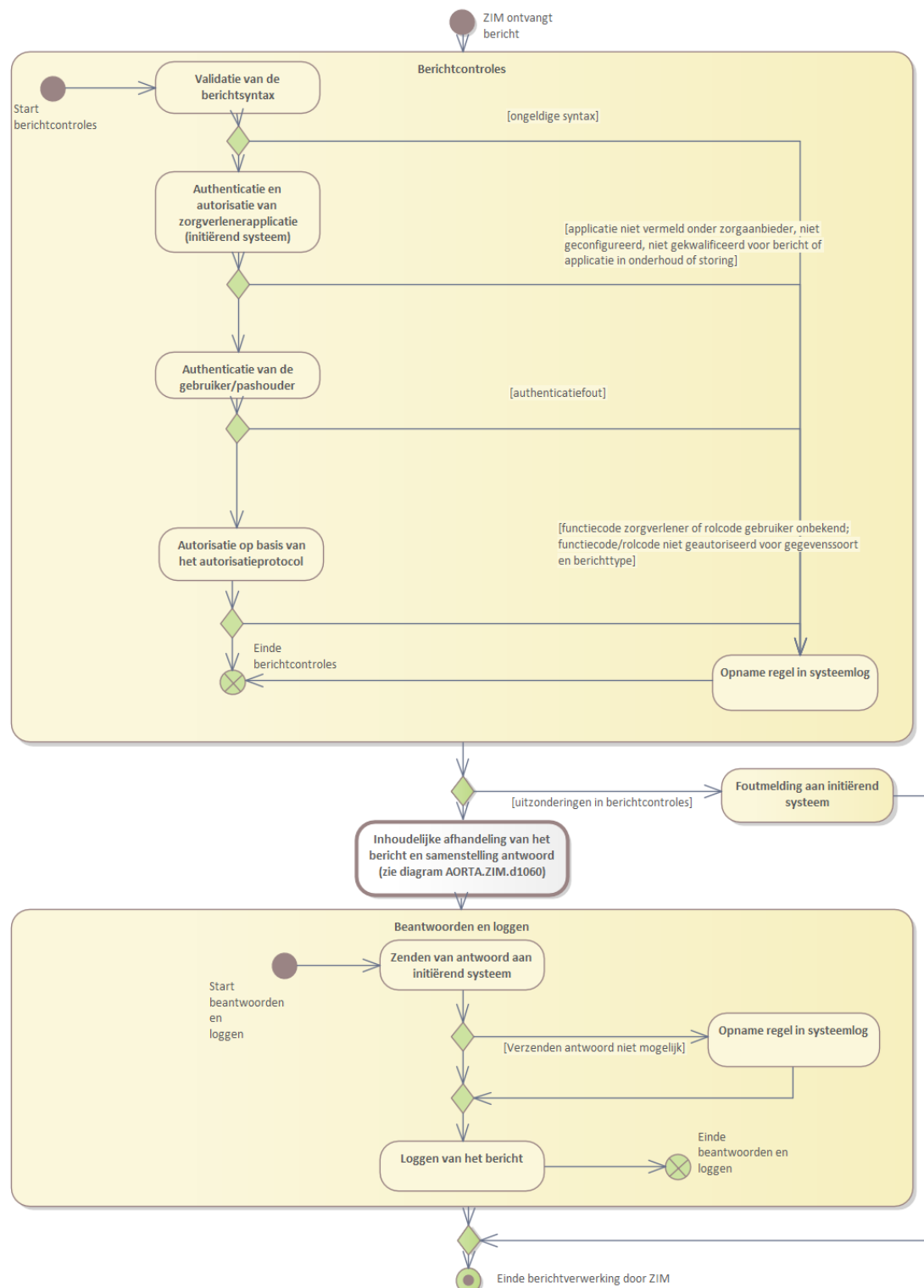


Diagram AORTA.ZIM.d1050.2 - standaard berichtafhandeling door de ZIM

Bij tokenauthenticatie komt een TLS-verbinding tot stand tussen GBx en ZIM op basis van het servercertificaat van het GBx en het servercertificaat van de ZIM. Op basis van het servercertificaat van het GBx wordt vastgesteld vanuit welke organisatie de berichtuitwisseling is geïnitieerd.

Daarnaast kunnen ten behoeve van de authenticatie en autorisatie van de gebruiker in het bericht meerdere tokens worden opgenomen:

- **Transactietoken (T):**
Dit token is gekoppeld aan een uniek bericht en bevat informatie zoals de *interactionId* en *messageId*, waardoor het bericht onlosmakelijk verbonden is met het token. Het transactietoken wordt ondertekend door een servercertificaat van het versturende systeem of, indien van toepassing, door het persoonlijke UZI-certificaat van de gebruiker of het authenticiteitscertificaat op de ZORG-ID Smartcard of ZORG-ID Mobile App. Dit token waarborgt de integriteit van het bericht en biedt een beveiligingslaag tegen hergebruik. Zie [IH TRANS] voor een volledige beschrijving en afhandeling van het transactietoken.
- **PKIO-token (P):**
Dit token dient voor de authenticatie van een specifieke gebruiker in het kader van een unieke interactie. Het wordt ondertekend met het persoonlijke PKIO-certificaat van de gebruiker, wat de betrouwbaarheid en traceerbaarheid van de handeling garandeert. Zie [IH PKIO] voor een volledige beschrijving en afhandeling van het PKIO-token.
- **Mandaattoken (M):**
Dit token draagt autorisaties over van een mandaterende partij naar een gemandateerde partij. Het mandaattoken bevat specifieke afspraken over de acties die de gemandateerde partij mag uitvoeren, zoals toegang tot patiëntgegevens of andere zorggerelateerde taken. Het token is essentieel voor het aantonen van de gedelegeerde autorisatie en wordt gegenereerd door het systeem van de mandaterende partij. Zie [IH MAN] voor een volledige beschrijving en afhandeling van het mandaattoken.
- **Inschrijftoken (I):**
Dit token wordt gebruikt om een patiënt te koppelen aan een behandelende organisatie. Het inschrijftoken fungeert als een bewijs dat de patiënt is geïdentificeerd en de inschrijving is uitgevoerd door een geauthentiseerde zorgverlener. Dit token is een essentieel onderdeel van de registratie van patiënten binnen zorgprocessen. Zie [IH INSCHRIJF] voor een volledige beschrijving en afhandeling van het inschrijftoken.

Het gebruik en voorkomen van een token is afhankelijk van meerdere factoren, waaronder het vertrouwensniveau dat vereist is voor een berichtuitwisseling, de aanwezigheid van een mandaat, en het specifieke uitwisselingsmechanisme dat wordt toegepast. In **Tabel 1** worden de verschillende combinaties van tokens en uitwisselingsmechanismen gedetailleerd beschreven.

Bij het uitwisselen van berichten met de ZIM zijn twee vertrouwensniveaus gedefinieerd: **'laag'** en **'midden'**. Het vereiste vertrouwensniveau wordt bepaald op basis van het type bericht en de gevoeligheid van de gegevens die worden uitgewisseld.

- **Niveau 'laag':**
Dit niveau richt zich uitsluitend op het vaststellen van de herkomstorganisatie van de afzender, zonder authenticatie van een specifieke gebruiker. De identiteit van de gebruiker is in dit geval niet relevant. De afzenderorganisatie wordt vastgesteld op basis van het servercertificaat

(bijvoorbeeld GBx-certificaat). Er is geen vereiste voor een persoonlijke pas of aanvullende tokens. Dit niveau is geschikt voor berichten waarbij geen persoonlijke of medisch inhoudelijke gegevens worden verwerkt.

- **Niveau ‘midden’:**

Dit niveau vereist een hogere mate van zekerheid door de authenticatie van de individuele afzender (zorgmedewerker of zorgverlener). Voor dit vertrouwensniveau is een persoonlijke token(s) verplicht in het bericht, afhankelijk van de situatie zoals beschreven in **Tabel 1**. Dit niveau is minimaal vereist voor berichten die medisch inhoudelijke gegevens bevatten of waarbij de afzender direct verantwoordelijk is voor de inhoud en de actie. Het gebruik van een persoonlijke UZI-pas is noodzakelijk om de identiteit van de gebruiker te waarborgen.

Zie voor een verdere discussie van dit aspect het [Ontw Authenticatie].

Tabel 1: Gebruik van de diverse tokens

Uitwisseling	Vertrouwensniveau	Uitwisseling onder mandaat	Tokens (T, P, M, I)
Generieke opvraag/ Versturen berichten/ Infrastructurele berichten	Laag		
Generieke opvraag/ Versturen berichten/ Infrastructurele berichten	Midden (of hoger)		T of P
Generieke opvraag/ Versturen berichten/ Infrastructurele berichten	Midden (of hoger)	X	T
Conditionele opvraag/ Conditioneel versturen/ Conditionele infrastructurale berichten	Midden ^[1]	X	T en I

Het vereiste vertrouwensniveau bepaalt de mate van authenticatie en de noodzaak voor specifieke tokens. Niveau ‘laag’ vereist geen persoonlijke authenticatie en kan volstaan met organisatievalidatie via servercertificaten. Niveau ‘midden’ vereist daarentegen de authenticatie van individuele gebruikers en stelt specifieke eisen aan de aanwezigheid van tokens zoals het PKIO-token en, indien relevant, het mandaattoken.

Voor tokens die zijn getekend met een persoonlijke UZI-pas, PKIO-pas of ZORG-ID Smartcard van de gebruiker geldt dat de authenticatie van de gebruiker geheel los staat van het certificaat dat is gebruikt voor de opbouw van de sessie tussen GBx en ZIM.^[2]

Sessie-authenticatie (het tot stand brengen van een TLS-verbinding tussen GBx en ZIM op basis van het certificaat van een persoonlijke UZI- of PKIO- pas of ZORG-ID Smartcard ^[3] en het servercertificaat van de ZIM) wordt niet ondersteund.

7.8.5.4 Autorisatie op basis van het autorisatieprotocol

Het autorisatieprotocol controleert of de zorgverlenerfunctie (op basis van rolcode) is geautoriseerd voor de combinatie van de gegevenssoort of context en de specifieke interactie tussen GBx en ZIM. In het geval er geen sprake is van een gegevenssoort of context in het bericht, wordt alleen gekeken of de zorgverlener functie geautoriseerd is voor het verzenden van een specifieke interactie.

In het geval van patiënttoegang of toegang van een klantenloketmedewerker wordt de combinatie van interactie en rolcodes gecontroleerd.

Zie voor een verdere discussie van autorisatie op basis van het autorisatieprotocol het [Ontw APT].

7.8.5.5 Inhoudelijke verwerking van het bericht

De acties die nodig zijn voor de inhoudelijke verwerking van het bericht door de ZIM zijn afhankelijk van het type bericht. Enkele aspecten hiervan zijn echter generiek; deze zijn weergegeven in diagram AORTA.ZIM.d1060.

Inhoudelijke afhandeling binnen de ZIM

Een deel van de berichttypen kan door de ZIM zelf inhoudelijk worden afgehandeld (bijvoorbeeld het aanmaken van een nieuwe verwijzing in de verwijsindex). De ZIM kan dan direct het antwoordbericht opstellen (waarin eventuele foutmeldingen kunnen worden opgenomen).

ZIM stuurt berichten naar ander systeem

Voor de overige berichten zijn interacties nodig met één of meer reagerende systemen (meestal GBZ'en). De manier waarop wordt bepaald welke reagerende systemen dit zijn is afhankelijk van het scenario (bijvoorbeeld gegevens opvragen versus gegevens sturen).

In verband met het minimaliseren van de tijd nodig voor beantwoording moeten meerdere reagerende systemen parallel kunnen worden benaderd. Voor elk reagerend systeem worden globaal dezelfde stappen doorlopen:

- De ZIM raadpleegt het applicatieregister om te controleren of het reagerende systeem is gekwalificeerd voor het onderhanden berichttype en om te controleren of het systeem actief is (en niet in onderhoud of storing).
- De ZIM bouwt een TLS-sessie op met het reagerende systeem op basis van wederzijdse authenticatie met behulp van servercertificaten.
- De ZIM gaat een berichtuitwisseling aan met het reagerend systeem. Zie voor details de deelontwerpen [Ontw OPV] en [Ontw STU]).
- De ZIM verwerkt het resultaat van de berichtuitwisseling tot een partieel antwoordbericht.

Bij het raadplegen van elk reagerend systeem kunnen zich problemen voordoen: indien de uitslag van de controle van het applicatieregister negatief is, geen sessie kan worden opgebouwd of zich een fout voordoet bij de berichtuitwisseling met het reagerend systeem, neemt de ZIM een regel op in het systeemlog en stelt een partieel antwoord samen waarin een foutmelding wordt opgenomen.

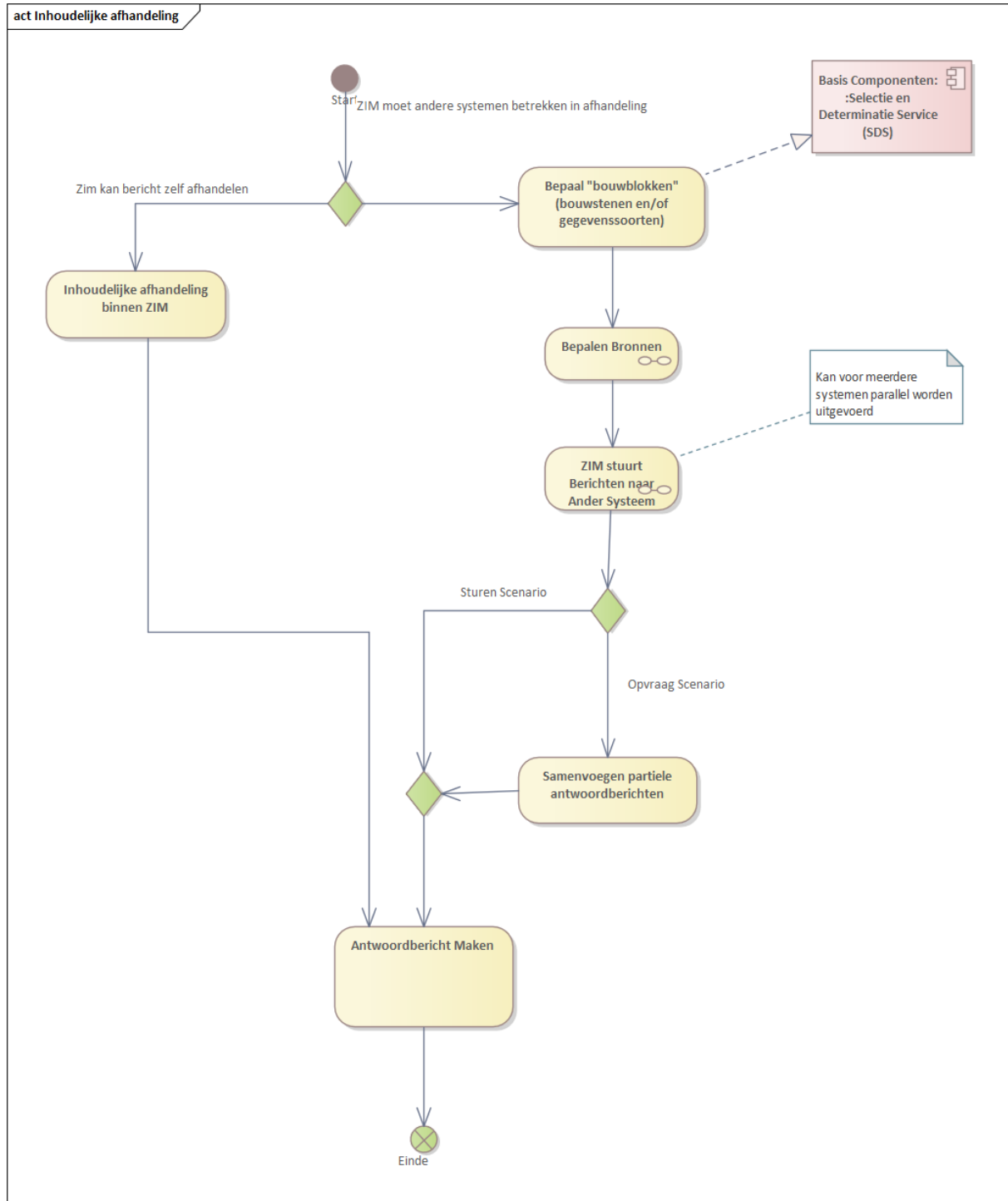


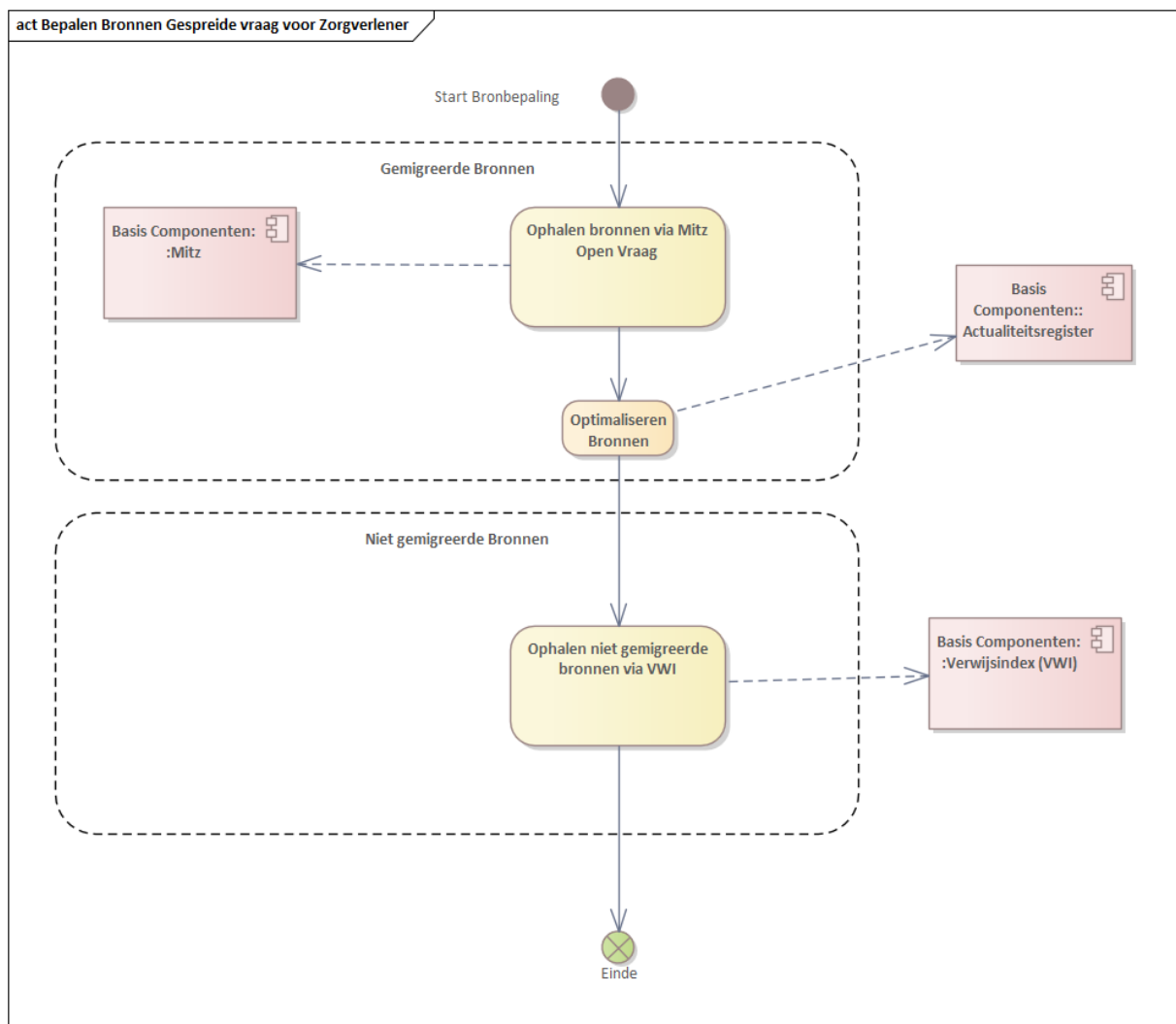
Diagram AORTA.ZIM.d1060 - generieke aspecten van inhoudelijke afhandeling bericht door ZIM

In het geval dat sprake is van 'opvragen van patiëntgegevens' moeten de antwoorden van de verschillende reagerende systemen worden gecombineerd tot één samengesteld ('batch')-antwoord aan het initiërende systeem (ook indien in werkelijkheid slechts één systeem is benaderd wordt de berichtstructuur van een samengesteld antwoord gebruikt). In het geval van 'sturen van patiëntgegevens', waarbij nooit meer dan één reagerend systeem betrokken is, hoeft geen samengesteld antwoord gemaakt te worden.

Na de inhoudelijke afhandeling (hetzij volledig door de ZIM of in samenwerking met reagerende systemen) wordt het uiteindelijke antwoord aan het initiërend systeem gestuurd (zie diagram AORTA.ZIM.d1050.2).

7.8.5.6 Bepaal bronnen

Voor het LSP iets kan opvragen, moet het eerste weten wat en waar het opgehaald moet worden. Het opvragingstype bepaalt hoe dat gebeurt.



Figuur 1 Diagram AORTA.ZIM.d1063a Bepalen Bronnen Gespreide vraag voor Zorgverlener

7.8.5.6.1 Bepalen Bronnen Gespreide vraag voor Zorgverlener

Zolang nog niet alle systemen gemigreerd zijn naar Mitz, zullen er twee sporen zijn waarop de bronnen bepaald moeten worden. Deze sporen zijn onafhankelijk van elkaar, maar zijn in het figuur na elkaar getekend.

Gemigreerde bronnen

In het eerste spoor worden bij Mitz via een **open vraag** de bronnen bepaald waar de opvragende zorgverlener de gegevens van de patiënt kan ophalen.

Omdat de rubrieken bij Mitz breder zijn dan bij het LSP, worden in de volgende actie de bronnen geoptimaliseerd. Optimalisatie vindt plaats door in de AR te kijken welke bronnen de bouwstenen/gegevenssoorten hebben zoals bepaald door de SDS.

Niet Gemigreerde bronnen

In de andere tak wordt de VWI bevraagd om alle **niet gemigreerde** bronnen op te leveren waar er gegevens staan voor deze patiënt (alleen de bouwstenen en gegevenssoort zoals bepaald door de SDS).

Deze twee stromen kunnen nu samenkomen om de bronnen te bevragen en de afhandeling op een eenduidige manier verder af te werken.

7.8.5.6.2 Bepalen Bron Gerichte vraag voor Zorgverlener

In dit opvragingstype is de bron al bekend, en moet er alleen gekeken worden of er toestemming is voor het ophalen.

Ook hier moet weer onderscheid worden gemaakt tussen gemigreerde bronnen en niet gemigreerde bronnen.

Als eerste wordt er bepaald of de bron al gemigreerd is.

Gemigreerde bron

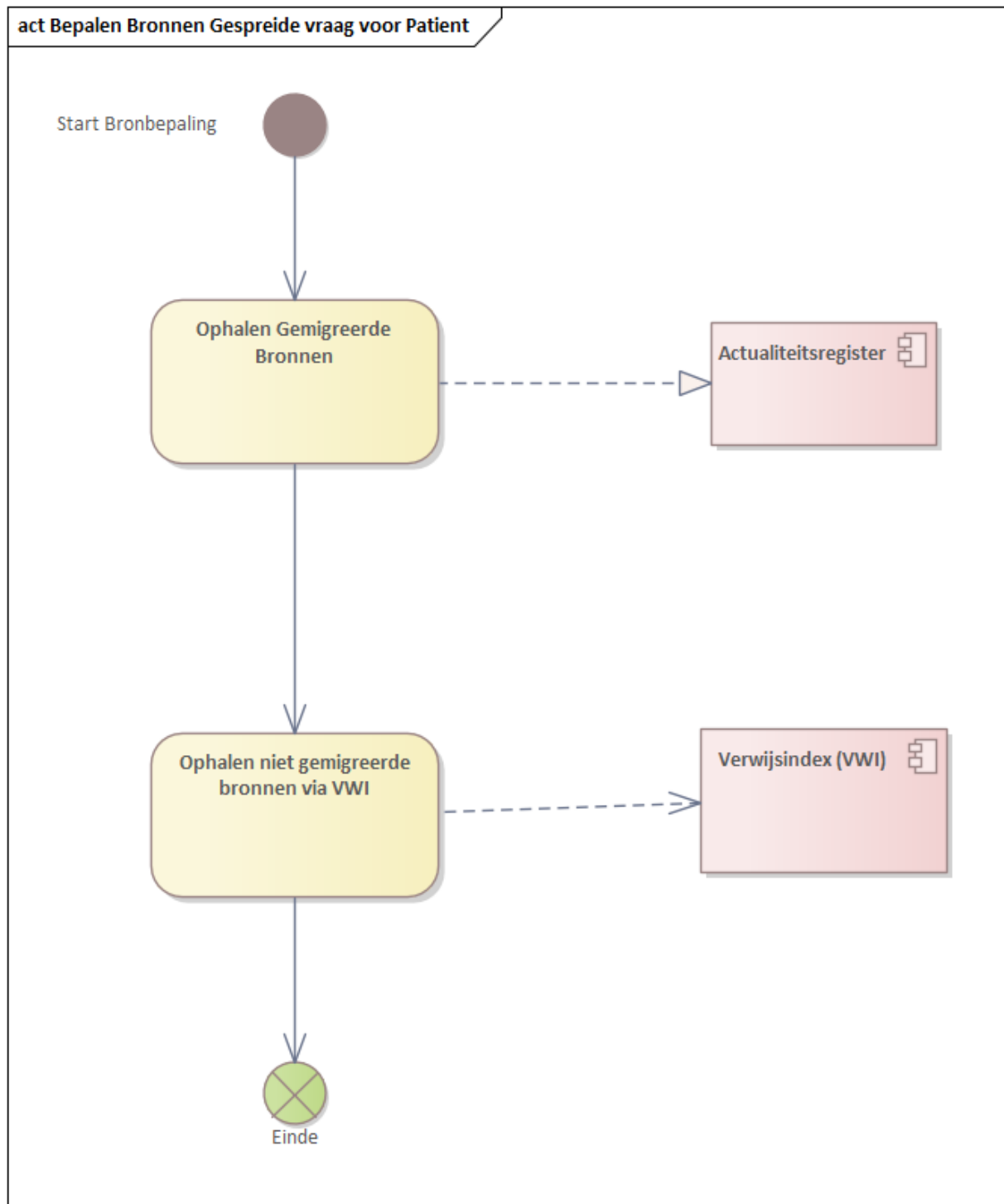
Bij een gemigreerde bron, wordt er via een **gesloten vraag** bij Mitz gekeken of er wel toestemming is om de gegevens op te halen.

Daarna wordt er in het AR gekeken of er wel gegeven zijn om op te halen.

Niet Gemigreerde bron

Bij een niet gemigreerde bron, moet er worden gekeken in de VWI of er wel toestemming is gegeven voor uitwisseling en voor welke bouwstenen/gegevenssoorten.

7.8.5.6.3 Bepalen Bronnen Gespreide vraag voor Patiënt

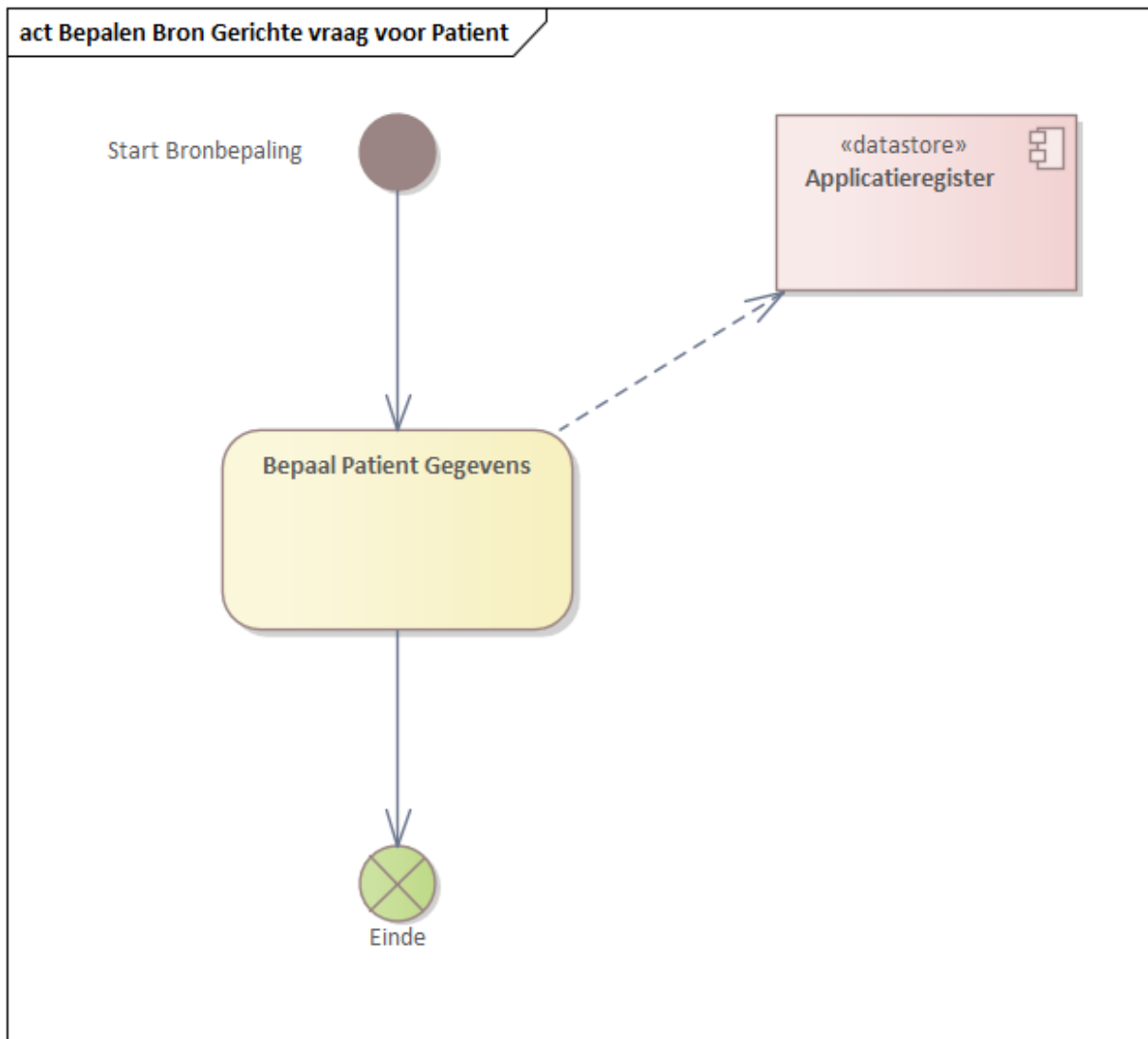


Figuur 3 Diagram AORTA.ZIM.d1063c Bepalen Bronnen Gespreide vraag voor Patiënt

Gemigreerde en niet gemigreerde bron

In het VWI wordt er gekeken welke bronnen er gegevens hebben voor deze patiënt. Al deze bronnen mogen bevraagd worden.

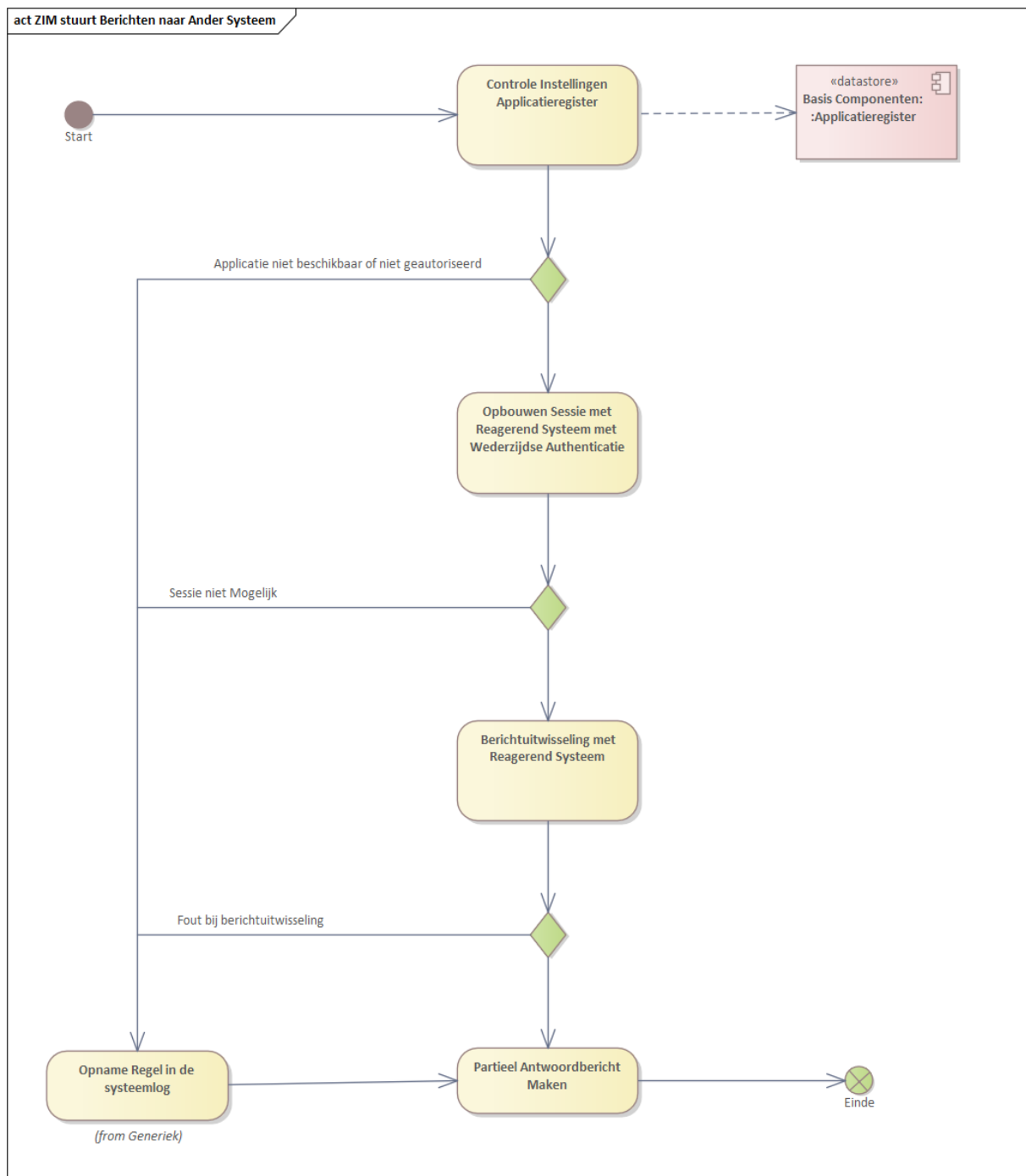
7.8.5.6.4 Bepalen Bron Gerichte vraag voor Patiënt



Figuur 4 Diagram AORTA.ZIM.d1063d Bepalen Bron Gerichte vraag voor Patiënt

Bij een gerichte vraag door patiënten moet alleen de vraag worden geoptimaliseerd (eigenlijk alleen kijken of de zorgaanbieder de opgevraagde data wel kan opleveren). Deze optimalisatie gebeurt door het checken van de systeemrol van de bronapplicatie.

7.8.5.7 ZIM stuurt berichten naar ander systeem



Figuur 5 Diagram AORTA.ZIM.d1066 ZIM stuurt berichten naar ander systeem

Voor de overige berichten zijn interacties nodig met één of meer reagerende systemen (meestal GBZ'en). De manier waarop wordt bepaald welke reagerende systemen dit zijn is afhankelijk van het scenario (bijvoorbeeld gegevens opvragen versus gegevens sturen (dat kan **niet** naar meerdere systemen)).

In verband met het minimaliseren van de tijd nodig voor beantwoording moeten meerdere reagerende systemen parallel kunnen worden benaderd. Voor elk reagerend systeem worden globaal dezelfde stappen doorlopen:

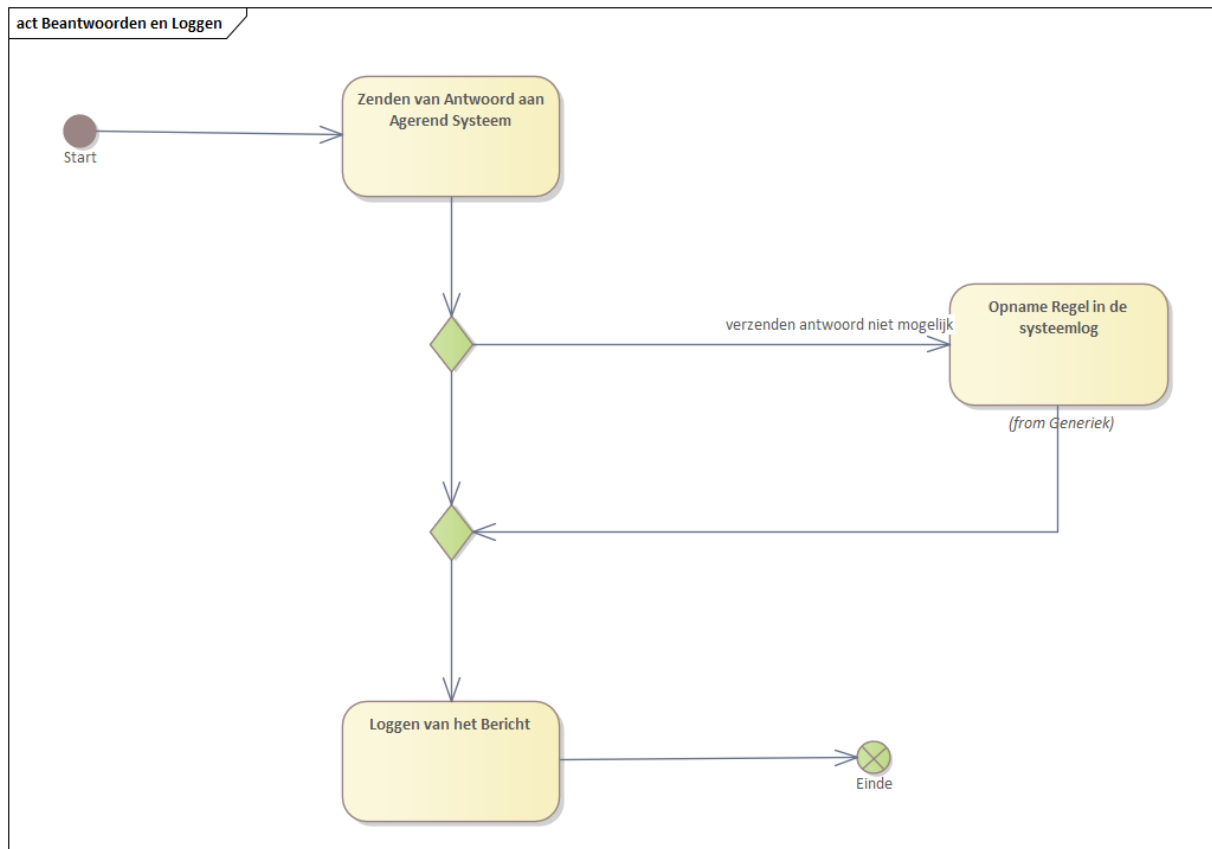
- De ZIM raadpleegt het applicatieregister om te controleren of het reagerende systeem is gekwalificeerd voor het onderhanden berichttype en om te controleren of het systeem actief is (en niet in onderhoud of storing).
- De ZIM bouwt een TLS-sessie op met het reagerende systeem op basis van wederzijdse authenticatie met behulp van servercertificaten.
- De ZIM gaat een berichtuitwisseling aan met het reagerend systeem).
- De ZIM verwerkt het resultaat van de berichtuitwisseling tot een partieel antwoordbericht.

Bij het raadplegen van elk reagerend systeem kunnen zich problemen voordoen: indien de uitslag van de controle van het applicatieregister negatief is, geen sessie kan worden opgebouwd of zich een fout voordoet bij de berichtuitwisseling met het reagerend systeem, neemt de ZIM een regel op in het systeemlog en stelt een partieel antwoord samen waarin een foutmelding wordt opgenomen.

In het geval dat sprake is van 'opvragen van patiëntgegevens' moeten de antwoorden van de verschillende reagerende systemen worden gecombineerd tot één samengesteld ('batch')-antwoord aan het initiërende systeem (ook indien in werkelijkheid slechts één systeem is benaderd wordt de berichtstructuur van een samengesteld antwoord gebruikt). In het geval van 'sturen van patiëntgegevens', waarbij nooit meer dan één reagerend systeem betrokken is, hoeft geen samengesteld antwoord gemaakt te worden.

Na de inhoudelijke afhandeling (hetzij volledig door de ZIM of in samenwerking met reagerende systemen) wordt het uiteindelijke antwoord aan het initiërend systeem gestuurd (zie diagram AORTA.ZIM.d1070).

7.8.5.8 Loggen van het bericht



Figuur 6 AORTA.ZIM.d1070 Antwoord bericht versturen en bericht loggen

Indien een inhoudelijke berichtverwerking heeft plaatsgevonden wordt een regel opgenomen in de toegangslog zodat alle toegang tot inhoudelijke gegevens traceerbaar is.

Er wordt een regel weggeschreven in de toegangslog indien de afhandeling niet in een eerder stadium is *afgebroken* met opname van een regel in het systeemlog.

[1] De conditionele query kent m.b.t. het gebruik van tokens geen onderscheid in vertrouwensniveau. Het is alleen maar mogelijk om de conditionele query te gebruiken i.c.m. het mandaat-, transactie- en inschrijftoken. Hiermee wordt een vergelijkbaar vertrouwensniveau bereikt als AORTA vertrouwensniveau 'midden'.

[2] Een voordeel hiervan is dat het hierdoor mogelijk wordt dat de organisatie vermeld op het servercertificaat van het GBx afwijkt van de naam van de organisatie op het certificaat van de persoonlijke gebruikerspas, hetgeen 'gastgebruik' van passen mogelijk maakt; een zorgverlener die werkzaam is bij meer dan één zorgaanbieder heeft dan maar één persoonlijke UZI-pas nodig.

[3] Vanuit infrastructureel oogpunt is dit complex omdat dit betekent dat de TLS-verbinding niet kan starten vanaf de server van het GBx, maar moet starten bij het workstation van de gebruiker.

[1] Het ontwerp elektronische handtekening voegt hier nog een niveau ‘hoog’ aan toe, waarbij (een deel van) de inhoud wordt ondertekend. Het is echter niet gebruikelijk om andere aspecten dan authenticatie te betrekken in het definiëren van vertrouwensniveaus. Zie ook volgende voetnoot.

[2] De hier gehanteerde definities van ‘laag’ en ‘midden’ zijn niet geheel in lijn met de niveaus van vergelijkbare indelingen zoals die van STORK (<http://www.eid-stork.eu>) en zullen naar verwachting op termijn worden herzien. Gezien de waarborgen die gelden bij de uitgifte van de UZI-pas of ZORG-ID Smartcard en het gebruik van twee-factor authenticatie geldt in feite dat bij authenticatie op basis van een UZI-pas of ZORG-ID Smartcard de identiteit van de eindgebruiker met hoge betrouwbaarheid wordt vastgesteld.

7.9 Infrastructurele aspecten

In dit hoofdstuk worden de infrastructurele aspecten en de gerelateerde onderdelen beschreven.

7.9.1 Conceptueel overzicht infrastructuur

{

Diagram AORTA.INF.d1010.4 geeft een conceptueel overzicht van de infrastructuur van AORTA. Hierin wordt weergegeven op welke wijze de informatiesystemen die zijn beschreven in het hoofdstuk ‘Informatiesystemen’⁸³ logisch worden gekoppeld om berichtenuitwisseling tussen deze systemen te faciliteren.

Voor de duidelijkheid is de figuur opgedeeld in lagen.

7.9.1.1 Initiërende systemen

De bovenste laag toont de informatiesystemen die een interactie via AORTA kunnen initiëren. Zoals besproken in de systeeminteracties zijn dit GBZ’en, GBP’en het GBK en de DVZA samen aangeduid als GBx.

7.9.1.2 Communicatienetwerken

Opvragende systemen en bronsystemen worden gekoppeld aan de centrale infrastructuur via een datacommunicatienetwerk (DCN). Onder een DCN wordt hier verstaan: een netwerk van datacommunicatieverbindingen, inclusief de daarvoor benodigde voorzieningen op de locatie van de aangesloten partijen, dat door één datacommunicatiedienstverlener wordt geëxploiteerd en beheerd. In technisch opzicht is een DCN een privaat of virtueel privaat TCP/IP-netwerk.

Indien dit voor het bereiken van het juiste beschikbaarheidsniveau noodzakelijk is, kan een GBx door middel van redundante verbindingen aan een DCN gekoppeld worden. DCN’s worden door middel van redundante verbindingen gekoppeld aan de centrale infrastructuur.

83. <https://vzvz.atlassian.net/wiki/x/twIRBQ>

7.9.1.2.1 Goedbeheerd ZorgNetwerk (GZN)

Binnen AORTA worden aan het DCN eisen gesteld voor onder meer functionaliteit, beschikbaarheid en beveiliging; daarnaast worden eisen gesteld aan de dienstverlening van de datacommunicatiedienstverlener die optreedt als leverancier van het DCN. Een datacommunicatiedienstverlener die voldoet aan dit programma van eisen en hiervoor een kwalificatie behaalt wordt binnen AORTA aangeduid als een Goed Beheerd Zorgnetwerk (GZN) (voorheen was dit Zorg Service Provider, ZSP). Een GBx kan uitsluitend gekoppeld worden aan de ZIM via het DCN van een GZN.^[1]

7.9.1.2.2 Domain Name Service

Elke GZN beheert een eigen Domain Name Service (DNS) die de hostnaam van elk aangesloten GBx vertaalt naar het IP-adres waarop het GBx bereikbaar is. Uit het oogpunt van beschikbaarheid biedt het LSP een gemeenschappelijke secundaire DNS voor alle aangesloten GZN's. Systemen binnen AORTA dienen elkaar te benaderen via de DNS en niet rechtstreeks op IP-adres.

7.9.1.2.3 Domein aorta-zorg.nl⁸⁴

Het GZN kent aan een GBx een hostnaam toe, zodat de GZN het IP-adres kan wijzigen zonder dat dit effect heeft op de bereikbaarheid van de GBx voor de buitenwereld (waaronder de ZIM). Deze hostnaam wordt ook vastgelegd in servercertificaten van het UZI-register als 'Fully Qualified Domain Name' (FQDN). Wijzigingen van het IP-adres zijn overigens beperkt tot de door het LSP toegekende reeks, zie hieronder bij 'IP-adresreeksen'.

84. <http://aorta-zorg.nl>

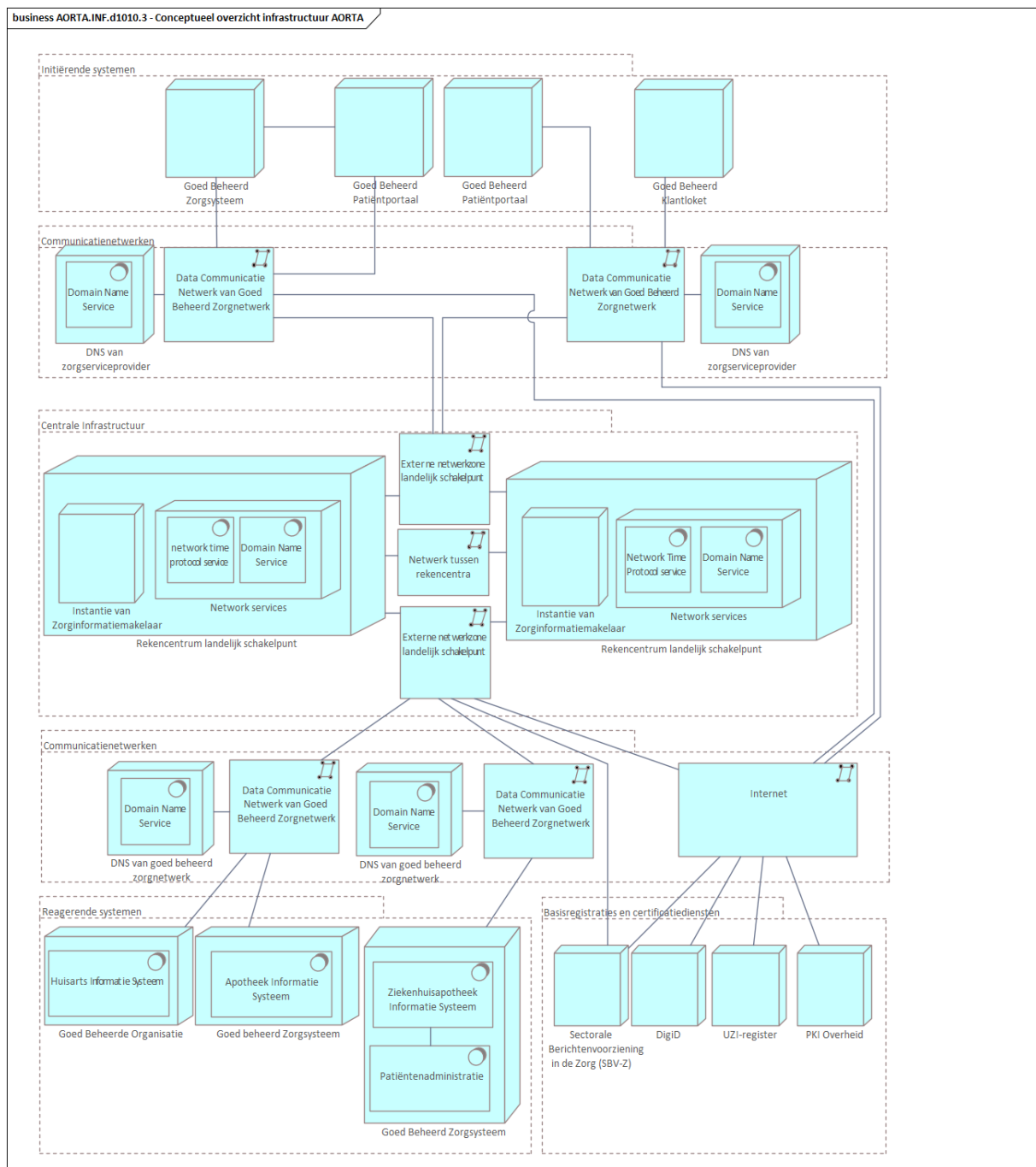


Diagram AORTA.INF.d1010.4: conceptueel overzicht van de AORTA infrastructuur

Het UZI-register eist dat de relatie tussen FQDN en zorgaanbieder kan worden getoetst bij de Stichting Internet Domeinregistratie Nederland (SIDN) of bij het LSP. Daarom krijgt elk op de ZIM aangesloten informatiesysteem een hostnaam onder het geregistreerde domein 'aorta-zorg.nl'⁸⁵. De FQDN wordt tevens vastgelegd als URI van het GBx in het applicatieregister van de ZIM.

85. <http://aorta-zorg.nl>

7.9.1.2.4 IP-adresreeksen

Een GBx dat via een GZN wordt aangesloten op de centrale infrastructuur krijgt een IP-adres toegekend door de GZN. Aan een GZN wordt hiertoe een reeks van IP-adressen toegekend door het Landelijk Schakelpunt (LSP), die vervolgens aan specifieke GBx'en kunnen worden toegekend. Elk GBx moet binnen het DCN bereikbaar zijn op het toegekende IP-adres (maar moet via de DNS benaderd worden).

Het kan voorkomen dat het door het GZN toegekende IP-adres botst met adressen binnen het lokale netwerk van het GBx of dat de door het LSP toegekende reeks van IP-adressen botst met adressen binnen het DCN van de GZN. In deze gevallen moet op het koppelvlak van het LAN waartoe het GBZ behoort en het DCN en/of op de grens van DCN en het externe netwerk van het LSP een vorm van adresconversie worden toegepast, zoals NAT (Network Address Translation).

7.9.1.2.5 Internet-koppeling

GBx'en hebben toegang nodig tot het internet om een aantal redenen:

- de services van de SBV-Z voor verificatie van het burgerservicenummer en wettelijk identificatiedocument (zie [subparagraaf 10.4 \(see page 115\)](#)) worden via het internet geleverd.
- GBZ'en moeten in staat zijn om de digitale certificaten op de UZI-passen of ZORG-ID Smartcards van hun gebruikers op geldigheid te controleren; daartoe moeten zij controleren of deze certificaten zijn ingetrokken. Om dit te kunnen controleren moeten zij toegang hebben tot de 'certificate revocation lists' (CRL) die op het internet worden gepubliceerd door de 'certificate authority' (CA), in dit geval het UZI-register.
- Volgens de regels van PKIO moet ook de geldigheid van het certificaat van de CA zelf worden gecontroleerd en deze keten van CA's moet worden gevolgd tot aan de 'Root CA van de Staat der Nederlanden'. Hiertoe moeten ook de CRL's van deze CA's worden gecontroleerd, die op het internet worden gepubliceerd.
- GBZ, GBP en GBK moeten in staat zijn om het PKIO-certificaat van de ZIM op geldigheid te controleren en moeten daartoe controleren of dit certificaat is ingetrokken. Om dit te kunnen controleren moeten zij toegang hebben tot de CRL van de CA die het ZIM-certificaat uit geeft.

De GZN *kan* een ontsluiting bieden naar het internet via een beveiligde netwerkpoort in het DCN. Overigens kan deze ontsluiting naar het internet ook via een andere service provider worden geleverd.

[1]

7.9.1.2.6 Protocollen

Voor de datacommunicatie tussen GBx en ZIM wordt, ter bevordering van interoperabiliteit, gebruik gemaakt van gangbare internetprotocollen, namelijk HTTP met TLS (HTTPS) over TCP/IP (de applicatie-protocollen boven de HTTP-laag zijn reeds besproken in 'Protocollen'⁸⁶). Voor het opzetten van een beveiligde verbinding tussen GBZ en ZIM volgens het TLS protocol met wederzijdse authenticatie moet het GBZ over een UZI-servercertificaat of een PKIO-servercertificaat beschikken en de ZIM over een PKIO-servercertificaat. Een GBP moet beschikken over een PKIO-servercertificaat. Het GBK heeft evenals de ZIM een PKIO-servercertificaat.

86. <https://vzvz.atlassian.net/wiki/x/TAMRBQ>

7.9.1.3 Centrale infrastructuur

De ZIM is de belangrijkste component in de centrale infrastructuur. Vanuit het oogpunt van continuïteit en beschikbaarheid voorziet de architectuur in twee instanties van de ZIM, verspreid over rekencentra op afzonderlijke locaties, gekoppeld door een netwerk. Het bestaan van meerdere instanties van de ZIM dient functioneel transparant te zijn voor informatiesystemen die communiceren met de ZIM, dat wil zeggen dat de instanties van de ZIM zich dienen te gedragen als ware er één ZIM.

In de rekencentra van het LSP zijn tevens netwerkdiensten aanwezig die zorgdragen voor het functioneren van de AORTA-infrastructuur als geheel:

- De centrale infrastructuur biedt een routeerfunctie, waardoor netwerkverkeer dat afkomstig is van een systeem binnen een aangesloten DCN en is gericht aan een systeem in een ander aangesloten DCN, correct kan worden afgeleverd. Hiertoe wordt dynamische routing toegepast.^[1]
- Een Domain Name Service binnen de centrale infrastructuur dient als secundaire DNS voor de primaire DNS-services van de aangesloten DCN'en.
- Voor tijdsynchronisatie tussen de op de centrale infrastructuur aangesloten systemen biedt de centrale infrastructuur een Network Time Protocol service.

7.9.1.4 Externe systemen/infrastructuren

Er kunnen externe systemen of infrastructuren aangesloten worden op AORTA. Vanuit AORTA zullen er eisen gesteld worden aan het koppelvlak met deze externe systemen/infrastructuren. De AORTA infrastructuur mag geen nadelige gevolgen ondervinden van een extern aangesloten systeem of infrastructuur. Nadelige gevolgen kunnen bestaan uit bijvoorbeeld een degeneratie van het beveiligingsniveau of de prestaties van AORTA.

7.9.1.5 Reagerende systemen

Diverse XIS-systemen (huisartsinformatiesystemen, apotheekinformatiesystemen, ziekenhuisapothekinformatiesystemen, etc.) waarvoor een XIS-typekwalificatie is verkregen en waarvan de implementatie voldoet aan de eisen voor een GBZ, kunnen fungeren als reagerende systemen in interacties die via AORTA verlopen.

Een GBZ kan meerdere XIS-applicaties omvatten, zoals aangegeven in het diagram met het voorbeeld van een GBZ dat bestaat uit een ziekenhuisapothekinformatiesysteem en patiëntadministratiesysteem.

Een GBZ kan overigens in de ene interactie het initiërend systeem zijn en in een andere interactie het reagerend systeem.

7.9.1.6 Basisregistraties en certificatiediensten

Onder basisregistraties en certificatiediensten vallen de infrastructuren van UZI-register, PKloverheid, DigiD en SBV-Z. Deze zijn beschikbaar via het internet voor zowel de ZIM (met uitzondering van het SBV-Z) als voor GBX'en. UZI-register en PKloverheid zijn voor GBX'en adresseerbaar via het internet óf via de netwerkinfrastructuur van de ZIM.

[1] Dit is een voorbereiding op eventuele rechtstreekse gegevensuitwisseling tussen aangesloten GBZ'en zonder tussenkomst van de ZIM, bijvoorbeeld van multimediale bestanden op basis van het DICOM-protocol.

[1] In theorie kunnen de UZI- en PKIO-services ook benaderd worden via de centrale infrastructuur omdat ook daar een internetkoppeling aanwezig is om deze zelfde services te bereiken. Hiervoor zijn binnen het lokale netwerk van het GBZ in het algemeen configuratiehandelingen nodig om internetverkeer met UZI- en PKIO-register om te leiden ten opzichte van overig internetverkeer. In het algemeen loopt de toegang van het GBZ tot deze services niet via de centrale infrastructuur.

[1] Strikt genomen geldt deze eis niet voor het GBK, maar het datacommunicatienetwerk waarmee het GBK wordt gekoppeld aan de ZIM, evenals het beheer van dit netwerk worden wel gehouden aan dezelfde eisen als die gelden voor een GZN, waardoor ook deze netwerkdienst als een GZN kan worden beschouwd.

7.9.2 Operationele aspecten

7.9.2.1 14.2.1 Beschikbaarheid

Zorgverleners kunnen idealiter 7 dagen per week en 24 uur per dag patiëntgegevens opvragen en versturen. Dit geldt ook voor patiënttoegang via een GBP. Dit stelt hoge eisen aan verschillende platformen in de basisinfrastructuur, waaronder de aangesloten GBZ'en en DCN'en. Immers, als één GBZ patiëntgegevens opvraagt die verspreid liggen bij andere GBZ'en, moeten deze ook beschikbaar en bereikbaar zijn.

Beschikbaarheid wordt in het algemeen uitgedrukt in percentages van de totale mogelijke beschikbaarheid, waarbij geplande niet-beschikbaarheid wegens onderhoud niet wordt meegerekend. Voor onderhoud worden in het algemeen vaste tijdsintervallen ingesteld. In een keten van systemen is de totale beschikbaarheid het product van de beschikbaarheidspercentages van de individuele componenten.

In het geval van AORTA hangt de samenstelling van de keten af van het gebruiksscenario, maar bestaat meestal uit:

- Het initiërend systeem dat een bericht stuurt naar de ZIM;
- het DCN tussen GBx en ZIM;
- de ZIM;
- het DCN tussen ZIM en reagerend systeem of reagerende systemen;
- het reagerend GBZ of register.

Ten aanzien van de individuele componenten in de keten worden eisen gesteld in programma's van eisen.

Enkele belangrijke maatregelen binnen AORTA ten aanzien van beschikbaarheid zijn:

- het stellen van eisen aan infrastructuur en beheer van aangesloten systemen, netwerken en de centrale infrastructuur en het uitvoeren van controles op de naleving van deze eisen;

- het vastleggen en naleven van afspraken tussen de verschillende systeembeheerpartijen in het kader van de inrichting van operationeel beheer (zie ook [AORTA DAP]);
- het dubbel uitvoeren van de ZIM en het spreiden van de ZIM over twee locaties;
- het verzorgen van een redundante aansluiting tussen DCN en ZIM;
- de aanwezigheid van test- en acceptatieomgevingen van de ZIM, waardoor de aansluiting van nieuwe GBx'en en het installeren van nieuwe software-releases kan worden getest voordat de productieomgeving wordt aangepast.

Voor GBx'en zijn twee statussen gedefinieerd die gerelateerd zijn aan de beschikbaarheid:

- opengesteld;
- geblokkeerd.

Voor de individuele applicaties die zijn geregistreerd onder een GBx zijn vier statussen gedefinieerd die gerelateerd zijn aan de beschikbaarheid. Deze zijn:

- gereed: de applicatie is na een periode van onbeschikbaarheid (toestand 'onderhoud' of 'storing') gereed om weer actief te worden;
- actief: de applicatie is in staat tot berichtuitwisseling;
- storing: de applicatie is ongepland niet beschikbaar;
- onderhoud: de applicatie is gepland niet beschikbaar.

De actuele beschikbaarheidstoestand van elk GBx en applicatie onder een GBx wordt centraal in het applicatieregister van de ZIM geregistreerd. De beheerder van het GBx dient de beheerder van de ZIM te informeren over de actuele status. De ZIM kent dezelfde vier statussen als een applicatie: gereed, actief, storing en onderhoud. De beheerder van de ZIM informeert de beheerders van informatiesystemen over de actuele status.

7.9.2.2 14.2.2 Capaciteit en schaalbaarheid

Om te komen tot een schatting van de vereiste capaciteit voor de AORTA infrastructuur is een schatting gemaakt van de aantallen te verwachten gebruikersinteracties voor de zorgtoepassingen 'medicatieproces' en 'huisartswaarneminggegevens'. Dergelijke schattingen zijn vertaald naar 'service level agreements' met de leverancier van de ZIM.

Aan de leverancier van de ZIM en beheerders van aangesloten DCN'en en GBx'en worden eisen gesteld ten aanzien van de schaalbaarheid van de systemen. De schaalbaarheid van een systeem is de mate waarin het systeem is voorbereid op toename van het gebruik zonder merkbare verslechtering van het functioneren van het systeem.

7.9.2.3 14.2.3 Responstijden

Net als bij het onderwerp beschikbaarheid geldt dat de snelheid van AORTA als geheel afhangt van de snelheid van de componenten in de keten. Ten aanzien van de gemiddelde responstijden van AORTA zijn gebruikerswensen geïnventariseerd en zijn streefgetallen vastgesteld. Gewenste responstijden worden vastgelegd in programma's van eisen.

7.10 Beveiliging

Vanwege het vertrouwelijke karakter van patiëntgegevens is beveiliging een centraal aspect van de AORTA-architectuur dat verweven is met andere aspecten van de architectuur. Diverse aspecten van beveiliging zijn dan ook al in voorgaande hoofdstukken aangestipt. Dit hoofdstuk heeft dan ook het karakter van een overzicht.

De [AVG] vereist bij de verwerking van persoonsgegevens een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van de te

beschermen gegevens met zich meebrengen. In [AV23] worden vier risicoklassen voor persoonsgegevens opgevoerd (publiek niveau, basisniveau, verhoogd risico en hoog risico). Volgens de in [AV23] gestelde criteria valt de verwerking van persoonsgegevens in AORTA onder risicoklasse III (hoog risico) omdat sprake is van:

- bijzondere persoonsgegevens, namelijk gezondheidsgegevens;
- veel persoonsgegevens, namelijk in principe van alle patiënten van zorgaanbieders in Nederland.

De beveiligingsmaatregelen van AORTA moeten daarom zijn afgestemd op een hoog risico.

De beveiliging van AORTA is gebaseerd op een [Vertrouwensmodel]. Dit model is het geheel van technische, organisatorische en juridische waarborgen voor het vertrouwen in de landelijke elektronische uitwisseling van medische gegevens.

In dit hoofdstuk wordt vooral ingegaan op de technische waarborgen. Details van diverse beveiligingsaspecten worden daarnaast verder uitgewerkt in de ontwerpdocumenten van deelcomponenten van de ZIM [Ontw Authenticatie], [Ontw APT] en [Ontw APR].

Er is sprake van technische beveiligingswaarborgen in drie fasen van het gebruik van de AORTA infrastructuur:

- vooraf, bij het aansluiten op de infrastructuur;
- tijdens het gebruik van de infrastructuur, bij gegevensuitwisseling;
- achteraf, na uitwisseling van gegevens.

Voorafgaand aan het aansluiten op de infrastructuur moet voor een XIS een XIS-typekwalificatie worden behaald. Hiervoor moet worden voldaan aan een programma van eisen, waarvan beveiligingseisen een onderdeel zijn. Voordat een specifieke implementatie van een XIS bij een zorgaanbieder daadwerkelijk kan worden aangesloten, moet voldaan worden aan de implementatie-eisen voor een GBZ. Ook voor GBP en GBK gelden dergelijke eisen.

Een GBx moet bij aansluiting worden geregistreerd in het applicatieregister van de ZIM. Binnen dit register krijgt het systeem een status toegekend en wordt per interactietype vastgelegd of het systeem dit type interactie mag uitvoeren. Een GBx dat niet de status actief heeft en dat niet geregistreerd is voor het deelnemen aan de juiste interactietypen zal geen gegevens kunnen uitwisselen.

Het GBx zelf moet van de juiste servercertificaten worden voorzien. Deze zijn afkomstig van het UZI-register. In het geval van GBP's, GBK's en niet-UZI-abonnees zijn deze afkomstig van PKI-overheid. De gebruikers van een GBZ moeten beschikken over een UZI-pas, ZORG-ID Smartcard of ZORG-ID Mobile App. Voor het GBK moeten gebruikers beschikken over een PKIO-pas. Voorafgaand aan de verstrekking van dergelijke passen worden controles uitgevoerd om vast te stellen of de gebruiker voor

de pas in aanmerking komt. Passen kunnen centraal worden gedeactiveerd in geval van vermissing. Het gebruik van de pas vereist de kennis van een beveiligingscode.

Bij het uitwisselen van gegevens met de ZIM wordt de vertrouwelijkheid gegarandeerd doordat het GBx een beveiligde verbinding opbouwt op basis van TLS, waarbij het GBx en de ZIM wederzijdse authenticatie uitvoeren op basis van certificaten.

Bij het uitwisselen van patiëntgegevens worden aan het GBZ onder meer eisen gesteld ten aanzien van (zie [paragraaf 6.4 \(see page 110\)](#)):

- het inloggen van de gebruiker met een vertrouwensmiddel;
- het vastleggen van en controleren op de toestemming (opt-in) van de patiënt voor het beschikbaar maken van gegevens via AORTA;
- het verifiëren van de identiteit en het Burgerservicenummer van de patiënt;
- het vastleggen van de behandelrelatie tussen zorgverlener en patiënt;
- het bijhouden van de autorisatieregels met betrekking tot mandaten.

Bij elke berichtuitwisseling tussen GBx en de ZIM geldt een vaste reeks van controles:

- de geldigheid van de berichtsyntax wordt gecontroleerd;
- het applicatieregister wordt geraadpleegd om vast te stellen of het GBx de onderhavige interactie mag uitvoeren;
- er vindt authenticatie plaats van de gebruiker op basis van het gebruikte vertrouwensmiddel;
- de integriteit van een aantal kerngegevens in het bericht wordt gecontroleerd (deze is geborgd door versleuteling van deze gegevens in het authenticatietoken);
- er wordt gecontroleerd of de gebruiker voldoet aan de voorwaarden in het autorisatieprotocol; dit houdt onder meer in dat de toegang tot specifieke gegevenssoorten en bouwstenen is voorbehouden aan zorgverleners met de juiste beroepscode.

Niet alleen voor de implementatie en exploitatie van GBx'en, maar ook op de implementatie en exploitatie van de ZIM is een programma van eisen van toepassing, waarvan beveiligingseisen een onderdeel zijn. Onder meer wordt van de beheerorganisatie van de ZIM verlangd dat deze voldoet aan de [NEN 7510].

Als wordt geconstateerd dat een GBx afwijkt van het programma van eisen, kan in het uiterste geval door de ZIM-beheerder worden overgegaan tot het tijdelijk uitsluiten van gegevensuitwisseling via de ZIM – en uiteindelijk zelfs tot definitieve afsluiting. Daarbij wordt het belang van continuïteit van de zorgcommunicatie nadrukkelijk meegewogen.

In de ZIM bevinden zich geen inhoudelijke patiëntgegevens. De ZIM houdt uitsluitend bij welke aangesloten informatiesystemen gegevens bevatten over patiënten. De GBZ-gebruiker kan op elk gewenst moment de beschikbaarheid van gegevens aanmelden, in geval er sprake is van opt-in van de betreffende patiënt, of afmelden.

Na afloop van elke interactie die verloopt via de ZIM wordt de interactie geregistreerd in een toegangslog, zodat achteraf exact kan worden nagegaan welke toegangsgebeurtenissen hebben plaatsgevonden. Er zijn maatregelen getroffen om ongebruikelijke interactiepatronen te signaleren.

}

8 Zorgtoepassingen

In dit hoofdstuk vindt u alle *zorgtoepassingen* die zijn beschreven in het AORTA-afsprakenstelsel en beschikbaar zijn op het Landelijk Schakelpunt:

8.1 Acute Zorg

8.1.1 Opvragen professionele samenvatting RAV & SEH

Deze PvE's worden voornamelijk alleen verstrekt op expliciet verzoek van een XIS-leverancier. Deze PvE's zullen hier worden gepubliceerd zodra dit is afgestemd in de projectgroep.

8.1.2 Spoedverwijzing HAP-SEH

Deze PvE's worden voornamelijk alleen verstrekt op expliciet verzoek van een XIS-leverancier. Deze PvE's zullen hier worden gepubliceerd zodra dit is afgestemd in de projectgroep.

8.2 Huisartswaarneminggegevens

De toepassing Huisartswaarneminggegevens omvat zowel de professionele samenvatting (PS) als het waarnemerbericht (WB). De PS ondersteunt de waarneming door inzage te geven in een selectie van de medische gegevens uit het medisch dossier van de patiënt bij zijn of haar huisarts, arts voor verstandelijk gehandicapten of specialist ouderengeneeskunde. Het WB is de terugrapportage van de waarneming aan de vaste huisarts.

8.2.1 Vast Huisartssysteem

8.2.1.1 PvE HWG Vast Huisartssysteem

In het PvE HWG Vast huisartssysteem zijn alle eisen opgenomen waaraan een vast huisartssysteem dient te voldoen om aangesloten te worden op de AORTA infrastructuur. Het betreft de voormalige 6.12.15 versie van HWG die is gebaseerd op de AORTA 8.3 infrastructuur. Zorgtoepassingen zullen voortaan de versie van de infrastructuur aannemen.

Het PvE HWG voor een vast huisartssysteem is hieronder als pdf toegevoegd.



8.2.2 Waarnemend Huisartssysteem

8.2.2.1 PvE HWG Waarnemend Huisartssysteem

In het PvE HWG Waarnemend huisartssysteem zijn alle eisen opgenomen waaraan een vast huisartssysteem dient te voldoen om aangesloten te worden op de AORTA infrastructuur. Het betreft de voormalige 6.12.15 versie van HWG die is gebaseerd op de AORTA 8.3 infrastructuur. Zorgtoepassingen zullen voortaan de versie van de infrastructuur aannemen.

Het PvE HWG voor een waarnemend huisartssysteem is hieronder als pdf toegevoegd.



8.3 Jeugdgezondheidszorg

Deze PvE's worden voornamelijk alleen verstrekt op expliciet verzoek van een XIS-leverancier. Deze PvE's zullen hier worden gepubliceerd zodra dit is afgestemd in de projectgroep.

8.4 LSP Ketenzorg

8.4.1 HIS Ketenzorg

8.4.1.1 PvE Ketenzorg HIS

In het PvE Ketenzorg HIS zijn alle eisen opgenomen waaraan een vast huisartssysteem ten behoeve van ketenzorg dient te voldoen om aangesloten te worden op de AORTA infrastructuur. Zorgtoepassingen zullen voortaan de versie van de infrastructuur aannemen.

Het PvE Ketenzorg voor een vast huisartssysteem is hieronder als pdf toegevoegd.



8.4.2 KIS Ketenzorg

8.4.2.1 PvE Ketenzorg KIS

In het PvE Ketenzorg KIS zijn alle eisen opgenomen waaraan een ketenzorginformatiesysteem ten behoeve van ketenzorg dient te voldoen om aangesloten te worden op de AORTA infrastructuur. Zorgtoepassingen zullen voortaan de versie van de infrastructuur aannemen.

Het PvE Ketenzorg voor een ketenzorginformatiesysteem is hieronder als pdf toegevoegd.



8.5 MedMij

8.5.1 MedMij Bronsysteem

8.5.1.1 PvE Bronsysteem tbv MedMij

Datum: 15 juni 2022
Status: Definitief
Versie:
Classificatie: Openbaar
Revisie: 1.0

8.5.1.1.1 Documenthistorie

Documentversies

Datum	Status	Versie	Omschrijving
15 juni 2022	Definitief		Eerste opzet PvE Bronsysteem tbv MedMij

Inhoudsopgave

Documenthistorie

1 Inleiding (see page 160)

1.1 Doelgroep voor dit document (see page 160)

1.2 Doel en scope (see page 160)

2 Diagrammen Kwaliteitseisen (see page 161)

2.1 AORTA Eisen Kwaliteit aangesloten systemen (see page 161)

2.1.1 Tijdige verwerking van berichten (see page 161)

2.1.2 Genereren time-out (see page 162)

2.1.3 Borgen van minimale verwerkingssnelheid (see page 162)

2.1.4 Borgen van de beschikbaarheid van een GBx (see page 164)

2.1.5 Minimaliseren van de impact van gepland onderhoud (see page 164)

2.1.6 Borgen van de betrouwbaarheid bij kleine storingen (see page 165)

2.1.7 Borgen van de betrouwbaarheid bij grote storingen (see page 165)

2.1.8 Beveiliging van patiëntgegevens in het GBx (see page 167)

2.1.9 Borgen van plicht tot uitwisselen van patiëntgegevens (see page 167)

2.1.10 Een GBx beschikt over een geldig UZI/PKIO-servercertificaat (see page 168)

2.1.11 Beveiligde opslag (see page 168)

2.1.12 Communicatie met het LSP via een GZN (see page 170)

2.1.13 Gebruik van IP en DNS (see page 170)

2.1.14 Tijdsynchronisatie GBx en ZIM (see page 171)

2.1.15 Aansluiting op productie-omgeving LSP (see page 172)

2.2 AORTA Eisen Kwaliteit applicatie (see page 173)

2.2.1 Afbreken van een gebruikerssessie (see page 173)

2.2.2 Opzetten beveiligde verbinding met de ZIM (see page 174)

2.2.3 Instellen configuratieparameters t.b.v. communicatie en authenticatie van de ZIM (see page 174)

2.2.4 Opzetten en gebruiken van TLS-sessies (see page 175)

2.2.5 Opzetten beveiligde verbinding vanuit de ZIM met een GBx (see page 175)

2.2.6 Hardening (see page 176)

2.2.7 Toegangslog bijhouden (FHIR) (see page 177)

2.2.8 Onderscheiden van fictieve gegevens (see page 178)

2.2.9 Ondersteunen servercertificaten en ondertekeningalgoritmen (see page 179)

2.2.10 Kenbaar maken Certificate Authorities (see page 180)

2.2.11 Afhandelen transactietoken (see page 180)

2.2.12 Protocolstack voor gegevensuitwisseling o.b.v. FHIR (see page 181)

2.3 Eisen aan de beheerorganisatie van een GBX (see page 183)

2.3.1 Ondersteuning van gebruikers bij problemen met de landelijke uitwisseling van informatie (see page 183)

2.3.2 Instrueren systeemgebruikers over beveiligingsbeleid (see page 184)

2.3.3 Toekennen functiescheiding tussen systeemgebruikers (see page 185)

2.3.4 Beheren van en toegang verschaffen tot de toegangslog (see page 185)

2.3.5 Systeembeheer van een GBx (see page 186)

2.3.6 Actueel houden van het applicatieregister (see page 187)

2.3.7 Beperking inzage door beheerder (see page 187)

2.3.8 Bijhouden van een beheerlog (see page 187)

- 2.3.9 Kennisvergaring m.b.t. GBX-beheer (see page 188)
- 2.3.10 Een GBx valt onder Nederlandse wet- en regelgeving (see page 188)
- 2.3.11 Vernietigen materialen volgens standaarden (see page 189)
- 2.3.12 Voldoen aan wet- en regelgeving (see page 189)
- 2.3.13 Loggen toegangsregeling (see page 190)
- 2.3.14 Bewaartermijn loggegevens (see page 190)
- 2.3.15 Loggen inzage logging (see page 191)
- 2.3.16 Uitschakelen logging (see page 191)
- 2.3.17 Vernietigen loggegevens (see page 192)
- 2.3.18 Wijzigen logging (see page 192)
- 2.3.19 Toegangsbeheer tot logging (see page 193)
- 2.4 Eisen Infrastructurele Systeemrollen (see page 193)
- 2.4.1 Afschermen patiëntgegevens voor bevraging patiënt (see page 193)
- 2.4.2 Compatibiliteit bieden met de diverse (zorg)toepassingen (see page 194)
- 2.4.3 Leeftijdscontrole patiënt (see page 195)
- 2.4.4 Opnemen BSN in opleverbericht (see page 195)
- 2.4.5 Wijzigen TKID applicatie o.b.v. FHIR (see page 197)
- 2.4.6 Bevestigen applicatiekoppeling o.b.v. FHIR (see page 197)
- 2.4.7 Verwerken geboortedatum waarin nullen zijn opgenomen (see page 198)
- 2.4.8 Voorlopig koppelen van patiëntgegevens aan een BSN (see page 199)
- 2.4.9 Definitief koppelen van patiëntgegevens aan een BSN (see page 199)
- 2.4.10 Controleren geldigheid van een WID (see page 201)
- 2.4.11 Opzoeken en tonen patiëntgegevens (see page 201)
- 2.4.12 Gebruik van geverifieerde BSN's (see page 202)
- 2.5 Eisen XIS-leverancier (see page 203)
- 2.5.1 Beschikbaarheid XIS-servicedesk (see page 203)
- 2.5.2 Inrichten XIS-servicedesk (see page 204)
- 2.5.3 Gebruik Supportal (see page 204)
- 2.6 Eisen specifieke gegevensdienst (see page 205)
- 2.6.1 Implementeren gegevensdienst Verzamelen Huisartsgegevens 2.0 (see page 205)
- 2.6.2 Implementeren gegevensdienst Verzamelen Medicatiegegevens 9.0 (see page 206)
- 2.6.3 Implementeren gegevensdienst Verzamelen Medicatiegerelateerde Overgevoeligheden 2.A (see page 207)
- 2.6.4 Implementeren gegevensdienst Verzamelen Basisgegevens GGZ 2.0 (see page 208)
- 2.6.5 Implementeren gegevensdienst Verzamelen Basisgegevens zorg 3.0 (see page 209)
- 2.6.6 Implementeren gegevensdienst Delen antwoorden op vragenlijsten 2.0 (see page 210)
- 2.6.7 Implementeren Ontvankelijkheidstoets (see page 211)
- 2.6.8 Controleren behandelrelatie (see page 211)
- 2.6.9 Bijhouden behandelrelatie (see page 211)
- 2.6.10 Implementeren gegevensdienst Delen Meetwaarden vitale functies 2.0 (see page 213)
- 2.6.11 Implementeren gegevensdienst Verzamelen Afspraken 2.0 (see page 214)
- 2.6.12 Implementeren gegevensdienst Verzamelen Documenten 3.0 (see page 215)
- 2.6.13 Implementeren gegevensdienst Meetwaarden vitale functies 2.0 (see page 216)
- 2.6.14 Implementeren gegevensdienst Verzamelen verwijzingen naar vragenlijsten 2.0 (see page 217)

8.5.1.1.2 Inleiding

Dit programma van eisen gaat over de toepassing bronsysteem t.b.v. MedMij. Het PVE Bronsysteem t.b.v. MedMij betreft een document waarin eisen zijn opgenomen waaraan een GBZ moet voldoen om aangesloten te worden op de AORTA-infrastructuur.

8.5.1.1.2.1 Doelgroep voor dit document

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

8.5.1.1.2.2 Doel en scope

Het doel van dit document is om de eisen te beschrijven waaraan moet worden voldaan om een GBZ als bronsysteem t.b.v. MedMij aan te sluiten op de AORTA-infrastructuur. De hierin opgenomen hoofdstukken gelden voor alle bronsystemen ongeacht de gegevensdienst waarvoor zij gegevens beschikbaar stellen. Paragraaf 1.6 bevat per gegevensdienst de specifieke eisen voor die gegevensdienst. Deze zijn alleen van toepassing indien de betreffende XIS ook daadwerkelijk gegevens beschikbaar wil stellen t.b.v. die gegevensdienst.

Section: Section1

8.5.1.1.3 Diagrammen Kwaliteitseisen

8.5.1.1.3.1 AORTA Eisen Kwaliteit aangesloten systemen

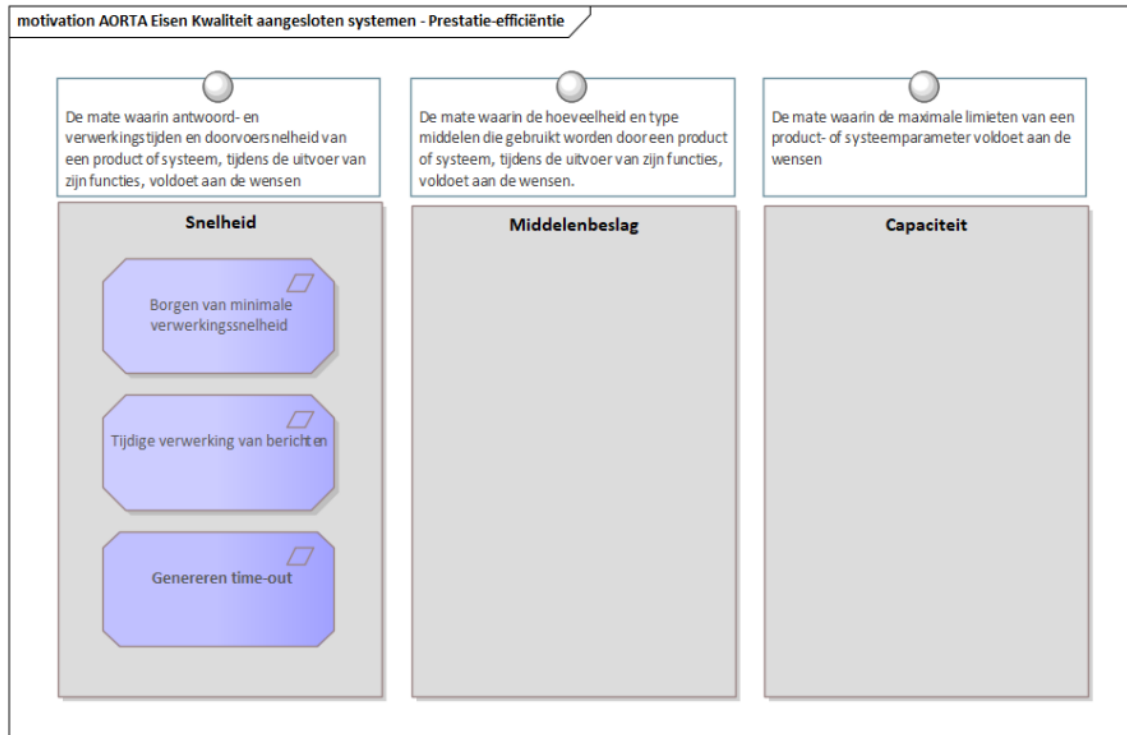


Figure 1 : AORTA Eisen Kwaliteit aangesloten systemen - Prestatie-efficiëntie

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

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. Vooralsnog blijft de waarde zoals opgenomen in deze eis gehandhaafd. Het DVZA zal in dat geval na 60 seconden een time-out versturen naar het PGO.

Vzvv_Moscow: n/a
Vzvv_Req_Verificatie: Acceptatietest
Vzvv_Req_Soort: Functional
Vzvv_Req_Type: Product

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 <GBx-verwerkingssnelheid-sturen>

Opvragen van gegevens <GBx-verwerkingssnelheid-opvragen>

Een GBx dient een zodanige capaciteit te hebben voor het beantwoorden en ontvangen van berichten van de ZIM dat het kan voldoen aan de gestelde verwerkingssnelheden. Indien dat als gevolg van een onverwacht hoge piekbelasting tijdelijk niet mogelijk is, dan prevaleren de eisen inzake beschikbaarheid boven de eisen inzake verwerkingssnelheid.

Toelichting bij eis:

Deze eis is nodig opdat een XIS-applicatie tijdig berichten van de ZIM kan verwerken/beantwoorden ten behoeve van andere zorgaanbieders, ook als de belasting zodanig hoog is, dat de volgende berichten binnenkomen terwijl de vorige nog niet verwerkt/beantwoord zijn.

Deze eis betekent voor de organisatie dat de applicatie is geïnstalleerd op ICT-voorzieningen met voldoende capaciteit om een variabele belasting van berichten vanwege de ZIM te kunnen verwerken. Omdat de exacte belasting per GBx flink kan verschillen moet iedere organisatie zelf een inschatting maken van de benodigde capaciteit en ervoor zorgen dat het GBx die belasting aankan.

De waarden <GBx-verwerkingssnelheid-sturen> en <GBx-verwerkingssnelheid-opvragen> kunnen verschillen per gebruikte technologie. Voor de HL7v3-berichten gelden de waarden zoals opgenomen in de het configuratieinstellingendocument. 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.

Vz vz_Moscow: Verplicht

Vz vz_Req_Verificatie: Monitoring

Vz vz_Req_Soort: Non-Functional

Vz vz_Req_Type: Product

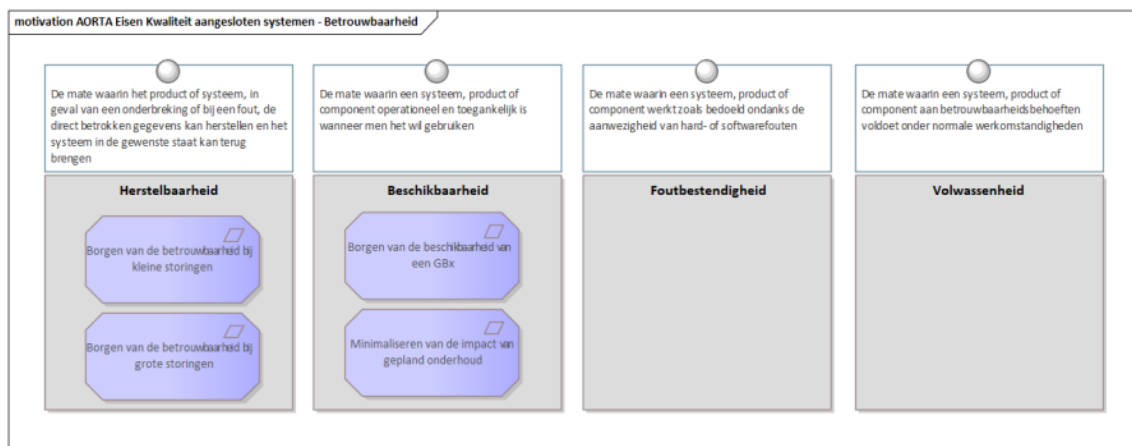


Figure 2 : AORTA Eisen Kwaliteit aangesloten systemen - Betrouwbaarheid

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

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**Minimaliseren van de impact van gepland onderhoud****Alias:** GBX.BES.e4020**Details****Eis:**

Gepland onderhoud van een GBX-applicatie mag niet meer dan twaalf keer per jaar voorkomen en dient niet langer dan een uur te duren. Gepland onderhoud wordt bij voorkeur uitgevoerd binnen aangetoonde daluren.

De beheerders van de ZIM moeten twee weken van tevoren worden ingelicht door de systeembeheerder.

Toelichting bij eis:

Deze eis is nodig om te voorkomen dat een GBZ wegens onderhoud onnodig lang onbereikbaar is, ze betekent voor de organisatie dat onderhoud van de ICT-voorzieningen zoveel mogelijk wordt gepland en zodanig voorbereid dat het GBZ slechts kort onbeschikbaar hoeft te zijn. Omdat het GBK signaleringen kan ontvangen, is de eis verplicht voor GBK.

Implicaties:

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

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

Borgen van de betrouwbaarheid bij kleine storingen

Alias: GBX.BET.e4010.1

Details	
Eis: Kleine storingen in een GBx mogen niet meer dan gemiddeld keer per maand voorkomen en dienen dan binnen 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. <ac:structured-macro ac:name="unmigrated-wiki-markup" ac:schema-version="1" ac:macro-id="aed2ce65-1953-4e10-9197-9db154973d09"><ac:plain-text-body><![CDATA[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.]]></ac:plain-text-body></ac:structured-macro> <ac:structured-macro ac:name="unmigrated-wiki-markup" ac:schema-version="1" ac:macro-id="c0af72eb-27c0-45c6-9c0c-f23bcd270c27"><ac:plain-text-body><![CDATA[Voor de waarden en moeten de waardes gehanteerd worden zoals zijn opgenomen in de [AORTA DAP]. Deze eis dient als kapstok. Het is mogelijk dat de tekst en variabele namen in de [AORTA DAP] afwijken van deze eis.]]></ac:plain-text-body></ac:structured-macro>	]]></ac:plain-text-body></ac:structured-macro>

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

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

Vzvv_Req_Type: Product

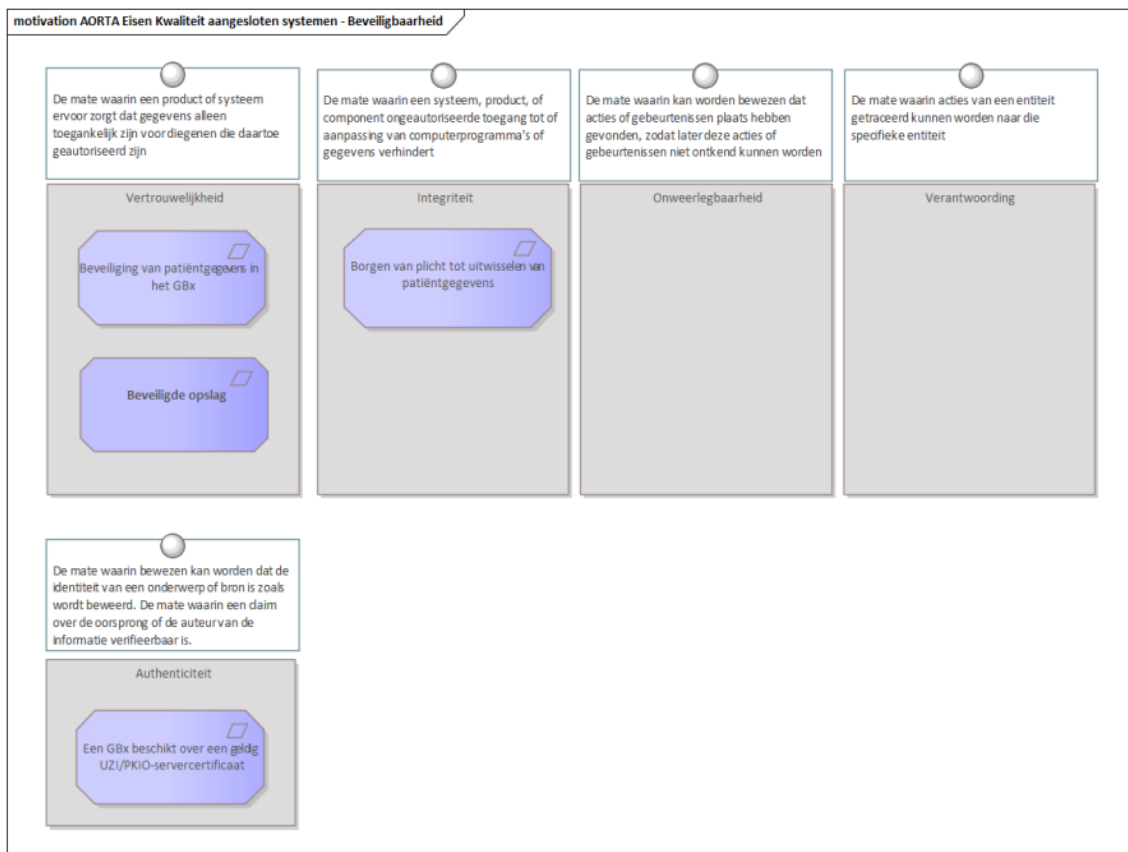


Figure 3 : AORTA Eisen Kwaliteit aangesloten systemen - Beveiligbaarheid

ISO 25010 definieert Beveiligbaarheid als: De mate waarin een product of systeem informatie en gegevens beschermt zodat personen, andere producten of systemen de juiste mate van

gegevenstoegang hebben passend bij hun soort en niveau van autorisatie.

Dit schema toont de subcategorieën van Beveiligbaarheid volgens ISO 25010.

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

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

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

Beveiligde opslag

Alias: SYS.BVL.e4010

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 de DVZA-opdrachtgever.

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

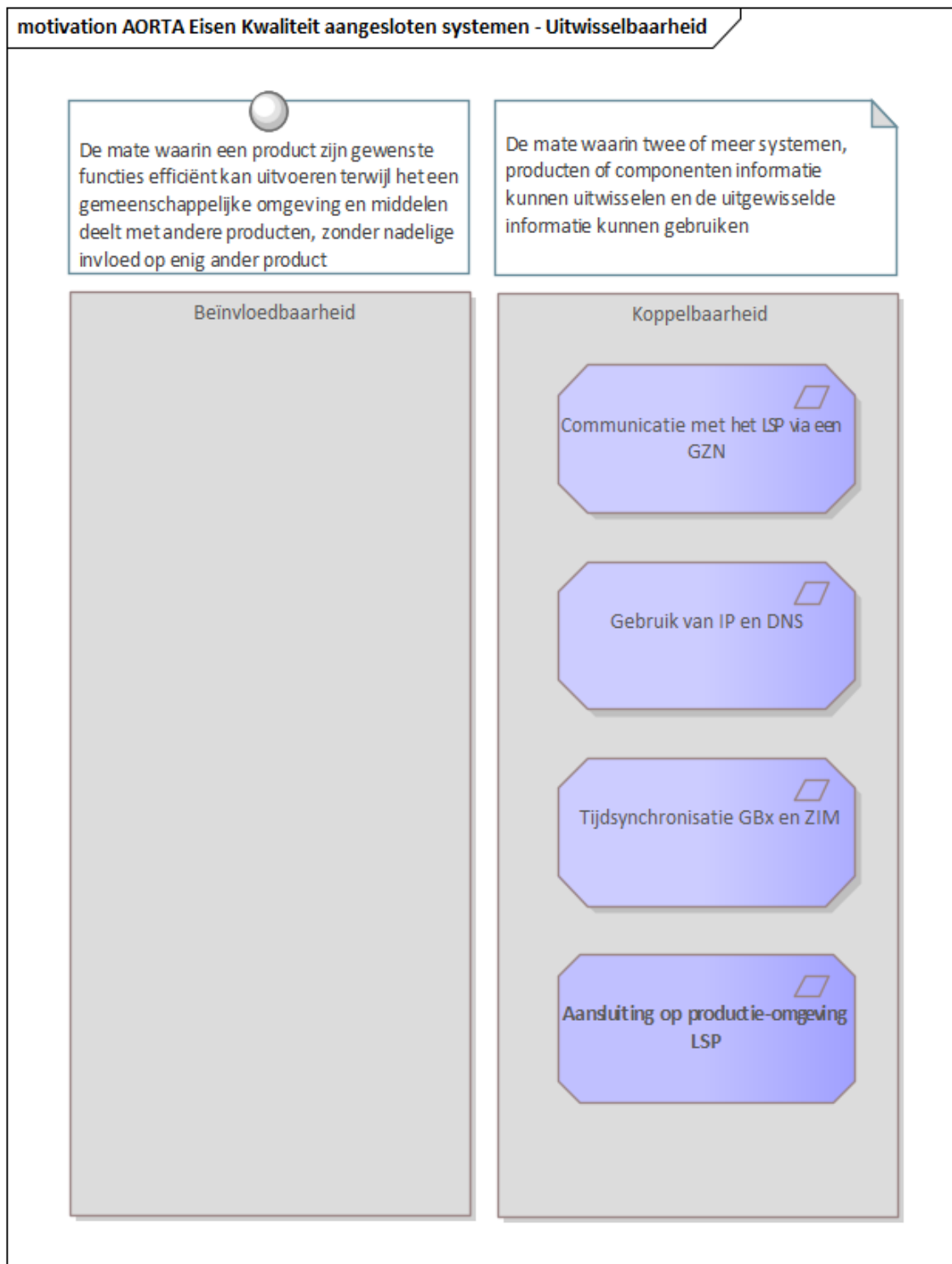


Figure 4 : AORTA Eisen Kwaliteit aangesloten systemen - Uitwisselbaarheid

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.

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.

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

4. de hostnaam een maximale time-to-live (TTL) heeft voor verversing van de cache;
5. het IP-adres van de ZIM zich binnen een vooraf overeengekomen range bevindt die altijd gerouteerd moet worden naar de GZN;
6. 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:

7. het IP-adres dat door het LSP is uitgegeven voor het GBx als geheel,
8. de IP-adressen die zijn gereserveerd voor de ZIM,
9. 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

Tijdsynchronisatie GBx en ZIM

Alias: GBX.CON.e4030, GBX.CON.e4030.1

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

Vzvv_Moscow: Verplicht (Must)

Vzvv_Req_Verificatie: Monitoring

Vzvv_Req_Soort: Non-Functional

Vzvv_Req_Type: Product

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: n/a

Vzvv_Req_Verificatie: Monitoring

Vzvv_Req_Soort: Non-Functional

Vzvv_Req_Type: Product

8.5.1.1.3.2 AORTA Eisen Kwaliteit applicatie

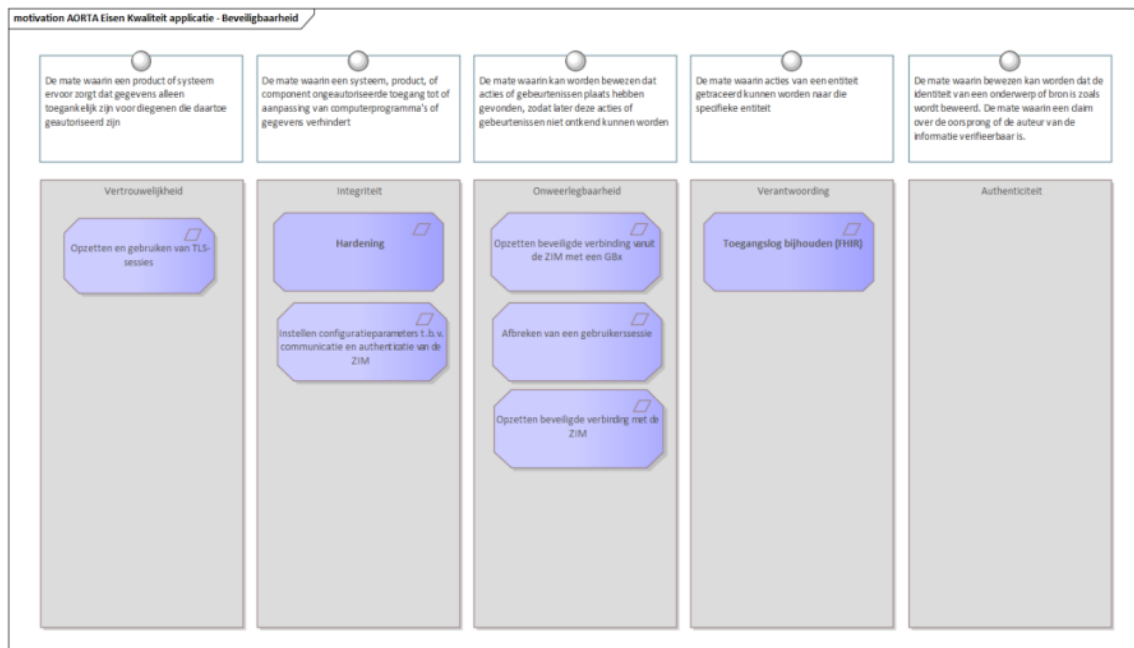


Figure 5 : AORTA Eisen Kwaliteit applicatie - Beveiligbaarheid

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.

Afbreken van een gebruikerssessie

Alias: GBX.IDA.e4090

Details

Eis:

Het systeem moet een gebruikerssessie voor het landelijk uitwisselen van patiëntgegevens op vertrouwensniveau laag of midden afsluiten:

1. op commando van de gebruiker (zoals een muisklik of toetsencombinatie);
2. door uitnemen van het vertrouwensmiddel door de zorgverlener/medewerker;
3. wanneer de applicatie gedurende gebruiker-max-applicatie-onbruik niet is gebruikt;
4. wanneer de sessie *gedurende* open staat.
5. IP-adres van gebruiker gedurende een sessie wijzigt.

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

Toelichting bij eis:

Dit is nodig opdat een gebruiker zelf zijn gebruikerssessie kan uitloggen met de zekerheid dat niemand anders zijn sessie kan voortzetten en vervolgens zijn bevoegdheden kan misbruiken. Daarnaast is deze eis nodig om te tegen te gaan dat een in onbruik geraakte sessie door een onbevoegde kan worden misbruikt.

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

Opzetten beveiligde verbinding met de ZIM

Alias: GBX.CON.e4080.4

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 applicatie-max-sleutel-duur ververs worden door middel van TLS Secure Renegotiation;
 - ☒ gebruikmakend van Cipher Suites die door het NCSC minimaal worden gekenmerkt als voldoende;
 - ☒ 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 ten hoogste ongebruikte TLS-sessie van applicatie-max-sessie-onbruik.

Toelichting bij eis:

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

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

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

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

Alias: GBX.FBH.e4050.2

Details

Eis:

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

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

Toelichting bij eis:

Dit is nodig opdat een GBx deze parameters kan gebruiken bij de HTTP-communicatie met en authenticatie van de ZIM.

De in het GBx ingestelde waarden komen overeen met de in het applicatieregister van de ZIM geregistreerde gegevens.

Vzvv_Moscow: Verplicht (Must)

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

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

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

Toelichting bij eis:

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

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

Vzvv_Moscow: Conditioneel.

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

Hardening

Alias: SYS.BVL.e4065

Details

Eis:

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

Alle systeemparameters dienen zodanig te zijn ingesteld dat met behoud van de gewenste functionaliteit een zo hoog mogelijk niveau van beveiliging bestaat.

Toelichting bij eis:

De intentie van deze eis is dat datgene wordt gedaan dat in de markt onder de gangbare maatregelen wordt gerekend op het gebied van hardening. Hierbij moet er uiteraard een afweging worden gemaakt tussen gebruiksvriendelijkheid en veiligheid.

Vzvv_Moscow: Verplicht

Vzvvz_Req_Verificatie: Audit
Vzvvz_Req_Soort: Non-Functional
Vzvvz_Req_Type: Product

Toegangslog bijhouden (FHIR)

Alias: GBX.LOG.e4016

Details

Eis:

Het systeem moet alle binnenkomende en uitgaande berichten loggen in de toegangslog. Hierbij dienen onderstaande gegevens gelogd te worden, indien aanwezig in het bericht:

1. de identiteit van de patiënt/cliënt/burger (BSN) waar het bericht betrekking op heeft;
2. de identiteit van de organisatie waar het bericht vandaan komt of naar toe wordt gestuurd;
3. de functie en identiteit van de zorgverlener, medewerker of patiënt zoals opgenomen in het verstuurd en/of ontvangen bericht. De functie is de aorta-rolcode zoals opgenomen in het claim-element van het transactietoken.
4. de gebruikersinteractied. Dit is een combinatie van HTTP-operatie, de URL inclusief de ontvangen zoekparameters en de contentVersion uit de AORTA-Version header;
5. het tijdstip en tijdzone (ten opzichte van UTC) van het moment dat het bericht ontvangen/verstuurd is;
6. de bericht-id van het ontvangen/verstuurd bericht. Dit is het messageId in de HTTP header;
7. het initiële bericht-id van het ontvangen/verstuurd bericht. Dit is het initialMessageID in de HTTP header;
8. de aan het bericht gekoppelde gegevensdienst. Dit is de waarde zoals opgenomen in de scope van het transactietoken;
9. een indicatie van eventueel opgetreden foutsituaties met betrekking tot het ontvangen en verzenden van de berichten. Hierbij dient de HTTP-foutcode, alle informatie in de eventueel aanwezige operationOutcome en de eventuele WWW-Authenticate HTTP response header gelogd te worden.

Toelichting bij eis:

Het doel van de logging is het inzichtelijk kunnen maken van de datastroom door de gehele keten. Het inzichtelijk maken van de loggegevens kan van belang zijn voor auditredenen of beheerwerkzaamheden zoals het oplossen van fouten in de keten. Deze eis is conform de vereisten zoals beschreven in de NEN7513.

Vzvvz_Moscow: n/a
Vzvvz_Req_Verificatie: Acceptatietest
Vzvvz_Req_Soort: Functional
Vzvvz_Req_Type: Product



Figure 6 : Generieke eisen

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.

Vzvv_Moscow: Verplicht (Must)

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: n/a

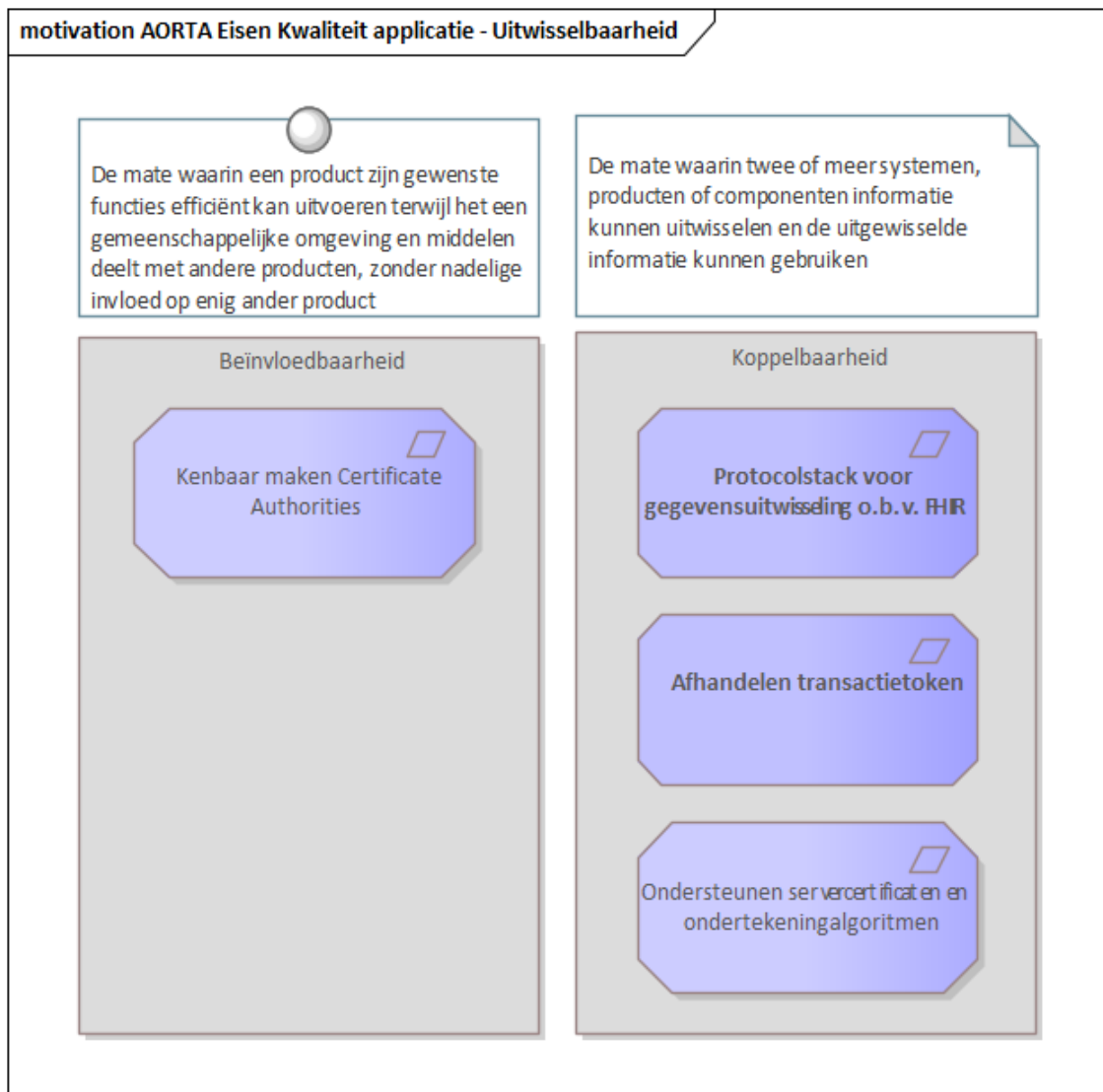


Figure 7 : AORTA Eisen Kwaliteit applicatie - Uitwisselbaarheid

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.

Ondersteunen servercertificaten en ondertekeningalgoritmen

Alias: GBX.CON.e4110.2

Details

Eis:

Het GBx dient UZI/PKIo-servercertificaten van de (verschillende) generatie(s) te ondersteunen zoals beschikbaar wordt gesteld door het UZI-Register.

Er moet gebruik worden gemaakt van het SHA-256 ondertekeningsalgoritme.

Toelichting bij eis:

Het UZI-register geeft UZI-servercertificaten uit onder één of meerdere certificaatbomen. In het geval er onder diverse certificaatbomen UZI-servercertificaten wordt uitgegeven, is het zaak om alle servercertificaten uitgegeven onder de diverse certificaatbomen te kunnen ondersteunen.

Een GBX-communicatieserver dient te zijn ingericht op het ondertekeningsalgoritme SHA-256.

Vzvv_Moscow: Verplicht (Must)

Vzvv_Req_Verificatie: Monitoring

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

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

Afhandelen transactietoken

Alias: GBX.CON.e4140.2

Details

Eis:

Het XIS moet een ontvangen transactietoken correct kunnen verwerken. Hiervoor dienen door het ontvangende systeem de controles uitgevoerd te worden zoals beschreven in de Implementatiehandleiding Transactietoken JWT ((

<https://vzvz.atlassian.net/wiki/display/UBEBVLEL/Implementatiehandleiding+Reagerend+GBZ>□

).

Indien een FHIR-search niet wordt begeleid door een transactietoken, dan dient de bevraging beantwoord te worden met een foutmelding.

Toelichting bij eis:

In combinatie met bepaalde berichten is het mogelijk dat er transactietokens worden toegevoegd. De specificatie en de juiste technische verwerking van het transactietoken staan beschreven in de IH Transactietoken JWT (

<https://vzvz.atlassian.net/wiki/display/UBEBVLEL/Implementatiehandleiding+Reagerend+GBZ>□

).

Het doel van het transactietoken is tweeledig:

- Ten eerste is het bedoeld als gegevensdrager. Er worden een aantal gegevenselementen opgenomen, die niet in het bericht zitten. Deze gegevenselementen dienen uit het token gehaald te worden en te worden gebruikt in de verdere verwerking van het bericht. Hierbij dienen de controles plaats te vinden zoals beschreven in de IH Transactietoken.
- Ten tweede kan het transactietoken gebruikt worden t.b.v. authenticatie of als bewijs van autorisatie. Het is mogelijk om op basis van de certificaatreferenties te controleren of het token van de juiste afzender afkomstig is en dat de opvrager geautoriseerd is voor bevraging van specifieke patiëntgegevens.

Vzvz_Moscow: n/a

Vzvz_Req_Verificatie: Acceptatietest

Vzvz_Req_Soort: Functional

Vzvz_Req_Type: Product

Protocolstack voor gegevensuitwisseling o.b.v. FHIR

Alias: GBX.CON.e4130.1

Details

Eis:

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

- HL7 FHIR
- JWT
- HTTP v1.1/HTTP v2.0
- TLS-verbindingen met NCSC beveiligingsniveau "goed"
- TCP
- IPv4

Toelichting bij eis:

Het is niet toegestaan om een lagere protocolversie te hanteren dan die in deze protocolstack vermeld is.

Vz vz_Moscow: n/a

Vz vz_Req_Verificatie: Acceptatietest

Vz vz_Req_Soort: Functional

Vz vz_Req_Type: Product

8.5.1.1.3.3 Eisen aan de beheerorganisatie van een GBX

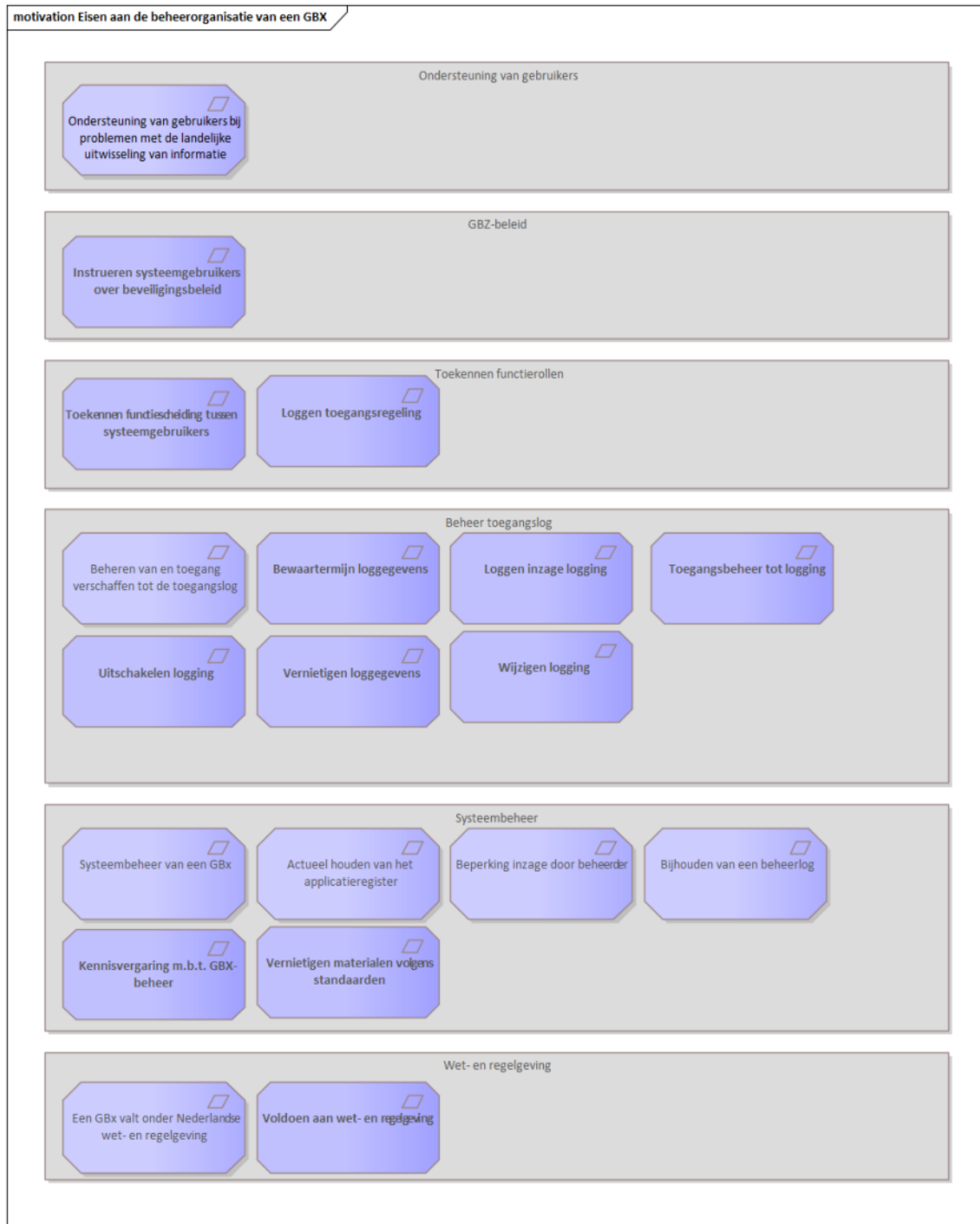


Figure 8 : Eisen aan de beheerorganisatie van een GBX

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 DAP⁸⁷](#));
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

Instrueren systeemgebruikers over beveiligingsbeleid

Alias: GBX.FBH.e4015

Details

87. https://www.vzvv.nl/uploaded/FILES/htmlcontent/AORTA_DAP_20140130_v2.3.pdf

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

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

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

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

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](https://supportal.vzv.nl)⁸⁸.

Toelichting bij eis:

Deze eis is nodig om te kunnen participeren in berichtuitwisselingen via AORTA. Het actueel houden van het applicatieregister is belangrijk voor een correcte afhandeling van berichten.

Vzvv_Moscow: Verplicht (Must)**Vzvv_Req_Verificatie:** Documentverificatie**Vzvv_Req_Soort:** Non-Functional**Vzvv_Req_Type:** Product**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.

Vzvv_Moscow: Verplicht (Must)**Vzvv_Req_Verificatie:** Acceptatietest**Vzvv_Req_Soort:** Non-Functional**Vzvv_Req_Type:** Product**Bijhouden van een beheerlog**

88. <https://supportal.vzv.nl>

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**Vzvv_Req_Type:** Product**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**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

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 \(E\)](#)⁸⁹. 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

Voldoen aan wet- en regelgeving

Alias: GBX.ALG.e4010

89. <http://www.dss.mil/documents/odaa/nispom2006-5220.pdf>

Details

Eis:

Een GBX dient te voldoen aan de NEN751x normen.

Toelichting bij eis:

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

Vzvv_Moscow: Verplicht (Must)

Vzvv_Req_Verificatie: Eigenverklaring

Vzvv_Req_Soort: Non-Functional

Vzvv_Req_Type: Product

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

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: n/a

Vzvv_Req_Verificatie: Monitoring

Vzvv_Req_Soort: Non-Functional

Vzvv_Req_Type: Business

Loggen inzage logging

Alias: AGE.LOG.e4020

Details

Eis:

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: n/a

Vzvv_Req_Verificatie: Audit

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

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

Vzvv_Moscow: n/a

Vzvv_Req_Verificatie: n/a

Vzvv_Req_Soort: n/a

Vzvv_Req_Type: n/a

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.

Vzvv_Moscow: n/a

Vzvv_Req_Verificatie: n/a

Vzvv_Req_Soort: n/a

Vzvv_Req_Type: n/a

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

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

Vzvv_Moscow: n/a

Vzvv_Req_Verificatie: n/a

Vzvv_Req_Soort: n/a

Vzvv_Req_Type: n/a

8.5.1.1.3.4 Eisen Infrastructurele Systeemrollen

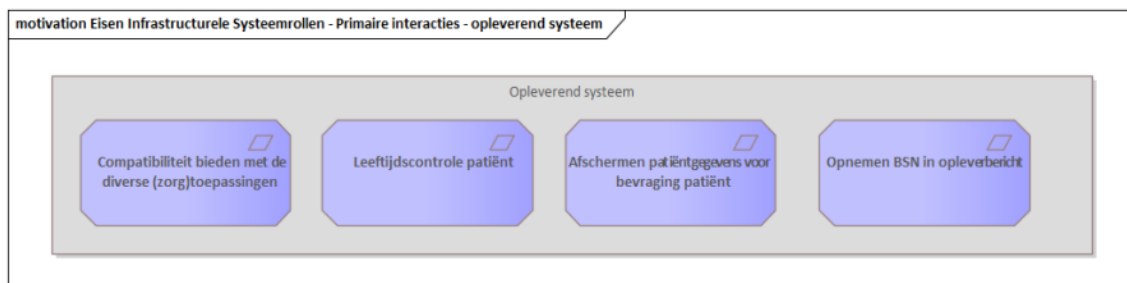


Figure 9 : Eisen Infrastructurele Systeemrollen - Primaire interacties - opleverend systeem

Afschermen patiëntgegevens voor bevraging patiënt

Alias: GBX.OPV.e4537

Details
Eis: Afscherming van patiëntgegevens voor bevraging door een patiënt moet op dossierniveau kunnen worden ingesteld door de zorgverlener. Toelichting bij eis: Naast de aggregatieniveaus die zijn beschreven in de domeinspecificaties (zoals beschreven in eis Afschermen van patiëntgegevens) dient het mogelijk te zijn om op verzoek van een patiënt of op inzicht van een zorgverlener het complete dossier af te schermen voor bevraging door een patiënt. Het afschermen van patiëntgegevens voor een patiënt is niet gebonden aan het afschermen van patiëntgegevens voor een zorgverlener (en vice versa).

Vzvv_Moscow: Verplicht**Vzvv_Req_Verificatie:** Acceptatietest**Vzvv_Req_Soort:** Functional**Vzvv_Req_Type:** Product**Compatibiliteit bieden met de diverse (zorg)toepassingen****Alias:** GBX.OPV.e4550.1

Details
Eis: Een bronsysteem moet bevragingen 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: • ZIM; • Patiëntenportaal (GBP); • Goed beheerde organisatie (GBO).

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

Leeftijdscontrole patiënt**Alias:** GBX.OPV.e4570

Details

Eis:

Indien de opvrager een patiënt is, dan dient het systeem te controleren of de leeftijd van de persoon van wie gegevens worden opgevraagd minimaal 16 jaar is.

Indien de opvrager jonger is dan 16 jaar, dan dient het systeem de opvraag te beantwoorden met een foutmelding (PATLFT).

Toelichting bij eis:

Een patiënt jonger dan 16 jaar is niet gerechtigd om zijn eigen gegevens op te vragen zonder toestemming van bijvoorbeeld een ouder of voogd. Op dit moment is het voor een patiënt niet mogelijk om een opvraag te doen onder mandaat.

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**Opnemen BSN in opleverbericht****Alias:** GBX.OPV.e4660

Details

Eis:

In FHIR-responses dient er altijd een BSN opgenomen te worden conform de technische specificaties.

Toelichting bij eis:

Een bronsysteem moet agnostisch zijn voor de infrastructuur ten behoeve waarvan opgeleverd wordt. Indien nodig, zal de resource broker het BSN verwijderen uit de FHIR-response. In de AORTA-communicatie tussen zorgaanbieders dient er altijd een BSN doorgestuurd te worden naar de uiteindelijke bevrager.

Vzvv_Moscow: n/a**Vzvv_Req_Verificatie:** Acceptatietest**Vzvv_Req_Soort:** Functional**Vzvv_Req_Type:** Product

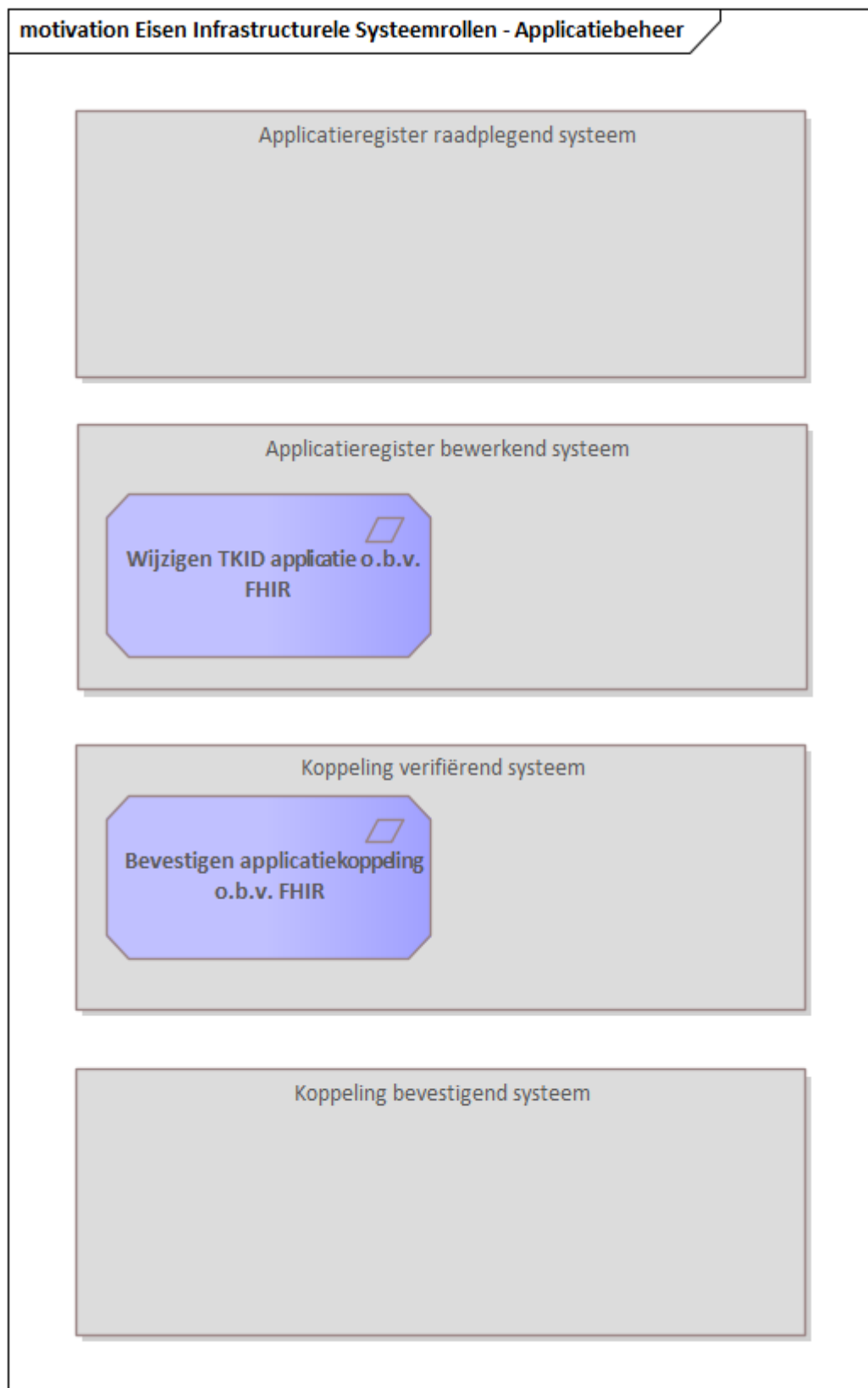


Figure 10 : Eisen Infrastructurele Systeemrollen - Applicatiebeheer

Wijzigen TKID applicatie o.b.v. FHIR**Alias:** GBX.APR.e4070.1

Details

Eis:

Het XIS moet op basis van het beherenTKID-bericht aangeven welke FHIR resources de bron kan opleveren en/of kan verwerken. Hiervoor dient de implementatie gevolgd te worden zoals beschreven in de implementatiehandleiding van het TKID-bericht.

Toelichting bij eis:

Momenteel wordt nog gewerkt aan de implementatiehandleiding voor de implementatie van het TKID-bericht. Deze eis dient dan ook vooralsnog als 'kapstokkeis' en kan worden uitgebreid en/of aangescherpt.

Vzvv_Moscow: n/a**Vzvv_Req_Verificatie:** Acceptatietest**Vzvv_Req_Soort:** Functional**Vzvv_Req_Type:** Product**Bevestigen applicatiekoppeling o.b.v. FHIR****Alias:** GBX.APR.e4080

Details

Eis:

Het XIS moet een applicatiekoppelingverificatie-bericht kunnen ontvangen en/of versturen. Hiervoor dient de implementatie gevolgd te worden zoals beschreven in de implementatiehandleiding van het applicatiekoppelingverificatie-bericht.

Toelichting bij eis:

Momenteel wordt nog gewerkt aan de implementatiehandleiding voor de implementatie van het applicatiekoppelingverificatie-bericht.. Deze eis dient dan ook vooralsnog als 'kapstokkeis' en kan worden uitgebreid en/of aangescherpt.

Vzvv_Moscow: n/a**Vzvv_Req_Verificatie:** Acceptatietest**Vzvv_Req_Soort:** Functional**Vzvv_Req_Type:** Product

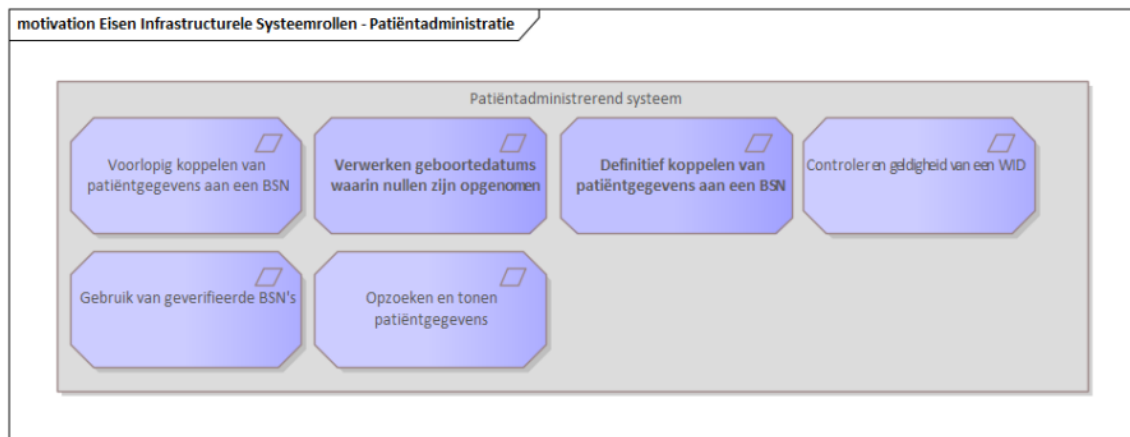


Figure 11 : Eisen Infrastructurele Systeemrollen - Patiëntadministratie

Verwerken geboortedatums waarin nullen zijn opgenomen

Alias: GBX.IDA.e4015

Details

Eis:

Een geboortedatum die teruggegeven wordt door de SBV-Z kan nullen bevatten (jjjjmm00, jjjj0000 of 00000000). Het XIS moet in staat zijn hiermee adequaat om te gaan zonder dat de applicatie vastloopt.

Toelichting bij eis:

Deze eis leidt tot de volgende aanvullende eisen:

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

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

Voorlopig koppelen van patiëntgegevens aan een BSN**Alias:** GBX.IDA.e4020**Details****Eis:**

Het systeem moet een gebruiker de mogelijkheid bieden het door een burgerregister geretourneerde BSN te koppelen aan de identificerende gegevens in de lokale patiëntenindex waarbij bij het overgenomen BSN automatisch wordt vastgelegd:

1. de bron van het BSN;
2. datum en tijd van koppelen;
3. UZI-nummer of andere identificatie van de gebruiker.

Er is dan sprake van een voorlopige koppeling tussen BSN en patiëntgegevens.

Toelichting bij eis:

Dit is nodig opdat een zorgverlener/medewerker kan voldoen aan de wettelijke verplichting van de zorgaanbieder om het BSN op te nemen in zijn administratie, zie Wbsn-z artikel 8. Voor het landelijk uitwisselen van medische patiëntgegevens moet de SBV-Z of de GBA / BRP zijn geraadpleegd.

Vzvz_Moscow: Verplicht**Vzvz_Req_Verificatie:** Acceptatietest**Vzvz_Req_Soort:** Functional**Vzvz_Req_Type:** Product**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,
 2. Datum en tijd van vaststellen,
 3. 2. indien beschikbaar het UZI-nummer of anders een unieke identificatie van de gebruiker, en het UZI-nummer van mandaterende zorgverlener indien van toepassing.
 4. zorgaanbieder-id van de gebruiker;
 5. 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.

```
<ac:structured-macro ac:name="unmigrated-wiki-markup" ac:schema-version="1" ac:macro-id="0d572124-6409-4149-9e8b-99c2fbf859ce"><ac:plain-text-body><![CDATA[Merk op dat de toelichting op [Bbsn-z] artikel 26 een grote verantwoordelijkheid legt bij de zorgaanbieder voor de afweging wel/niet WID controleren. Daarom is geautomatiseerde ondersteuning belangrijk. \]90></ac:plain-text-body></ac:structured-macro>
```

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.

Vzvz_Moscow: Optioneel

Vzvz_Req_Verificatie: Acceptatietest

90. <https://vzvz.atlassian.net/wiki/pages/createpage.action?spaceKey=A8&title=Merk+op+dat+de+toelichting+op+%5BBbsn-z%5D+artikel+26+een+grote+verantwoordelijkheid+legt+bij+de+zorgaanbieder+voor+de+afweging+wel%2Fni+et+WID+controleren.+Daarom+is+geautomatiseerde+ondersteuning+belangrijk.+%5C%5D>

Vzvvz_Req_Soort: Functional**Vzvvz_Req_Type:** Product**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.

Vzvvz_Moscow: Verplicht**Vzvvz_Req_Verificatie:** Acceptatietest**Vzvvz_Req_Soort:** Functional**Vzvvz_Req_Type:** Product**Opzoeken en tonen patiëntgegevens****Alias:** GBX.IDA.e4010.1

Details

Eis:

Het systeem moet een gebruiker de mogelijkheid bieden een patiënt op te zoeken in de lokale patiëntadministratie van de zorgaanbieder, door het invoeren van identificerende gegevens, waarna wordt getoond:

1. of de patiënt/cliënt is gevonden, en zo ja
2. of het BSN wel/niet is opgevraagd of geverifieerd bij de SBV-Z
3. de datum en tijd van koppelen
4. de manier van vaststellen van de identiteit:
 - Controle van echtheid en geldigheidsdatum van WID en de gelijkenis van de in de WID genoemde identificerende gegevens
 - Vergewissen,
 - ☒ indien beschikbaar het UZI-nummer of anders een unieke identificatie van de gebruiker en het UZI-nummer van mandaterende zorgverlener indien van toepassing
 - ☒ in geval van WID-controle: aard en nummer van het WID.

Toelichting bij eis:

Deze eis voorkomt dat de SBV-Z telkens opnieuw wordt geraadpleegd.

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

Gebruik van geverifieerde BSN's

Alias: GBX.IDA.e4060.1

Details

Eis:

Het systeem moet aan [Opzoeken en tonen patiënteninformatie](#) (see page 201), [Voorlopig koppelen van patiëntgegevens aan een BSN](#) (see page 199), [Controleren geldigheid van een WID](#) (see page 201), en [Bijhouden behandelrelatie](#) (see page 211) 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

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: n/a

8.5.1.1.3.5 Eisen XIS-leverancier

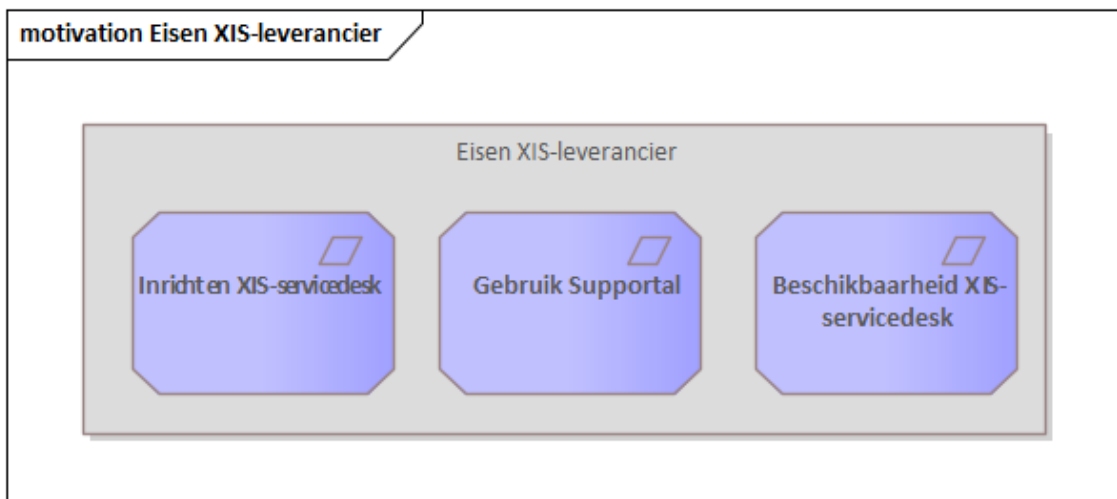


Figure 12 : Eisen XIS-leverancier

Beschikbaarheid XIS-servicedesk

Alias: XIS.SVD.e4010

Details

Eis:

Een ingericht XIS-Servicedesk moet tijdens kantoortijden beschikbaar zijn voor vragen vanuit VZVZ.

Toelichting bij eis:

Voor de oplostijden en de precieze beschikbaarheid van het XIS-servicedesk wordt verwezen naar de in de toekomst op te stellen DAP.

Vzvv_Moscow: n/a

Vzvv_Req_Verificatie: Monitoring

Vzvv_Req_Soort: Non-Functional

Vzvv_Req_Type: Business

Inrichten XIS-servicedesk

Alias: XIS.SVD.e4030

Details

Eis:

De XIS-leverancier moet een 'XIS-servicedesk' inrichten die als aanspreekpunt fungeert voor problemen m.b.t. het XIS. De XIS-servicedesk moet onderdeel uitmaken van het ketenbeheerproces.

Toelichting bij eis:

Via de GBZ-Servicedesks is niet altijd een goede voortgang te boeken met betrekking tot het oplossen van XIS gerelateerde problemen. Het ontbreken van voortgang wordt met name veroorzaakt doordat de GBZ-beheerder geen invloed heeft op de planning bij de leveranciers en doordat het precieze probleem en de ernst van het probleem niet altijd duidelijk doorkomen bij de XIS-leverancier. Daarnaast ontbreekt het de GBZ-beheerder in sommige gevallen aan de technische kennis, die nodig is om bepaalde problemen te detecteren en/of te benoemen.

De XIS-servicedesk moet de GBZ-beheerder ondersteunen bij het oplossen van eventuele technische bevindingen van het XIS. Daarnaast moet het XIS-servicedesk benaderbaar zijn voor VZVZ om bepaalde problemen en oplostijden te bespreken en de voortgang te bewaken. Het doel is om tot betere kwaliteit van de software te komen en om problemen in de keten effectiever op te lossen.

Vzvv_Moscow: n/a

Vzvv_Req_Verificatie: Monitoring

Vzvv_Req_Soort: Non-Functional

Vzvv_Req_Type: Business

Gebruik Supportal

Alias: XIS.SVD.e4020

Details

Eis:

De XIS-leverancier moet voor in gebruik name van een applicatie in productie, het XIS-aanspreekpunt en contactgegevens beschikbaar gesteld hebben via Supportal.

Toelichting bij eis:

Om een goed beheerproces te kunnen implementeren is het van belang dat de verantwoordelijke aanspreekpunten vindbaar en benaderbaar zijn. Het huidige ketenbeheerproces maakt voor communicatie binnen de keten gebruik van Supportal.

Het is van belang dat ook het XIS-aanspreekpunt vindbaar is in Supportal.

Vzvv_Moscow: n/a

Vzvv_Req_Verificatie: Monitoring

Vzvv_Req_Soort: Non-Functional

Vzvv_Req_Type: Business

8.5.1.1.3.6 Eisen specifieke gegevensdienst

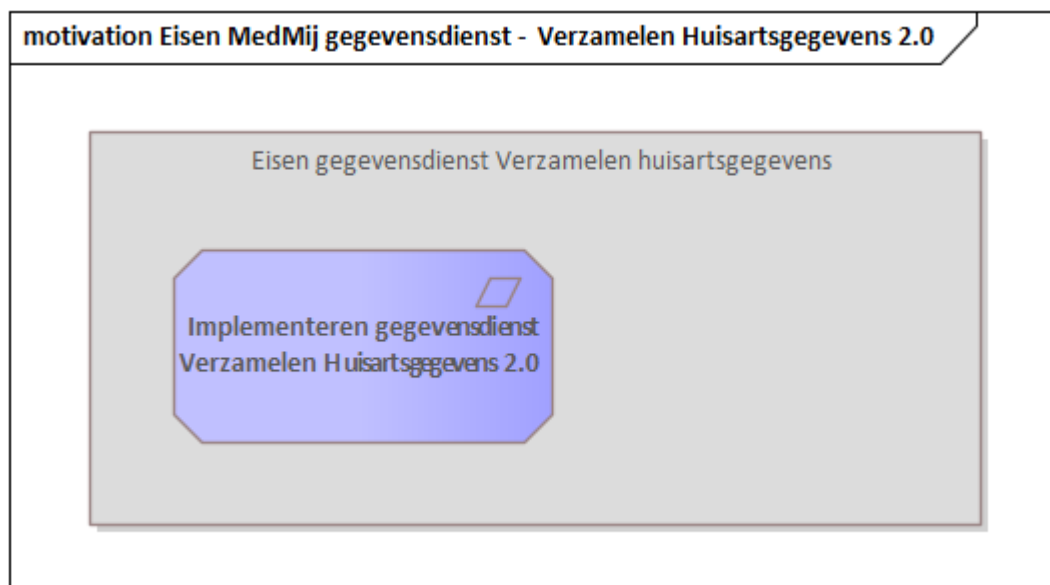


Figure 13 : Eisen MedMij gegevensdienst - Verzamelen Huisartsgegevens 2.0

Implementeren gegevensdienst Verzamelen Huisartsgegevens 2.0

Alias: GBZ.VEHU.e4010

Details

Eis:

Gegevensdienst Verzamelen Huisartsgegevens 2.0 met gegevensdienstid 49, dient ondersteund te worden door het bronsysteem.

Toelichting bij eis:

De specificaties van de te implementeren interfaces zijn te vinden via

<https://vzvz.atlassian.net/wiki/display/MMCatalogus/Actuele+Catalogus>

Vzvz_Moscow: n/a

Vzvz_Req_Verificatie: Acceptatietest

Vzvz_Req_Soort: Functional

Vzvz_Req_Type: Product

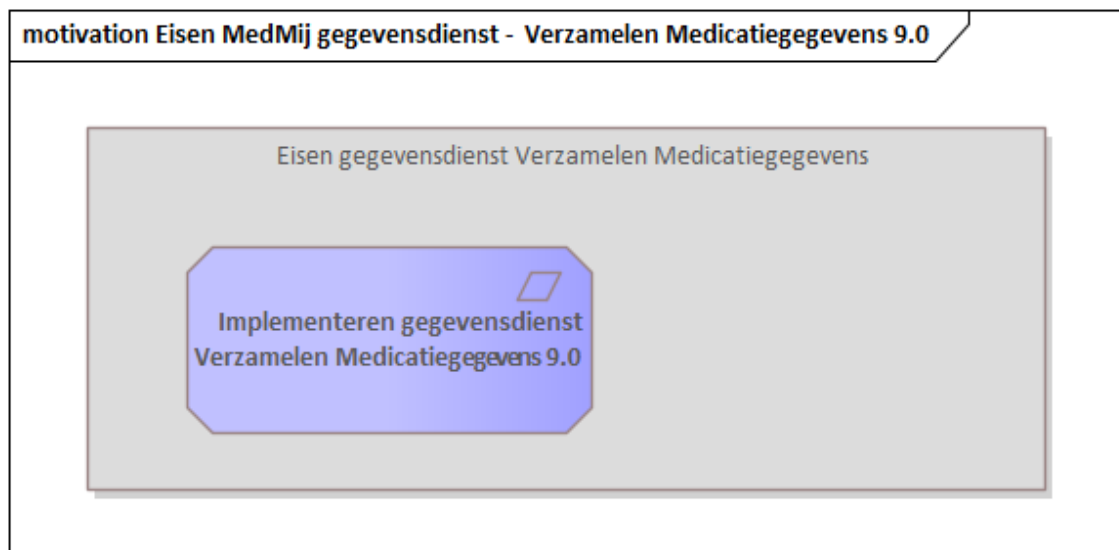


Figure 14 : Eisen MedMij gegevensdienst - Verzamelen Medicatiegegevens 9.0

Implementeren gegevensdienst Verzamelen Medicatiegegevens 9.0

Alias: GBZ.VEME.e4010

Details

Eis:

Gegevensdienst Verzamelen Medicatiegegevens 9.0 met gegevensdienstid 31, dient ondersteund te worden door het bronsysteem.

Toelichting bij eis:

De specificaties van de te implementeren interfaces zijn te vinden via

<https://vzvz.atlassian.net/wiki/display/MMCatalogus/Actuele+Catalogus>

Vz vz_Moscow: n/a

Vz vz_Req_Verificatie: Acceptatietest

Vz vz_Req_Soort: Functional

Vz vz_Req_Type: Product

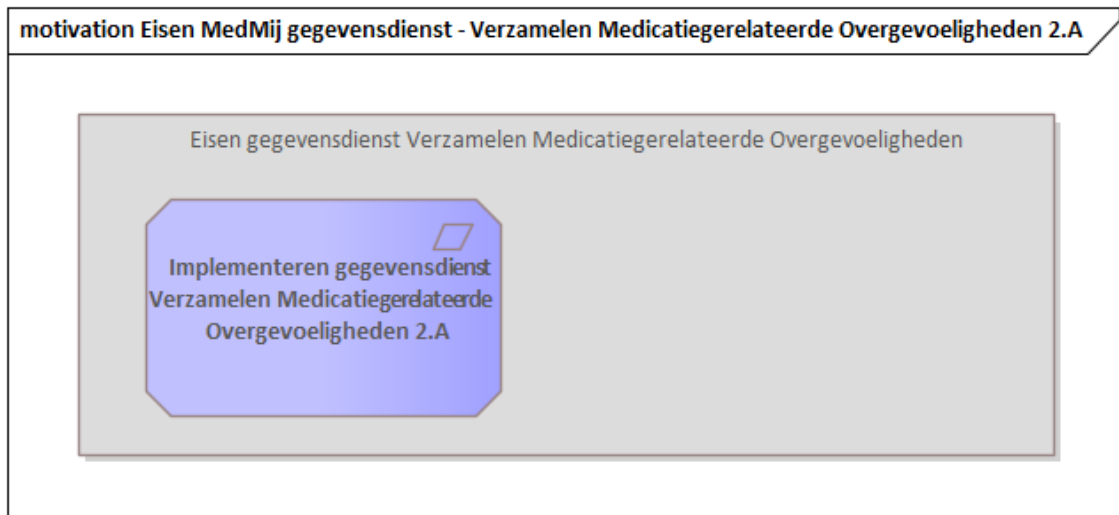


Figure 15 : Eisen MedMij gegevensdienst - Verzamelen Medicatiegerelateerde Overgevoeligheden 2.A

Implementeren gegevensdienst Verzamelen Medicatiegerelateerde Overgevoeligheden 2.A

Alias: GBZ.VEMO.e4010

Details

Eis:

Gegevensdienst Verzamelen Medicatiegerelateerde Overgevoeligheden 2.A met gegevensdienstid 58, dient ondersteund te worden door het bronsysteem.

Toelichting bij eis:

De specificaties van de te implementeren interfaces zijn te vinden via

<https://vz vz.atlassian.net/wiki/display/MMCatalogus/Actuele+Catalogus>

.

Vz vz_Moscow: n/a

Vz vz_Req_Verificatie: Acceptatietest

Vz vz_Req_Soort: Functional

Vz vz_Req_Type: Product

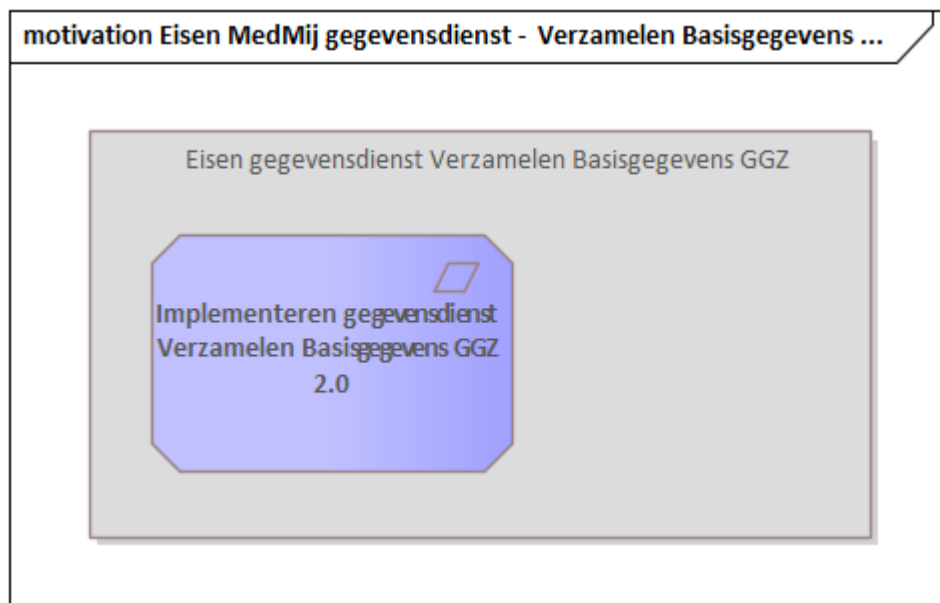


Figure 16 : Eisen MedMij gegevensdienst - Verzamelen Basisgegevens GGZ 2.0

Implementeren gegevensdienst Verzamelen Basisgegevens GGZ 2.0

Alias: GBZ.BGGZ.e4010

Details

Eis:

Gegevensdienst Verzamelen Basisgegevens GGZ 2.0 met gegevensdienstid 50, dient ondersteund te worden door het bronsysteem.

Toelichting bij eis:

De specificaties van de te implementeren interfaces zijn te vinden via

<https://vzvz.atlassian.net/wiki/display/MMCatalogus/Actuele+Catalogus>

Vzvz_Moscow: n/a

Vzvz_Req_Verificatie: Acceptatietest

Vzvz_Req_Soort: Functional

Vzvz_Req_Type: Product

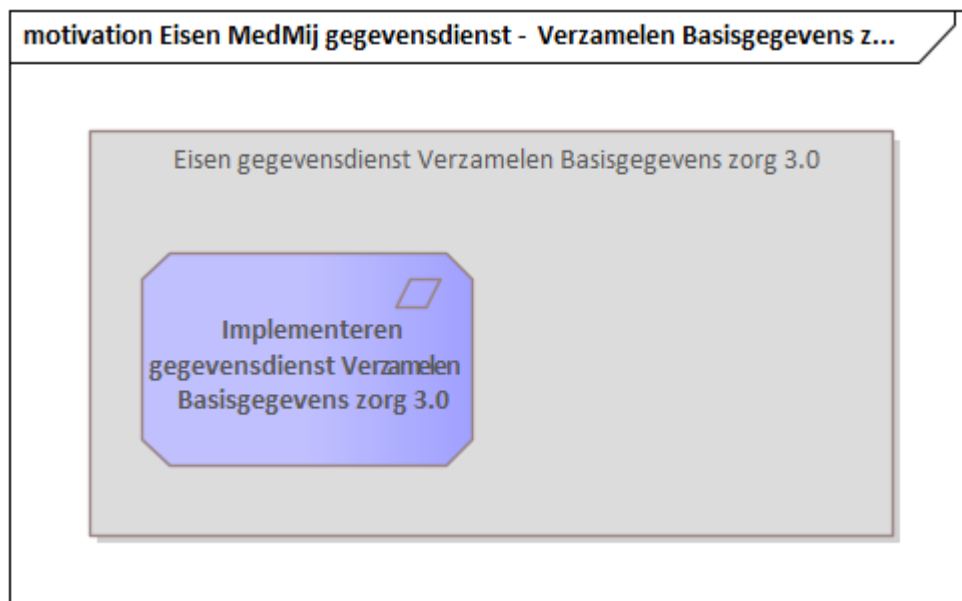


Figure 17 : Eisen MedMij gegevensdienst - Verzamelen Basisgegevens zorg 3.0

Implementeren gegevensdienst Verzamelen Basisgegevens zorg 3.0

Alias: GBZ.VBGZ.e4010

Details

Eis:

Gegevensdienst Verzamelen Basisgegevens zorg 3.0 met gegevensdienstid 48, dient ondersteund te worden door het bronsysteem.

Toelichting bij eis:

De specificaties van de te implementeren interfaces zijn te vinden via

<https://vzvz.atlassian.net/wiki/display/MMCatalogus/Actuele+Catalogus>

.

Vzvz_Moscow: n/a

Vzvz_Req_Verificatie: Acceptatietest

Vzvz_Req_Soort: Functional

Vzvz_Req_Type: Product

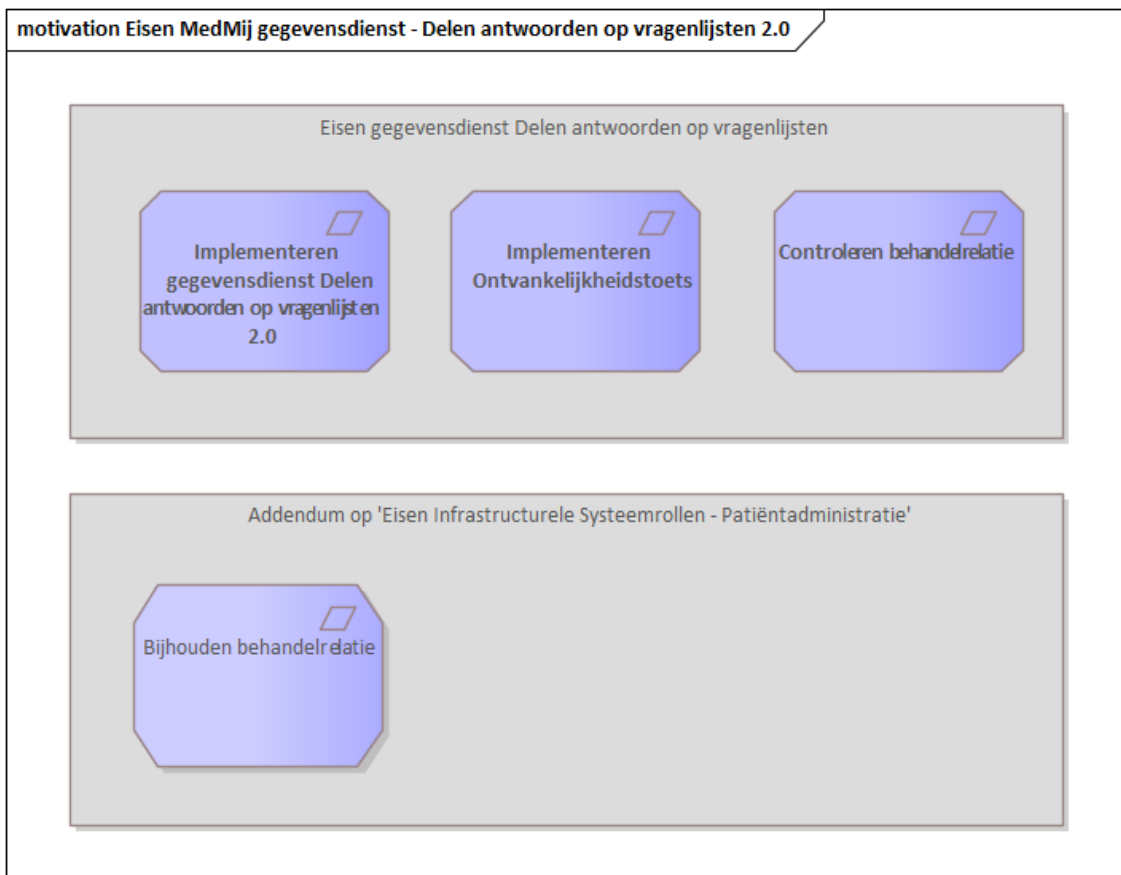


Figure 18 : Eisen MedMij gegevensdienst - Delen antwoorden op vragenlijsten 2.0

Implementeren gegevensdienst Delen antwoorden op vragenlijsten 2.0

Alias: GBZ.DAOV.e4020

Details

Eis:

Gegevensdienst Delen antwoorden op vragenlijsten 2.0 met gegevensdienstid 60, dient ondersteund te worden door het bronsysteem.

Toelichting bij eis:

De specificaties van de te implementeren interfaces zijn te vinden via

<https://vzvz.atlassian.net/wiki/display/MMCatalogus/Actuele+Catalogus>

Vzvz_Moscow: n/a

Vzvz_Req_Verificatie: Acceptatietest

Vzvz_Req_Soort: Functional

Vzvz_Req_Type: Product

Implementeren Ontvankelijkheidstoets**Alias:** GBZ.ONTV.e4010

Details

Eis:

Het XIS moet een ontvankelijkheidstoets-bericht kunnen ontvangen en beantwoorden. Hiervoor dient de implementatie gevolgd te worden zoals beschreven in de implementatiehandleiding van het ontvankelijkheidstoets-bericht.

Toelichting bij eis:

Momenteel wordt nog gewerkt aan de implementatiehandleiding voor de implementatie van het ontvankelijkheidstoets-bericht. Deze eis dient dan ook vooralsnog als 'kapstokkeis' en kan worden uitgebreid en/of aangescherpt.

Vzvv_Moscow: n/a**Vzvv_Req_Verificatie:** Acceptatietest**Vzvv_Req_Soort:** Functional**Vzvv_Req_Type:** Product**Controleren behandelrelatie****Alias:** GBZ.ONTV.e4020

Details

Eis:

Het systeem mag alleen gegevens ontvangen indien er in het patiëntadministrerende systeem een behandelrelatie met de patiënt staat geregistreerd.

Toelichting bij eis:

Er moet voorkomen worden, dat een patiënt onverhoopt gegevens stuurt naar een zorgaanbieder waar hij niet (meer) behandeld wordt.

Vzvv_Moscow: n/a**Vzvv_Req_Verificatie:** Acceptatietest**Vzvv_Req_Soort:** Functional**Vzvv_Req_Type:** Product**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:

3. begindatum;
4. UZI-nummer van de zorgverlener;
5. de URA van de zorgaanbieder ten behoeve van wie de behandelrelatie onderhouden wordt.

Een bestaande behandelrelatie beëindigen, waarbij wordt vastgelegd:

6. einddatum;
7. 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

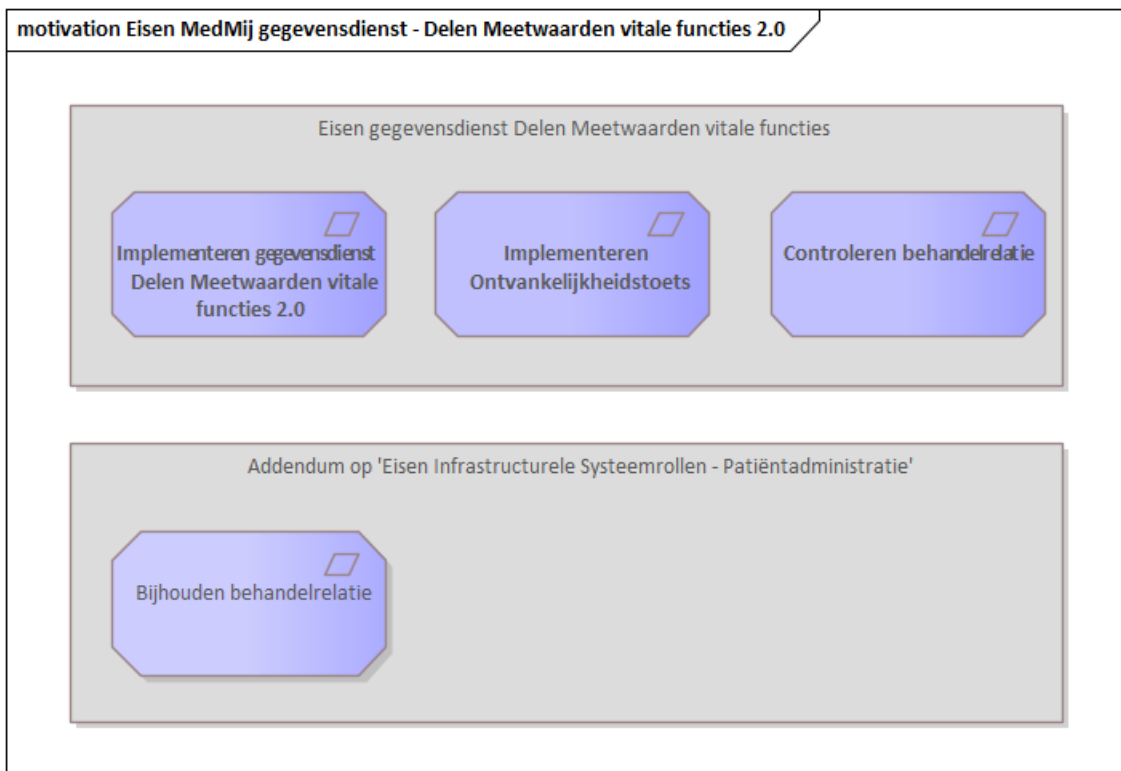


Figure 19 : Eisen MedMij gegevensdienst - Delen Meetwaarden vitale functies 2.0

Implementeren gegevensdienst Delen Meetwaarden vitale functies 2.0

Alias: GBZ.DMVF.e4010

Details

Eis:

Gegevensdienst Delen Meetwaarden vitale functies 2.0 met gegevensdienstid 53, dient ondersteund te worden door het bronsysteem.

Toelichting bij eis:

De specificaties van de te implementeren interfaces zijn te vinden via

<https://vzviz.atlassian.net/wiki/display/MMCatalogus/Actuele+Catalogus>

.

Vzviz_Moscow: n/a

Vzviz_Req_Verificatie: Acceptatietest

Vzviz_Req_Soort: Functional

Vzviz_Req_Type: Product

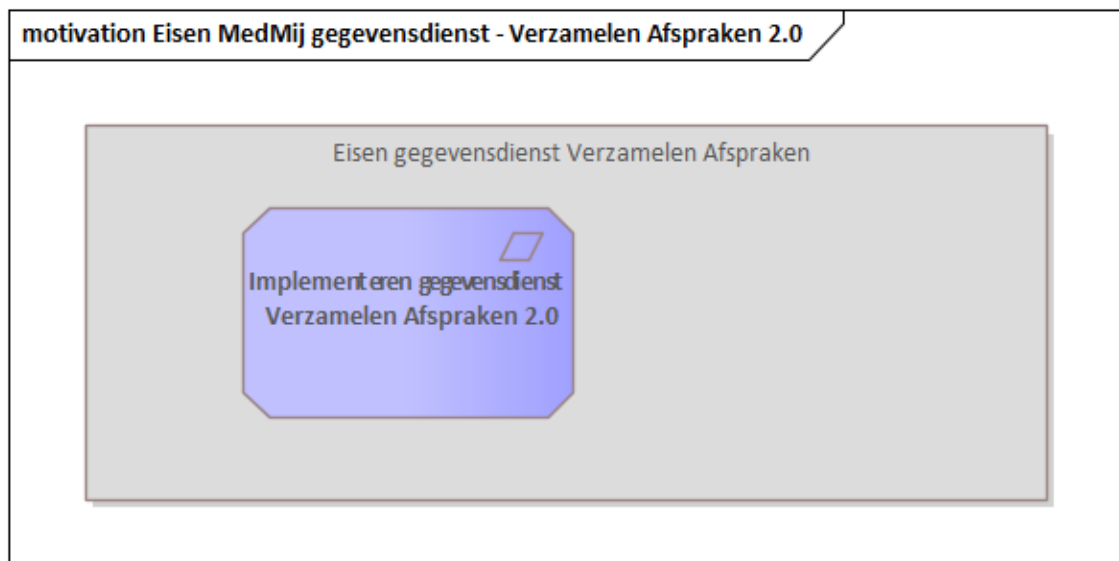


Figure 20 : Eisen MedMij gegevensdienst - Verzamelen Afspraken 2.0

Implementeren gegevensdienst Verzamelen Afspraken 2.0

Alias: GBZ.VAf.e4010

Details

Eis:

Gegevensdienst Verzamelen Afspraken 2.0 met gegevensdienstid 47, dient ondersteund te worden door het bronsysteem.

Toelichting bij eis:

De specificaties van de te implementeren interfaces zijn te vinden via

<https://vzvz.atlassian.net/wiki/display/MMCatalogus/Actuele+Catalogus>

Vzvz_Moscow: n/a

Vzvz_Req_Verificatie: Acceptatietest

Vzvz_Req_Soort: Functional

Vzvz_Req_Type: Product

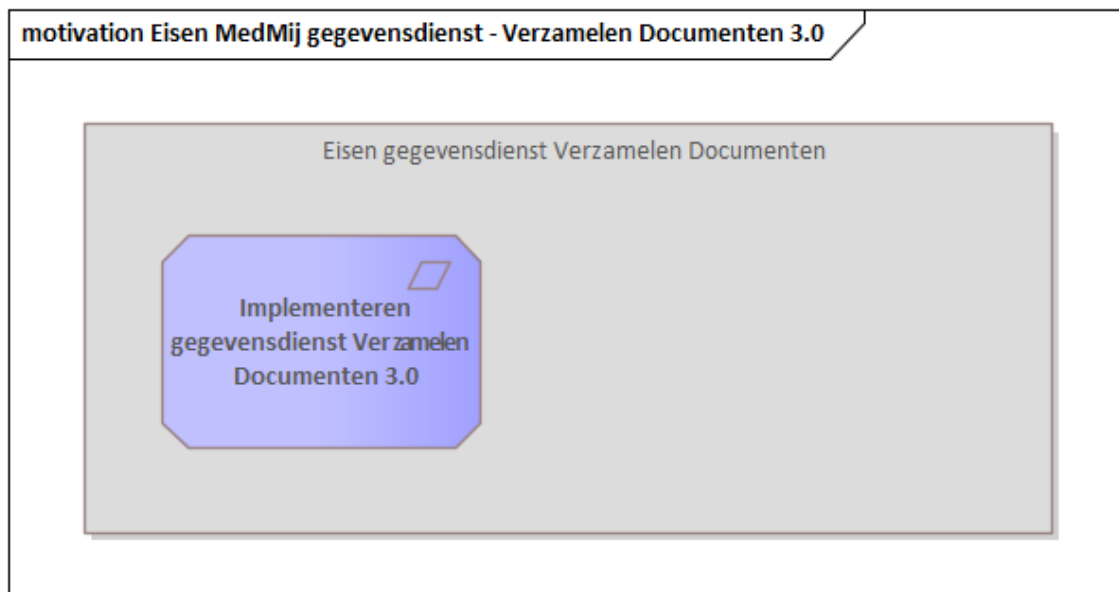


Figure 21 : Eisen MedMij gegevensdienst - Verzamelen Documenten 3.0

Implementeren gegevensdienst Verzamelen Documenten 3.0

Alias: GBZ.VDo.e4010

Details

Eis:

Gegevensdienst Verzamelen Documenten 3.0 met gegevensdienstid 51, dient ondersteund te worden door het bronsysteem.

Toelichting bij eis:

De specificaties van de te implementeren interfaces zijn te vinden via

<https://vzvz.atlassian.net/wiki/display/MMCatalogus/Actuele+Catalogus>

Vzvz_Moscow: n/a

Vzvz_Req_Verificatie: Acceptatietest

Vzvz_Req_Soort: Functional

Vzvz_Req_Type: Product

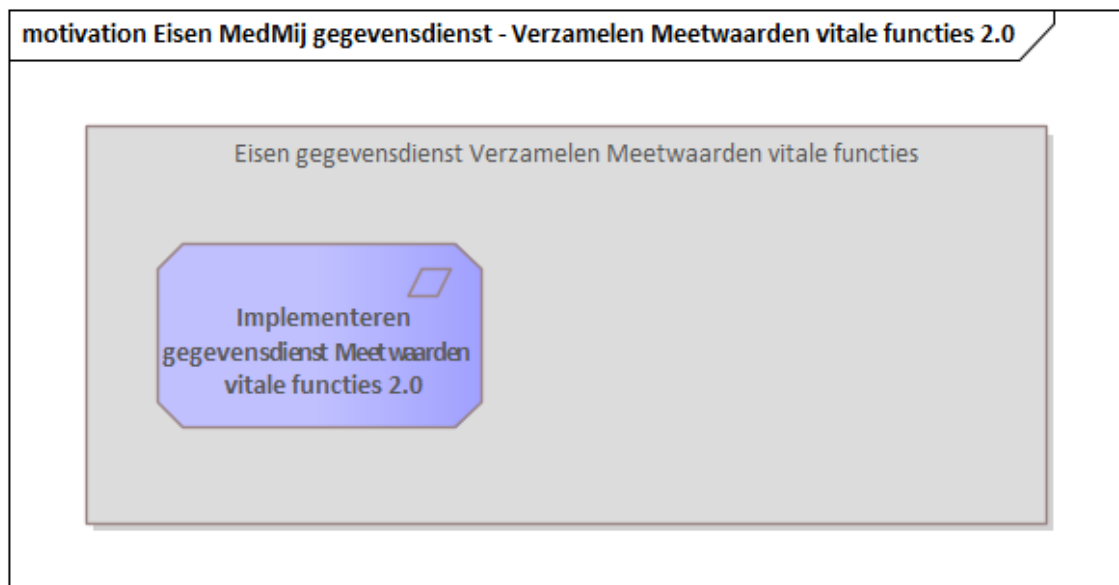


Figure 22 : Eisen MedMij gegevensdienst - Verzamelen Meetwaarden vitale functies 2.0

Implementeren gegevensdienst Meetwaarden vitale functies 2.0

Alias: GBZ.MVF.e4010

Details

Eis:

Gegevensdienst Delen Meetwaarden vitale functies 2.0 met gegevensdienstid 53, dient ondersteund te worden door het bronsysteem.

Toelichting bij eis:

De specificaties van de te implementeren interfaces zijn te vinden via

<https://vzvz.atlassian.net/wiki/display/MMCatalogus/Actuele+Catalogus>

Vzvz_Moscow: n/a

Vzvz_Req_Verificatie: Acceptatietest

Vzvz_Req_Soort: Functional

Vzvz_Req_Type: Product

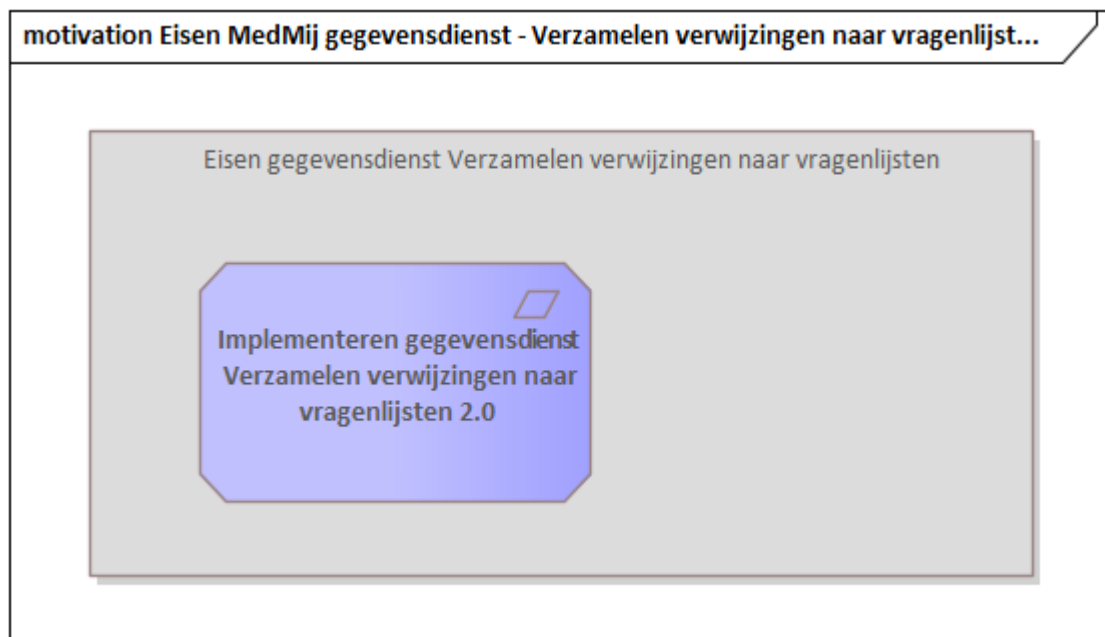


Figure 23 : Eisen MedMij gegevensdienst - Verzamelen verwijzingen naar vragenlijsten 2.0

Implementeren gegevensdienst Verzamelen verwijzingen naar vragenlijsten 2.0

Alias: GBZ.VVV.e4010

Details

Eis:

Gegevensdienst Verzamelen verwijzingen naar vragenlijsten 2.0 met gegevensdienstid 59, dient ondersteund te worden door het bronsysteem.

Toelichting bij eis:

De specificaties van de te implementeren interfaces zijn te vinden via

<https://vzvz.atlassian.net/wiki/display/MMCatalogus/Actuele+Catalogus>

Vzvz_Moscow: n/a

Vzvz_Req_Verificatie: Acceptatietest

Vzvz_Req_Soort: Functional

Vzvz_Req_Type: Product

End

8.5.2 MedMij HIS t.b.v. OPEN

8.5.2.1 PvE HIS tbv OPEN

Datum: 8-10-2025
Status: Definitief
Versie:
Classificatie: Openbaar
Revisie: 2.0

8.5.2.1.1 Documenthistorie

Documentversies

Datum	Status	Versie	Omschrijving
15 juni 2022	Definitief	1.0	Eerste opzet PvE Huisartsinformatiesysteem tbv Open
8-10-2025	Definitief	2.0	TLS-versies aangepast op basis van NCSC richtlijnen (2025-05)

Inhoudsopgave

Documenthistorie

[1 Inleiding \(see page 220\)](#)

[2 Eisen HIS t.b.v. OPEN \(see page 220\)](#)

[2.1 AORTA Eisen Infrastructurele Systeemrollen \(see page 220\)](#)

[2.1.1 Systeemrollen - Infrastructuur - Applicatiebeheer \(see page 220\)](#)

[2.1.2 Systeemrollen - Infrastructuur - Gegevens ontvangend systeem \(see page 227\)](#)

[2.1.3 Systeemrollen - Infrastructuur - Gegevens opleverend systeem \(see page 231\)](#)

[2.1.4 Systeemrollen - Infrastructuur - Patiëntadministratie \(see page 239\)](#)

[2.2 AORTA Eisen Kwaliteit Aangesloten Systemen \(see page 247\)](#)

[2.2.1 Genereren time-out \(see page 247\)](#)

[2.2.2 Tijdige verwerking van berichten \(see page 248\)](#)

[2.2.3 Borgen van minimale verwerkingssnelheid \(see page 248\)](#)

[2.2.4 Borgen van de betrouwbaarheid bij grote storingen \(see page 250\)](#)

[2.2.5 Borgen van de betrouwbaarheid bij kleine storingen \(see page 250\)](#)

[2.2.6 Minimaliseren van de impact van gepland onderhoud \(see page 251\)](#)

- 2.2.7 Borgen van de beschikbaarheid van een GBx (see page 251)
- 2.2.8 Beveiligde opslag (see page 253)
- 2.2.9 Een GBx beschikt over een geldig UZI/PKIO-servercertificaat (see page 254)
- 2.2.10 Borgen van plicht tot uitwisselen van patiëntgegevens (see page 254)
- 2.2.11 Beveiliging van patiëntgegevens in het GBx (see page 255)
- 2.2.12 Borgen betrouwbare koppeling tussen pas en applicatie (see page 255)
- 2.2.13 Aansluiting op productie-omgeving LSP (see page 258)
- 2.2.14 Tijdsynchronisatie GBx en ZIM (see page 258)
- 2.2.15 Gebruik van IP en DNS (see page 259)
- 2.2.16 Communicatie met het LSP via een GZN (see page 260)
- 2.3 AORTA Eisen Kwaliteit Applicatie (see page 260)
- 2.3.1 Toegangslog bijhouden (FHIR) (see page 260)
- 2.3.2 Hardening (see page 261)
- 2.3.3 Opzetten beveiligde verbinding vanuit de ZIM met een GBx (see page 262)
- 2.3.4 Opzetten en gebruiken van TLS-sessies (see page 263)
- 2.3.5 Instellen configuratieparameters t.b.v. communicatie en authenticatie van de ZIM (see page 263)
- 2.3.6 Bijhouden van een gebruikersregistratie (see page 264)
- 2.3.7 Opzetten beveiligde verbinding met de ZIM (see page 264)
- 2.3.8 Toegangslog bijhouden (see page 265)
- 2.3.9 Afbreken van een gebruikerssessie (see page 266)
- 2.3.10 Blokkeren van ingetrokken, verlopen en niet authentieke passen (see page 267)
- 2.3.11 Inloggen op vertrouwensniveau midden (see page 268)
- 2.3.12 Afhandelen transactietoken (see page 270)
- 2.3.13 Protocolstack voor gegevensuitwisseling o.b.v. FHIR (see page 270)
- 2.3.14 Kenbaar maken Certificate Authorities (see page 271)
- 2.3.15 Ondersteunen servercertificaten en ondertekeningalgoritmen (see page 271)
- 2.3.16 Bevorderen interoperabiliteit bij berichtuitwisseling (see page 272)
- 2.3.17 Juiste afhandeling van SOAP headers (see page 272)
- 2.3.18 Protocolstack voor berichtuitwisseling (see page 273)
- 2.4 AORTA Eisen Organisatie van een GBX (see page 274)
- 2.4.1 Afmelden patiënt na overlijden (see page 274)
- 2.4.2 Wijzigen logging (see page 275)
- 2.4.3 Vernietigen loggegevens (see page 275)
- 2.4.4 Uitschakelen logging (see page 276)
- 2.4.5 Toegangsbeheer tot logging (see page 276)
- 2.4.6 Loggen toegangsregeling (see page 277)
- 2.4.7 Loggen inzage logging (see page 277)
- 2.4.8 Bewaartermijn loggegevens (see page 278)
- 2.4.9 Voldoen aan wet- en regelgeving (see page 278)
- 2.4.10 Vernietigen materialen volgens standaarden (see page 279)
- 2.4.11 Een GBx valt onder Nederlandse wet- en regelgeving (see page 279)
- 2.4.12 Kennisvergaring m.b.t. GBX-beheer (see page 280)
- 2.4.13 Bijhouden van een beheerlog (see page 280)
- 2.4.14 Beperking inzage door beheerder (see page 281)
- 2.4.15 Actueel houden van het applicatieregister (see page 281)
- 2.4.16 Systeembeheer van een GBx (see page 282)
- 2.4.17 Beheren van en toegang verschaffen tot de toegangslog (see page 282)
- 2.4.18 Toekennen functiescheiding tussen systeemgebruikers (see page 283)
- 2.4.19 Verantwoordelijk UZI-pasbeleid (see page 283)

2.4.20 Instrueren systeemgebruikers over beveiligingsbeleid (see page 284)

2.4.21 Ondersteuning van gebruikers bij problemen met de landelijke uitwisseling van informatie (see page 284)

Section: Section1

8.5.2.1.2 Inleiding

End

Section: Section2

8.5.2.1.3 Eisen HIS t.b.v. OPEN

8.5.2.1.3.1 AORTA Eisen Infrastructurele Systeemrollen

Systeemrollen - Infrastructuur - Applicatiebeheer

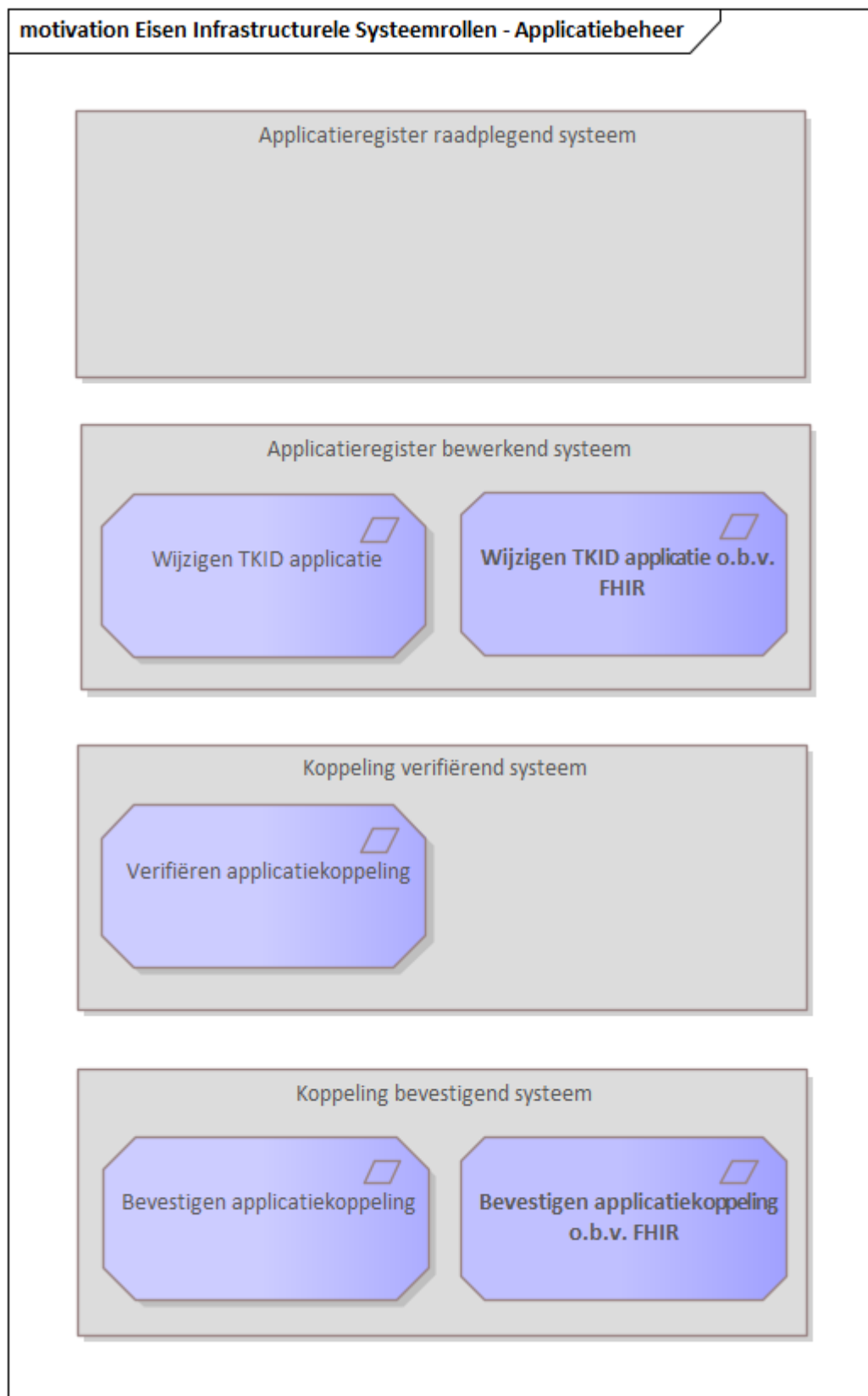


Figure 1 : Eisen Infrastructurele Systeemrollen - Applicatiebeheer

Bevestigen applicatiekoppeling o.b.v. FHIR**Alias:** GBX.APR.e4080

Details

Eis:

Het XIS moet een applicatiekoppelingverificatie-bericht kunnen ontvangen en/of versturen. Hiervoor dient de implementatie gevolgd te worden zoals beschreven in de implementatiehandleiding van het applicatiekoppelingverificatie-bericht.

Toelichting bij eis:

Momenteel wordt nog gewerkt aan de implementatiehandleiding voor de implementatie van het applicatiekoppelingverificatie-bericht.. Deze eis dient dan ook vooralsnog als 'kapstokkeis' en kan worden uitgebreid en/of aangescherpt.

Vzvv_Moscow: n/a**Vzvv_Req_Verificatie:** Acceptatietest**Vzvv_Req_Soort:** Functional**Vzvv_Req_Type:** Product**Wijzigen TKID applicatie o.b.v. FHIR****Alias:** GBX.APR.e4070.1

Details

Eis:

Het XIS moet op basis van het beherenTKID-bericht aangeven welke FHIR resources de bron kan opleveren en/of kan verwerken. Hiervoor dient de implementatie gevolgd te worden zoals beschreven in de implementatiehandleiding van het TKID-bericht.

Toelichting bij eis:

Momenteel wordt nog gewerkt aan de implementatiehandleiding voor de implementatie van het TKID-bericht. Deze eis dient dan ook vooralsnog als 'kapstokkeis' en kan worden uitgebreid en/of aangescherpt.

Vzvv_Moscow: n/a**Vzvv_Req_Verificatie:** Acceptatietest**Vzvv_Req_Soort:** Functional**Vzvv_Req_Type:** Product**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](#).⁹¹

Interacties

Het systeem stuurt een verifiërenApplicatiekoppelingAntwoord terug naar de verzender conform [IH AORTA](#).⁹²

Resultaat

Het antwoordbericht is teruggestuurd naar de verzender.

Uitzonderingen

Uitzonderingen zijn beschreven in de [Foutentabel](#)⁹³.

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

Verifiëren applicatiekoppeling

Alias: GBX.APR.e4140

Details

91. <https://decor.nictiz.nl/pub/vzvv/aorta-vzvv-html-20200821T140325/>

92. <https://decor.nictiz.nl/pub/vzvv/aorta-vzvv-html-20200821T140325/>

93. <https://www.aorta-lsp.nl/media/downloads/foutentabel-aorta-v8200xlsx/download>

Beginsituatie

De gebruiker is lokaal ingelogd op vertrouwensniveau laag of hoger.

Trigger

De gebruiker initieert de functie via het systeem.

Interacties

1. Het systeem verzendt en verifiërenApplicatiekoppeling bericht naar de ZIM of een ander GBX conform [IH APR](#)⁹⁴.
2. Het systeem ontvangt een verifiërenApplicatiekoppelingAntwoord bericht conform [IH APR](#)⁹⁵.

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](#)⁹⁶.

Opties

Het bericht moet een authenticatietoken kunnen bevatten.

Responsetijd

-

Betrouwbaarheid

Garantie geven dat versturen van gegevens niet zonder kennisgeving gestaakt wordt

Toelichting

-

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

Wijzigen TKID applicatie

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

Details

94. <https://decor.nictiz.nl/pub/vzvv/aorta-vzvv-html-20200821T140325/>

95. <https://decor.nictiz.nl/pub/vzvv/aorta-vzvv-html-20200821T140325/>

96. <https://www.aorta-lsp.nl/media/downloads/foutentabel-aorta-v8200xlsx/download>

Beginsituatie

De gebruiker is lokaal ingelogd op vertrouwensniveau laag of hoger.

Trigger

De gebruiker initieert de functie via het systeem.

Interacties

1. Het systeem verzendt een *beherenTKID*-bericht naar de ZIM conform [HL7v3 IH APR](#)⁹⁷.
2. Het systeem ontvangt een ontvangstbevestiging conform [HL7v3 IH APR](#)⁹⁸.

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**

97. https://www.aortadocumentatie.nl/Documenten/AORTA_ApBh_IH_Applicatieregister_HL7.pdf

98. https://www.aortadocumentatie.nl/Documenten/AORTA_ApBh_IH_Applicatieregister_HL7.pdf

-

Toelichting

De logische attributen van dit bericht zijn te vinden in het [Ontwerp Applicatieregister](#)⁹⁹.

Vanuit het XIS-acceptatieproces wordt er een typekwalificatied (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 interactied's gekoppeld. Een zorgaanbiederapplicatie (een bij de zorgaanbieder geïnstalleerde versie van een XIS-applicatie) kan meerdere TKID's ondersteunen. Zie het [ONTW APR](#)¹⁰⁰ 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](#)¹⁰¹) 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).

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

99. https://www.vzvv.nl/uploaded/FILES/htmlcontent/AORTA2015/AORTA_ApBh_Ontw_Applicatieregister.pdf

100. <https://www.aorta-lsp.nl/media/downloads/ontwerp-applicatieregister-aorta-v8200pdf/download>

101. <https://www.aorta-lsp.nl/media/downloads/foutentabel-aorta-v8200xlsx/download>

Vz vz_Req_Type: Product

Systemrollen - Infrastructuur - Gegevens ontvangend systeem

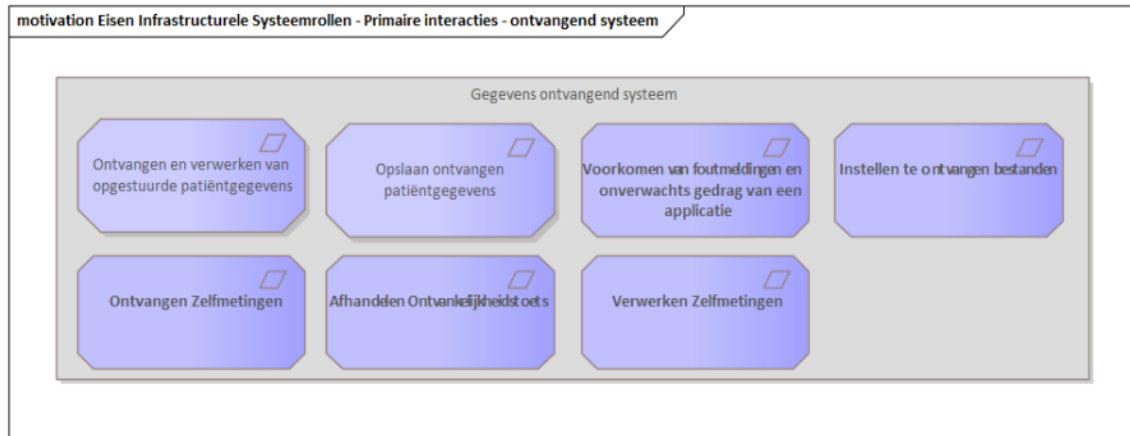


Figure 2 : Eisen Infrastructurele Systemrollen - Primaire interacties - ontvangend systeem

Voorkomen van foutmeldingen en onverwachts gedrag van een applicatie

Alias: GBX.OPV.e4190

Details

Eis:

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

Toelichting:

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

Vz vz_Moscow: Verplicht

Vz vz_Req_Verificatie: Acceptatietest

Vz vz_Req_Soort: Functional

Vz vz_Req_Type: Product

Opslaan ontvangen patiëntgegevens

Alias: GBX.STU.e4520

Details

Eis:

Wanneer patiëntgegevens, die conform [Ontvangen en verwerken van opgestuurde patiëntgegevens](#) (see page 228) 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.

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

Ontvangen en verwerken van opgestuurde patiëntgegevens

Alias: GBX.STU.e4510

Details

Conditities

•

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 [AORTA_Wrp_IH_Berichtwrappers_HL7](#)¹⁰².

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 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.

Vz vz_Moscow: Verplicht

Vz vz_Req_Verificatie: Acceptatietest

Vz vz_Req_Soort: Functional

Vz vz_Req_Type: Product

Ontvangen Zelfmetingen

Alias: GBX.ONT.e4170

Details

102. https://www.aortadocumentatie.nl/Documenten/AORTA_Wrp_IH_Berichtwrappers_HL7.pdf

Eis:

Het systeem moet delenZelfmetingen (ZTSM_IN000004NL01) kunnen verwerken en na ontvangst een Accept Acknowledgement (MCCI_IN000002) terugsturen.

Toelichting bij eis:

DelenZelfmetingen wordt verstuurd vanuit een PGO aan een HIS. Het HIS dient de zelfmetingen in zijn systeem te kunnen verwerken. Na ontvangst van delenZelfmetingen dient de HIS een accept acknowledgement terug te sturen.

De specificatie van delenZelfmetingen is opgenomen in de art-decorpublicatie van de specifieke zorgtoepassing.

Vzvv_Moscow: n/a

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

Afhandelen Ontvankelijkheidstoets

Alias: GBX.OPV.e4220

Details

Eis:

Het XIS dient het antwoord op de ontvankelijkheidstoets te baseren op:

- de leeftijd van de patiënt; de patiënt moet 16 jaar of ouder zijn;
- aanwezigheid van een geregistreerde behandelrelatie met de patiënt; er dient een behandelrelatie te zijn met een patiënt om zijn gegevens te mogen ontvangen;
- {optioneel} de zelfmetinginstelling van de zorgverlener; de zorgverlener moet expliciet aangeven of het open staat om gegevens van een specifieke patiënt te ontvangen (zie eis GBX.OPV.e4210).

Toelichting bij eis:

Om zelfmetingen te mogen ontvangen dienen aan een aantal randvoorwaarden te worden voldaan. Deze randvoorwaarden dienen gecontroleerd te worden op het moment dat een ontvankelijkheidstoets wordt ontvangen. Afhankelijk van de uitkomsten van de controle van de randvoorwaarden, dient er een positief of negatief antwoord verstuurd te worden.

Vzvv_Moscow: n/a

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

Verwerken Zelfmetingen

Alias: GBX.OPV.e4230

Details

Eis:

Zelfmetingen die ontvangen zijn na een positieve ontvankelijkheidstoets dienen verwerkt en opgeslagen te kunnen worden in het XIS van de zorgaanbieder. Overige zelfmetingen dienen door het XIS geweigerd te worden.

Toelichting bij eis:

Verwerking en opslaan van zelfmetingen houdt in ieder geval in dat zelfmetinggegevens opgeslagen moeten kunnen worden en door een zorgverlener op een later moment in de tijd inzichtelijk gemaakt kan worden. Hierbij dient rekening te worden gehouden met de eisen zoals beschreven in het Normenkader-ICT-basiseisen-OPEN-02-2021.

Deze eis zegt verder niets over de logica hoe verder om te moeten gaan met deze gegevens.

Vzvv_Moscow: n/a

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

Instellen te ontvangen bestanden

Alias: GBX.OPV.e4210

Details

Eis:

Een zorgverlener moet in zijn XIS kunnen aangeven of het zelfmetingen van een specifieke patiënt wil ontvangen.

Toelichting bij eis:

Het is denkbaar dat een zorgverlener alleen maar zelfmetingen wil ontvangen van die patiënten, waarmee hij een bepaalde behandelafpraak heeft gemaakt. Het moet mogelijk zijn om in het XIS per patiënt aan te geven of het ontvangen zelfmetingen moet gaan verwerken.

Het is denkbaar dat er in de toekomst nog meer gegevens kunnen worden verstuurd met als afzender de patiënt. Er zou dus al nagedacht kunnen worden over een generieke oplossing.

Vzvv_Moscow: n/a

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

Systeemrollen - Infrastructuur - Gegevens opleverend systeem

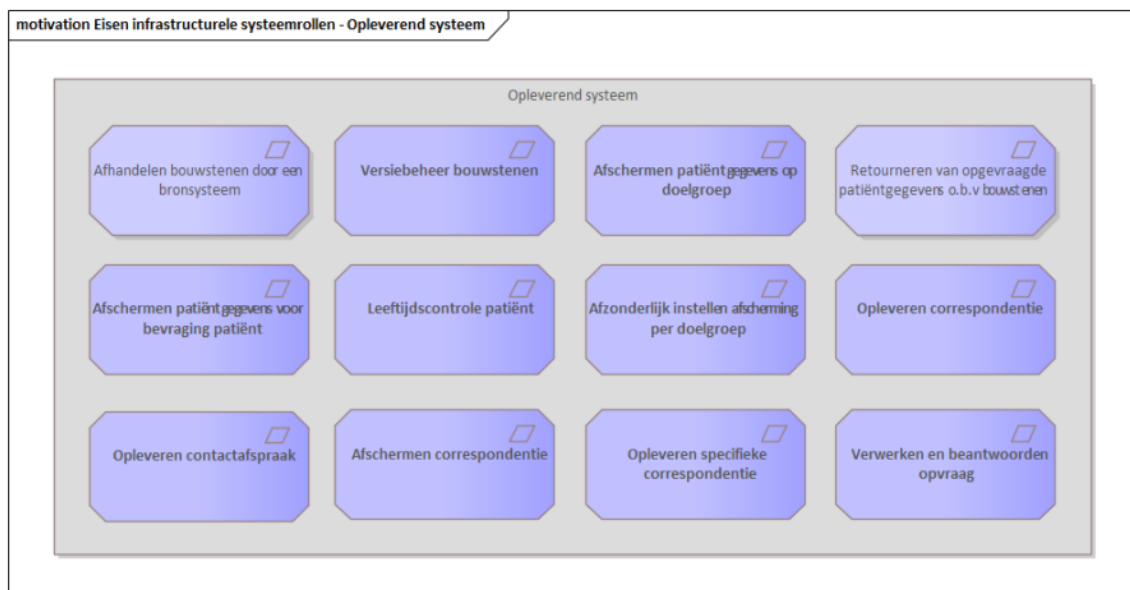


Figure 3 : Eisen infrastructurele systeemrollen - Opleverend systeem

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: n/a

Vzvz_Req_Verificatie: Acceptatietest

Vzvz_Req_Soort: Functional

Vzvz_Req_Type: Product

Opleveren specifieke correspondentie

Alias: GBX.OPV.e4640

Details

Eis:

Het bronsysteem moet, voor zover van toepassing binnen de applicatie, minimaal de volgende correspondentie kunnen opleveren:

- Specialistenberichten (ontvangen als MedSpe berichten);
- Radiologieberichten (ontvangen als MedRad berichten);
- Verwijsbrieven.

De hierboven genoemde correspondentie dient in één van de onderstaande MIME types opgeleverd te worden:

- application/pdf;
- application/msword;
- application/vnd.openxmlformats-officedocument.wordprocessingml.document;
- text/plain
- application/rtf.

Toelichting bij eis:

De in deze eis benoemde correspondentie betreft een minimale lijst. Een bronsysteem is in principe niet beperkt tot het soort correspondentie dat het mag opleveren. Voor andere dan in de eis genoemde soorten correspondentie geldt niet de verplichting om op te leveren in één van de genoemde MIME types.

MedMij vereist dat correspondentie wordt opgeleverd aan een PGO o.b.v. de standaard PDF/A. Om bronsystemen te ontlasten biedt LSP+ de functionaliteit om de in de eis beschreven MIME types te vertalen naar de PDF/A standaard.

Conditie:

- Indien een bronsysteem correspondentie beschikbaar stelt t.b.v. LSP+, dan geldt deze eis;
- Indien een bronsysteem wil voldoen aan de OPEN vereisten.

Vzvz_Moscow: n/a

Vzvz_Req_Verificatie: Acceptatietest

Vzvz_Req_Soort: Functional

Vzvz_Req_Type: Product

Afschermen correspondentie

Alias: GBX.OPV.e4650

Details

Eis:

Correspondentie moet kunnen worden afgeschermd op basis van een bepaalde tijdsperiode. Hierdoor moet het voor de systeemgebruiker mogelijk worden om alleen gegevens beschikbaar te stellen die zijn opgenomen na een specifieke datum.

Het afschermen op basis van een bepaalde tijdsperiode moet mogelijk zijn voor:

- de gehele patiëntenpopulatie als geheel;
- per individuele patiënt.

Toelichting bij eis:

De NHG heeft een richtlijn 'Online inzage in het H-EPD door patiënt' opgesteld voor het beschikbaar stellen van patiëntgegevens t.b.v. de patiënt. Eén van de voorwaarden die is opgenomen in de richtlijn dient ingebouwd te worden in de XIS-applicaties die dienen als bronsysteem voor correspondentie. Het gaat er hierbij expliciet om dat een gebruiker de mogelijkheid krijgt om alleen correspondentie beschikbaar te stellen vanaf 1 juli 2020. Indien een gebruiker dat wenst, moeten ook eerder verkregen correspondentie beschikbaar gesteld kunnen worden.

Conditie:

- Indien een bronsysteem correspondentie beschikbaar stelt t.b.v. LSP+, dan is deze eis verplicht;
- Indien een bronsysteem wil voldoen aan de OPEN vereisten.

Vzvv_Moscow: n/a

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

Versiebeheer bouwstenen

Alias: GBX.OPV.e4580

Details**Eis:**

Bronsystemen, die bevraagd worden voor bouwsteentypes, dienen de bouwsteeninstanties die opgeleverd worden altijd zo volledig mogelijk te vullen met informatie. Hierbij dient het bronsysteem alle velden altijd met indien mogelijk alle waardes die beschikbaar zijn te vullen.

Toelichting:

Om succesvol bouwstenen te kunnen uitwisselen moet er een versiebeheer mechanisme worden toegepast. Dit versiebeheer mechanisme verplicht opleverende systemen alle velden die zij kunnen vullen te vullen met waardes. Hierdoor zijn opleverende systemen ontkoppeld van de context of toepassing waarin de opvrager een vraag stelt via AORTA.

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

Leeftijdscontrole patiënt**Alias:** GBX.OPV.e4570

Details
Eis: Indien de opvrager een patiënt is, dan dient het systeem te controleren of de leeftijd van de persoon van wie gegevens worden opgevraagd minimaal 16 jaar is. Indien de opvrager jonger is dan 16 jaar, dan dient het systeem de opvraag te beantwoorden met een foutmelding (PATLFT). Toelichting bij eis: Een patiënt jonger dan 16 jaar is niet gerechtigd om zijn eigen gegevens op te vragen zonder toestemming van bijvoorbeeld een ouder of voogd. Op dit moment is het voor een patiënt niet mogelijk om een opvraag te doen onder mandaat. 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**Afschermen patiëntgegevens voor bevraging patiënt****Alias:** GBX.OPV.e4537

Details
Eis: Afscherming van patiëntgegevens voor bevraging door een patiënt moet op dossierniveau kunnen worden ingesteld door de zorgverlener. Toelichting bij eis: Naast de aggregatieniveaus die zijn beschreven in de domeinspecificaties (zoals beschreven in eis Afschermen van patiëntgegevens) dient het mogelijk te zijn om op verzoek van een patiënt of op inzicht van een zorgverlener het complete dossier af te schermen voor bevraging door een patiënt. Het afschermen van patiëntgegevens voor een patiënt is niet gebonden aan het afschermen van patiëntgegevens voor een zorgverlener (en vice versa).

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

Afschermen 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 Afschermen van patiëntgegevens .

Vzvv_Moscow: Verplicht**Vzvv_Req_Verificatie:** Acceptatietest**Vzvv_Req_Soort:** Functional**Vzvv_Req_Type:** Product**Afhandelen bouwstenen door een bronsysteem****Alias:** GBX.OPV.e4514

Details
Eis: Een XIS dat bouwsteentypen oplevert, moet van die bouwsteentypen alle mogelijke bouwsteeninstantiaties kunnen opleveren. Toelichting bij eis: Een zorgtoepassing bepaalt welke context(en) er opgevraagd kunnen worden. Er dienen gehele bouwstenen afgehandeld te kunnen worden en niet alleen de specifieke bouwsteeninstantiaties zoals beschreven in de zorgtoepassing. Dit is van belang om eventuele compatibiliteit met andere zorgtoepassingen te kunnen garanderen. Daarnaast leiden eventuele aanpassingen in de SDS tabellen niet noodzakelijk tot wijzigingen bij het bronsysteem. Deze eis garandeert snellere doorlooptijden aan de kant van een XIS met betrekking tot de implementatie van nieuwe zorgtoepassingen en/of wijzigingen aan de SDS.

Vzvv_Moscow: Verplicht**Vzvv_Req_Verificatie:** Acceptatietest**Vzvv_Req_Soort:** Functional**Vzvv_Req_Type:** Product**Retourneren van opgevraagde patiëntgegevens o.b.v bouwstenen****Alias:** GBX.OPV.e4513.2

Details

Beginsituatie

1. Het reagerende systeem beschikt over de voor deze functie vereiste vertrouwensmiddelen.
2. Het reagerende systeem heeft de opgevraagde patiëntgegevens aangemeld bij de VWI.
3. Voor de op te leveren patiëntgegevens is sprake van een definitieve koppeling met BSN.
4. Er is een opt-in geregistreerd in het systeem.

Trigger

Het systeem ontvangt een opvragenBouwsteeninstantiaties-bericht

Interacties

Het systeem retourneert een opleverenBouwsteeninstantiaties-bericht, zoals beschreven in de eisen aan de concrete systeemrol.

Resultaat

Het bericht is afgehandeld en de opgevraagde gegevens zijn, indien toegestaan, binnen de gestelde responstijd geretourneerd.

Uitzonderingen

Uitzonderingen zijn beschreven in de Foutentabel.

Opties

Het retourbericht bevat alle, in het systeem aanwezige, vrijgegeven patiëntgegevens, die voldoen aan de criteria die zijn meegegeven in het opvragenBouwsteeninstantiaties-bericht. Dit kunnen criteria zijn die zijn overgenomen uit het opvragenPatiëntgegevensContext-bericht (vraagparameters) of door het LSP zijn bepaald (selectieparameters) en toegevoegd aan het opvragenBouwsteeninstantiaties-bericht. De criteria zijn beschreven in de eisen aan de zorgtoepassingen.

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 opvragenBouwsteeninstantiaties-bericht moet rekening gehouden worden met dat dit gebeurt vòòr het tijdstip dat in het bericht is meegegeven (uiterste-oplevertijd-gbz). 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 gbx-opleversnelheid kilobytes aan berichtinhoud per seconde te retourneren.

Toelichting

-

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

Opleveren correspondentie

Alias: GBX.OPL.e4130

Details	
Eis: Het XIS moet een opvraag correspondentie (QUCO_IN990001NL01) kunnen ontvangen en verwerken. Op basis van deze opvraag dient het XIS een antwoord correspondentie (QUCO_IN990003NL01) te versturen. Toelichting bij eis: <ac:structured-macro ac:name="unmigrated-wiki-markup" ac:schema-version="1" ac:macro-id="ccbc0250-82f8-4e4e-9651-89df57eb8b83"><ac:plain-text-body><![CDATA[Het is mogelijk dat de opvraag specifieke parameters bevat. Het XIS moet op basis van het ontvangen bericht met de daarin opgenomen parameters een antwoord samenstellen. Zowel het binnenkomende opvraagbericht als het uitgaande antwoordbericht staan uitgewerkt in [Art-Decor].]]></ac:plain-text-body></ac:structured-macro> <ac:structured-macro ac:name="unmigrated-wiki-markup" ac:schema-version="1" ac:macro-id="a1157966-ed45-4036-935a-431d0d4720d6"><ac:plain-text-body><![CDATA[Indien bij het verwerken van het binnenkomende opvraagbericht een fout optreedt of een andere reden waarom het opvraagbericht niet verwerkt kan worden, dan dient er een (fout)melding geretourneerd te worden volgens de [Foutentabel].]]></ac:plain-text-body></ac:structured-macro>	]]></ac:plain-text-body></ac:st

Vzvv_Moscow: n/a

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

Opleveren contactafpraak

Alias: GBX.OPL.e4170

Details	
Eis: Het XIS moet een opvraag contactafpraak (QUAF_IN990001NL01) kunnen ontvangen en verwerken. Op basis van deze opvraag dient het XIS een antwoord contactafpraak (QUAF_IN990003NL01) te versturen. Toelichting bij eis: <ac:structured-macro ac:name="unmigrated-wiki-markup" ac:schema-version="1" ac:macro-id="2d9760ad-7604-41a9-89d8-59ced736b087"><ac:plain-text-body><![CDATA[Het is mogelijk dat de opvraag specifieke parameters bevat. Het XIS moet op basis van het ontvangen bericht met de daarin opgenomen parameters een antwoord samenstellen. Zowel het binnenkomende opvraagbericht als het uitgaande antwoordbericht staan uitgewerkt in [Art-Decor].]]></ac:plain-text-body></ac:structured-macro> <ac:structured-macro ac:name="unmigrated-wiki-markup" ac:schema-version="1" ac:macro-id="813b09fc-4294-4bef-bf55-52a3fd322ea2"><ac:plain-text-body><![CDATA[Indien bij het verwerken van het binnenkomende opvraagbericht een fout optreedt of een andere reden waarom het opvraagbericht niet verwerkt kan worden, dan dient er een (fout)melding geretourneerd te worden volgens de [Foutentabel].]]></ac:plain-text-body></ac:structured-macro>	

Vzvv_Moscow: n/a

Vzvvz_Req_Verificatie: Acceptatietest**Vzvvz_Req_Soort:** Functional**Vzvvz_Req_Type:** Product**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.

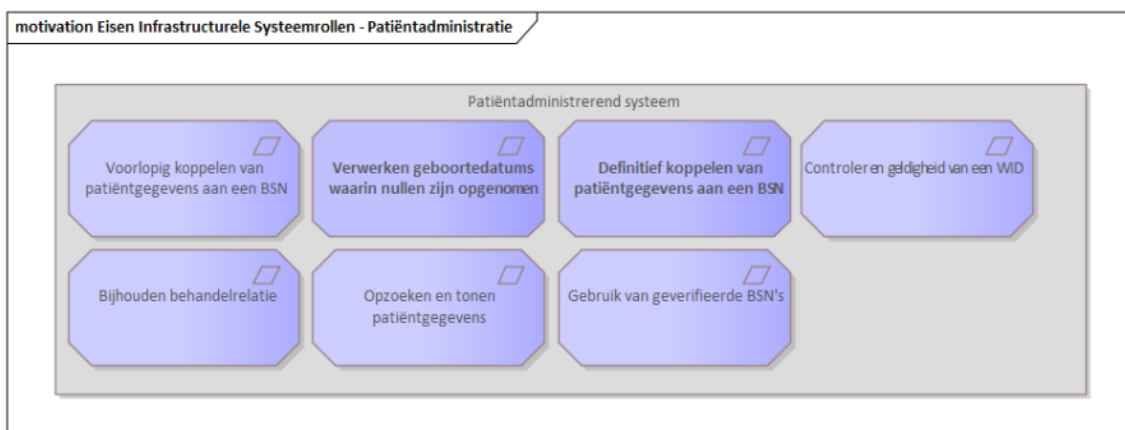
Vzvvz_Moscow: Conditioneel**Vzvvz_Req_Verificatie:** Acceptatietest**Vzvvz_Req_Soort:** Functional**Vzvvz_Req_Type:** Product**Systeemrollen - Infrastructuur - Patiëntadministratie**

Figure 4 : Eisen Infrastructurele Systeemrollen - Patiëntadministratie

Gebruik van geverifieerde BSN's**Alias:** GBX.IDA.e4060.1

Details

Eis:

Het systeem moet aan [Opzoeken en tonen patiënteninformatie](#) (see page 240), [Voorlopig koppelen van patiëntgegevens aan een BSN](#) (see page 245), [Controleren geldigheid van een WID](#) (see page 242), en [Bijhouden behandelrelatie](#) (see page 241) 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

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: n/a

Opzoeken en tonen patiëntgegevens

Alias: GBX.IDA.e4010.1

Details

Eis:

Het systeem moet een gebruiker de mogelijkheid bieden een patiënt op te zoeken in de lokale patiëntadministratie van de zorgaanbieder, door het invoeren van identificerende gegevens, waarna wordt getoond:

1. of de patiënt/cliënt is gevonden, en zo ja
2. of het BSN wel/niet is opgevraagd of geverifieerd bij de SBV-Z
3. de datum en tijd van koppelen
4. de manier van vaststellen van de identiteit:
 - Controle van echtheid en geldigheidsdatum van WID en de gelijkenis van de in de WID genoemde identificerende gegevens
 - Vergewissen,
 - ☒ indien beschikbaar het UZI-nummer of anders een unieke identificatie van de gebruiker en het UZI-nummer van mandaterende zorgverlener indien van toepassing
 - ☒ in geval van WID-controle: aard en nummer van het WID.

Toelichting bij eis:

Deze eis voorkomt dat de SBV-Z telkens opnieuw wordt geraadpleegd.

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

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:

3. begindatum;
4. UZI-nummer van de zorgverlener;
5. de URA van de zorgaanbieder ten behoeve van wie de behandelrelatie onderhouden wordt.

Een bestaande behandelrelatie beëindigen, waarbij wordt vastgelegd:

6. einddatum;
7. 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

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

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,
 2. Datum en tijd van vaststellen,
 3. 2. indien beschikbaar het UZI-nummer of anders een unieke identificatie van de gebruiker, en het UZI-nummer van mandaterende zorgverlener indien van toepassing.
 4. zorgaanbieder-id van de gebruiker;
 5. 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.

```
<ac:structured-macro ac:name="unmigrated-wiki-markup" ac:schema-version="1" ac:macro-id="f2c2a335-529c-4d4c-b43e-b16fec91add8"><ac:plain-text-body><![CDATA[Merk op dat de toelichting op [Bbsn-z] artikel 26 een grote verantwoordelijkheid legt bij de zorgaanbieder voor de afweging wel/niet WID controleren. Daarom is geautomatiseerde ondersteuning belangrijk. ]^103></ac:plain-text-body></ac:structured-macro>
```

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

103. <https://vzvv.atlassian.net/wiki/pages/createpage.action?spaceKey=A8&title=Merk+op+dat+de+toelichting+op+%5BBbsn-z%5D+artikel+26+een+grote+verantwoordelijkheid+legt+bij+de+zorgaanbieder+voor+de+afweging+wel%2Fniet+WID+controleren.+Daarom+is+geautomatiseerde+ondersteuning+belangrijk.+%5C%5D>

Vzvv_Req_Soort: Functional**Vzvv_Req_Type:** Product**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**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

8.5.2.1.3.2 AORTA Eisen Kwaliteit Aangesloten Systemen

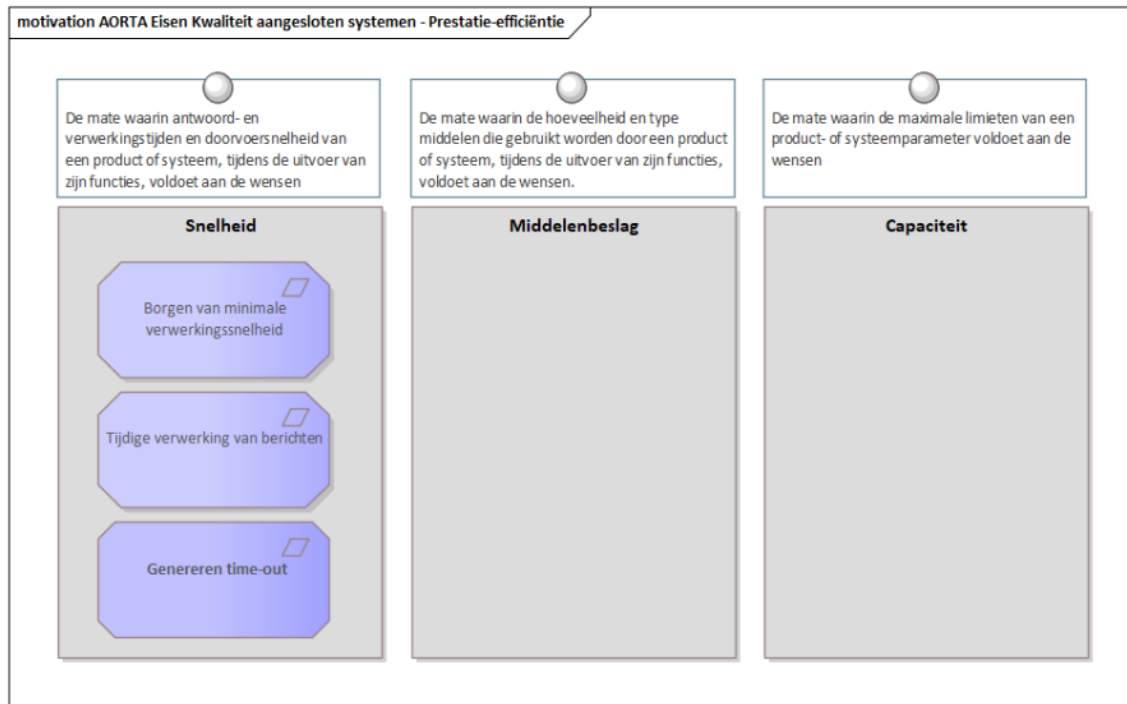


Figure 5 : AORTA Eisen Kwaliteit aangesloten systemen - Prestatie-efficiëntie

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. Vooralsnog blijft de waarde zoals opgenomen in deze eis gehandhaafd. Het DVZA zal in dat geval na 60 seconden een time-out versturen naar het PGO.

Vzvv_Moscow: n/a**Vzvv_Req_Verificatie:** Acceptatietest**Vzvv_Req_Soort:** Functional**Vzvv_Req_Type:** Product**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**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 <GBx-verwerkingssnelheid-sturen>

Opvragen van gegevens <GBx-verwerkingssnelheid-opvragen>

Een GBx dient een zodanige capaciteit te hebben voor het beantwoorden en ontvangen van berichten van de ZIM dat het kan voldoen aan de gestelde verwerkingssnelheden. Indien dat als gevolg van een onverwacht hoge piekbelasting tijdelijk niet mogelijk is, dan prevaleren de eisen inzake beschikbaarheid boven de eisen inzake verwerkingssnelheid.

Toelichting bij eis:

Deze eis is nodig opdat een XIS-applicatie tijdig berichten van de ZIM kan verwerken/beantwoorden ten behoeve van andere zorgaanbieders, ook als de belasting zodanig hoog is, dat de volgende berichten binnenkomen terwijl de vorige nog niet verwerkt/beantwoord zijn.

Deze eis betekent voor de organisatie dat de applicatie is geïnstalleerd op ICT-voorzieningen met voldoende capaciteit om een variabele belasting van berichten vanwege de ZIM te kunnen verwerken. Omdat de exacte belasting per GBx flink kan verschillen moet iedere organisatie zelf een inschatting maken van de benodigde capaciteit en ervoor zorgen dat het GBx die belasting aankan.

De waarden <GBx-verwerkingssnelheid-sturen> en <GBx-verwerkingssnelheid-opvragen> kunnen verschillen per gebruikte technologie. Voor de HL7v3-berichten gelden de waarden zoals opgenomen in de het configuratieinstellingendocument. 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.

Vz vz_Moscow: Verplicht

Vz vz_Req_Verificatie: Monitoring

Vz vz_Req_Soort: Non-Functional

Vz vz_Req_Type: Product

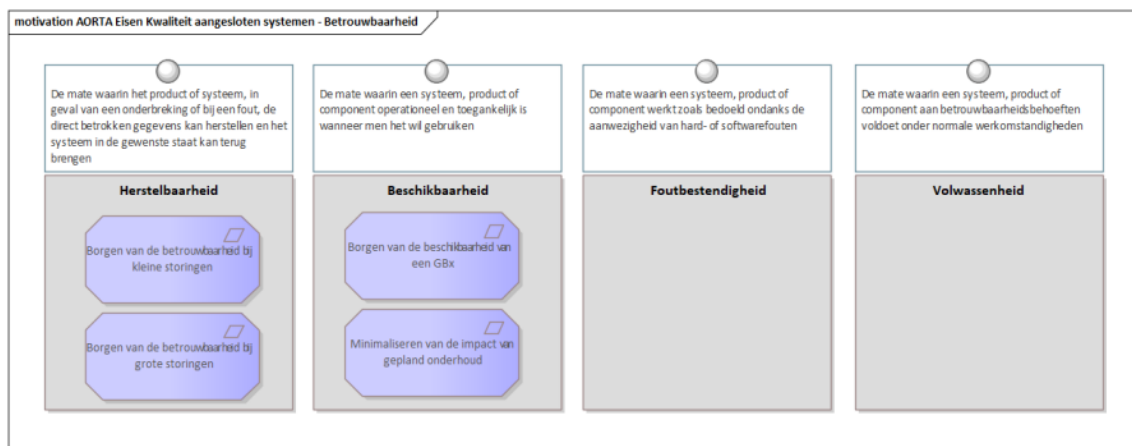


Figure 6 : AORTA Eisen Kwaliteit aangesloten systemen - Betrouwbaarheid

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

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**Vzvv_Req_Type:** Product**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. <ac:structured-macro ac:name="unmigrated-wiki-markup" ac:schema-version="1" ac:macro-id="d3ac455e-4a17-4530-974d-d745dbf01642"><ac:plain-text-body><![CDATA[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.	]]></ac:plain-text-body></ac:structured-macro>

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

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.

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

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.

Vz vz_Moscow: Verplicht (Must)

Vz vz_Req_Verificatie: Monitoring

Vz vz_Req_Soort: Non-Functional

Vz vz_Req_Type: Product

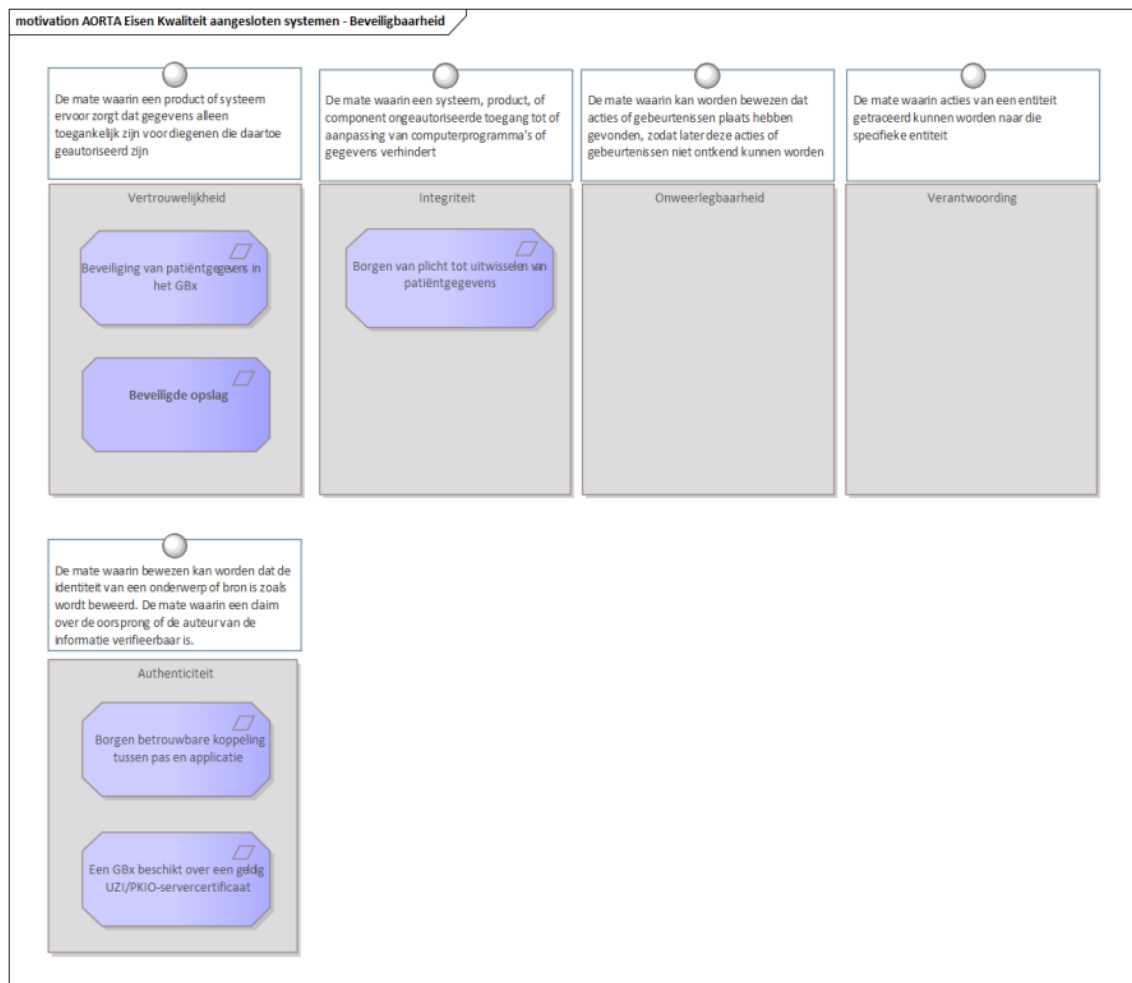


Figure 7 : AORTA Eisen Kwaliteit aangesloten systemen - Beveiligbaarheid

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.

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

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

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

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

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)

Vzvv_Req_Verificatie: Audit

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

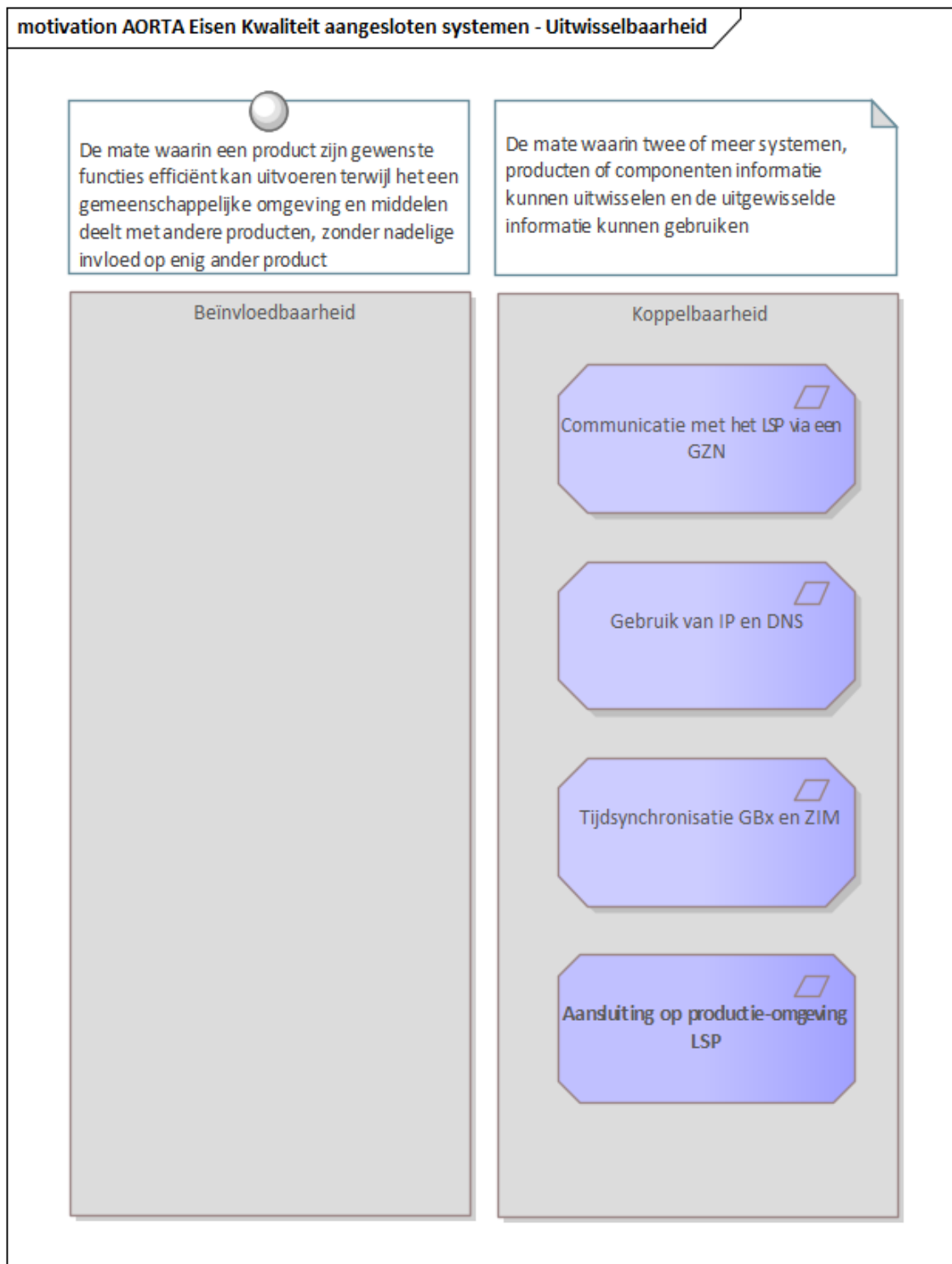


Figure 8 : AORTA Eisen Kwaliteit aangesloten systemen - Uitwisselbaarheid

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.

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: n/a**Vzvv_Req_Verificatie:** Monitoring**Vzvv_Req_Soort:** Non-Functional**Vzvv_Req_Type:** Product**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 toegangsllog van het GBx als de centrale toegangsllog van het LSP wil raadplegen.

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

Deze eis betekent voor de organisatie dat het GBx periodiek moet synchroniseren tegen een NTP-server om synchroon te blijven met de ZIM.

Vzvv_Moscow: Verplicht (Must)**Vzvv_Req_Verificatie:** Monitoring

Vzvvz_Req_Soort: Non-Functional**Vzvvz_Req_Type:** Product**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:

4. de hostnaam een maximale time-to-live (TTL) heeft voor verversing van de cache;
5. het IP-adres van de ZIM zich binnen een vooraf overeengekomen range bevindt die altijd gerouteerd moet worden naar de GZN;
6. 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:

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

Toelichting bij eis:

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

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

Vzvvz_Moscow: Verplicht (Must)**Vzvvz_Req_Verificatie:** Aansluittoets

Vzvvz_Req_Soort: Non-Functional

Vzvvz_Req_Type: Product

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.

Vzvvz_Moscow: Verplicht (Must)

Vzvvz_Req_Verificatie: Aansluittoets

Vzvvz_Req_Soort: Non-Functional

Vzvvz_Req_Type: Product

8.5.2.1.3.3 AORTA Eisen Kwaliteit Applicatie

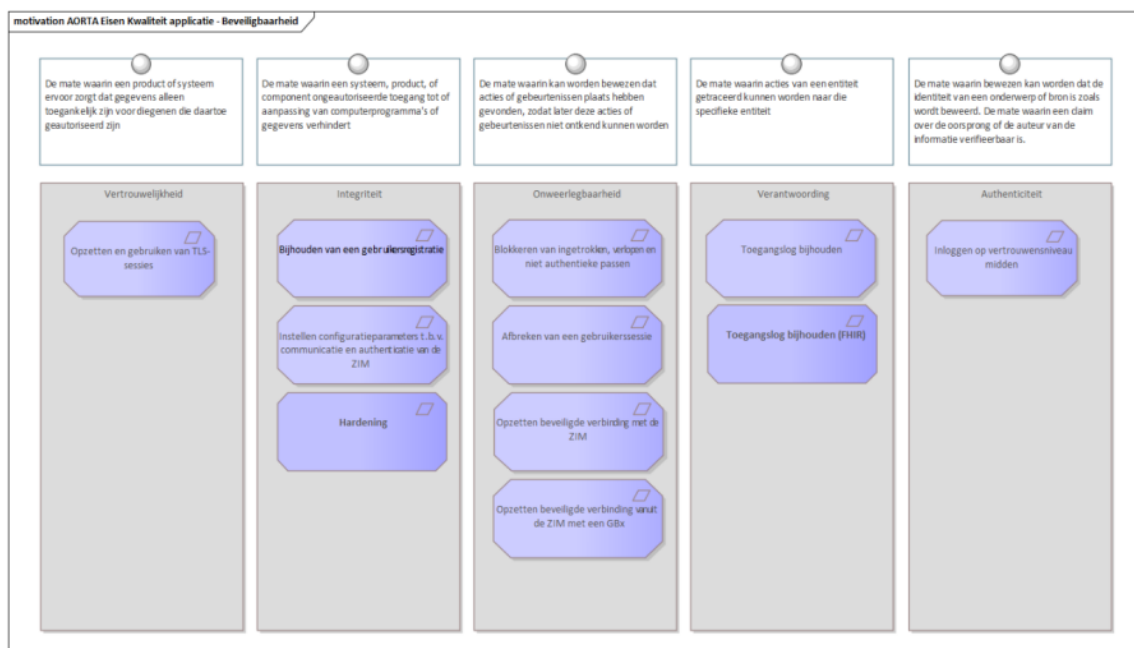


Figure 9 : AORTA Eisen Kwaliteit applicatie - Beveiligbaarheid

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.

Toegangslog bijhouden (FHIR)

Alias: GBX.LOG.e4016**Details****Eis:**

Het systeem moet alle binnenkomende en uitgaande berichten loggen in de toegangslog. Hierbij dienen onderstaande gegevens gelogd te worden, indien aanwezig in het bericht:

1. de identiteit van de patiënt/cliënt/burger (BSN) waar het bericht betrekking op heeft;
2. de identiteit van de organisatie waar het bericht vandaan komt of naar toe wordt gestuurd;
3. de functie en identiteit van de zorgverlener, medewerker of patiënt zoals opgenomen in het verstuurd en/of ontvangen bericht. De functie is de aorta-rolcode zoals opgenomen in het claim-element van het transactietoken.
4. de gebruikersinteractieID. Dit is een combinatie van HTTP-operatie, de URL inclusief de ontvangen zoekparameters en de contentVersion uit de AORTA-Version header;
5. het tijdstip en tijdzone (ten opzichte van UTC) van het moment dat het bericht ontvangen/verstuurd is;
6. de bericht-id van het ontvangen/verstuurd bericht. Dit is het messageId in de HTTP header;
7. het initiële bericht-id van het ontvangen/verstuurd bericht. Dit is het initialMessageID in de HTTP header;
8. de aan het bericht gekoppelde gegevensdienst. Dit is de waarde zoals opgenomen in de scope van het transactietoken;
9. een indicatie van eventueel opgetreden foutsituaties met betrekking tot het ontvangen en verzenden van de berichten. Hierbij dient de HTTP-foutcode, alle informatie in de eventueel aanwezige operationOutcome en de eventuele WWW-Authenticate HTTP response header gelogd te worden.

Toelichting bij eis:

Het doel van de logging is het inzichtelijk kunnen maken van de datastroom door de gehele keten. Het inzichtelijk maken van de loggegevens kan van belang zijn voor auditredenen of beheerwerkzaamheden zoals het oplossen van fouten in de keten. Deze eis is conform de vereisten zoals beschreven in de NEN7513.

Vz vz_Moscow: n/a**Vz vz_Req_Verificatie:** Acceptatietest**Vz vz_Req_Soort:** Functional**Vz vz_Req_Type:** Product**Hardening****Alias:** SYS.BVL.e4065**Details**

Eis:

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

Alle systeemparemeters dienen zodanig te zijn ingesteld dat met behoud van de gewenste functionaliteit een zo hoog mogelijk niveau van beveiliging bestaat.

Toelichting bij eis:

De intentie van deze eis is dat datgene wordt gedaan dat in de markt onder de gangbare maatregelen wordt gerekend op het gebied van hardening. Hierbij moet er uiteraard een afweging worden gemaakt tussen gebruiksvriendelijkheid en veiligheid.

Vzvv_Moscow: Verplicht

Vzvv_Req_Verificatie: Audit

Vzvv_Req_Soort: Non-Functional

Vzvv_Req_Type: Product

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 ververs worden,
3. gebruikmakend van Cipher Suites die door het NCSC minimaal worden gekenmerkt als goed en tevens worden ondersteund door de ZIM. Voor encryptie moet altijd de sterkste vorm als eerste worden geprobeerd,
4. een maximale sessieduur van 8 uur,
5. een 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

Vzvvz_Req_Soort: Functional**Vzvvz_Req_Type:** Product**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.

Vzvvz_Moscow: Verplicht (Must)**Vzvvz_Req_Verificatie:** Acceptatietest**Vzvvz_Req_Soort:** Functional**Vzvvz_Req_Type:** Product**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.

Vzvvz_Moscow: Verplicht (Must)

Vz vz_Req_Verificatie: Acceptatietest

Vz vz_Req_Soort: Functional

Vz vz_Req_Type: Product

Bijhouden van een gebruikersregistratie

Alias: GBX.FBH.e4030

Details

Eis:

Binnen het GBx dient te worden bijgehouden welke UZI-passen worden toegelaten voor gebruik. Deze gebruikersregistratie is uitsluitend toegankelijk voor gebruikers van de gastheerinstelling, na authenticatie op basis van een sterk authenticatiemiddel (2 factorauthenticatie bijvoorbeeld via een UZI-pas) van diezelfde gastheerinstelling.

Toelichting bij eis:

Dit is nodig om te voorkomen dat een willekeurig persoon de gebruikersregistratie kan aanpassen. Deze bevoegdheid komt bij een specifiek persoon te liggen.

Dit betekent voor de zorgaanbieder dat hij moet zorgen dat de bovenstaande rol van autorisatiebeheerder door een van zijn medewerkers wordt ingevuld.

Vz vz_Moscow: Verplicht (Must)

Vz vz_Req_Verificatie: Acceptatietest

Vz vz_Req_Soort: Functional

Vz vz_Req_Type: Product

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

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:

4. de identiteit van de patiënt/cliënt (BSN)
5. identiteit van de opvragende/versturende en bestemde organisatie
6. de functie en identiteit van de opvragende of versturende zorgverlener of medewerker of patiënt.
7. type van de uitgevoerde gebruikersinteractie
8. het tijdstip en tijdzone (ten opzichte van UTC) van de gebruikersinteractie
9. de bericht-id van het ontvangen (opvraag- of bevestig-) bericht
10. de bericht-id van het verzonden (oplever- of opdracht-) bericht
11. de gegevenssoorten of contextcodes van de verzonden en ontvangen patiëntstukken;
12. 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.

Vz vz_Moscow: Verplicht (Must)

Vz vz_Req_Verificatie: Acceptatietest

Vz vz_Req_Soort: Functional

Vz vz_Req_Type: Product

Afbreken van een gebruikerssessie

Alias: GBX.IDA.e4090.1

Details

Eis:

Het systeem moet een gebruikerssessie voor het landelijk uitwisselen van patiëntgegevens op vertrouwensniveau laag of midden afsluiten:

1. op commando van de gebruiker (zoals een muisklik of toetsencombinatie);
2. door uitnemen van het vertrouwensmiddel door de zorgverlener/medewerker;
3. wanneer de applicatie gedurende maximaal 60 minuten niet is gebruikt. Deze tijd dient instelbaar te zijn in het systeem, maar mag niet de 60 minuten overschrijden;
4. wanneer de sessie gedurende 1 uur open staat;
5. IP-adres van gebruiker gedurende een sessie wijzigt.

Toelichting bij eis:

Dit is nodig opdat een gebruiker zelf zijn gebruikerssessie kan uitloggen met de zekerheid dat niemand anders zijn sessie kan voortzetten en vervolgens zijn bevoegdheden kan misbruiken. Daarnaast is deze eis nodig om te tegen te gaan dat een in onbruik geraakte sessie door een onbevoegde kan worden misbruikt.

Vzvv_Moscow: Verplicht (Must)

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

Blokkeren van ingetrokken, verlopen en niet authentieke passen

Alias: GBX.IDA.e4085.2

Details

Eis:

Het GBx dient het starten van een gebruikerssessie op vertrouwensniveau midden te weigeren indien:

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

Toelichting bij eis:

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

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

Vzvv_Moscow: Verplicht (Must)

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

Inloggen op vertrouwensniveau midden**Alias:** GBX.IDA.e4080.3**Details****Eis:**

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

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

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

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

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

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

Toelichting bij eis:

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

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

Vzvv_Moscow: Verplicht (Must)**Vzvv_Req_Verificatie:** Audit**Vzvv_Req_Soort:** Functional**Vzvv_Req_Type:** Product

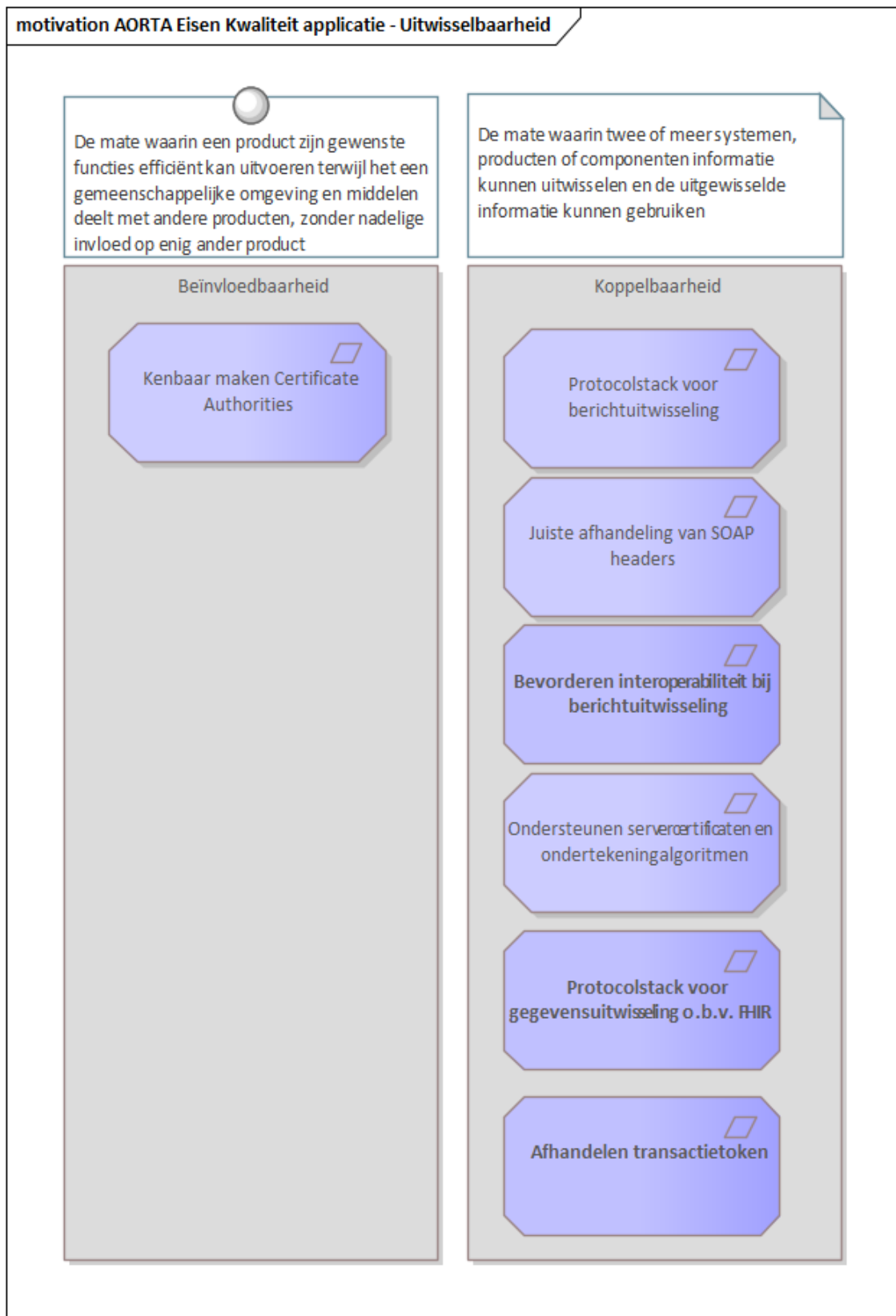


Figure 10 : AORTA Eisen Kwaliteit applicatie - Uitwisselbaarheid

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.

Afhandelen transactietoken

Alias: GBX.CON.e4140.2

Details

Eis:

Het XIS moet een ontvangen transactietoken correct kunnen verwerken. Hiervoor dienen door het ontvangende systeem de controles uitgevoerd te worden zoals beschreven in de Implementatiehandleiding Transactietoken JWT ((

<https://vz.vz.atlassian.net/wiki/display/UBEBVLEL/Implementatiehandleiding+Reagerend+GBZ>

).

Indien een FHIR-search niet wordt begeleid door een transactietoken, dan dient de bevraging beantwoord te worden met een foutmelding.

Toelichting bij eis:

In combinatie met bepaalde berichten is het mogelijk dat er transactietokens worden toegevoegd. De specificatie en de juiste technische verwerking van het transactietoken staan beschreven in de IH Transactietoken JWT (

<https://vz.vz.atlassian.net/wiki/display/UBEBVLEL/Implementatiehandleiding+Reagerend+GBZ>

).

Het doel van het transactietoken is tweeledig:

- Ten eerste is het bedoeld als gegevensdrager. Er worden een aantal gegevenselementen opgenomen, die niet in het bericht zitten. Deze gegevenselementen dienen uit het token gehaald te worden en te worden gebruikt in de verdere verwerking van het bericht. Hierbij dienen de controles plaats te vinden zoals beschreven in de IH Transactietoken.
- Ten tweede kan het transactietoken gebruikt worden t.b.v. authenticatie of als bewijs van autorisatie. Het is mogelijk om op basis van de certificaatreferenties te controleren of het token van de juiste afzender afkomstig is en dat de opvrager geautoriseerd is voor bevraging van specifieke patiëntgegevens.

Vz.vz_Moscow: n/a

Vz.vz_Req_Verificatie: Acceptatietest

Vz.vz_Req_Soort: Functional

Vz.vz_Req_Type: Product

Protocolstack voor gegevensuitwisseling o.b.v. FHIR

Alias: GBX.CON.e4130.1

Details

Eis:

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

- HL7 FHIR
- JWT
- HTTP v1.1/HTTP v2.0
-
- TCP
- IPv4

Toelichting bij eis:

Het is niet toegestaan om een lagere protocolversie te hanteren dan die in deze protocolstack vermeld is.

Vzvv_Moscow: n/a

Vzvv_Req_Verificatie: Acceptatietest

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

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

Ondersteunen servercertificaten en ondertekeningalgoritmen

Alias: GBX.CON.e4110.2

Details

Eis:

Het GBx dient UZI/PKIo-servercertificaten van de (verschillende) generatie(s) te ondersteunen zoals beschikbaar wordt gesteld door het UZI-Register.

Er moet gebruik worden gemaakt van het SHA-256 ondertekeningsalgoritme.

Toelichting bij eis:

Het UZI-register geeft UZI-servercertificaten uit onder één of meerdere certificaatbomen. In het geval er onder diverse certificaatbomen UZI-servercertificaten wordt uitgegeven, is het zaak om alle servercertificaten uitgegeven onder de diverse certificaatbomen te kunnen ondersteunen.

Een GBX-communicatieserver dient te zijn ingericht op het ondertekeningsalgoritme SHA-256.

Vzvv_Moscow: Verplicht (Must)

Vzvv_Req_Verificatie: Monitoring

Vzvv_Req_Soort: Functional

Vzvv_Req_Type: Product

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

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

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-verbindingen met NCSC beveiligingsniveau "goed"
- 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 beveiligingsniveau "goed" te ondersteunen, tenzij beveiligingsniveau "voldoende" nodig is voor de ondersteuning van oudere clients. 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

8.5.2.1.3.4 AORTA Eisen Organisatie van een GBX

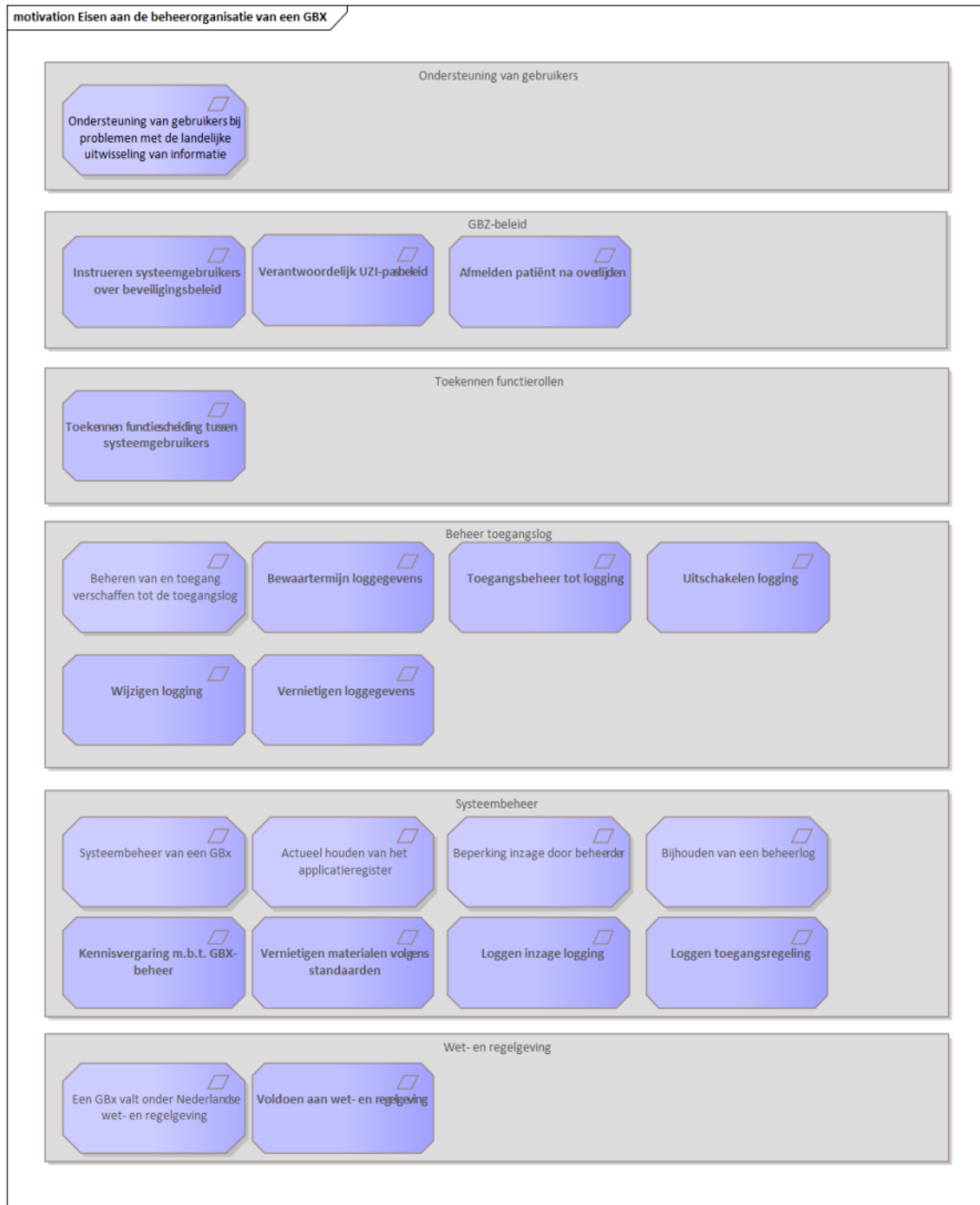


Figure 11 : Eisen aan de beheerorganisatie van een GBX

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 verwijsindex 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 verwijsindex 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

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

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.

Vzvv_Moscow: n/a

Vzvv_Req_Verificatie: n/a

Vzvv_Req_Soort: n/a

Vzvv_Req_Type: n/a

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

Vzvv_Moscow: n/a

Vzvv_Req_Verificatie: n/a

Vzvv_Req_Soort: n/a

Vzvv_Req_Type: n/a

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

Vzvv_Moscow: n/a

Vzvv_Req_Verificatie: n/a

Vzvv_Req_Soort: n/a

Vzvv_Req_Type: n/a

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

Loggen inzage logging

Alias: AGE.LOG.e4020

Details

Eis:

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: n/a

Vzvvz_Req_Verificatie: Audit**Vzvvz_Req_Soort:** Functional**Vzvvz_Req_Type:** Product**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.

Vzvvz_Moscow: n/a**Vzvvz_Req_Verificatie:** Monitoring**Vzvvz_Req_Soort:** Non-Functional**Vzvvz_Req_Type:** Business**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 bedoeld 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.

Vzvvz_Moscow: Verplicht (Must)**Vzvvz_Req_Verificatie:** Eigenverklaring

Vzvvz_Req_Soort: Non-Functional**Vzvvz_Req_Type:** Product**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 \(E\)](#)¹⁰⁴. 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.

Vzvvz_Moscow: Verplicht (Must)**Vzvvz_Req_Verificatie:** Eigenverklaring**Vzvvz_Req_Soort:** Functional**Vzvvz_Req_Type:** Business**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.

104. <http://www.dss.mil/documents/odaa/nispom2006-5220.pdf>

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

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

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

Vzvvz_Req_Soort: Non-Functional**Vzvvz_Req_Type:** Product**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**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](https://supportal.vzvvz.nl)¹⁰⁵.

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

105. <https://supportal.vzvvz.nl>

Vzvvz_Req_Soort: Non-Functional**Vzvvz_Req_Type:** Product**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.

Vzvvz_Moscow: Verplicht (Must)**Vzvvz_Req_Verificatie:** Documentverificatie**Vzvvz_Req_Soort:** Non-Functional**Vzvvz_Req_Type:** Product**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

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

Verantwoordelijk UZI-pasbeleid

Alias: GBX.FBH.e4017

Details

Eis:

Een organisatie moet zorgdragen dat er voldoende UZI-passen binnen een organisatie actief zijn. Het aantal benodigde UZI-passen is afhankelijk van de organisatiestructuur en de toepassing waarbinnen een UZI-pas wordt gebruikt.

Toelichting:

Zorgaanbieders waar veel zorgverleners werkzaam zijn mogen niet uit kostenoverwegingen besparen op UZI-passen en daarom bijvoorbeeld de mandatering in de gehele organisatie bij een of enkele specialisten leggen. Er dient goed afgewogen te worden wie verantwoordelijk is voor bepaalde interacties met het LSP. Verantwoordelijkheid wordt onder andere bepaald door de rol van de zorgverlener en het hebben van een (afgeleide) behandelrelatie met een patiënt.

Vzvv_Moscow: Verplicht
Vzvv_Req_Verificatie: Monitoring

Vzvvz_Req_Soort: Non-Functional**Vzvvz_Req_Type:** Product**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.

Vzvvz_Moscow: Verplicht**Vzvvz_Req_Verificatie:** Monitoring**Vzvvz_Req_Soort:** Non-Functional**Vzvvz_Req_Type:** Product**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 DAP¹⁰⁶](#));
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.

Vz vz_Moscow: Verplicht (Must)

Vz vz_Req_Verificatie: Aansluittoets

Vz vz_Req_Soort: Non-Functional

Vz vz_Req_Type: Product

End

8.6 Medicatieproces

De documenten met betrekking tot de kickstart van medicatieoverdracht (Medicatieproces 9) zijn te vinden op de volgende pagina: <https://zt-medicatieoverdracht.public.vz vz.nl/>

De documenten met betrekking tot Medicatieproces 6.12 zijn te vinden op de volgende pagina: <https://www.aorta-lsp.nl/documentatie-medicatiegegevens>

106. https://www.vz vz.nl/uploaded/FILES/htmlcontent/AORTA_DAP_20140130_v2.3.pdf

9 Processen

Dit onderdeel beschrijft de operationele processen voor het aansluiten op Mitz.

9.1 Aansluiten Mitz



9.2 Contracttoken

9.3 Vereenvoudigd gebruik UZI-pas (VGU)

9.3.1 Inleiding

Het proces met betrekking tot het gebruik van de UZI-pas is aangepast. Het is binnen AORTA mogelijk gemaakt voor XIS-leveranciers om functionaliteiten te bouwen, waardoor het werkproces van de

zorgverlener met betrekking tot de UZI-pas sterk vereenvoudigd kan worden. Naast een sterke vereenvoudiging in het werkproces is het ook mogelijk dat er kostenbesparing kan plaatsvinden vanwege de mogelijkheid dat er minder UZI-passen nodig zijn.

De implementatie van het vereenvoudigd gebruik van de UZI-pas (VGU) binnen een organisatie kan sterk verschillen; implementatie is afhankelijk van de zorgtoepassing en het werkproces van de zorgverlener en/of organisatie. Het doel van de beschrijving van het VGU-proces is om voor zorgaanbieders en koepelorganisaties inzichtelijk te maken hoe ze het meest kunnen profiteren van de oplossing voor het vereenvoudigde gebruik van de UZI-pas met de wettelijke normen in het achterhoofd. Daarnaast is het bedoeld als beschrijving voor XIS-leveranciers. Ze kunnen de beschrijving van het VGU proces gebruiken om de mogelijkheden met betrekking tot de oplossing beter in beeld te krijgen en om met een zorgorganisatie in gesprek te gaan om tot een goed geïmplementeerde oplossing te komen.

Er is een generieke beschrijving van de oplossing opgenomen. Eventuele voorbeelden zijn niet leidend voor de uiteindelijke implementatie. Per zorgtoepassing kan de oplossing op details verschillen. Deze details zullen in het ontwerp van de zorgtoepassing zijn opgenomen.

9.3.2 Vereenvoudigd proces UZI-pas

9.3.2.1 Probleem

Het gebruik van de UZI-pas leidt in sommige zorgprocessen tot vertragingen en vanuit informatiebeveiligingsoogpunt tot onveilige werksituaties als gevolg van onjuist gebruik. Uit verschillende reacties van leveranciers, zorgverleners en andere betrokkenen is dan ook de wens gekomen om de werkwijze met de UZI-pas te herzien. Met name binnen ziekenhuizen en zorgbehandelcentra is gebleken dat de werkwijze m.b.t. de UZI-pas niet aansluit bij de zorgprocessen; men wil patiëntinformatie reeds opgevraagd hebben voordat de patiënt langs komt voor behandeling (het zogenaamde 'prefetching').

Binnen AORTA is een oplossing geïntroduceerd waardoor het gebruik van de UZI-pas sterk vereenvoudigd kan worden. Het gaat hierbij om een generieke oplossing die het werkproces van een zorgaanbieder kan ondersteunen. Het werkproces kan binnen een zorgtoepassing en zelfs per instelling sterk verschillen. Het is dus aan een individuele instelling om te bepalen hoe men gebruik wil maken van de oplossing zoals binnen AORTA is opgenomen.

9.3.2.2 Generieke oplossing

Met de generieke oplossing is het mogelijk om vooraf een aantal waarborgen af te geven, waarmee een zorgverlener op het moment van het versturen van een bericht (bijvoorbeeld een bevraging van patiëntgegevens, het versturen van patiëntgegevens of het afsluiten van een abonnement) geen UZI-pas meer nodig heeft. Het wordt mogelijk om op basis van bepaalde triggers het systeem berichten te laten versturen.

9.3.2.2.1 Tokens

Voor interactie met het LSP zonder het gebruik van de UZI-pas op het moment van de interactie worden er drie verschillende waarborgen onderscheiden. Deze waarborgen komen in de vorm van

zogenaamde tokens en moeten worden meegestuurd met een interactie. Het selecteren en toevoegen van de tokens is niet een handeling die een zorgverlener hoeft uit te voeren. Dit zal geautomatiseerd door de XIS-applicatie aan een uitgaande interactie worden toegevoegd. Elk token staat voor een ander waarborg en kunnen op verschillende momenten in de tijd worden aangemaakt. De combinatie van waarborgen zorgen voor een vergelijkbaar beveiligingsniveau als een interactie verstuurt met een UZI-pas.

Met het **inschrijftoken** wordt gewaarborgd dat een patiënt is ingeschreven bij een organisatie. Van een ingeschreven patiënt dient een token te worden gegenereerd door middel van het gebruik van een UZI-pas. Een technische beschrijving van het inschrijftoken is opgenomen in de IH Inschrijftoken.

Een verantwoordelijke zorgverlener geeft in een **mandaattoken** aan welke zorgverleners of onder welke omstandigheden het systeem onder zijn verantwoordelijkheid een interactie mag versturen. Een technische beschrijving van het mandaattoken is opgenomen in de IH Mandaattoken.

Het **transactietoken** is een waarborg dat wordt aangemaakt door het systeem op het moment van uitsenden van een bericht. Het transactietoken waarborgt dat een interactie met betrekking tot een specifieke patiënt wordt verstuurd onder verantwoordelijkheid van een verantwoordelijke zorgverlener. Het transactietoken koppelt het inschrijftoken, het mandaattoken en het uit te sturen bericht aan elkaar. Een gebruiker van het systeem heeft geen weet van het transactietoken. Het genereren van het transactietoken wordt gedaan door het systeem met behulp van het UZI-servercertificaat. Een technische beschrijving van het transactietoken is opgenomen in de IH Transactietoken.

9.3.2.2.2 Triggers

Een XIS-applicatie kan indien een zorgverlener via het mandaattoken toestemming heeft gegeven om het systeem onder zijn verantwoordelijkheid te laten opvragen, op basis van verschillende triggers een bericht uitsenden met betrekking tot een specifieke patiënt. Deze triggers zijn niet vast voor gedefinieerd, maar kunnen verschillen per zorgtoepassingen en/of per werkproces. Voorbeelden van triggers zijn:

- Het ontvangen van een signaal als gevolg van een afgenomen abonnement; een zorgaanbieder heeft nieuwe informatie beschikbaar gesteld via het LSP en het LSP stuurt een signaal naar alle abonneehouders.
- Een agenda-afspraak met een patiënt; een patiënt heeft die dag een afspraak en het systeem krijgt hiermee het verzoek om de patiëntgegevens van die patiënt op te vragen.
- Een bepaalde tijdsperiode; elke eerste van de maand bevraagt het systeem bepaalde gegevens t.b.v. bijvoorbeeld een bewakings- of rapportageproces.
- Het openen van een dossier; een geautoriseerde zorgverlener opent een dossier van een patiënt en het systeem zorgt ervoor dat de zorgverlener de meest actuele gegevens opgeleverd krijgt door alle nieuwe informatie op te vragen.
- Een handeling door een daarvoor geautoriseerde gebruiker; een zorgverlener kan het systeem actief opdracht geven om een bevraging te doen m.b.t. een specifieke patiënt.

Het is mogelijk dat een XIS-applicatie meerdere triggers ondersteunt. Binnen een zorgtoepassing zal worden bepaald welke triggers van belang zijn en welke potentiële eisen er gelden m.b.t. deze triggers. Op verzoek van een XIS-leverancier kan in overleg met VZVZ worden nagedacht over mogelijke andere triggers. Deze zullen echter altijd in een zorgtoepassing opgenomen moeten worden en een XIS zal altijd moeten worden geaccepteerd voor deze nieuwe trigger. Het kan dus voor een zorgaanbieder interessant zijn om met zijn XIS-leverancier in gesprek te gaan over de implementatie van VGU in de

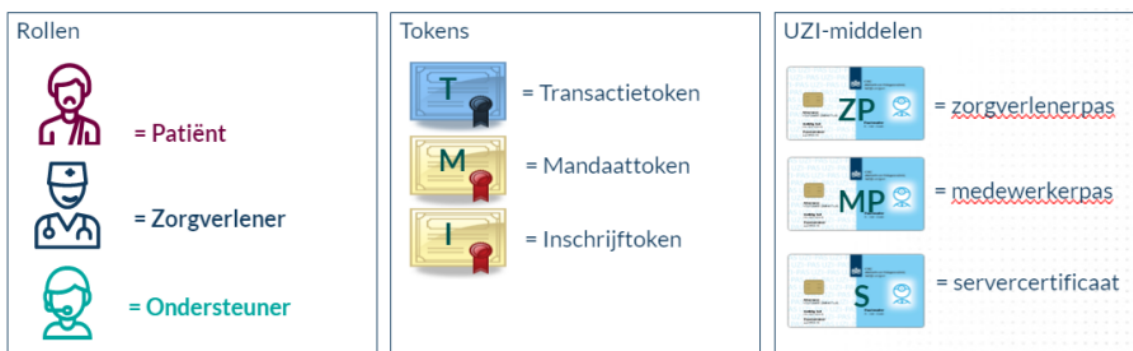
diverse werkprocessen.

9.3.3 Generieke uitwerking vereenvoudigd gebruik van de UZI-pas (VGU)

Hieronder staat uitgewerkt hoe het vereenvoudigd gebruik van de UZI-pas (VGU) toegepast kan worden. Het betreft een generieke uitwerking die toegepast kan worden op elke interactie die over de AORTA infrastructuur wordt verstuurd. Het gaat daarbij zowel om infrastructurele berichten gericht aan het LSP als om zorginhoudelijke berichten gericht aan een ontvangende XIS.

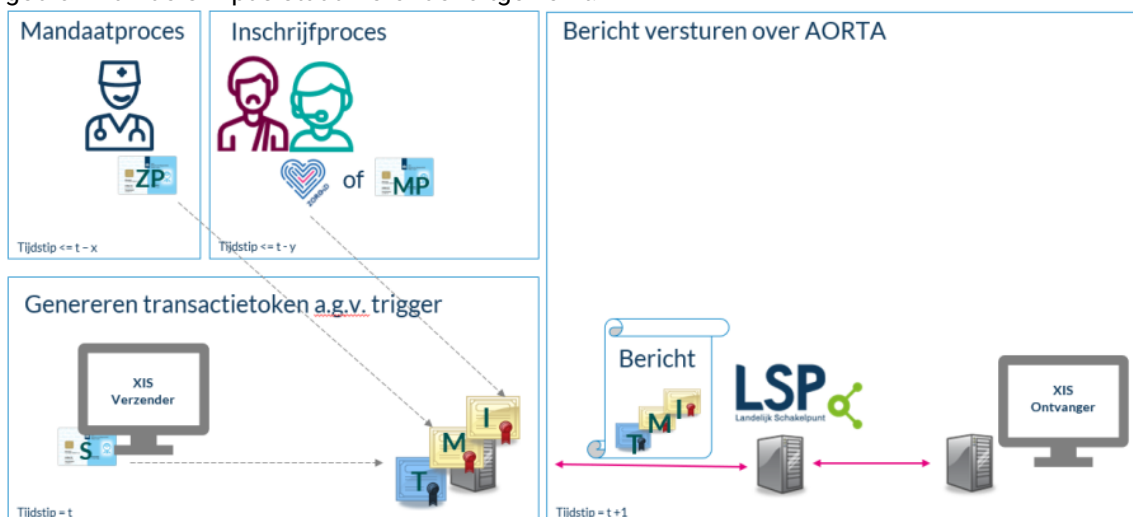
9.3.3.1 Legenda

Onderstaande legenda toont de symbolen zoals gebruikt in onderstaande diagram



9.3.3.2 Generiek proces

Het generieke proces dat gevolgd dient te worden om gebruik te maken van het vereenvoudigde gebruik van de UZI-pas staat hieronder uitgewerkt.



9.3.3.3 Samenvatting

Onderstaande tabel beschrijft de actoren, UZI-middelen en resultaat van de tokens in de tijd.

Tijdstip	Proce s	Actore n	Tok en	Duur token	Middel
T-x (x>0) Het tijdstip ligt in ieder geval voor het moment dat een transactietoken aangemaakt wordt. Op welk moment het mandaattoken precies aangemaakt wordt, is afhankelijk van het zorgproces.	Manda atproc es	Verant woorde lijke zorgver lener XIS	Man daat toke n	Richtlijn 5 minuten, maximaal 90 minuten.	UZI- zorgverlene r pas, handtekeni ngcertificaa t
T-y (y>0) Het tijdstip ligt in ieder geval voor het moment dat een transactietoken aangemaakt wordt. Op welk moment het mandaattoken precies aangemaakt wordt, is afhankelijk van het zorgproces. Hierbij geldt dat er geen verband is tussen x en y.	Inschri jfproce s	Medew erker Patiënt XIS	Insc hrijft oke n	Maximaal de geldigheidsduur van het handtekeningce rtificaat waarmee is ondertekend .	UZI- medewerke r pas-op- naam, authenticati ecertificaat, of ZORG-ID
T	Gener eren transa ctietok en a.g.v. trigger	XIS	Tran sact ieto ken	Maximaal 1,5 jaar	UZI- servercertifi caat
T+1	Bericht verstur en over AORT A	XIS LSP	Man daat toke n Tran sact ieto ken Insc hrijft oke n		UZI- servercertifi caat

9.3.4 UZI-middel gebruik

9.3.4.1 Processen met betrekking tot UZI-middelen

Het vereenvoudigd gebruik met de UZI-pas sluit het gebruik van de UZI-pas niet helemaal uit. De UZI-pas blijft nodig binnen twee deelprocessen:

- Bij de bevestiging van inschrijving van een patiënt;
- Bij het afgeven van een mandaat door een verantwoordelijke zorgverlener.

Deze twee deelprocessen kunnen op afzonderlijke momenten in de tijd plaatsvinden. Het is aan een zorgaanbieder in overleg met zijn XIS-leverancier zaak om een goede invulling te vinden, die aansluit bij het werkproces zoals geïmplementeerd binnen de zorgaanbieder.

Naast de UZI-passen dient er gebruik te worden gemaakt van servercertificaten. Deze zijn nodig voor het proces om een specifieke zorgaanbieder te identificeren en te authenticeren. Hieronder wordt gesproken over een UZI-servercertificaat. Het is mogelijk dat in sommige gevallen gebruik wordt gemaakt van een PKI-servercertificaat.

9.3.4.1.1 UZI-middelen

Er zijn verschillende soorten UZI-middelen te onderscheiden. Het gaat hierbij om persoonlijke als organisatie UZI-middelen.



Zorgverlenerspas: Pas ten behoeve van zorgverlener waarvan het beroep valt onder artikel 3, 34 of 36a beroepen van de Wet BIG. De certificaten op de pas bevatten de unieke identificatie (UZI-nummer) en de functie (UZI-rolcode) van de betreffende zorgverlener.

Medewerkerspas: Pas voor medewerkers die geen beroep uitoefenen wat valt onder artikel 3, 34 of 36a van de Wet BIG. Met de certificaten op deze pas is het niet mogelijk om je te authenticeren voor toegang tot de AORTA infrastructuur. Een alternatief voor deze pas is het gebruik van ZORG-ID.

Medewerkerspas-op-naam: Pas voor medewerkers die geen beroep uitoefenen wat valt onder artikel 3, 34 of 36a van de Wet BIG. De certificaten die opgenomen zijn bevatten een unieke identificatie van de medewerker (UZI-nummer). Deze medewerker vervult niet een functie die valt onder artikel 3, 34 of 36a van de Wet BIG en krijgt hiermee geen unieke rolcode toegekend. Ook een UZI-medewerkerspas op naam kan toegang krijgen tot het LSP, maar alleen als deze is gemandateerd door een BIG-geregistreerde zorgverlener met een UZI-zorgverlenerspas. Een alternatief voor de medewerkerspas-op-naam is het gebruik van ZORG-ID.

Servercertificaat: zorgt voor identificatie en authenticatie van de zorgaanbiederapplicatie. Met een servercertificaat kunnen beveiligde verbindingen worden opgezet met het LSP. Binnen AORTA geldt dat er gebruik moet worden gemaakt van UZI-servercertificaten, tenzij het niet mogelijk is voor de

betreffende zorgaanbieder om een UZI-servercertificaat aan te vragen. In dat geval zal gewerkt worden met een PKI-servercertificaat.

9.3.4.1.2 Inschrijfproces

Zodra een patiënt is ingeschreven en er een WID- en een BSN-controle heeft plaatsgevonden bij het SBV-Z, dan is het mogelijk om een inschrijftoken te ondertekenen. Het ondertekenen kan op verschillende momenten in de tijd gebeuren:

- Direct na de initiële inschrijving en de benodigde SBV-Z controles;
- Op een later moment na de initiële inschrijving en de benodigde SBV-Z controles Het is hierbij van belang dat er extra waarborgen zijn dat een patiënt daadwerkelijk door een geautoriseerd persoon is ingeschreven inclusief alle benodigde controles. Een kwaadwillende mag niet in staat gesteld worden om inschrijftokens te laten genereren. ;
- Op het moment van bevraging en er nog geen inschrijftoken beschikbaar is.

Het is aan een zorgaanbieder in overleg met zijn XIS-leverancier zaak om een goede invulling te vinden, die aansluit bij het werkproces zoals geïmplementeerd binnen de zorgaanbieder.

Het inschrijftoken moet worden ondertekend met het authenticatiecertificaat van minimaal Dit kan ook met een zorgverlenerpas gebeuren. een medewerkerpas-op-naam pas. Deze pas dient geldig te zijn op het moment van ondertekenen van een inschrijftoken. Een inschrijftoken is 1.5 jaar geldig, ongeacht de geldigheidsduur van de UZI-pas. Na 1.5 jaar dient de inschrijving opnieuw bevestigd te worden door middel van ondertekening.

Als gevolg van deze ondertekening kan onweerlegbaar worden vastgesteld dat een geautoriseerde gebruiker binnen de organisatie heeft vastgesteld dat de inschrijving van de patiënt door deze persoon is gedaan of dat deze persoon heeft geconstateerd dat de inschrijving correct heeft plaatsgevonden. Registratie en ondertekening van het inschrijftoken dient te gebeuren voordat het systeem gebruik kan maken van het vereenvoudigd gebruik van de UZI-pas.

9.3.4.1.3 Mandaatproces

Een zorgverlener kan door middel van een mandaat zijn autorisaties overdragen aan een andere zorgverlener. Op een soortgelijke wijze kan een zorgverlener het XIS delegeren om onder zijn verantwoordelijkheid een interactie te versturen met betrekking tot de patiënten waar de betreffende zorgverlener een behandelrelatie mee heeft.

Het mandaat dat een verantwoordelijke zorgverlener heeft geregistreerd, wordt vastgelegd in de vorm van een mandaattoken. Voor het vereenvoudigd gebruik van de UZI-pas dient de applicatieID van het systeem van waaruit een AORTA-interactie wordt verstuurd, opgenomen te zijn in het mandaat. Na het registreren van een mandaat, dient de verantwoordelijke zorgverlener het mandaat te ondertekenen met het handtekeningcertificaat van zijn UZI-pas. Het mandaattoken is maximaal net zolang geldig als de geldigheidsduur van de zorgverlenerpas. Indien een zorgverlenerpas verlopen is, dan zal het mandaattoken niet meer gebruikt kunnen worden.

Registratie en ondertekening van het mandaattoken dient te gebeuren voordat het systeem gebruik kan maken van het vereenvoudigd gebruik van de UZI-pas.

9.3.4.1.4 Genereren transactietoken a.g.v. trigger

Om zeker te weten dat een bericht ook daadwerkelijk door een zorgaanbieder is opgesteld, dient er een transactietoken te worden ondertekend door het UZI-servercertificaat. Het transactietoken bevestigd

dat een specifiek bericht is opgesteld onder verantwoordelijkheid van een specifieke zorgaanbieder die een behandelrelatie heeft met de patiënt op wie het bericht betrekking heeft. Het aanmaken van een transactietoken wordt geïnitieerd door een trigger zoals omschreven in de pagina Vereenvoudigd proces UZI-pas.

9.3.4.1.5 Bericht versturen over AORTA

Voor het versturen van een bericht, dient het versturende XIS een verbinding op te zetten met het LSP. Een verbinding wordt opgezet op basis van het servercertificaat van de XIS. Het bericht dat verstuurd wordt, dient begeleidt te worden met:

- het inschrijftoken van de patiënt die onderwerp is van het bericht;
- het mandaattoken van de verantwoordelijke zorgverlener die een behandelrelatie heeft met deze patiënt;
- het transactietoken die is aangemaakt als gevolg van een trigger.

Het XIS moet deze tokens koppelen aan een bericht.

Het is mogelijk dat er meerdere mandaattokens beschikbaar zijn, die gebruikt zouden kunnen worden. Afhankelijk van de trigger zou een gebruiker van het systeem het juiste mandaattoken kunnen kiezen of kan het systeem op basis van de context van het bericht zelf een mandaattoken kunnen kiezen. De wijze van implementeren kan afhankelijk zijn van het zorgproces waarin dit proces wordt toegepast. Het is dan ook aan de XIS-leverancier om hier goed mee om te gaan. VZVZ zal hier bij de implementatie in kunnen begeleiden.

9.3.4.2 Voor wie UZI-passen?

Om patiëntgegevens op te mogen vragen, dient de verantwoordelijke zorgverlener een behandelrelatie te hebben met de patiënt wiens gegevens worden opgevraagd. Het is aan de verantwoordelijke zorgverlener en/of de organisatie om de behandelrelatie te verantwoorden aan een patiënt of inspectiedienst.

De rol van de verantwoordelijke zorgverlener bepaalt welke inhoudelijke informatie er bij een opvraag wordt opgeleverd. Welke informatie wordt opgeleverd voor een bevraging door een specifieke rol heeft te maken met de autorisatierichtlijnen die worden opgesteld door de verschillende koepels; niet elke zorgverlener krijgt vanzelfsprekend dezelfde dataset opgeleverd.

Met name voor organisaties waar verschillende zorgverlenerrollen actief zijn, is het van belang om een goede afweging te maken over welke zorgverlener met welke zorgverlenerrol een UZI-pas moet bezitten. Hierbij kan de autorisatierichtlijn van een zorgtoepassing meer inzicht geven. Voor alle interactietypes (opvragen, versturen, infrastructurele berichten etc.) geldt dat het Medische Autorisatie Protocol (MAP) bepaalt of een bepaalde rolcode een bericht mag versturen. Ook hiervoor geldt dat VZVZ de MAP-configuratie beschikbaar kan stellen om een goede afweging te maken voor welke rollen er UZI-passen aangeschaft dienen te worden.

9.3.4.3 Aantal UZI-passen?

Het aantal benodigde UZI-passen is sterk afhankelijk van de organisatiestructuur en de werkprocessen binnen een organisatie. Er zijn wel een aantal zaken aan te geven, waar organisaties rekening mee kunnen houden bij het bepalen van het aantal benodigde UZI-passen:

- Verschillende soorten zorgverlenerrollen binnen de organisatie; autorisaties worden binnen AORTA toegekend per zorgverlenerrol. Niet elke zorgverlener heeft dezelfde autorisaties. Er dient dus nagedacht te worden welke zorgverlenerrollen een UZI-pas dienen aan te vragen om de juiste patiëntgegevens te kunnen opvragen.
- Onderkennen verantwoordelijke zorgverlener binnen zorgprocessen; een zorgverlener dient een behandelrelatie te hebben met een patiënt om diens gegevens op te vragen. Het is aan de zorgaanbieder om een behandelrelatie te verantwoorden aan een patiënt of inspectiedienst.
- Doorstroom van personeel; een UZI-pas is gekoppeld aan een persoon. Indien deze persoon uit dienst gaat, mag de UZI-pas en de hiermee getekende tokens niet meer gebruikt worden.
- Vervangen verlopen en/of ingetrokken UZI-pas; een UZI-pas die verlopen is, moet niet leiden tot een verstoord zorgproces. Het is dus aan te raden om altijd meerdere actieve UZI-passen in een instelling te gebruiken, zodat bij het verlopen of intrekken van een UZI-pas het zorgproces niet stil valt.

9.3.4.4 Rol VZVZ

VZVZ kan een XIS-leverancier en/of zorgaanbieder begeleiden met het implementeren en in gebruik nemen van het proces met betrekking tot het vereenvoudigd gebruik van de UZI-pas.

VZVZ kan advies geven over het aantal te gebruiken UZI-passen en aan wie die UZI-passen het best kunnen worden toegekend. Dit zal echter een niet bindend advies zijn. Het is aan de zorgaanbieder om hierin de juiste keuzes voor zijn organisatie te maken.

Indien een zorgaanbieder in overleg met zijn XIS-leverancier bepaalde tekortkomingen ziet met betrekking tot het vereenvoudigd gebruik van de UZI-pas, dan gaat VZVZ graag in gesprek om een oplossing te vinden voor deze tekortkomingen. Hierbij valt bijvoorbeeld te denken aan het ontbreken van een juiste trigger voor het initiëren van het versturen van een bericht. VZVZ zal hierbij altijd de geldende normen, regels, wetten en afspraken met het veld in ogenschouw nemen.

9.3.5 Aandachtspunten

9.3.5.1 Inzage logging

Patiënten hebben de mogelijkheid om via Volgjezorg Het goed beheerde patiëntenportaal onder verantwoordelijkheid van VZVZ, volgjezorg.nl in te zien welke zorgaanbieder welke gegevens heeft opgevraagd bij welke zorgaanbieder en/of naar welk zorgaanbieder gegevens zijn verstuurd. Hierbij worden geen individuele zorgverleners getoond. Echter, de patiënt heeft wel het recht om bij de zorgaanbieder op te vragen welke zorgverleners er bij de bevraging betrokken zijn geweest. Hierbij dient dan in ieder geval de verantwoordelijke zorgverlener aan de patiënt kenbaar te worden gemaakt. Het is dus van belang dat een zorgaanbieder te allen tijde kan uitleggen, waarom er een bericht is verstuurd onder het mandaat van een bepaalde zorgverlener.

9.3.5.2 Verlopen UZI-passen

Een verlopen UZI-pas kan leiden tot een verstoord zorgproces. De UZI-pas en het mandaattoken getekend met de bewuste UZI-pas kunnen respectievelijk mogen dan niet meer gebruikt worden. Het is

aan de zorgaanbieder om een goed proces in te richten om genoeg UZI-passen beschikbaar te hebben binnen de organisatie en om deze UZI-passen (in overleg met de verantwoordelijke zorgverleners) tijdig te verlengen.

9.3.5.3 Verlopen UZI-servercertificaten

Afhankelijk van de grootte van de organisatie is het mogelijk dat er twee servercertificaten worden vereist. Met deze twee servercertificaten kan er onderscheid worden gemaakt tussen het opzetten van een beveiligde verbinding en het daadwerkelijk dataverkeer (d.m.v. ondertekening van het transactietoken). Het is van belang dat beide UZI-servercertificaten tijdig worden vervangen. Met een verlopen of ingetrokken servercertificaat is het niet mogelijk om patiëntgegevens op te vragen of te versturen via AORTA.

9.3.6 Acceptatie

Voor implementatie van het vereenvoudigd gebruik UZI-pas bij een zorgaanbieder moet de leverancier zijn XIS laten accepteren door het VZVZ-acceptatieteam. Daarnaast dient de zorgaanbieder die de functionaliteit in productie gaat nemen een self assesment in te vullen.

9.3.6.1 Self assesment vereenvoudigd gebruik UZI-pas

Met betrekking tot het vereenvoudigd gebruik van de UZI-pas heeft VZVZ geen beveiligingsconcessies willen doen t.o.v. het gebruik van de UZI-pas. Om te kunnen blijven voldoen aan de NEN 7510 en de NEN 7512, wordt een deel van de beveiligingsverantwoordelijkheid overgedragen aan een zorgaanbieder. Indien een zorgaanbieder er voor kiest om gebruik te maken van het vereenvoudigd gebruik van de UZI-pas, dan dient de zorgaanbieder expliciet aan te geven dat hij voldoet aan de maatregelen behorend bij die beveiligingsverantwoordelijkheid. Deze maatregelen zijn opgenomen in de PvE (Programma van Eisen) van een zorgtoepassing en benoemd in een self assesment in de vorm van een aantal vragen. De zorgaanbieder dient deze vragen te beantwoorden en te ondertekenen, voordat er gebruik mag worden gemaakt van het proces met betrekking tot het vereenvoudigd gebruik van de UZI-pas.

Het self assesment staat gepubliceerd op de VZVZ-website:

[selfassesment_zorgaanbieders_vereenvoudigd_gebruik_uzi_pas \(formdesk.com\)](https://fd2.formdesk.com/vzvz/selfassesment_zorgaanbieders_vereenvoudigd_gebruik_uzi_pas)¹⁰⁷.

9.3.6.2 PvE Zorgtoepassing

In een PvE van de zorgtoepassing zijn alle eisen opgenomen die van toepassing zijn voor die zorgtoepassing. Het betreft hier zorgaanbiederorganisatie-, XIS-applicatie- en XIS-leverancierseisen. Hierin zijn ook alle eisen opgenomen die geïmplementeerd dienen te worden om gebruik te kunnen maken van het proces met betrekking tot het vereenvoudigd gebruik van de UZI-pas.

Een zorgaanbieder dient te voldoen aan de zorgaanbiedereisen zoals opgenomen in het PvE van de zorgtoepassing.

Een XIS-leverancier dient het reguliere acceptatietraject te doorlopen om zijn applicatie geaccepteerd te krijgen.

107. https://fd2.formdesk.com/vzvz/selfassesment_zorgaanbieders_vereenvoudigd_gebruik_uzi_pas

9.4 Abonnement- en signaalfunctie

De abonnement- en signaalfunctie is bedoeld voor situaties waarin zorgverleners actief over een actueel medisch dossier willen beschikken. De wijze waarop de abonnement- en signaalfunctie wordt ingericht is afhankelijk van de zorgtoepassing, sector-specifieke keuzes en de wijze waarop de leverancier van het informatiesysteem de functionaliteit heeft ingezet en ingericht. In onderstaande documentatie wordt de generieke werking beschreven.

9.4.1 Gebruik abonnement

9.4.1.1 Registreren abonnement

Een zorgverlener kan met een systeem een abonnement registreren voor het verkrijgen van een signaal indien er nieuwe gegevens beschikbaar worden gesteld van een specifieke patiënt. Hiervoor dient het systeem onder verantwoordelijkheid van een zorgverlener een 'Registreren abonnement'-bericht te versturen. Dit kan geïnitieerd worden door:

- een zorgverlener zelf op basis van zijn UZI-pas of ZORG-ID Smart;
- een medewerker die onder mandaat werkt van de betreffende zorgverlener;
- Vereenvoudigd gebruik UZI-pas (VGU) in combinatie met een mandaattoken getekend door de verantwoordelijke zorgverlener.

Een abonnement wordt centraal in het abonnementenregister geregistreerd op basis van de unieke combinatie van:

- PatiëntID;
- Contextcode of gegevenssoort;
- ApplicatieID;
- Organisatie;
- Gebeurtenistype (dit zal altijd betrekking hebben op een wijziging in de verwijzindex).
- Rolcode

De precieze invulling van het 'Registreren abonnement'-bericht is opgenomen in DECOR informatie voor project: [DECOR informatie voor project: AORTA \(aorta-vzvz-\) \(nictiz.nl\)](https://decor.nictiz.nl/pub/vzvz/index.php?prefix=aorta-vzvz-)¹⁰⁸. Hierbij is in ieder geval de geldigheidsduur van het abonnement verplicht. Een abonnement mag niet langer geldig zijn dan 1,5 jaar. Indien dit wel het geval is, wordt dit abonnement afgewezen en wordt een foutmelding geretourneerd.

Daarnaast dient het abonnement lokaal in het systeem geregistreerd te worden, zodat functionaliteiten als verlengen en beëindigen van het abonnement mogelijk worden.

9.4.1.1.1 Registreren abonnement o.b.v. VGU-functionaliteit

Met gebruik van de VGU-functionaliteit is het mogelijk om automatisch een abonnement af te sluiten op basis van een bepaalde trigger. Voorbeelden van triggers:

108. <https://decor.nictiz.nl/pub/vzvz/index.php?prefix=aorta-vzvz->

- Er wordt een behandelrelatie geregistreerd voor een patiënt;
- Een zorgverlener sluit zelf expliciet een abonnement af;
- Een zorgverlener geeft aan medicatiebewaking te willen doen voor een patiënt.

Voor het afsluiten van een abonnement op basis van de VGU-functionaliteit zijn een aantal randvoorwaarden van toepassing:

- Er dient een inschrijftoken aanwezig te zijn van de patiënt van wie een abonnement afgesloten dient te worden;
- Er dient een behandelrelatie te zijn tussen de abonneenemer en de patiënt op het moment van afsluiten van een abonnement;
- Er dient een mandaattoken te zijn van de abonneenemer t.b.v. de VGU-functionaliteit;
- Een zorgverlener dient de juiste autorisaties te hebben om een abonnement te mogen afsluiten.

Autorisaties worden centraal bepaald op basis van de rolcode van een zorgverlener, de contextcode (in het geval van een bevraging) en interactieID. Elke rolcode kan in theorie andere autorisaties kennen voor een bevraging van een specifieke contextcode of een andere invulling van de te bevragen medische gegevens (conform de Selectie en Determinatie tabel).

9.4.1.1.2 Toepassingen voor registreren abonnement

Er zijn verschillende toepassingen voor gebruik van de signaalfunctie:

- Medicatiebewaking;
- Vereenvoudigd gebruik UZI-pas (VGU);
- Bepalen actualiteit van gegevens.

Ten behoeve van medicatiebewaking is het van belang om een signaal te krijgen indien er een aanpassing is geweest in de medicatiegegevens van een patiënt die onder medicatiebewaking staat. Het ontvangen van een signaal dient te leiden tot een expliciet signaal aan de abonenthouder.

Indien een abonnement wordt afgesloten om de VGU-functionaliteit te ondersteunen, dan zal het signaal een trigger zijn voor automatische bevraging,

Het is mogelijk om aan de hand van de signaalfunctie lokaal vast te stellen of er nieuwe gegevens zijn van een bepaalde patiënt. Hierbij hoeft een zorgverlener dus alleen zijn UZI-pas (het gebruik van de UZI-pas kan geautomatiseerd worden i.c.m. de VGU-functionaliteit) te gebruiken indien er eerder al een signaal is ontvangen.

9.4.1.1.3 Aandachtspunten m.b.t. registreren abonnement

Een abonnement wordt niet afgesloten op basis van een specifieke zorgverlener en diens rol, maar op basis van een zorgaanbieder (o.b.v. applicatieID). Echter, het 'Registreren abonnement'-bericht wordt wel geautoriseerd op basis van de autorisatie van de zorgverlener, die verantwoordelijk is voor het versturen van het 'Registreren abonnement'-bericht (het versturen van het 'Registreren abonnement'-bericht kan ook onder mandaat gebeuren). Autorisatie gebeurt op basis van rolcode en contextcode.

Deze rolcode bepaalt welke signalen het systeem ontvangt. Als systeem kun je maar één abonnement nemen op een patiënt voor een bepaalde contextcode en rolcode. Het is dus van belang dat nagedacht wordt onder wiens verantwoordelijkheid een abonnement wordt afgesloten. Daarom moet ook in het

lokale systeem het abonnement geregistreerd worden, waarbij in ieder geval de ingangsdatum van het abonnement dient te worden bijgehouden. Een abonnement mag niet langer dan 1,5 jaar geldig zijn. Dit moet lokaal worden bijgehouden (kunnen meerdere zorgverleners zijn), zodat bijvoorbeeld bij einde dienstverband duidelijk is of een abonnement nog geldig is of dat er een nieuw abonnement moet worden genomen. Uiteraard zal ook lokaal de behandelrelatie gecontroleerd moeten worden.

9.4.1.2 Verlengen Abonnement

Zoals aangegeven heeft een geregistreerd abonnement een beperkte geldigheidsduur van maximaal 1,5 jaar. Indien gewenst door een zorgverlener, dan dient dit abonnement te worden verlengd. Hiervoor kan het systeem onder verantwoordelijkheid van een zorgverlener een 'Registreren abonnement'-bericht versturen. Dit kan geïnitieerd worden door:

- een zorgverlener op basis van zijn UZI-pas;
- een medewerker met UZI-pas die onder mandaat werkt van de betreffende zorgverlener;
- Vereenvoudigd gebruik UZI-pas (VGU) in combinatie met een mandaattoken getekend door de verantwoordelijke zorgverlener.

De zorgverlener onder wiens verantwoordelijkheid het abonnement verlengd wordt, hoeft niet dezelfde zorgverlener te zijn onder wiens verantwoordelijkheid het abonnement initieel is genomen.

Voor het verlengen van het abonnement wordt hetzelfde bericht gebruikt als voor het afsluiten van het abonnement. Indien het AORTA abonnementenregister een 'Registreren abonnement'-bericht ontvangt met een reeds bestaande combinatie van patiëntID, Contextcode/Gegevenssoort, Rolcode, Gebeurtenistype en applicatieID, dan zal de geldigheidsduur in het AORTA abonnementenregister worden bijgewerkt op basis van de geldigheidsduur zoals opgenomen in het 'Registreren abonnement'-bericht.

Er zijn geen voorschriften over hoe de momenten van verlengen dienen te worden gekozen. Wel zijn hiervoor Best Practices opgenomen.

9.4.1.2.1 Aandachtspunten m.b.t. verlengen abonnement

In het geval een abonnement wordt verlengd door middel van VGU, dan dienen er nog wel geldige tokens t.b.v. de VGU aanwezig zijn. Daarnaast dient nog steeds sprake van een behandelrelatie te zijn.

Indien een abonnement niet verlengd wordt, dient dit abonnement te worden verwijderd, zowel lokaal als in het abonnementenregister.

9.4.2 Verwijderen Abonnement

Een verlopen abonnement zal na het verstrijken van de geldigheidsduur niet automatisch verwijderd worden uit het abonnementenregister. Een gebruiker is zelf verantwoordelijk voor het verwijderen van een abonnement. Hiervoor dient het systeem onder verantwoordelijkheid van een zorgverlener een 'Opzeggen abonnement'-bericht te versturen. Dit kan geïnitieerd worden door:

- De abonneehouder zelf op basis van zijn UZI-pas;
- Een zorgverlener op basis van zijn UZI-pas met de juiste autorisaties (die hoeft dus niet de abonneehouder te zijn);

- Een medewerker met UZI-pas die onder mandaat werkt van de betreffende zorgverlener of abonneehouder;
- Vereenvoudigd gebruik UZI-pas (VGU) in combinatie met een mandaattoken getekend door een abonneehouder of een zorgverlener met de juiste autorisaties.

Het verwijderen van een abonnement gebeurt op basis van het abonnementID dat door het systeem is verkregen na het registreren van een abonnement. Bij verwijdering uit het abonnementenregister wordt gecontroleerd of de zorgverlener (rolcode) geautoriseerd is om een abonnement te verwijderen.

De precieze invulling van het 'Opzeggen abonnement'-bericht is opgenomen in [DECOR informatie voor project: AORTA \(aorta-vzvz-\) \(nictiz.nl\)](#)¹⁰⁹.

9.4.2.1 Aandachtspunten m.b.t. verwijderen abonnement

Het verwijderen van een abonnement is niet evident:

- Er kunnen meerdere zorgverleners gebruik maken van één afgesloten abonnement, nl. zorgverleners met dezelfde rolcode;
- Een abonnement is afgesloten door een zorgverlener t.b.v. VGU.

Voordat een abonnement wordt verwijderd, dient dus met zekerheid te worden vastgesteld, dat het verwijderen van het abonnement géén impact heeft op het zorgproces.

Het abonnement dient zowel lokaal als uit het abonnementenregister verwijderd te worden. Lokaal mag er dan niet ook nog eenzelfde abonnement bij een andere zorgverlener bestaan. Er kunnen lokaal meerdere abonneehouders lokaal geregistreerd staan, die gebruik maken van hetzelfde abonnement. Voordat de applicatie een abonnement daadwerkelijk centraal laat verwijderen, dient er gecontroleerd te worden of er lokaal nog andere abonneehouders zijn, die gebruik maken van het abonnement. Indien dat het geval is, dan dient het abonnement centraal niet verwijderd te worden. Het verwijderen van een abonnement binnen een organisatie kan alleen als er geen abonneehouder meer is voor de combinatie patiënt, gegevenssoort/contextcode en applicatielID, rolcode of zorgverlener-ID.

In het geval een zorgaanbiederorganisatie gebruik maakt van VGU in combinatie met de signaalfunctie als trigger, dan is het aannemelijk dat er een abonnement staat geregistreerd voor elke patiënt waarvan een behandelrelatie staat geregistreerd. Van die patiënten dient dus goed overwogen te worden of een abonnement verlengd dient te worden i.p.v. verwijderd.

In het geval de signaalfunctie wordt toegepast t.b.v. de medicatiebewaking van een patiënt, dan dient er altijd een abonnement op aanpassingen van medicatiegegevens van die specifieke patiënt te zijn geregistreerd. Een abonnement zal in dit geval pas verwijderd worden indien de medicatiebewaking wordt gestopt.

9.4.3 Synchronisatie met Abonnementenregister

Om te voorkomen dat de lokale abonnementenregistratie uit de pas loopt met de AORTA abonnementenregistratie, is het van belang dat er een synchronisatieproces wordt geïmplementeerd. Hiervoor wordt hetzelfde mechanisme zoals is geïntroduceerd voor de VWI-synchronisatie toegepast. De definitieve uitwerking hiervan volgt.

109. <https://decor.nictiz.nl/pub/vzvz/index.php?prefix=aorta-vzvz->

9.4.4 Lokaal abonnementenregister

Het lokale abonnementenregister moet de systeemgebruiker inzichtelijk maken wie welke abonnementen op welke patiënten heeft afgesloten voor welke gegevens. Daarnaast dient de geldigheidsduur van het abonnement te worden bijgehouden.

Attribuut	Beschrijving	Cardinaliteit
AbonnementID	Het abonnementID dat is verkregen na het afsluiten van een abonnement	1..1
PatiëntID	De identifier (BSN) van de patiënt waarop een abonnement is genomen.	1..1
Context ^[1] (see page 296)	De context waarvoor een abonnement is afgesloten.	1..1
Gegevenssoort ^[2] (see page 296)	De gegevenssoort waarvoor een abonnement is afgesloten	0 .. 1
Abonneehouder	De abonneehouder die lokaal een abonnement heeft afgesloten. Dit omvat een abonneehouderID en afhankelijk van het XIS-type de rolcode van de betreffende abonneehouder ^[3] (see page 296).	1..*
ApplicatieID	ApplicatieID waarvoor een abonnement is afgesloten	0 .. 1
Geldigheidsduur	Geldigheidsduur van een abonnement	1 .. 1

^[1] (see page 296) Verplicht aanwezig indien hier ook daadwerkelijk een abonnement op is afgesloten.

^[2] (see page 296) Optioneel aanwezig indien hier ook daadwerkelijk een abonnement op is afgesloten.

^[3] (see page 296) Het opnemen van een rolcode staat verder uitgewerkt in het hoofdstuk voor het opvragen n.a.v. een signaal.

9.4.5 Afhandelen signalen

9.4.5.1 Ontvangen signalen

Een signaal als gevolg van een abonnement bevat de volgende attributen die van belang zijn voor de verwerking van het signaal:

- PatiëntID;
- Gegevenssoort of bouwsteentype;
- AbonnementID.

De precieze invulling van het ‘afleveren abonnementsignaal’-bericht is opgenomen in [DECOR informatie voor project: AORTA \(aorta-vzvz-\) \(nictiz.nl\)](#)¹¹⁰. Het systeem dient dit signaal te verwerken op de manier zoals is opgenomen in het PvE van de zorgtoepassing. Op hoofdlijnen geldt dat een signaal is verwerkt indien:

- als gevolg van het signaal de gegevens o.b.v. de VGU-functionaliteit zijn opgevraagd (afhankelijk van de toepassing kan dit direct gebeuren of op een later moment in de tijd);
- als gevolg van het signaal kunnen een of meerdere abonneehouders op de hoogte worden gesteld van het beschikbaar zijn van nieuwe gegevens, waarna een abonneehouder zelf een bevraging kan initiëren.

9.4.5.1.1 Aandachtspunten m.b.t. ontvangen signaal

In het signaal wordt géén contextcode opgenomen. Een signaal bevat het bouwsteentype dat is aangepast. Op basis van het abonnementID dat is opgenomen in het signaal, dient in het lokale abonnementenregister te worden opgezocht welke contextcode bij dit abonnement hoort. Het systeem mag maar één bevraging doen per abonnement. Het systeem zal dus moeten voorkomen dat hij op elk signaal direct een zelfde bevraging doet.

9.4.5.2 Afhandelen signaal verlopen abonnement

Indien de geldigheidsduur van een abonnement verlopen is, dan zal het XIS als gevolg hiervan een signaal ontvangen. In dat geval is de gebeurtenis-type in het signaal gevuld met het kenmerk ‘geldigheidsduur verlopen’. De precieze invulling van het ‘niet abonneerbaar signaal’ is opgenomen in [DECOR informatie voor project: AORTA \(aorta-vzvz-\) \(nictiz.nl\)](#)¹¹¹.

Een abonnerend systeem zal dit signaal moeten kunnen verwerken. Op basis van dit signaal zal een abonneehouder op de hoogte moeten worden gesteld, dat zijn abonnement verlengd of verwijderd dient te worden. Het is ook mogelijk dat het systeem op basis van dit signaal het abonnement automatisch verlengd met behulp van de VGU-functionaliteit.

9.4.5.3 Opvragen n.a.v. signalen

De afhandeling van een signaal is afhankelijk van de toepassing waarvoor een abonnement is afgesloten. Indien een signaal dient als trigger voor het initiëren van de VGU-functionaliteit, dan dient het systeem onder verantwoordelijkheid van een zorgverlener een opvraagbericht te versturen met de juiste contextcode.

Het is ook mogelijk dat een zorgverlener zelf of onder mandaat een opvraag initieert n.a.v. een ontvangen signaal. Het moet dan wel inzichtelijk zijn voor de zorgverlener of gemandateerde, dat er nieuwe gegevens op te vragen zijn.

110. <https://decor.nictiz.nl/pub/vzvz/index.php?prefix=aorta-vzvz->

111. <https://decor.nictiz.nl/pub/vzvz/index.php?prefix=aorta-vzvz->

9.4.5.3.1 Aandachtspunten m.b.t. opvragen n.a.v. signalen

9.4.5.3.1.1 Autorisatie

Autorisatie voor het opvragen van gegevens gebeurt op basis van de rolcode van een verantwoordelijke zorgverlener. Het is mogelijk dat er meerdere abonneehouders met verschillende rolcodes een abonnement hebben afgesloten voor een zelfde combinatie van patiënt, contextcode en applicatieID.

Het is zaak om de AORTA infrastructuur niet overmatig te bevragen. Dit kan namelijk een bronsysteem zodanig belasten, dat het de gegevensstroom niet meer kan verwerken. Echter, het is ook van belang om alle informatie op te vragen die een abonneehouder verwacht; een bevraging o.b.v. een rolcode met een autorisatiebeperking mag niet leiden tot het missen van medische gegevens.

VZVZ dient een lijst beschikbaar te stellen met vergelijkbare autorisaties. Deze is te vinden in de autorisatierichtlijn Medicatieveiligheid. Hierin dient te zijn opgenomen welke rolcode voor welke contextcode eenzelfde autorisatie kent. Een opvragend systeem moet op basis van deze lijst zo efficiënt als mogelijk bevragingen uit sturen.

9.4.5.3.1.2 Minimale bevraging o.b.v. contextcode

Een contextcode bestaat uit één of meerdere bouwsteentypes. Het kan dus zijn dat er voor één abonnementID meerdere signalen nagenoeg tegelijkertijd ontvangen worden. Indien de XIS-applicatie een signaal verwerkt op basis van de VGU-functionaliteit, dan dient de applicatie binnen een tijdsbestek van 5 seconden éénmaal een bevraging te doen t.b.v. dit abonnementID. Er dient dus niet op elk signaal met hetzelfde abonnementID te worden gereageerd. Indien de XIS-applicatie de abonneehouder op de hoogte stelt van het ontvangen van een signaal, dan dient er als gevolg van initiatie van een bevraging door een abonneehouder, maar één bevraging gedaan te worden per abonnementID.

Een bouwsteentype kan voor komen in meerdere contextcodes. Indien er voor meerdere contextcodes een abonnement is afgesloten, dan kan dit er toe leiden dat er meerdere bevragingen tegelijkertijd gedaan dient te worden met deze contextcodes.

9.4.5.4 Tonen verwerking signaal aan gebruiker

Een abonneehouder moet afhankelijk van de toepassing van de signaalfunctie inzichtelijk krijgen of er nieuwe gegevens zijn opgevraagd (i.h.g.v. VGU) of opvraagbaar zijn. Voor medicatiebewaking is het van belang dat een abonneehouder heel expliciet een melding krijgt van nieuwe gegevens op het moment van ontvangen van een signaal.

Voor de overige situatie is het afhankelijk van de situatie of zorgverlener op de hoogte gesteld moet worden van nieuw opgevraagde gegevens. Een zorgverlener moet zich in ieder geval bewust zijn, dat er door middel van de VGU op elk moment nieuwe gegevens opgevraagd kunnen zijn van een patiënt.

9.4.5.5 Hybride situatie

Een abonnement kan zowel op contextcode als op gegevenssoort worden afgesloten. Afhankelijk van de situatie, dient een systeem zowel een abonnement af te sluiten op contextcode als op gegevenssoort.

Indien een abonnement afgesloten wordt op gegevenssoort, dan zullen er alleen signalen ontvangen worden indien een bronsysteem een gegevenssoort (her)aanmeldt of verwijderd. In het signaal is opgenomen welk specifieke gegevenssoort en welk abonnementID het betreft. Op basis van de gegevenssoort moet worden bepaald welke interactie eruit gestuurd dient te worden. De XIS-applicatie moet de vertaling van gegevenssoort naar interactieID geconfigureerd hebben in zijn applicatie.

Indien een abonnement afgesloten wordt op contextcode, dan zullen er alleen signalen ontvangen worden indien een bronsysteem een bouwsteen (her)aanmeldt of verwijderd. In het signaal is opgenomen welk specifieke bouwsteentype en welk abonnementID het betreft. Op basis van het abonnementID dient de XIS-applicatie te bepalen welk contextcode dient te worden opgenomen in de bevraging.

Het nemen van het niveau waarop een abonnement genomen moet worden, is afhankelijk van de specifieke versie van de zorgtoepassing dat geïmplementeerd wordt door de XIS-leverancier. Er is een overgangperiode waarbij bronnen binnen die zorgtoepassing alleen nog op gegevenssoort aanmelden, op gegevenssoort en bouwsteentype of alleen nog maar op bouwsteentype. Afhankelijk van hoe de bronnen binnen een zorgtoepassing aanmelden, dient er op contextcode of gegevenssoort een abonnement te worden afgesloten.

Indien er tegelijkertijd meerdere signalen wordt ontvangen van een systeem met bouwstenen en gegevenssoorten, dan is het afdoende om alleen een vraag te stellen met de bijbehorende contextcode.

9.4.6 Processen m.b.t. signaalfunctie

9.4.6.1 Proces na verlopen geldigheidsduur abonnement

Om het zorgproces niet in gevaar te brengen, zullen abonnementen na de geldigheidsduur niet automatisch verwijderd worden. Deze abonnementen zullen actief blijven en de signaalfunctie zal dus blijven werken. Echter, het is wel van belang dat een abonneehouder actie onderneemt om het abonnement te verwijderen of te verlengen. Er zijn diverse processen om te borgen dat dit ook daadwerkelijk gebeurt.

9.4.6.1.1 Rol GBZ-beheerder

Indien de geldigheidsduur van een abonnement is verlopen, dan zal dit kenbaar worden gemaakt aan de daarvoor verantwoordelijke rollen binnen VZVZ. Deze zullen contact opnemen met de GBZ-beheerder die verantwoordelijk is voor het systeem waarin de abonnementen staan geregistreerd. De GBZ-beheerder dient vervolgens met de betreffende abonnementID's te achterhalen welke abonnementen verlengd of verwijderd dienen te worden en dient de verantwoordelijke abonneehouder hierop aan te spreken.

9.4.6.1.2 Proces binnen applicatie

Indien een abonnement verlopen is, dan zal het systeem hiervan op de hoogte worden gebracht door een 'niet abonneerbaar signaal'. Het 'niet abonneerbaar signaal' zal een melding bevatten dat een specifiek abonnement (o.b.v. abonnementID) is verlopen. Een abonneehouder dient deze melding getoond te krijgen en dient hier op te acteren door middel van het verlengen of verwijderen van een abonnement.

9.4.6.1.3 Best Practice

Om te voorkomen dat een abonnement verloopt is het aan te raden om een abonneehouder vroegtijdig op de hoogte te stellen van het verlopen van een abonnement. Op basis van de lokaal geregistreerde geldigheidsduur van een abonnement kan het systeem een melding genereren, die getoond wordt aan de abonneehouder. Een abonneehouder kan hier dan op reageren door het abonnement te verlengen of te verwijderen.

Indien het systeem werkt met de VGU-functionaliteit, dan is het mogelijk om het verlopen van de geldigheidsduur als trigger te laten werken voor het verlengen van het abonnement. In dat geval dient wel een behandelrelatie en een inschrijftoken aanwezig te zijn van de patiënt op wiens gegevens geabonneerd dient te worden. Daarnaast dient het systeem de beschikking te hebben over een geldig mandaattoken van de abonneehouder.

Het automatisch verwijderen van een abonnement o.b.v. de VGU-functionaliteit wordt beschreven in 'Proces m.b.t. VGU'.

9.4.6.2 Uitdiensttreding zorgverlener

Indien een zorgverlener uit dienst treedt, dient een abonnement die centraal onder zijn verantwoordelijkheid staat geregistreerd verwijderd te worden.

Mogelijk dient dit abonnement opnieuw te worden afgesloten door de vervangende zorgverlener of een reeds geregistreerde abonneehouder. Bij 'het verwijderen van een abonnement' staat beschreven waar men op moet letten in het geval een abonnement wordt verwijderd.

10 Aansluit- en Implementatiewijzer Kern

10.1 Berichttransport

10.1.1 AORTA_Trp_IH_Berichttransport

- **IH Berichttransport**

Datum: 1 mei 2022

Publicatie: V8.3.0.0

10.1.1.1 Inleiding Berichttransport

10.1.1.1.1 Doel en scope

Dit document specificeert het berichttransport over SOAP/HTTP zoals dat in AORTA wordt toegepast. Het berichttransport vormt de verbinding tussen de HTTP(S)-laag, en de er bovenliggende HL7v3-berichten. Dit document beschrijft:

- hoe HL7v3-interacties worden verpakt in SOAP voor transport op basis van webservices;
- hoe SOAP op hoofdlijnen wordt toegepast binnen AORTA;
- hoe webservices worden gedefinieerd met behulp van WSDL;
- de toepassing van HTTP(S)-transport in relatie tot de webservices;
- versionering van webservices en end point uri's;
- betrouwbaarheidsaspecten van dat transport.

10.1.1.1.2 Doelgroep voor dit document

Dit document is bedoeld voor softwareontwikkelaars van zorgtoepassingen en de Zorg Informatie Makelaar (ZIM), die op grond van de HL7v3-communicatiestandaard en dit document berichten in AORTA willen transporteren.

De lezer wordt verondersteld kennis te hebben van [XML], [SOAP] en [WSDL]. Lezing van de AORTA-documentatie wordt ten zeerste aanbevolen.

10.1.1.1.3 Documenthistorie

Versie	Datum	Omschrijving
6.10.0.0	12-okt-2011	Initiële versie na herstructurering AORTA-documentatie. RFC 46142: Wijziging in verband met elektronische handtekening: gebruik SOAP Header attributen (§4.3). RFC 46691: HTTP Fouten doorgeven door ZIM verduidelijkt in Par 4.5 en 4.5.4.
6.10.0.0	2-apr-2012	RFC 51940: toegestane waarden voor faultactor opgenomen in Par 4.5.2.
6.11.0.0	5-dec-2012	Herpublicatie als onderdeel van AORTA-Infrastructuur v6.11
6.12.0.0	13-aug-2013	RfC 52089: Fout met ZIM als tussenstation verduidelijkt.
8.0.1.0	15-mei-2017	RfC 52477: Uitwisseling op basis van bouwstenen
8.0.1.0	15-mei-2017	RfC 76206: SSL verwijderen

8.0.3.0	15-nov-2018	Opgenomen in publicatie 8.0.3.0
8.1.0.0	1-aug-2019	INI-8877: Toevoegen inschrijftoken t.b.v. conditionele query

10.1.1.1.4 Legenda

Dit document gebruikt de volgende symbolen:

	Let op! Dit is een aandachtspunt. Een opmerking die de aandacht vestigt op een bepaald opvallend aspect.
	Dit is een 'open issue' of 'known issue'. Een kwestie die nog open ligt voor discussie, maar onderkend is.
	Dit is een frequently asked question (FAQ) met antwoord.

10.1.1.1.5 Structuur

Dit document is als volgt opgebouwd:

- Inleiding (niet normatief).
- Berichtuitwisselingsstandaarden (niet normatief): inleiding in de relevante gebruikte standaarden.
- Informatiestromen (niet normatief): een overzicht van berichtuitwisseling zoals gebruikt bij het landelijk EPD.
- XML, SOAP en HTTP (normatief): richtlijnen voor het gebruik. Voor GBx'en geldt dat §3 alleen verplicht is bij ondersteuning van elektronische handtekening^[1].
- AORTA en WSDL (normatief): algemene toelichting bij de WSDL bestanden.
- Betrouwbaar transport (normatief).

Normatief betekent dat het verplicht is om te conformeren aan de specificaties. De niet normatieve hoofdstukken zijn bedoeld als achtergrondinformatie.

Noot: dit document gebruikt veel voorbeelden van XML materialen (WSDL, XSD, XML), de XML materialen die AORTA publiceert zijn mogelijk recenter, en leidend.

[1] De elektronische handtekening wordt binnen AORTA vooralsnog niet toegepast.

10.1.1.2 Berichtuitwisselingsstandaarden

Het transport van documenten in AORTA is gebaseerd op een aantal standaarden: SOAP, WSDL, WS-I Basic Profile, Web Service Security (WSS) en relevante delen van de HL7v3-standaard (met name Transmission Infrastructure en Query Infrastructure). Dit hoofdstuk licht deze standaarden kort toe.

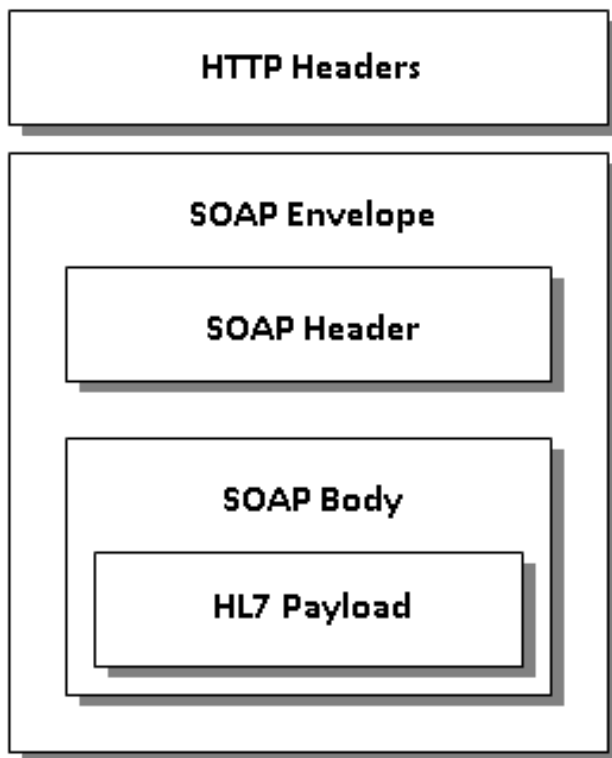
10.1.1.2.1 SOAP

SOAP 1.1 – Simple Object Access Protocol – is een “de facto standaard” voor uitwisseling van gegevens over – onder andere - internet. AORTA gebruikt SOAP 1.1.

Een SOAP-document is een XML-document. Het bestaat uit drie onderdelen:

1. De SOAP Envelope is het omringende deel.
2. De SOAP Header is een optionele verzameling headers die bijvoorbeeld meta-informatie over het bericht kunnen bevatten. Eventuele tokens, zoals bijvoorbeeld voor authenticatie, worden opgenomen in de SOAP Header.
3. De SOAP Body bevat het eigenlijke bericht. De Body bevat de "data", de Header de bijbehorende "metadata".

SOAP kent een mapping op HTTP, waarbij HTTP als transportmechanisme gebruikt wordt om een SOAP-document te transporteren. Zie Figuur 1 voor een overzicht van een SOAP bericht.



Figuur 1 - Overzicht SOAP bericht

De verschillende onderdelen zien er als volgt uit.

```

<?xml version="1.0" encoding="utf-8"?>

<Envelope ... namespace declaraties ... >

  <Header>

    ... headers ...

  </Header>

  <Body>

    ... payload ...

  </Body>

</Envelope>

```

De SOAP Envelope is het omsluitende XML-element. Dit element bevat de SOAP Headers en de SOAP Body. Er hoeven geen headers aanwezig te zijn; een SOAP Body is wel verplicht. SOAP Headers worden meestal gebruikt voor meta-informatie die te maken heeft met authenticatie, beveiliging, transactiemanagement of betalingen. De Body bevat de "payload", de eigenlijke gegevens die verzonden worden.

10.1.1.2.2 WSDL

WSDL – Web Services Description Language – is een taal om Web Services te beschrijven. Het is een hulpmiddel en het vereenvoudigt het bouwen van interoperabele Web Services. WSDL 1.1 is een W3C Note, die als “de facto” standaard geldt. AORTA gebruikt WSDL 1.1.

WSDL dient de volgende doelen:

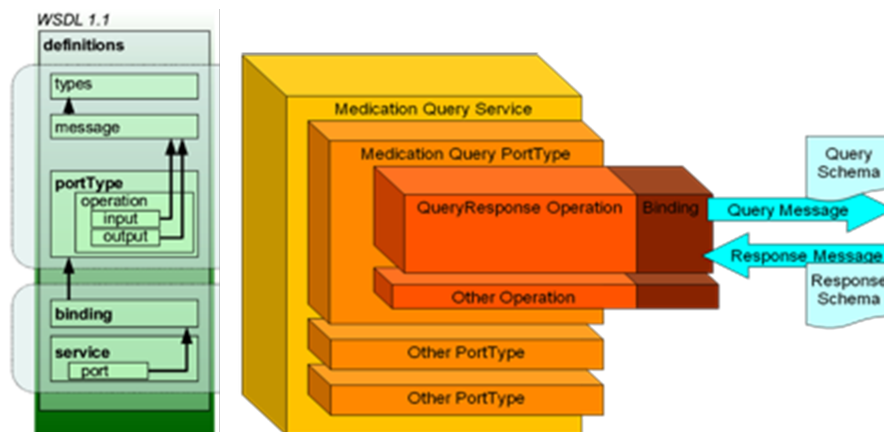
- Eenduidige en machine leesbare beschrijving van de Web Service.
- Invoer voor een codegenerator die een deel van de voor de Web Service benodigde code genereert.

Een WSDL document bestaat uit de volgende onderdelen:

- Hier worden abstracte XML-structuren beschreven in XML Schema formaat.

- Met de elementen en elementtypen uit de Types worden Messages samengesteld – dit zijn generieke berichten gedefinieerd in XML.
- Een PortType is een logische “applicatiepoort” die één of meer Operations ondersteunt. Een Operation bestaat uit één of meer Inputs en Outputs. Deze Inputs en Outputs verwijzen naar de Messages die hierboven beschreven zijn. Een Message beschrijft dus de interne structuur van één of meer Inputs of Outputs.
- Een Binding verbindt een – logisch – PortType met een specifiek transportprotocol, zoals SOAP over HTTP. Alle Operations, Inputs en Outputs uit de Port Type worden toegewezen aan SOAP.
- Een Service bestaat uit één of meer fysieke Ports. Een Port verbindt een Binding met een locatie, normaal gesproken een URI waarmee de Port over het Internet aangeroepen kan worden.

Twee manieren van een grafische weergave van de onderdelen van een WSDL zijn opgenomen in Figuur 2.



Figuur 2 – Twee grafische weergaven van wsdl onderdelen

10.1.1.2.3 WS-I Basic Profile

WS-I Basic Profile 1.0 is een specificatie gepubliceerd door WS-I, een ad hoc consortium van voornamelijk softwareleveranciers. Het Basic Profile beschrijft hoe SOAP 1.1 en WSDL 1.1 gebruikt kunnen worden om interoperabele Web Services te bouwen en geeft richtlijnen over hoe SOAP en WSDL het beste gebruikt kunnen worden. Op deze wijze corrigeert het Basic Profile veel van de tekortkomingen van SOAP en WSDL. AORTA volgt het Basic Profile tenzij anders aangegeven.

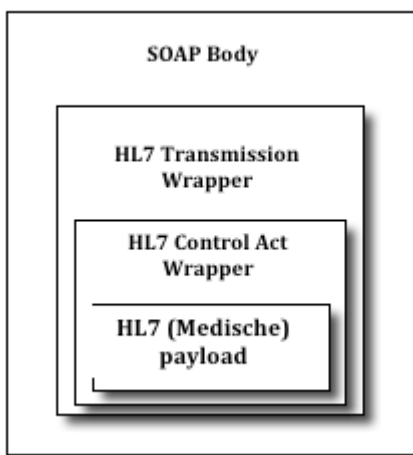
10.1.1.2.4 HL7v3

HL7v3 kent verder een aantal onderdelen die te maken hebben met het transport van gegevens. HL7v3 definieert de volgende onderdelen:

- In de Transmission Wrapper worden metagegevens opgeslagen die te maken hebben met het bericht zelf: id, datum waarop het is aangemaakt, afzender, geadresseerde en dergelijke.

- De Trigger Event Control Act Wrapper bevat gegevens over de gebeurtenis die aanleiding was het bericht te versturen. Ook zijn hierin gegevens opgenomen die te maken hebben met de verwerking van het bericht, bijvoorbeeld het aantal records dat een query terug moet sturen (er zijn veel specialisaties van deze wrapper).
- De Batch Wrapper kan gebruikt worden om meerdere berichten van dezelfde of verschillende soort in te pakken.

Tezamen met de eigenlijke (medische) gegevens, de payload, vormen deze wrappers een XML-document. De inhoud van de SOAP Body is weergegeven in Figuur 3.



Figuur 3 - Inhoud SOAP Body

10.1.1.3 Informatiestromen

10.1.1.3.1 AORTA en gegevensuitwisseling

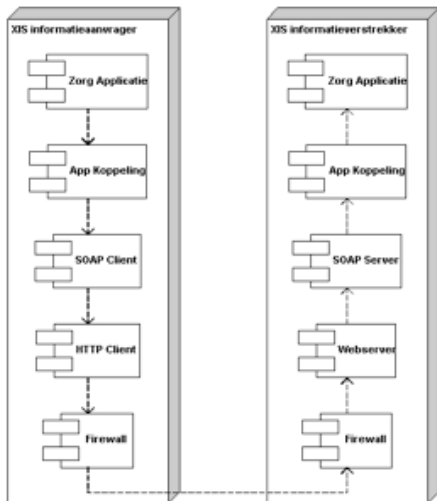
In AORTA vindt gegevensuitwisseling plaats op basis van SOAP/HTTP over met TLS beveiligde verbindingen en hierbij zijn webservices beschreven in WSDL.

WSDL is, strikt gesproken, optioneel. Veel tools genereren op basis van WSDL een deel van de code. Het is echter ook mogelijk de webservice te bouwen zonder WSDL, en in die zin is gebruik van WSDL optioneel.

10.1.1.3.2 Globaal overzicht informatiestroom

Een SOAP-interactie kent een client en een server. De SOAP client stuurt een request naar de server via HTTP, en ontvangt het antwoord via HTTP.

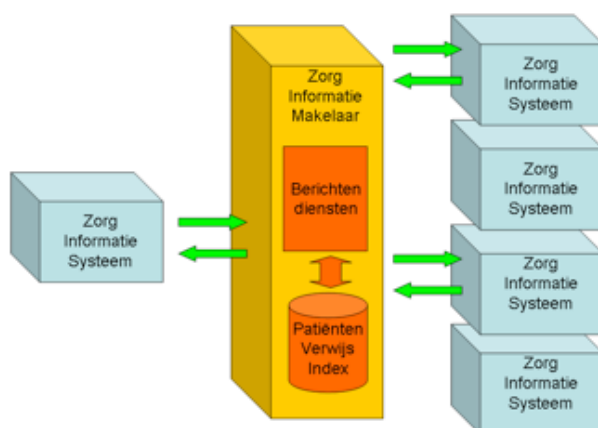
Een dergelijke interactie stelt verschillende eisen aan de client en de server. Een client hoeft alleen een verbinding te hebben en beschikbaar te zijn op het moment dat de aanroep gedaan wordt. De server zal echter continu moeten luisteren op een poort of er een aanroep binnenkomt. De pijlen in Figuur 4 geven het verloop van een SOAP request aan. Een response volgt de omgekeerde weg.



Figuur 4 - AORTA interactie

10.1.1.3.3 SOAP en de ZIM

In bovenstaande beschrijving is alleen gesproken over berichtenuitwisseling tussen een client en een server. In AORTA worden berichten echter grotendeels uitgewisseld tussen een client en server via de Zorg Informatie Makelaar (ZIM), zie Figuur 5.



Figuur 5 - Berichtenuitwisseling via de ZIM

Voorbeeld van AORTA berichtenuitwisseling.

Een ziekenhuis vraagt een overzicht van medicijnverstrekkingen voor een patiënt op. De opvraging van het ziekenhuis is geadresseerd aan de ZIM. De ZIM is verantwoordelijk voor het opzoeken van de applicaties die deze gegevens kunnen leveren en zendt de opvraging door aan één of meer applicaties. De ZIM zal de adressering van de berichten aanpassen: deze doorgezonden opvragingen zijn geadresseerd aan de zorginstellingen die over de gevraagde medicatiegegevens beschikken. Alle berichten zijn SOAP berichten. In SOAP client/server terminologie betekent dit het volgende. Het opvragende, initiërende zorg informatiesysteem is client, de ZIM fungeert als server voor dit systeem. Wanneer de ZIM de opvragingen doorstuurt is de ZIM client en zijn de reagerende zorg informatiesystemen die de gevraagde gegevens opleveren server. De ZIM is vervolgens weer, als server, verantwoordelijk voor het doorsturen van de antwoorden aan het initiërende ziekenhuis.

Voorbeeld van AORTA berichtenuitwisseling o.b.v. context.

Een ziekenhuis vraagt een overzicht van medicijnverstrekkingen voor een patiënt op. In het opvraagbericht wordt de juiste contextcode opgenomen behorende bij "het opvragen van een overzicht van medicijnverstrekkingen". De opvraging van het ziekenhuis is geadresseerd aan de ZIM. De ZIM is verantwoordelijk voor het opzoeken van de applicaties die deze gegevens kunnen leveren. Hiervoor zoekt de ZIM de juiste bouwstenen op behorende bij de context en bepaalt welke bouwsteeninteracties verzonden moeten worden naar welke bronsystemen. Het is mogelijk dat een bronsysteem meerdere bouwsteeninteracties ontvangt. Alle berichten zijn SOAP berichten. In SOAP client/server terminologie betekent dit het volgende. Het opvragende, initiërende zorg informatiesysteem is client, de ZIM fungeert als server voor dit systeem. Wanneer de ZIM de opvragingen doorstuurt is de ZIM client en zijn de reagerende zorg informatiesystemen die de gevraagde gegevens opleveren server. De ZIM is vervolgens weer, als server, verantwoordelijk voor het doorsturen van de antwoorden aan het initiërende ziekenhuis. Het doorsturen van de ontvangen antwoorden gebeurt met behulp van een batchwrapper. Alle antwoorden zijn hiermee opgenomen in één antwoordbericht.

10.1.1.4 XML, SOAP en HTTP

10.1.1.4.1 XML

Berichten worden uitgewisseld in XML 1.0.

UTF-8 is voor XML de meest gangbare Unicode-encoding. Encoding wordt aangegeven in een XML-prolog:

```
<?xml version="1.0" encoding="utf-8"?>
```

Berichten worden uitgewisseld en gelogd in UTF-8 encoding.

10.1.1.4.2 SOAP berichtformaat

Berichten worden verpakt volgens de SOAP 1.1 standaard.

Het HL7v3-bericht wordt opgenomen in de SOAP Body van de SOAP Envelope.

Hieronder staat een voorbeeld van een HL7v3-bericht dat is verpakt in een SOAP Envelope. Het betreft een opvraag van medicatieverstrekkingen. De voorbeelden in dit document gaan uit van een opvraag met behulp van een zorgtoepassing specifieke interactie. De opbouw van een generieke interactie is in grote lijnen hetzelfde. Eventuele afwijkingen ten opzichte van de voorbeelden worden in het hoofdstuk besproken.

```

<?xml version="1.0" encoding="utf-8"?>

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <soapenv:Body>

        <QURX_IN990111NL xmlns="urn:hl7-org:v3">

            <id extension="0032616767" root="2.16.840.1.113883.2.4.6.2.451.12.21"/>

            <creationTime value="20040910170245"/>

            ... andere elementen van de Transmission Wrapper...

            <ControlActProcess moodCode="EVN">

                <subject>

                    <QueryByParameterPayload>

                        ... verdere inhoud ...

                    </QueryByParameterPayload>

                </subject>

            </ControlActProcess>

        </QURX_IN990111NL>

    </soapenv:Body>

</soapenv:Envelope>

```

Het voorbeeld is hieronder in stukken geknipt en van commentaar voorzien.

De prolog met UTF-8 declaratie.

```
<?xml version="1.0" encoding="utf-8"?>
```

SOAP Envelope met daarin namespace declaraties.

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
```

SOAP Body met daarin het omsluitende element van de opvraging van medicatieverstrekkingen. Omdat dit element de HL7v3-namespace tot default namespace maakt, maken alle elementen daarin automatisch deel uit van de HL7v3-namespace.

```
<soapenv:Body>
  <QURX_IN990111NL xmlns="urn:hl7-org:v3">
```

Elementen uit de Transmission Wrapper van HL7v3.

```
<id extension="0032616767" root="2.16.840.1.113883.2.4.6.2.451.12.21"/>
  <creationTime value="20040910170245"/>
  ... andere elementen van de Transmission Wrapper...
```

De Control Act Wrapper.

```
<ControlActProcess moodCode="RQ0">
  <subject>
```

Het feitelijke bericht, een opvraging naar medicatie van een bepaald PatientId.

```
<QueryByParameterPayload>
  ... verdere inhoud ...
</QueryByParameterPayload>
```

Afsluiting van de onderdelen.

```
</subject>
</ControlActProcess>
</QURX_IN990111NL>
</soapenv:Body>
</soapenv:Envelope>
```

10.1.1.4.3 SOAP Header attributen

Er zijn verschillende soorten SOAP Headers mogelijk. De beveiliging implementatiehandleidingen [IH BA DigiD] [IH BA PKIO-pas] [IH BA Transactietoken] [IH BA Mandaattoken] [IH BA Inschrijftoken] [IH tokens generiek] beschrijven deze headers. Deze paragraaf beschrijft de mogelijke attributen van SOAP-headers.

SOAP 1.1 kent twee attributen voor headers, namelijk “actor” en “mustUnderstand”. De hierna volgende paragrafen beschrijven deze achtereenvolgens.

10.1.1.4.3.1 SOAP actor

SOAP headers kunnen verschillende bestemmingen hebben. AORTA kent de Zorg Informatie Makelaar (ZIM) en het Goed Beheerde Informatiesysteem (GBx), zie [Arch AORTA] voor een uitleg van deze begrippen.

Het attribuut soap:actor geeft aan welke “actor” een bepaalde header moet verwerken. Met de soap:actor wordt in AORTA een functie aangegeven: bijvoorbeeld de ZIM of het GBx dat als eindbestemming dient. De soap:actor geeft in AORTA dus geen adres van een specifiek GBx.

```
<soap:Header xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  ...
  <wss:Security xmlns:wss=
    "http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd"
    soap:actor="http://www.aortarelease.nl/actor/gbx" soap:mustUnderstand="1">
    ...
  </wss:Security>
</soap:Header>
```

Voor de headers voor tokenauthenticatie en andere headers gericht aan de ZIM wordt aangeraden de waarde <http://www.aortarelease.nl/actor/zim> te gebruiken. Voor headers gericht op een GBx is de waarde <http://www.aortarelease.nl/actor/gbx> verplicht.

```
<ao:authenticationTokens ... soap:actor="http://www.aortarelease.nl/actor/zim">
<wss:Security ... soap:actor="http://www.aortarelease.nl/actor/gbx">
```

Andere waarden voor actor zijn niet toegestaan. De ZIM dient een header gericht aan een GBx ongewijzigd door te geven aan het GBx van bestemming.

10.1.1.4.3.2 SOAP mustUnderstand

Het SOAP mustUnderstand attribuut geeft aan of de ontvanger de header moet verwerken. Dit geldt voor de bestemming (actor) van de header, zoals beschreven in voorgaande [paragraaf 4.3.1 \(see page 319\)](#). Het mustUnderstand attribuut werkt dus samen met het actor attribuut. Een ontvanger die niet de bestemming van de header vertegenwoordigt, dus niet de actor is, verwerkt de header sowieso niet. De ZIM moet een header zonder actor interpreteren alsof die voor de ZIM bedoeld is.

De waarde van het mustUnderstand attribuut kan "1" of "0" zijn. Afwezigheid van het mustUnderstand attribuut is gelijk aan waarde "0".

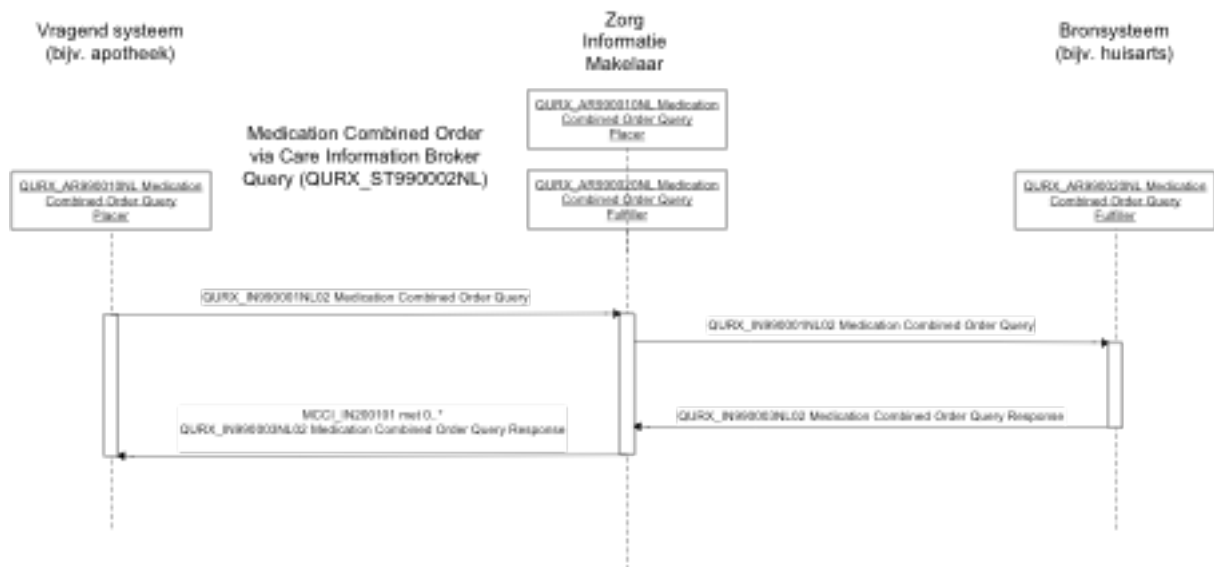
Als de header een SOAP mustUnderstand attribuut bevat met waarde "1", dan is de actor verplicht om deze header correct te verwerken òf moet de actor het gehele bericht weigeren met een SOAP:MustUnderstand fout, zie [paragraaf 4.5.2 \(see page 327\)](#).

Als de header een SOAP mustUnderstand attribuut bevat met waarde "0", dan mag de actor deze header verwerken, maar het hoeft niet. Het is dan niet toegestaan om een SOAP mustUnderstand fout te genereren ten gevolge van deze header.

10.1.1.4.4 HTTP Binding

HTTP voegt aan een te transporteren document – bijvoorbeeld een SOAP-document – een aantal HTTP Headers toe. HTTP uitwisseling vindt altijd in paren plaats – een HTTP request wordt beantwoord met een HTTP response. HTTP kent een aantal verschillende methoden – zoals GET (opvragen van een resource), PUT (afleveren van een resource) en POST (wijzigen van een resource). Voor SOAP is alleen POST van belang.

SOAP 1.1 definieert een binding op HTTP waarbij SOAP requests en responses met HTTP POST worden uitgewisseld. Daarbij wordt het SOAP request als HTTP request met de method POST verzonden naar een server, die (behoudens fouten) een SOAP response, verpakt in een HTTP response, terugzendt als antwoord op de POST. Hieronder een voorbeeld van een SOAP request – response over HTTP. Dit voorbeeld is gebaseerd op het volgende interactiediagram, een fragment van “medicatieverstrekkingen opvragen”.



Figuur 6 – Interactiediagram “medicatieverstrekkingen opvragen”

Hieronder het verzoek, dus zowel het HTTP als het SOAP request, als de HL7v3-interactie QURX_IN990111NL (Medication Dispense List Query).

```

POST /VerstrekkingsLijstquery HTTP/1.1
Host: www.zim.nl
SOAPAction: "urn:hl7-org:v3/VerstrekkingsLijstquery_QueryResponse"
Connection: Close
Content-Length: 1874
Content-Type: text/xml; charset=UTF-8

```

```

<?xml version="1.0" encoding="utf-8"?>
<soapenv:Envelope
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Body>
    <QURX_IN990111NL xmlns="urn:hl7-org:v3">

      ... inhoud ...

    </QURX_IN990111NL>
  </soapenv:Body>
</soapenv:Envelope>

```

Eerst wordt de HTTP methode genoemd (POST), en de versie, dan volgen een aantal headers met HTTP gegevens. SOAP 1.1 verplicht het noemen van "text/xml" als Content-Type.



Merk op: de HTTP Header "Content-Type" moet waarde "text/xml" bevatten.

SOAP 1.1 verplicht het gebruik van een SOAPAction HTTP Header bij SOAP over HTTP. De quotes eromheen zijn verplicht volgens het WS-I Basic Profile, om te voorkomen dat een header met en zonder quotes als verschillend geïnterpreteerd kunnen worden. Een HTTP Server kan deze SOAPAction gebruiken om het verkeer binnen een Goed Beheerd Zorgsysteem (GBZ), Goed Beheerd Patiëntenportaal (GBP), Goed Beheerd Klantenloket (GBK) of ZIM verder te routeren naar de verwerkende applicatie zonder het SOAP bericht zelf te hoeven openen.

Hieronder een voorbeeld van de HTTP response op de POST methode. Dit is tevens de SOAP response, en de HL7v3-interactie QURX_IN990113NL (Medication Dispense List Query Response):

```

HTTP/1.1 200 OK

Content-Length: 7904

Content-Type: text/xml; charset=utf-8

Date: Wed, 03 Feb 2010 12:59:18 GMT

Server: Apache-Coyote/1.1


<?xml version="1.0" encoding="utf-8"?>

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <soapenv:Body>

        <QURX_IN990113NL xmlns="urn:hl7-org:v3">

            ... inhoud ...

        </QURX_IN990113NL>

    </soapenv:Body>

</soapenv:Envelope>

```

Eerst wordt de HTTP-versie aangegeven en de status (200 OK). Vervolgens weer enige HTTP Headers en dan de SOAP Envelope.

Het is belangrijk in te zien dat er requests / responses zijn op drie verschillende niveaus:

- een HTTP request / response paar

- een SOAP request / response paar
- een HL7v3-interactie en een HL7v3-antwoordinteractie.

Deze drie niveaus zijn in principe onafhankelijk van elkaar. In dit voorbeeld is er voor gekozen het HL7v3-antwoord in de SOAP response te verpakken, en die weer in de HTTP response. Dit is echter niet noodzakelijk. Het is bijvoorbeeld heel goed mogelijk de HL7v3-interactie in een apart HTTP request/response paar te verpakken, en het HL7v3-antwoord in een tweede HTTP request/response paar. De HTTP Binding van SOAP bepaalt de manier waarop een SOAP request en response op HTTP afgebeeld worden. De SOAP Binding van HL7v3 bepaalt de wijze waarmee een HL7v3-request en -response (bijvoorbeeld een QueryContinuation en QueryResponse) afgebeeld worden op SOAP.

In AORTA is er, behoudens HTTP- en SOAP-fouten, altijd een HTTP Response met daarin een SOAP Body die een HL7v3-interactie bevat. Een SOAP request/response paar wordt dus gebonden op één HTTP request/response paar en er wordt voor deze response altijd een HL7v3-interactie gemodelleerd.

10.1.1.4.5 Bij HTTP- en SOAP-fouten kan niet altijd een HL7v3-bericht en/of SOAP response worden geconstrueerd. HTTP errors en SOAP Faults

Foutafhandeling kan plaatsvinden op diverse niveaus. Fouten op TCP-niveau of lager in de stack (IP tot en met fysiek medium) worden hier niet besproken. Relevant zijn fouten op de volgende niveaus:

- HTTP;
- SOAP;
- HL7v3.

Bij alle fouten moet onderscheid gemaakt worden tussen foutsituaties waarbij de fout ligt bij het bericht dat ingezonden wordt (client fouten) en de server (server fouten). Wanneer er iets mis is met het bericht (volgens de ontvanger), is het niet zinvol hetzelfde bericht later nogmaals te sturen: dat zal tot dezelfde fout leiden. Wanneer er iets mis is met de server, is dat vaak tijdelijk. Dan is later opnieuw proberen wel zinvol.

Protocol	Client fouten	Server fouten
HTTP	HTTP statuscode in de range 4xx	HTTP statuscode in de range 5xx
SOAP	soap:Client faults	soap:Server faults
HL7v3	Error met typecode CE (Commit Error)	Error met typecode CR (Commit Reject)

Bij alle fouten heeft het de voorkeur in beschikbare tekst elementen (zoals SOAP:detail of HTTP Body) meer informatie op te nemen omtrent de fout.

10.1.1.4.5.1 HTTP-foutsituaties

	AORTA volgt de door WS-I Basic Profile gedefinieerde richtlijnen voor HTTP-fouten bij gebruik van SOAP.

De meest relevante richtlijnen zijn opgenomen in onderstaande tabel.

Co de	Basic Profile tekst	Toelichting
R1 14 0	A MESSAGE SHOULD be sent using HTTP/1.1.	
R1 10 7	A RECEIVER MUST interpret SOAP messages containing only a soapenv:Fault element as a Fault.	Een applicatie mag dus niet alleen naar HTTP 200 OK kijken voor het bepalen van het succes. Hetzelfde geldt voor HL7v3-fouten: als het HL7v3-bericht een foutsituatie aangeeft, is het een fout, ook al is de HTTP status 200 OK.
R1 11 1	An INSTANCE SHOULD use a "200 OK" HTTP status code for responses that contain a SOAP message that is not a SOAP fault.	Aanbevolen wordt om alleen HTTP 200 OK te gebruiken als HTTP succes code.
R1 12 4	An INSTANCE MUST use a 2xx HTTP status code for responses that indicate a successful outcome of a request.	Ontvangers dienen HTTP responses met andere 2xx succes statussen wel te kunnen accepteren.
R1 12 5	An INSTANCE MUST use a 4xx HTTP status code for responses that indicate a problem with the format of the request.	
R1 11 3	An INSTANCE SHOULD use a "400 Bad Request" HTTP status code, if the request message is a malformed HTTP request, or not well-formed XML.	

R1 12 6	An INSTANCE MUST use a "500 Internal Server Error" HTTP status code if the response message is a SOAP Fault.	

De ontvanger van een HTTP response dient de HTTP status te controleren, en alle geldige HTTP statussen te accepteren en behandelen. Met name de HTTP "408 Request Timeout" dient behandeld te worden, zie hoofdstuk 6.

10.1.1.4.5.2 SOAP Faults

SOAP kent een Fault element dat onderdeel is van de SOAP Body en daar maar één keer mag voorkomen. Het SOAP Fault element heeft vier subelementen, hieronder kort toegelicht.

faultcode

Een verplicht element. De waarde van dit element moet namespace gekwalificeerd zijn. SOAP kent zelf vier foutcodes die verderop in deze paragraaf genoemd worden.

faultstring

Een verplicht element die een voor mensen leesbare uitleg bevat over de aard van de opgetreden fout.

faultactor

Dit element is bedoeld om informatie te geven over wie de fout gegenereerd heeft. Het lijkt op het SOAP actor attribuut, maar geeft de bron van de fout aan in plaats van het einddoel van de header. Applicaties die niet het eindpunt (ultimate destination) zijn van het SOAP bericht, moeten het faultactor element opnemen. Applicaties die wel het einddoel zijn, mogen het faultactor element opnemen.

Voor fouten gegenereerd door de ZIM is de waarde "<http://www.aortarelease.nl/actor/lsp>" verplicht (NB: deze waarde komt niet overeen met die van de SOAP actor, zie par 4.3.1). Voor fouten gegenereerd door de GBx wordt aangeraden de waarde "<http://www.aortarelease.nl/actor/gbx>" te gebruiken. Andere waarden voor faultactor zijn niet toegestaan.

detail

Het element detail is bedoeld voor applicatie specifieke foutinformatie die gerelateerd is aan het Body element van het SOAP request. Het is verplicht wanneer de inhoud van het Body element niet succesvol verwerkt kon worden. Het mag niet gebruikt worden voor foutinformatie over de header. Wanneer het element detail aanwezig is, betekent dit dat de fout gerelateerd is aan de verwerking van het element Body. Wanneer het element detail niet aanwezig is, dan is de fout niet gerelateerd aan de verwerking van het element Body.

SOAP kent de faultcodes zoals opgesomd in onderstaande tabel. Deze faultcodes kunnen worden opgenomen in het element faultcode en moeten dan ook namespace gekwalificeerd zijn.

Naam	Toelichting
VersionMismatch	De SOAP Envelope heeft een ongeldige namespace, wat gebruik van een SOAP-versie die niet ondersteund wordt kan aangeven. Wanneer de SOAP Envelope een andere namespace heeft dan "" http://schemas.xmlsoap.org/soap/envelope/ "" MOET deze Fault gegenereerd worden.
MustUnderstand	Er is een SOAP Header aanwezig die niet bekend is, maar met mustUnderstand = "1". In dit geval MOET deze Fault gegenereerd worden.
Client	Deze Faults kunnen gebruikt worden bij syntaxfouten in het SOAP bericht of HL7v3-payload. Het gaat daarbij bijvoorbeeld om berichten die niet voldoen aan de wsdl. Voor semantische fouten in de HL7v3-payload gebruikt AORTA HL7v3-foutberichten (Accept Acknowledgements). Een applicatie is niet verplicht zelf SOAP Client Faults te gebruiken, maar dient ze wel te accepteren.
Server	Deze Fault mag alleen gebruikt worden wanneer de ontvangende applicatie niet in staat is de HL7v3-payload te verwerken omdat de lokale HL7v3-applicatie niet beschikbaar is. Een applicatie is niet verplicht zelf SOAP Server Faults te gebruiken, maar dient ze wel te accepteren.

Het WS-I Basic Profile definieert een aantal richtlijnen voor het gebruik van SOAP Faults. De meest relevante zijn opgenomen in onderstaande tabel.

Code	Basic Profile tekst	Toelichting
R1000	When a MESSAGE contains a soapenv:Fault element, that element MUST NOT have element children other than faultcode, faultstring, faultactor and detail	SOAP staat dit wel toe, maar WS-I Basic Profile dus niet. Het child element detail, mag zelf wel child elementen hebben, zie ook R1002.
R1001	When a MESSAGE contains a soapenv:Fault element its element children MUST be unqualified	Dus faultcode, faultstring, faultactor and detail moeten unqualified zijn.
R1002	A RECEIVER MUST accept fault messages that have any number of elements, including zero, appearing as children of the detail element. Such children can be qualified or unqualified.	AORTA laat het gebruik van het detail element in principe vrij. Echter, het gebruik van de gekwalificeerde child elementen code en text wordt aanbevolen. Zie hieronder voor de voorbeelden.

R1 00 3	A RECEIVER MUST accept fault messages that have any number of qualified or unqualified attributes, including zero, appearing on the detail element. The namespace of qualified attributes can be anything other than " http://schemas.xmlsoap.org/soap/envelope/ ".	AORTA laat de te gebruiken namespaces voor de child elementen van het detail element vrij. Echter, het gebruik van de volgende namespace is een suggestie: http://www.aortarelease.nl/actor/[specificpart]/soapFault/detail . Bijvoorbeeld voor de ZIM: http:// www.aortarelease.nl/actor/lsp/soapFault/detail ¹¹² en bijvoorbeeld voor het GBK: http:// www.aortarelease.nl/actor/gbk/soapFault/detail ¹¹³ .
R1 01 6	A RECEIVER MUST accept fault messages that carry an xml:lang attribute on the faultstring element.	Het attribuut xml:lang geeft aan in welke taal de faultstring staat. In AORTA is alleen Nederlands of Engels toegestaan en is het gebruik van het attribuut xml:lang voor de zender optioneel.
R1 00 4	When a MESSAGE contains a faultcode element the content of that element SHOULD be one of the fault codes defined in SOAP 1.1 or a namespace qualified fault code.	Een gekwalificeerde foutcode is toegestaan, dus bijvoorbeeld: zim:AUTERR Waarbij de prefix zim in een bijbehorend xmlns:zim attribuut correct gedefinieerd moet worden.
R1 03 1	When a MESSAGE contains a faultcode element the content of that element SHOULD NOT use of the SOAP 1.1 "dot" notation to refine the meaning of the Fault.	AORTA staat het gebruik van de zogenaamde "dot" notatie niet toe.

Ter illustratie hieronder een voorbeeld van een correcte en een incorrecte SOAP Fault in AORTA.

112. <http://www.aortarelease.nl/actor/lsp/soapFault/detail>

113. <http://www.aortarelease.nl/actor/gbk/soapFault/detail>

CORRECT:

```

<soapenv:Fault xmlns:soap='http://schemas.xmlsoap.org/soap/envelope/' >
  <faultcode>soapenv:Client</faultcode>
  <faultstring>Het input document is niet valide.</faultstring>
  <faultactor>http://www.aortarelease.nl/actor/lsp</faultactor>
  <detail>
    <lsp:code xmlns:lsp= 'http://www.aortarelease.nl/actor/lsp/soapFault/detail'>
      MissingMandatoryElement
    </lsp:code>
    <lsp:text xmlns:lsp= 'http://www.aortarelease.nl/actor/lsp/soapFault/detail'>
      Een verplicht element mist in het input document: ....
    </lsp:text>
  </detail>
</soapenv:Fault>

```

INCORRECT:

```

<soapenv:Fault xmlns:soap='http://schemas.xmlsoap.org/soap/envelope/' >
  <!-- Onderstaande is fout omdat "dot" notatie niet is toegestaan -->
  <faultcode>soapenv:Client.ZIM.XSD_VALIDATION_ERR</faultcode>
  <!-- Onderstaande is fout omdat child elementen van soapenv:Fault
       niet namespace gekwalificeerd mogen zijn -->
  <soapenv:faultstring> Het input document is niet valide</soapenv:faultstring>
  <soapenv:faultactor>http://www.aortarelease.nl/actor/lsp</soapenv:faultactor>
  <detail>
    <code>MissingMandatoryElement</code>
    <text>Een verplicht element mist in het input document: ....</text>

    <lsp:extraInfo xmlns:lsp= 'http://www.zim.nl/soapFault/detail'>

      Het missende element is verplicht geworden in release....

    </lsp:extraInfo>
  </detail>
</soapenv:Fault>

```

	Bij ontvangst van een bericht dat geen well-formed XML bevat, wordt bij voorkeur een HTTP response met status 400 'Bad Request' gegeven. Een applicatie dient ook rekening te houden met een SOAP Client Fault of een HL7v3 Accept Acknowledgement Error.

Dit omdat het niet exact te bepalen is welke fouten een applicatie het eerst dient te signaleren. Er is bijvoorbeeld geen verplichting eerst het hele XML-document te parsen om op well-formedness te controleren voordat verdere verwerking plaatsvindt. Bij niet well-formed XML hoeft geen SOAP Fault of HL7v3-error gegeven te worden.

	Een applicatie dient altijd op een bericht te reageren - uiteraard zolang de applicatie überhaupt tot reageren in staat is. Een uitzondering is wanneer een applicatie reden heeft aan te nemen dat er sprake is van een malicieuze actie, zoals een Denial Of Service aanval.

	Wanneer een applicatie niet op HL7v3-niveau kan reageren, bijvoorbeeld omdat er geen zinnige HL7v3-interactie uit het bericht te destilleren valt, of omdat er geen geschikte HL7v3-reactie voorhanden is, heeft de volgende reactie de voorkeur: - als er een fout is in de SOAP syntax, (bijvoorbeeld soapenv:Envelope zonder soapenv:Body of soapenv:Fault): een SOAP Client Fault, met HTTP status 500 'Internal Server Error'; - als er een andere fout is in de syntax, een reactie met HTTP status 400 'Bad Request'; - wanneer er geen fout is in de syntax, maar er serverproblemen zijn, een reactie met HTTP Status 500 'Internal Server Error', eventueel gevuld met een SOAP Server Fault.

	Bij foutafhandeling dient het principe gevolgd te worden: "wees strikt in wat je zendt, en tolerant bij fouten die je ontvangt". De afhandeling als hier geschetst heeft de voorkeur, bij ontvangst van onverwachte fouten dient een applicatie echter adequaat te reageren, bijvoorbeeld door de fout te loggen voor menselijke afhandeling.

RFC 2616 (HTTP/1.1) beveelt het gebruik van een entity (HTTP berichtinhoud) aan bij een response met status 4xx of 5xx. "... Except when responding to a HEAD request, the server SHOULD include an entity containing an explanation of the error situation, and whether it is a temporary or permanent condition." Aanbevolen wordt uiteraard RFC 2616 hier te volgen. Deze specificatie geeft geen verdere richtlijnen voor de op te nemen boodschap. In de meeste gevallen zullen de toelichtingen bestemd zijn voor menselijk gebruik (systeembeheerders en applicatieontwikkelaars), omdat het ernstige fouten betreft.

10.1.1.4.5.3 HL7v3-fouten

HL7v3 kent eigen foutberichten. Deze vallen buiten de scope van dit document. Wel wordt in de tabel hieronder aangegeven welke HTTP status gebruikt dient te worden bij HL7v3-fouten.

Cod e	Naam	Toelichting (zie HL7v3 voor details)	HTTP Status
AA	Application Acknowledgement Accept	Succesvolle verwerking.	200 OK
AE	Application Acknowledgement Error	Fout in bericht (permanent).	200 OK
AR	Application Acknowledgement Reject	Fout, maar niet in inhoud of formaat van bericht (tijdelijk).	200 OK
CA	Accept Acknowledgement Commit Accept	Geaccepteerd.	200 OK
CE	Accept Acknowledgement Commit Error	Niet geaccepteerd (permanent).	200 OK ^[1]
CR	Accept Acknowledgement Commit Reject	Niet geaccepteerd (tijdelijk).	200 OK

	HL7v3 Application en Accept Acknowledgements worden behandeld als succes op HTTP niveau.

10.1.1.4.5.4 Fout bij de ZIM als tussenstation

Wanneer een versturend GBx een bericht zendt aan een ontvangend GBx, kan het ontvangende GBx een foutmelding genereren. De ZIM dient daar als volgt mee om te gaan:

- HL7 foutmeldingen dienen net als een gewoon HL7 antwoord ongewijzigd teruggegeven te worden aan het versturende GBx;
- SOAP Faults dienen net als een gewoon SOAP antwoord ongewijzigd teruggegeven te worden aan het versturende GBx;
- HTTP fouten worden vertaald naar HL7 fouten, waarbij HTTP client fouten naar HL7 client fouten vertaald worden en HTTP server fouten naar HL7 server fouten:

- HTTP fouten in de 4xx range worden vertaald naar een HL7 SYNGBX error uit LSP-tabel (OID 2.16.840.1.113883.2.4.6.6.1.1000) met typecode CE en als weergavenaam het applicatielid en de HTTP resultaatcode.
- HTTP fouten in de 5xx range worden vertaald naar een HL7 RTEDEST error uit HL7-tabel (OID 2.16.840.1.113883.5.1100) met typecode CR en als weergavenaam het applicatielid en de HTTP resultaatcode.

In het geval van opvragen van patiëntgegevens door een initiërend GBx wordt een eventuele foutmelding gegenereerd door het reagerende GBX door de ZIM in het batchopleverbericht opgenomen zoals hierboven beschreven. De ZIM zal in het uiteindelijk opleverbericht een extra foutmelding opnemen over de aard van de aanwezige foutmeldingen in het batchopleverbericht.

10.1.1.4.6 HTTP Redirects

Het gebruik van HTTP redirects is niet toegestaan.

In de internationale standaarden die AORTA voorschrijft, met name [Basic Profile], staat dat voor HTTP Redirects alleen 307 gebruikt mag worden. De betekenis van 307 is "temporary redirect". De rest is in [Basic Profile] expliciet verboden vanwege interoperabiliteitsproblemen. In AORTA zijn ook de 307 redirects verboden.

[1] In versie 1.1 en eerder was dit "400: Bad Request". Het gebruik van een HTTP status anders dan 2xx voor SOAP berichten die geen SOAP Fault zijn, staat echter op gespannen voet met SOAP 1.1 en WS-I Basic Profile 1.0, en deze beide standaarden worden gevolgd in AORTA. Er was dus sprake van een inconsistentie.

10.1.1.5 AORTA en WSDL

Een WSDL in AORTA dient als documentatie en contract, omdat de WSDL precies beschrijft aan wat voor service de gegevensleverancier zich gecommitteerd heeft.

	Beschrijvingen van webservices worden opgesteld in WSDL 1.1.

10.1.1.5.1 Inhoud WSDL

Deze paragraaf beschrijft de inhoud van een AORTA WSDL stap voor stap.

De uitwerking maakt gebruik van een voorbeeldtransactie: VerstrekkingLijstquery. Volgens het interactiediagram bestaat deze transactie uit:

- de vraag QURX_IN990111NL (Medication Dispense List Query);
- het antwoord QURX_IN990113NL (Medication Dispense List Query Response).

Ieder bericht is in HL7v3 gedefinieerd met een XML Schema. Zo is er een XML Schema QURX_IN990111NL.xsd, QURX_IN990113NL.xsd, etcetera. In de XML Schema's ligt de structuur van het bericht vast, inclusief de HL7v3-Transmission en -Control Act Wrappers.

In de WSDL worden allereerst benodigde XML Schema's gedeclareerd als WSDL Types. Hieronder volgt een uitleg aan de hand van een voorbeeld.

```

<?xml version="1.0" encoding="UTF-8"?>

<definitions xmlns:xsd="http://www.w3.org/2001/XMLSchema"

    xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"

    xmlns="http://schemas.xmlsoap.org/wsdl/"

    xmlns:hl7="urn:hl7-org:v3"

    targetNamespace="urn:hl7-org:v3"

    name="VerstrekkingsLijstquery">

    <documentation> WSDL implementatie van VerstrekkingsLijstquery

    </documentation>

    <types>

        <xsd:schema targetNamespace="urn:hl7-org:v3" elementFormDefault="qualified">

            <xsd:include schemaLocation="../schemas_codeGen/QRX_IN990111NL.xsd"/>

        </xsd:schema>

        <xsd:schema targetNamespace="urn:hl7-org:v3" elementFormDefault="qualified">

            <xsd:include schemaLocation="../schemas_codeGen/QRX_IN990113NL.xsd"/>

        </xsd:schema>

    </types>

```

Eerst is er een inleidend deel, daarna worden schema's gekoppeld. De schema's worden opgenomen met een schema-include om een en ander beknopt, leesbaar en onderhoudbaar te houden. Er zijn in dit geval twee schema's:

- xsd (Medication Dispense Event List Query)
- xsd (Medication Dispense Event List Query Response)

Vervolgens worden de nodige berichten gedeclareerd als WSDL Message. De berichten krijgen een unieke naam: die van de interactie.

```

<message name="QURX_IN990111NL">
    <part name="body" element="hl7:QURX_IN990111NL"/>
</message>

<message name="QURX_IN990113NL">
    <part name="body" element="hl7:QURX_IN990113NL"/>
</message>

```

Er zijn ook twee verschillende berichten:

- QURX_IN990111NL (Medication Dispense List Query)
- QURX_IN990113NL (Medication Dispense List Query Response)

De verschillende samenhangende interacties uit het Storyboard worden vertaald naar WSDL Port Types. Hierin zijn bij elkaar horende in- en outputs gekoppeld tot WSDL operations.

```

<portType name="VerstrekkingsLijstquery_PortType">
    <operation name="VerstrekkingsLijstquery_QueryResponse">
        <input message="hl7:QURX_IN990111NL"/>
        <output message="hl7:QURX_IN990113NL"/>
    </operation>
</portType>

```

Hierboven is een operation getoond volgens het synchrone model van berichtenuitwisseling: het antwoord op de query komt synchroon binnen over hetzelfde SOAP en HTTP request/response paar.

Dit levert de volgende operation op: `VerstrekkingsLijstquery_QueryResponse`. Deze bestaat weer uit de eerder gedefinieerde berichten, die als input en output message zijn gedefinieerd.

In sommige gevallen is bij een HL7v3-interactie die verzonden wordt meer dan één interactie als antwoord mogelijk. WSDL staat dit niet toe: iedere WSDL-operation mag maximaal één input en één output hebben. De oplossing is een samengesteld xsd element te maken waarin alle HL7v3-antwoordinteracties mogelijk zijn. In onderstaand fragment is deze stijl te zien. Er wordt aan het schema één extra element toegevoegd, met een keuze tussen beide HL7v3-interacties. Dit element heet `[request-interaction-id]Response`. Dit element wordt vervolgens gebruikt in de message definitie en de operation, zodat de operation weer een enkele output heeft.

```

<types>
  <xsd:schema targetNamespace="urn:hl7-org:v3" elementFormDefault="qualified"

      xmlns:hl7="urn:hl7-org:v3" xmlns:xsd="http://www.w3.org/2001/
XMLSchema">

    ...

    <xsd:include schemaLocation="../schemas/COMT_IN800310.xsd" />

  </xsd:schema>

  <xsd:schema targetNamespace="urn:hl7-org:v3" elementFormDefault="qualified"

      xmlns:hl7="urn:hl7-org:v3" xmlns:xsd="http://www.w3.org/2001/
XMLSchema">
    <xsd:include schemaLocation="../schemas/COMT_IN800320.xsd" />

  </xsd:schema>

  <xsd:schema targetNamespace="urn:hl7-org:v3" elementFormDefault="qualified"

      xmlns:hl7="urn:hl7-org:v3" xmlns:xsd="http://www.w3.org/2001/
XMLSchema">
    <xsd:element name="COMT_IN800300Response">
      <xsd:complexType>
        <xsd:choice>
          <xsd:element ref="hl7:COMT_IN800310"/>
          <xsd:element ref="hl7:COMT_IN800320"/>
        </xsd:choice>
      </xsd:complexType>
    </xsd:element>
  </xsd:schema>
</types>
...

<message name="COMT_IN800300Response">
  <part name="body" element="hl7:COMT_IN800300Response" />
</message>
<portType name="OverdrachtVerantwoordelijkheid_PortType">
  ...

  <operation name="OverdrachtVerantwoordelijkheid_VerzoekOverdrachtVervallen">
    <input message="hl7:COMT_IN800300" />
    <output message="hl7:COMT_IN800300Response" />
  </operation>
</portType>

```

De WSDL Port Types worden gekoppeld aan WSDL Bindings waar meer details over de SOAP-interactie gegeven worden. Hier wordt gespecificeerd dat de stijl van gegevensuitwisseling "document/literal" is.

In de Binding wordt ook de waarde van SOAPAction bepaald. Deze SOAPAction komt terug in de HTTP Header, zie [paragraaf 4.4 \(see page 320\)](#).

```
<binding type="hl7:VerstrekkingsLijstquery_PortType"
        name="VerstrekkingsLijstquery_Binding">
  <soap:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"
/>
  <operation name="VerstrekkingsLijstquery_QueryResponse">
    <soap:operation soapAction="urn:hl7-org:v3/
VerstrekkingsLijstquery_QueryResponse"/>
    <input>
      <soap:body use="literal"/>
    </input>
    <output>
      <soap:body use="literal"/>
    </output>
  </operation>
</binding>
```

Ten slotte wordt van de WSDL Bindings een WSDL Service gemaakt, die het webadres van een specifieke webservice geeft.

```

<service name="VerstrekkingsLijstquery_Service">
  <port binding="hl7:VerstrekkingsLijstquery_Binding"
        name="VerstrekkingsLijstquery_Port">
    <!--Deze service location URI verwijst niet naar een echt bestaande
    webservice. -->
    <soap:address location="http://www.xis.nl/VerstrekkingsLijstquery"/>
  </port>
</service>
</definitions>

```

De waarde van "location" is hier nog fictief. Zie [paragraaf 5.2 \(see page 340\)](#) voor meer details.

10.1.1.5.2 Locatie van een webservice

De ZIM of een GBx vervullen in HL7v3-terminologie zogenaamde Application Roles. Een WSDL beschrijft de webservice voor iedere Application Role. Nictiz levert WSDL's waarin alleen de locatie (de url) van de service nog niet definitief is. Ieder GBx die een webservice aanbiedt in AORTA, biedt ook de echte locatie van de webservice.

Voor het opvragen van medicatie is er bijvoorbeeld een "VerstrekkingsLijstquery.wsdl" bestand waarin de locatie van de webservice nog niet definitief is ingevuld. Als locatie staat er:

```

<!--Deze service location URI verwijst niet naar een echt bestaande webservice. -->

```

```

<soap:address location="http://www.gbx.nl/VerstrekkingsLijstquery" />

```

Voor ieder GBx komt er dan een specifieke invulling van de locatie. Stel dat er een GBx is met het (fictieve) adres <http://www.gbx1.nl>, dan kan de ZIM deze webservice aanroepen met onderstaande webservice locatie.

```
<soap:address location="http://www.gbx1.nl/VerstrekkingsLijstquery" />
```

De padnamen zijn verplicht: <http://www.gbx1.nl/VerstrekkingsLijstquery>¹¹⁴ is goed, <http://www.gbx1.nl/VerstrekkingsLijstquery.py>¹¹⁵ of <http://www.gbx1.nl/MijnVerstrekkingsLijstquery>¹¹⁶ is dat niet.

Een GBx-applicatie mag maar één hostname gebruiken voor alle webservices die de GBx-applicatie aanbiedt. Dus in bovenstaand voorbeeld wordt de webservice locatie van een Voorschriftquery van dezelfde GBx-applicatie:

```
<soap:address location="http://www.gbx1.nl/Voorschriftquery" />
```

Dit om te voorkomen dat de ZIM een registratie moet bijhouden van alle webservices per GBx, met de bijbehorende plicht voor GBx'en om deze aan te melden en wijzigingen door te geven.^[1]

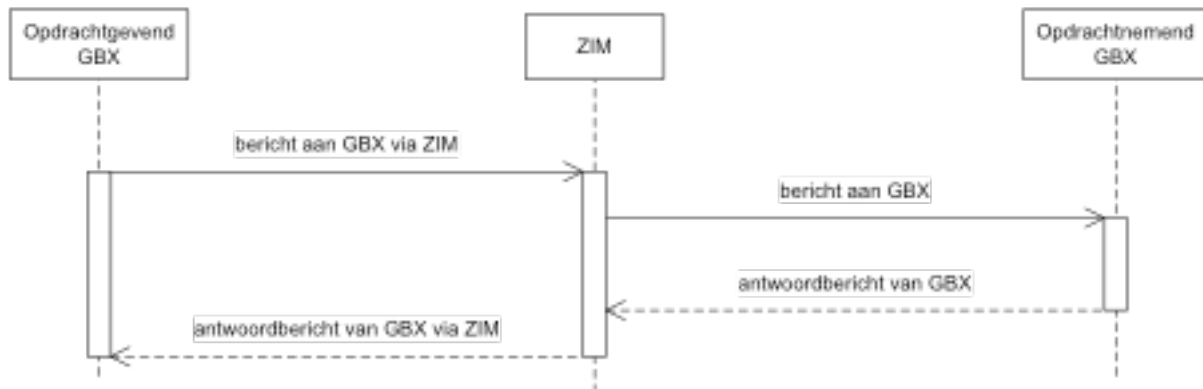
10.1.1.5.3 Opvragen patiëntgegevens en “batch” wsdl's

Opvragen patiëntgegevens betreft een berichtuitwisselingspatroon in AORTA, waarbij een initiërend GBx een opvraging doet via de ZIM aan nul of meer reagerende GBZ'en. De ZIM bundelt de antwoorden van de reagerende systemen in een zogenaamde batch wrapper en retourneert dit batch bericht aan het initiërende systeem. Zie onderstaand sequentiediagram in Figuur 7 voor een illustratie hiervan met twee reagerende GBZ'en bij een VerstrekkingsLijstQuery (zie [Ontw OPV] voor een volledig overzicht).

114. <http://www.gbz.nl/VerstrekkingsLijstquery>

115. <http://www.gbz.nl/Verstrekkingsquery.py>

116. <http://www.gbz.nl/MijnVerstrekkingsquery>



Figuur 7 - sequentie diagram opvragen patiëntgegevens: VerstrekkingsLijstQuery

Dit berichtuitwisselingspatroon vindt zijn weerslag in de WSDL's. Immers, het request/response paar tussen een initiërend GBx en de ZIM kent een ander antwoordbericht (namelijk een batch bericht) dan het request/response paar tussen ZIM en reagerend GBZ. Bij opvragen patiëntgegevens zijn er dan ook twee WSDL-ports gedefinieerd, een batch versie voor de webservice-port tussen initiërend GBx en de ZIM en een 'normale' versie voor de webservice-port tussen ZIM en reagerend GBZ.

Een voorbeeld hiervan is de VerstrekkingsLijstQuery, deze kent de volgende twee WSDL-service ports:

- VerstrekkingsLijstQueryBatch_Port (aangeropen door initiërend GBx bij ZIM),
- VerstrekkingsLijstQuery_Port (aangeropen door ZIM bij reagerend GBZ).

[Paragraaf 5.5](#) (see page 343) bevat illustraties van de html-documentatie van deze webservice in Figuur 8 en Figuur 9.

Merk op dat reagerende GBZ'en niet allemaal dezelfde AORTA release hoeven te ondersteunen en dat een batch antwoordbericht van de ZIM derhalve berichten met verschillende versies kan bevatten. Eén batch antwoordbericht kan dus zowel AORTA 6 als AORTA 7 berichten bevatten.

10.1.1.5.4 Versionering van webservices

Het kan voorkomen dat een webservice wijzigt bij een nieuwe AORTA publicatie, bijvoorbeeld omdat:

- een input of output bericht wijzigt;
- het pad van de webservice locatie wijzigt;
- een operation wijzigt of toegevoegd of verwijderd wordt;
- de soap action wijzigt.

De meest waarschijnlijke wijziging is overigens bij de eerstgenoemde: het input of output bericht.

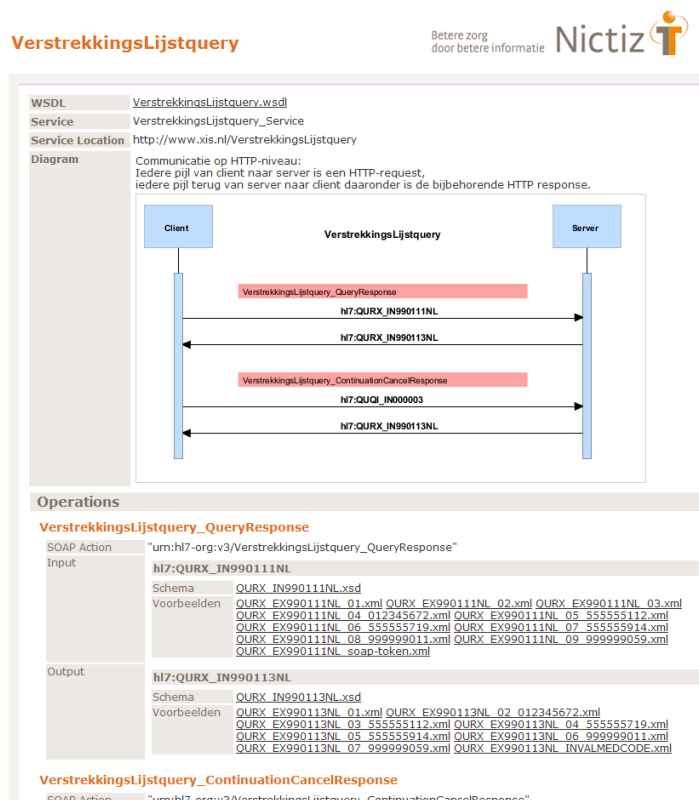
Als er iets wijzigt in de webservice, krijgt de webservice een (nieuw) versienummer, dat zich als volgt manifesteert:

- in de waarde van het definitions/service/@name attribuut, bijvoorbeeld: "VerstrekkingsLijstquery_02_Service";
- in de waarde van het definitions/service/port/soap:address/@location attribuut, bijvoorbeeld: "<http://www.gbx.nl/02/VerstrekkingsLijstquery>";
- in de bestandsnaam van de wsdl, bijvoorbeeld "VerstrekkingsLijstquery-02.wsdl";
- in de waarde van het definitions/@name attribuut, bijvoorbeeld "VerstrekkingsLijstquery_02";
- in de waarde van het definitions/documentation element, bijvoorbeeld "WSDL implementatie van VerstrekkingsLijstquery_02".

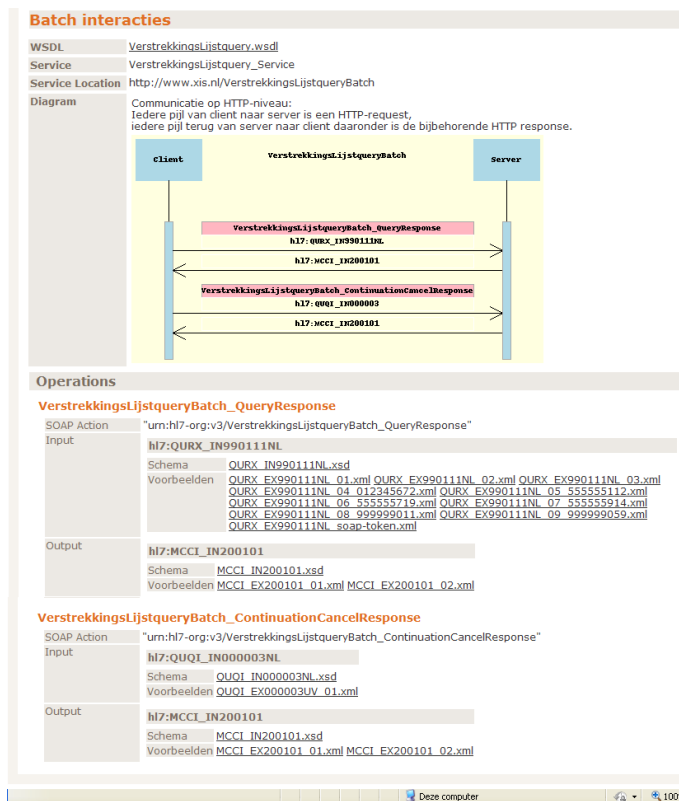
De eerste twee genoemde wijziging zijn het belangrijkste: een nieuwe servicenaam en een nieuwe (verplichte) padnaam voor de webservice locatie. Deze padnaam bevat het versienummer direct na de hostnaam van het GBx en/of ZIM.

10.1.1.5.5 WSDL documentatie

Bij ieder WSDL bestand wordt ook documentatie in HTML formaat geleverd. Deze bevat een grafische weergave van de communicatie op HTTP-niveau en een overzicht van de relevante parameters uit de WSDL. Figuur 8 en Figuur 9 bevatten een illustratie van deze HTML-documentatie voor VerstrekkingsLijstQuery.wsdl.



Figuur 8 - Schermafdruck WSDL-documentatie VerstrekkingsLijstQuery



Figuur 9 - Schermafdruck WSDL-documentatie VerstrekkingsLijstQueryBatch

[1] In AORTA kunnen IP-adressen gebruikt worden voor adressering. In de voorbeelden worden URI's gebruikt. In beide gevallen gelden de verplichte padnamen.

10.1.1.6 Betrouwbaar transport

Dit hoofdstuk beschrijft betrouwbare uitwisseling van berichten in AORTA. De eisen aan een GBx voor betrouwbaar transport zijn beschreven in [PvE GBx Rollen]. Dit hoofdstuk dient vooral om deze eisen nader toe te lichten.

Betrouwbaar transport stelt – in het algemeen - de volgende eisen:

- een bericht wordt eenmaal verwerkt (duplicaatdetectie en –verwijdering);
- berichten worden afgeleverd in de volgorde waarin ze verzonden zijn;
- er is garantie dat een bericht ofwel afgeleverd wordt, ofwel dat het falen gemeld wordt.

Voor betrouwbaar transport moet ieder systeem voorzieningen treffen tegen het falen van systemen. Een voorbeeld hiervan is dat een ontvanger een bericht persistent opslaat, voordat een antwoord verzonden wordt. Daarnaast is het van belang dat ieder bericht een unieke identificatie bevat zodat

een ontvanger duplicaten kan detecteren. Betrouwbare aflevering kan dan worden ingevuld op de volgende wijze:

- een verzender zendt een bericht aan een ontvanger;
- de ontvanger slaat het bericht persistent op en retourneert een antwoordbericht;
- wanneer de verzender een antwoordbericht ontvangt, is de status van de verzending bekend bij deze verzender;
- wanneer de verzender geen antwoordbericht ontvangt, mag deze een nieuwe poging doen;
- de ontvanger detecteert of het bericht al eerder verwerkt is; is dit het geval, dan verwerkt de ontvanger het bericht deze keer niet en informeert de verzender met een antwoordbericht;
- wanneer na herhaalde pogingen geen antwoordbericht komt, wordt de gebruiker (of diens beheerder) van het verzendende systeem gewaarschuwd.

10.1.1.6.1 Herhaald uitvoeren

Herhaald uitvoeren is een essentieel onderdeel van betrouwbaar transport. Het is mogelijk dat ergens in de keten een bericht niet verwerkt is zoals het door de verzender bedoeld was. De verzender zal een foutmelding of een waarschuwing melding ontvangen. De verzender kan hierdoor getriggerd worden om hetzelfde verzoek nogmaals te verzenden. Er zijn verschillende manieren om een actie herhaald uit te voeren. AORTA onderscheidt de volgende mogelijkheden:

- Herhalen met een duplicaat bericht. Een duplicaat is exact hetzelfde bericht als het origineel, inclusief wrappers. Dit betekent dus dat het bericht nogmaals verzonden wordt met een identiek message-id en bij tokenauthenticatie een identiek transactietoken.
- Herhalen met een nieuw bericht. Een nieuw bericht bevat weliswaar hetzelfde functionele verzoek, maar heeft (minimaal) een nieuw message id en bij tokenauthenticatie ook een nieuw transactietoken.

Wanneer de ZIM een bericht gaat verwerken, wordt het transactietoken op “gebruikt” gezet. Dit token kan dan niet nogmaals gebruikt worden. Bij tokenauthenticatie is een nieuwe poging met een duplicaat bericht dan ook alleen zinvol wanneer het originele bericht niet bij de ZIM is aangekomen. Het is dus sterk afhankelijk van waar in de keten zich een uitzonderingssituatie voordoet.

10.1.1.6.2 Duplicaatdetectie

Als gevolg van het toepassen van herhaald uitvoeren wordt duplicaatdetectie van belang. AORTA onderscheidt de volgende vormen:

- Duplicaatdetectie op transportniveau. Hierbij worden duplicaat berichten gedetecteerd aan de hand van een identieke transmission wrapper, meer specifiek op basis van het message id.
- Duplicaatdetectie op applicatieniveau. Hierbij worden duplicaten gedetecteerd aan de hand van de HL7v3-payload, meer specifiek op basis van het patiëntstuk-id (in HL7v3 ingevuld door “Act id”). Het betreft hier niet per definitie duplicaat berichten, er kan ook sprake zijn van nieuwe berichten met duplicaat payload.

Het kan zijn dat een bericht niet als duplicaat geldt op transportniveau, maar wel een duplicaat blijkt te zijn op applicatieniveau. Het betreft dan een nieuw bericht met een nieuw message id, maar met een duplicaat payload. Andersom kan dit niet: een duplicaat op transportniveau is altijd ook een duplicaat op applicatieniveau. Dit laatste is overigens de verantwoordelijkheid van de zender: een duplicaatbericht moet identiek zijn aan het originele bericht. De ontvanger mag hiervan uitgaan en hoeft de payload dus niet te evalueren wanneer een duplicaat gedetecteerd wordt op transportniveau.

Merk op dat het ook mogelijk is dat er nieuwe berichten zijn met hetzelfde patiëntstuk-id en nieuwe, bijgewerkte payload. Als dit mogelijk is, zal duplicaatdetectie op applicatieniveau niet van toepassing zijn.

De ZIM voert duplicaatdetectie op transportniveau uit bij tokenauthenticatie: duplicaat transactietokens worden geweigerd. Dit geldt niet in het geval van het GBP waar een DigiD-SAML-token kan worden hergebruikt. Inschrijf- en mandaattokens kunnen ook hergebruikt worden. Programma's van eisen stellen duplicaatdetectie op applicatieniveau verplicht voor specifieke berichten.

10.1.1.6.3 Beveiliging en betrouwbaarheid

Omdat herhaald uitvoeren onderdeel is van betrouwbaar transport, ontstaat een aanvullend risico voor aanvallen, zoals een "Denial of Service" (DoS) aanval of bij tokenauthenticatie een "Replay Attack".

Een DoS aanval is een poging met een grote hoeveelheid berichten een server zo te belasten dat deze het normale, valide verkeer niet meer aankan. De verplichting om een bericht te beantwoorden geldt niet bij een vermoeden van een DoS aanval. (Duplicaat) berichten hoeven niet verwerkt te worden wanneer er een vermoeden is van een DoS aanval.

Bij een replay attack steelt een aanvaller een bericht en verzendt dit opnieuw. De ZIM weigert duplicaat transactietokens en pareert zo dergelijke replay attacks.

10.1.1.6.4 Toepassing betrouwbaar transport in AORTA

Deze paragraaf beschrijft welke algemene aspecten van betrouwbaar transport van toepassing zijn voor AORTA. Daarom hier eerst nogmaals de eisen die geïntroduceerd zijn in het begin van dit hoofdstuk:

- een bericht wordt eenmaal verwerkt (duplicaatdetectie en –verwijdering);
- berichten worden afgeleverd in de volgorde waarin ze verzonden zijn;
- er is garantie dat een bericht ofwel afgeleverd wordt, ofwel dat het falen gemeld wordt.

AORTA ondersteunt eenmalige verwerking en aflevergarantie, en niet volgordelektheid.

Het garanderen van volgordelijkheid van berichten is geen vereiste omdat er (nog) geen use case is om dit aan de *ontvangende* kant te garanderen. Sommige berichten moeten wel in de goede volgorde afgehandeld worden, bijvoorbeeld: een heraanmelding verwijst na een aanmelding plaatsvinden en een afmelding moet na een aanmelding plaatsvinden. De verantwoordelijkheid voor volgordelijkheid ligt hier echter bij de verzender. Indien volgordelijkheid van belang is mag het GBx een tweede bericht pas verzenden, wanneer het eerste bericht succesvol afgehandeld is.

	Aflevering van berichten in de volgorde waarin ze verzonden zijn wordt niet ondersteund.

De aflevergarantie dwingt af dat er altijd gepoogd wordt om een antwoordbericht te versturen.

	Ieder HL7v3-bericht in AORTA moet beantwoord worden met een antwoordbericht, behalve wanneer er een vermoeden is van een DoS aanval.

In AORTA gelden de volgende uitgangspunten:

- De verzender is verantwoordelijk om te achterhalen hoe het bericht verwerkt is.
- Bij ontvangst van een antwoordbericht kan de verzender zeker weten dat het bericht ten minste één keer is afgeleverd.
- Bij het niet ontvangen van een antwoordbericht weet de verzender niets zeker over de aflevering van het bericht. Normaliter zal de verzender dan (automatisch) opnieuw proberen en wanneer dit blijvend niet lukt een beheerder of gebruiker alarmeren alsnog actie te ondernemen.
- De ontvanger is verantwoordelijk om te voorkomen dat een actie onterecht een tweede keer wordt verwerkt. De ontvanger moet dan duplicaatdetectie toepassen.

10.1.1.6.5 Uitwisselingspatronen

AORTA maakt onderscheid tussen de volgende primaire uitwisselingspatronen:

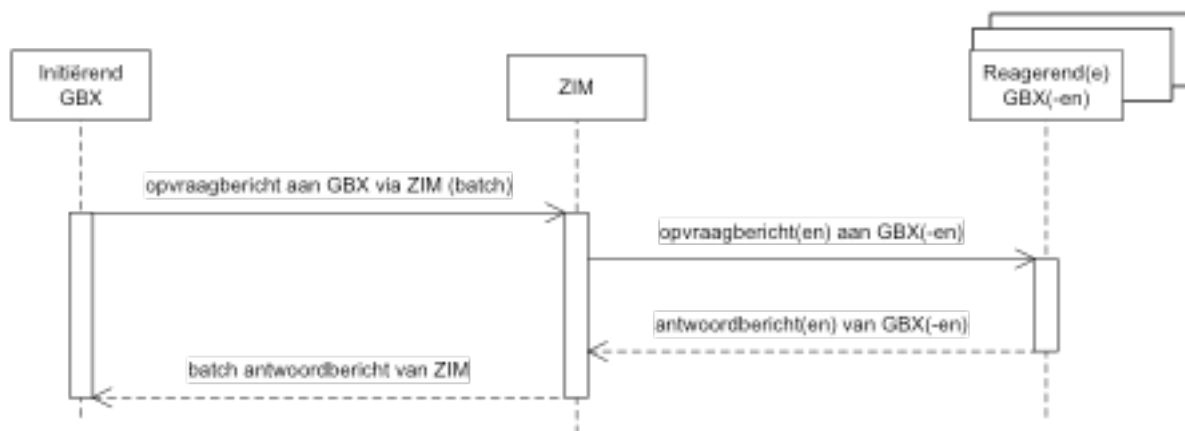
- Opvragen patiëntgegevens. Opvragen van GBX1 via ZIM aan GBX2.
- Versturen patiëntgegevens. Versturen van GBX1 via ZIM naar GBX2.

AORTA maakt onderscheid tussen de volgende ondersteunende uitwisselingspatronen:

- Opvragen van gegevens. Opvragen van GBX1 aan ZIM.
- Versturen van gegevens. Versturen van GBX1 naar ZIM.

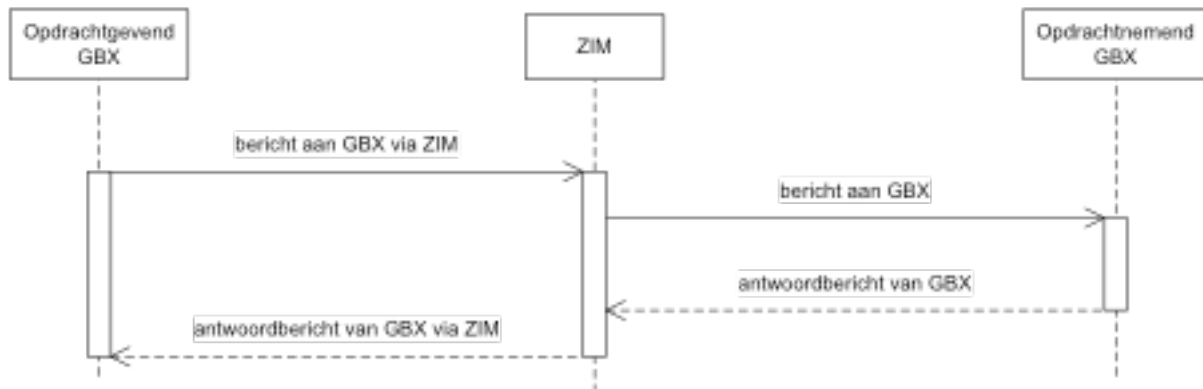
10.1.1.6.5.1 Primaire uitwisselingspatronen

Opvragen patiëntgegevens betreft opvragingen van een initiërend GBx aan één of meerdere reagerende GBx-en via de ZIM. De vraag wordt gesteld aan de ZIM, de ZIM divergeert de vraag naar de juiste GBx(-en). In het geval er sprake is van een generieke opvraag met context, stuurt de ZIM een specifiek bouwsteen opvraagbericht naar de juiste GBx-en. Het is mogelijk dat een GBx meerdere bouwsteen opvraagberichten te verwerken krijgt. Deze reagerende GBx-en sturen hun antwoord naar de ZIM. De ZIM bundelt deze antwoorden in een batch antwoord voor het initiërende GBx. Onderstaande figuur illustreert dit uitwisselingspatroon.



Figuur 10 - Opvragen patiëntgegevens

Versturen patiëntgegevens betreft berichten van een initiërend GBx aan een reagerend GBx via de ZIM. De ZIM stuurt dit bericht door naar het ontvangende, reagerende GBx. Het antwoord van dit reagerende GBx wordt ontvangen door de ZIM en doorgestuurd naar het initiërende GBx. Onderstaande figuur illustreert dit uitwisselingspatroon.



Figuur 11 - Versturen patiëntgegevens

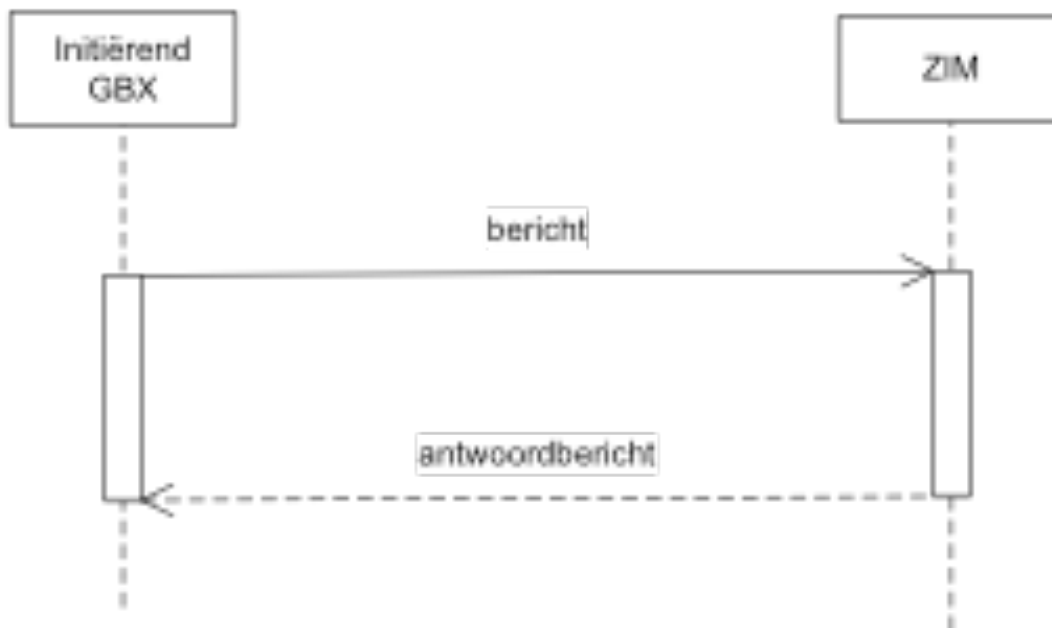
10.1.1.6.5.2 Ondersteunende uitwisselingspatronen

Opvragen van gegevens betreft opvragingen van een GBx aan de ZIM. Onderstaande figuur illustreert dit uitwisselingspatroon.



Figuur 12 - Opvragen gegevens

Versturen van gegevens betreft berichten van een GBx aan de ZIM. Onderstaande figuur illustreert dit uitwisselingspatroon.



Figuur 13 - Versturen gegevens

De invulling van betrouwbaar transport verschilt tussen deze uitwisselingspatronen en dan met name tussen opvragen en versturen. De volgende twee paragrafen lichten toe hoe AORTA betrouwbaar transport invult voor opvragen patiëntgegevens en opvragen gegevens respectievelijk versturen patiëntgegevens en versturen gegevens.

10.1.1.6.5.3 Opvragen patiëntgegevens en opvragen gegevens

Bij opvragen patiëntgegevens en opvragen gegevens gaat het om het opvragen van informatie. Er wordt dus niets gewijzigd in de geadresseerde applicatie. Het staat het initiërende GBx daarom vrij om nieuwe pogingen te ondernemen. Het verdient de voorkeur om mislukte opvragingen altijd terug te melden aan de gebruiker en deze gebruiker vrij te laten om nieuwe pogingen uit te voeren. Een nieuwe poging wordt daarmee altijd gedaan met een nieuw bericht.

10.1.1.6.5.4 Versturen patiëntgegevens en versturen gegevens

Bij versturen patiëntgegevens en versturen gegevens gaat het om een systeem dat een bericht verstuurt aan een ander systeem. [PvE GBx Rollen] specificeert algemene eisen voor betrouwbaar transport. De verschillende programma's van eisen definiëren per specifiek bericht welke eisen met betrekking tot betrouwbaar transport van toepassing zijn.

Bij het opstellen van deze programma's van eisen geldt de richtlijn dat wanneer het niet schadelijk is om een bericht een tweede keer te versturen, dit dan ook toegestaan is.

Bij versturen gegevens geldt dat de ZIM duplicaatdetectie op applicatieniveau toepast. Het is daarom toegestaan en zelfs aanbevolen om een retry-mechanisme in te bouwen voor versturen, bijvoorbeeld het (her)aanmelden en afmelden van gegevens in de verwijzindex.

Op het moment van schrijven van deze implementatiehandleiding zijn er twee interacties voor versturen patiëntgegevens bekend:

- Waarneemretourbericht (bedoeld voor rapportage van HAP naar huisarts).
- Voorschriftbericht.

Hoewel het voor de hand ligt om bij het Waarneemretourbericht duplicaatdetectie op applicatieniveau te implementeren, is dit niet expliciet geëist van het reagerende GBZ. Het opnieuw verwerken van hetzelfde bericht is hooguit lastig voor de zorgverlener, maar niet gevaarlijk voor de patiënt. Het is daarom ook voor dit bericht toegestaan om een retry mechanisme te gebruiken.

Op het moment van schrijven van de specificaties voor AORTA 2013, zijn er nog geen gekwalificeerde systemen voor het voorschriftbericht. In AORTA 2013 is duplicaatdetectie op applicatieniveau geëist voor het voorschriftbericht. Ook bij het versturen van het voorschriftbericht is het daarom toegestaan om een retry-mechanisme in te bouwen.

Overigens blijven de specificaties in de programma's van eisen leidend voor de vereiste implementatie van betrouwbaar transport. De beschrijving in deze gids dient slechts als toelichting.

10.1.1.7 Referenties Berichttransport

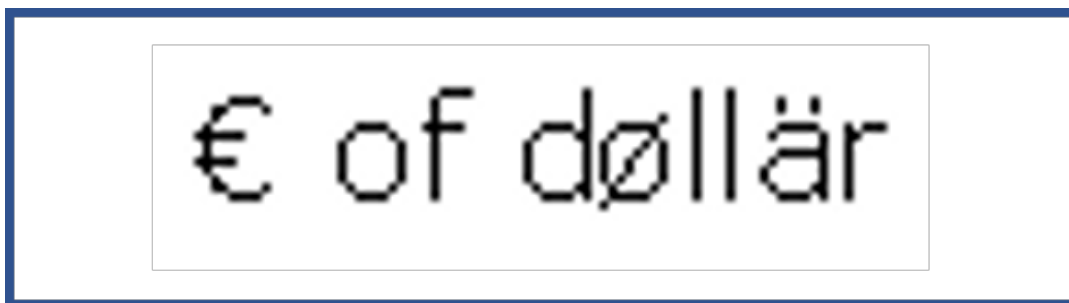
Referentie	Document	Versie
[Basic Profile]	Basic Profile Version 1.0 www.ws-i.org ¹¹⁷	1.0
[SOAP]	Simple Object Access Protocol (SOAP) 1.1 http://www.w3.org/TR/SOAP	1.1

117. <http://www.ws-i.org>

[WSDL]	Web Services Description Language (WSDL) 1.1, W3C Note, 15 March 2001 http://www.w3.org/TR/wsdl	15-mrt-2001
[XML]	Extensible Markup Language (XML) 1.0, W3C Recommendation, Fourth Edition, 16 August 2007 http://www.w3.org/TR/xml	16-aug-2007
[PvE GBx Rollen]	Programma van eisen infrastructurele systeemrollen	8.3.0.0
[IH BA Mandaattoken]	Implementatiehandleiding Berichtauthenticatie Mandaattoken (see page 475)	8.3.0.0
[IH tokens generiek]	Implementatiehandleiding security tokens generiek (see page 435)	8.3.0.0
[IH BA DigiD]	Implementatiehandleiding berichtauthenticatie met DigiD (see page 530)	8.3.0.0
[IH BA PKIO-pas]	Implementatiehandleiding berichtauthenticatie met PKIO-pas	8.3.0.0
[IH BA Transactietoken]	Implementatiehandleiding berichtauthenticatie transactietoken (see page 399)	8.3.0.0
[IH BA Inschrijftoken]	Implementatiehandleiding berichtauthenticatie inschrijftoken (see page 373)	8.3.0.0
[Arch AORTA]	Architectuur AORTA	8.3.0.0

10.1.1.8 Diakritische tekens

Het is van belang te verifiëren of diakritische en andere tekens goed gecodeerd zijn. Dat kan bijvoorbeeld met de volgende tekst:



Noot: afhankelijk van de instellingen van de PC kunnen diakritische tekens anders overkomen. Daarom is deze tekst grafisch opgenomen. Wanneer deze tekens hieronder er anders uitzien, gebruik de tekens uit het plaatje.

Deze tekst dient exact zo in het bronsysteem van de zender ingevoerd te worden in een veld dat vrije tekst toestaat. Bij de ontvanger dient de tekst in het doelsysteem weer zo leesbaar te zijn. Wanneer het doelsysteem één of meer van deze tekens niet ondersteunt, dient de ontvangende partij in de XML te verifiëren dat de tekst ongeschonden is overgekomen. De tekst is zo gekozen omdat ze de verschillen tussen de meest gebruikte tekstcoderingen, UTF-8, ISO-8859-1, ISO8859-15 en Windows-1252 blootlegt.

Hexadecimale representatie van enkele diakritische tekens			
Encoding	Euroteken (€)	Kleine letter o met forward slash (ø)	Kleine a met trema (ä)
UTF-8	E2 82 AC	C3 B8	C3 A4
ISO-8859-1	bestaat niet	F8	E4
ISO-8859-15	A4	F8	E4
Windows-1252	80	F8	E4

Een geschikte plaats voor deze tekst is (alleen in testomgevingen) het optionele element <softwareName> in de Transmission Wrapper. Dit komt in alle berichten voor, maar wordt veelal niet gebruikt in testen.

```

<?xml version="1.0" encoding="utf-8"?>

...

<sender>
  <device>
    <id extension="01234567" root="2.16.840.1.113883.2.4.6.6"/>
    <softwareName>€ of døllär</softwareName>
  </device>
</sender>

...

```

10.2 Toestemming

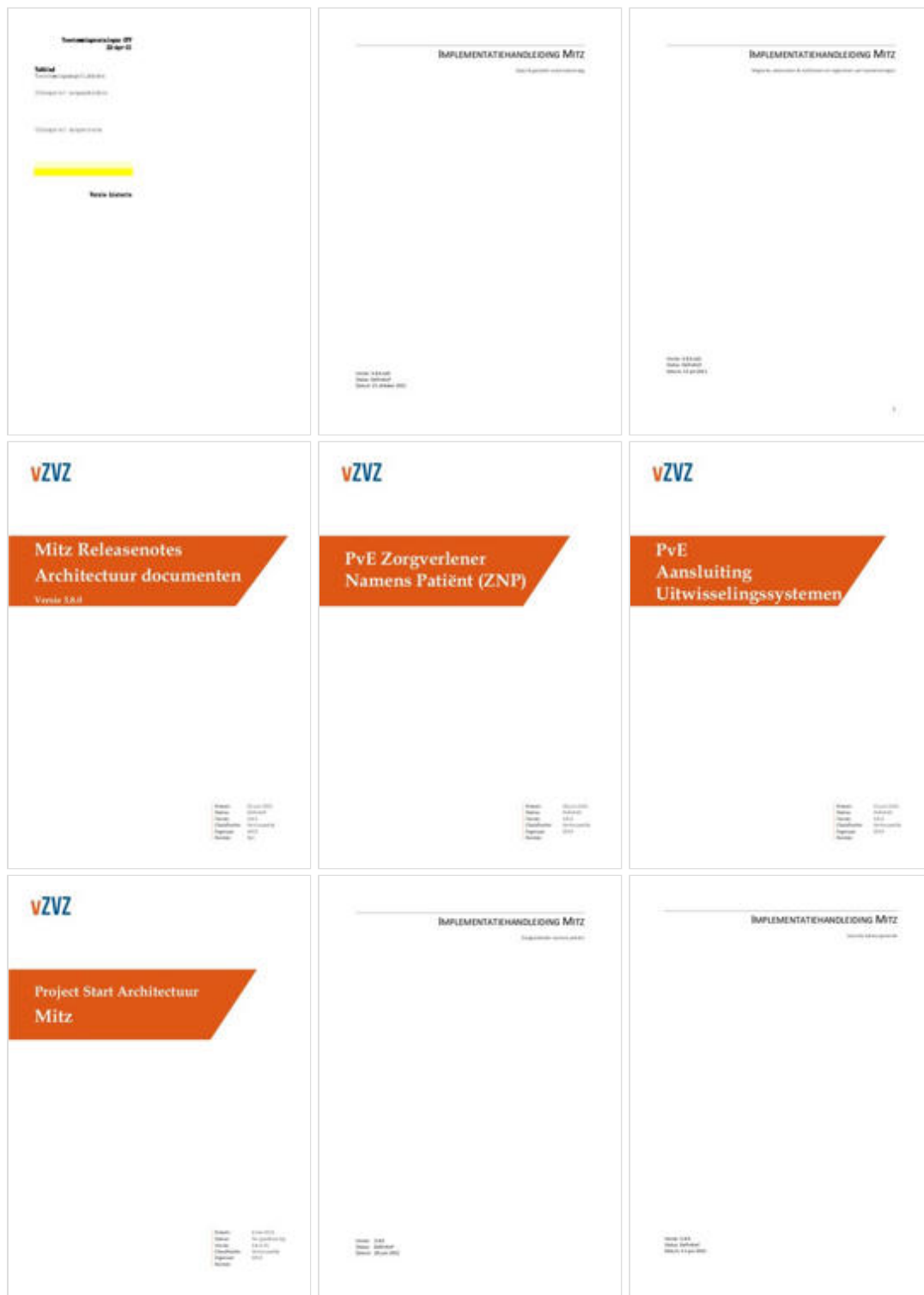
[PvE Aansluiten op Mitz via het LSP](#)¹¹⁸

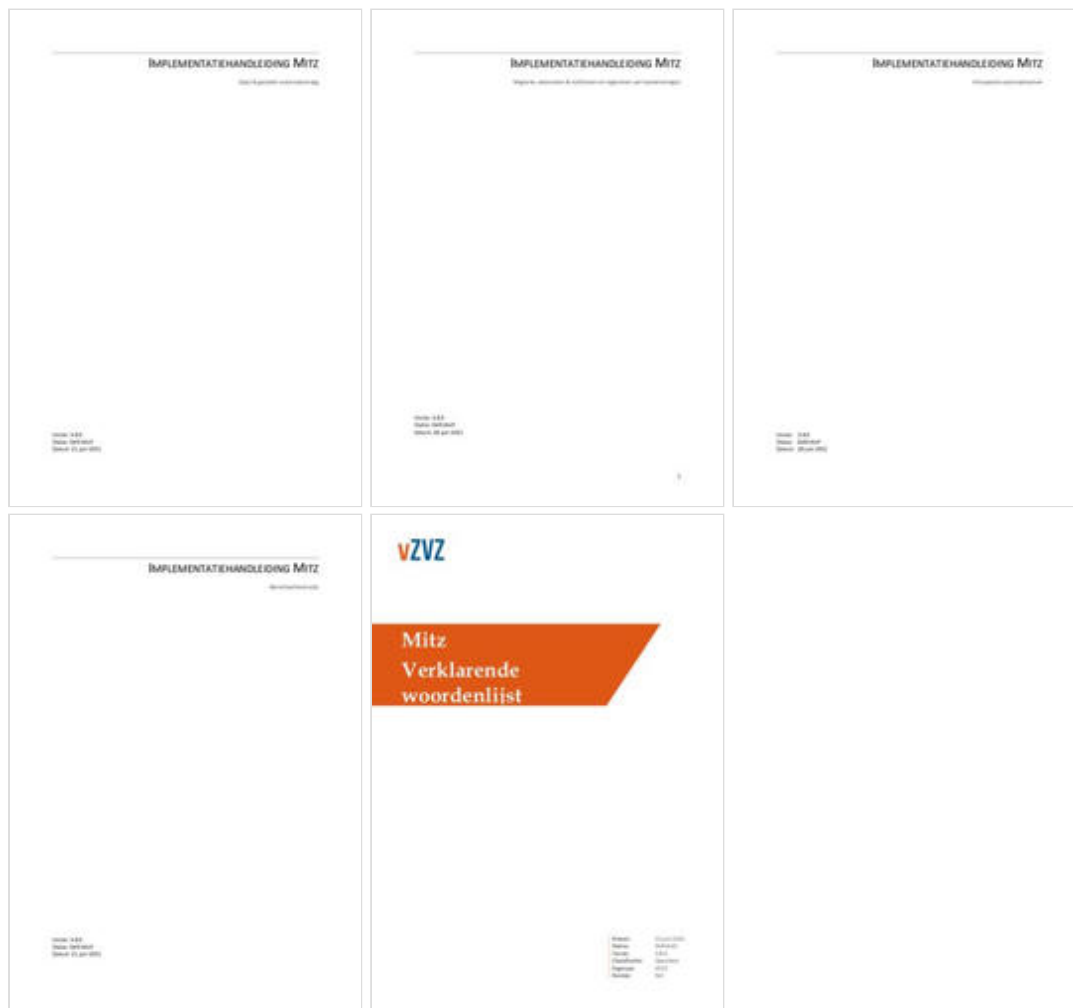
[Implementatie Handleiding Aorta On Mitz](#)¹¹⁹

10.2.1 Mitz 3.8.0_1

118. <https://aorta-on-mitz.scrollhelp.site/pve/current/>

119. <https://aorta-on-mitz.scrollhelp.site/ih/current/>





10.3 Token specificaties

- [JSON Web tokens \(see page 359\)](#)
 - [AORTA Access token \(see page 359\)](#)
 - [MedMij Access token \(see page 366\)](#)
- [AORTA SAML tokens \(see page 368\)](#)
 - [GBZ AORTA_Auth_IH_Inschrijftoken \(see page 373\)](#)
 - [Inleiding inschrijftoken \(see page 374\)](#)
 - [Het SAML inschrijftoken \(see page 376\)](#)
 - [Certificaten Inschrijftoken \(see page 393\)](#)
 - [Referenties inschrijftoken \(see page 396\)](#)
 - [Token afhandeling inschrijftoken \(see page 397\)](#)
 - [GBZ AORTA_Auth_IH_Berichtauthenticatie_Transactietoken \(see page 399\)](#)
 - [Inleiding transactietoken \(see page 400\)](#)

- [Het SAML transactietoken \(see page 401\)](#)
- [Certificaten transactietoken \(see page 429\)](#)
- [Token afhandeling transactietoken \(see page 431\)](#)
- [Referenties transactietoken \(see page 434\)](#)
- [GBx AORTA_Auth_IH_Security_tokens_generiek \(see page 435\)](#)
 - [Inleiding Security tokens generiek \(see page 436\)](#)
 - [Kaders en uitgangspunten \(see page 437\)](#)
 - [Het security token \(see page 439\)](#)
 - [Digitaal tekenen \(see page 441\)](#)
 - [Opbouw van de security header \(see page 458\)](#)
 - [Afhandeling van het security token \(see page 460\)](#)
 - [Referenties security tokens generiek \(see page 465\)](#)
 - [Technologieën en standaarden \(see page 467\)](#)
- [GBZ AORTA_Auth_IH_Mandaattoken \(see page 475\)](#)
 - [Inleiding mandaattoken \(see page 476\)](#)
 - [Het SAML mandaattoken \(see page 476\)](#)
 - [Compliance \(see page 490\)](#)
 - [Certificaten mandaattoken \(see page 490\)](#)
 - [Token afhandeling mandaattoken \(see page 491\)](#)
 - [Referenties mandaattoken \(see page 492\)](#)
- [GBZ AORTA_Auth_IH_Contracttoken \(see page 492\)](#)
 - [Inleiding contracttoken \(see page 492\)](#)
 - [Het SAML contracttoken \(see page 493\)](#)
 - [Token afhandeling contracttoken \(see page 506\)](#)
 - [Referenties contracttoken \(see page 508\)](#)
- [ZORG-ID AORTA_Auth_IH_Scantoken_en_WID_token \(see page 508\)](#)
 - [Inleiding Scan en WID token \(see page 509\)](#)
 - [Het SAML Scan en WID token \(see page 510\)](#)
 - [Token afhandeling Scan en WID token \(see page 527\)](#)
 - [Referenties Scan en WID token \(see page 529\)](#)
- [GBP AORTA_Auth_IH_Berichtauthenticatie_DigiD \(see page 530\)](#)
 - [Inleiding berichtauthenticatie DigiD \(see page 531\)](#)
 - [Het SAML authenticatietoken DigiD \(see page 532\)](#)
 - [Certificaten berichtauthenticatie DigiD \(see page 543\)](#)
 - [Token afhandeling berichtauthenticatie DigiD \(see page 544\)](#)
 - [SSO \(profiel, verificatie, meldingen\) \(see page 545\)](#)
 - [Referenties authenticatie DigiD \(see page 562\)](#)
- [AORTA_Auth_IH_Berichtauthenticatie_PKIO \(see page 563\)](#)

- [Inleiding Berichtauthenticatie PKIO \(see page 564\)](#)
- [Het SAML authenticatietoken Berichtauthenticatie PKIO \(see page 565\)](#)
- [Certificaten Berichtauthenticatie PKIO \(see page 580\)](#)
- [Token afhandeling Berichtauthenticatie PKIO \(see page 581\)](#)
- [Referenties Berichtauthenticatie PKIO \(see page 582\)](#)
- [AORTA_Auth_IH_Berichtauthenticatie_UZI \(see page 582\)](#)
 - [Inleiding Berichtauthenticatie UZI \(see page 583\)](#)
 - [Het SAML authenticatietoken Berichtauthenticatie UZI \(see page 585\)](#)
 - [Certificaten Berichtauthenticatie UZI \(see page 596\)](#)
 - [Token afhandeling Berichtauthenticatie UZI \(see page 598\)](#)
 - [Referenties Berichtauthenticatie UZI \(see page 599\)](#)
 - [Bijlage B Technische context \(gebruik UZI-pas\) \(see page 600\)](#)
 - [Bijlage C Token implementatie \(see page 604\)](#)

10.3.1 JSON Web tokens

10.3.1.1 AORTA Access token

10.3.1.1.1 Inhoud en formaat van het AORTA access_token

AOF.TS.AAT.100.v1

Het JWT-based [AORTA access_token](#) bestaat uit een header, een payload en een signature, waarbij gebruik wordt gemaakt van [JWS Compact Serialization](#)¹²⁰.

AOF.TS.AAT.200.v2

De header van het token bevat de volgende attributen:

Claim	Vaste waarde	Toelichting
alg	RS256	
typ	aorta-at+JWT	"aorta-at" is een afkorting voor AORTA access_token.
kid	-	The identifier of the key-pair used to sign this JWT

120. <https://tools.ietf.org/html/rfc7515#section-3.1>

AOF.TS.AAT.300.v1

Het token wordt op basis van RS256 (RSA Signature met SHA-256), digitaal ondertekend met de private key van de Autorisatie Server. De signature wordt geplaatst over de header en de payload.

AOF.TS.AAT.400.v2

De payload van het token is omschreven in onderstaande tabel.

Claim	Cardinaliteit	Vaastewarde	Toelichting
jti	1..1	-	jti bevat een globaal uniek ID van het betreffende token . Aanbevolen wordt om een UUID te gebruiken.
iat	1..1	-	iat bevat het tijdstip van uitgifte van dit token (aantal seconden sinds 1970-01-01T0:0:0Z gemeten in UTC).
iss	1..1	-	iss bevat de HTTPS-URL van de autorisatieserver die het token heeft uitgegeven. Op deze manier kan automatisch de juiste metadata, met daarin de juiste endpoints, worden opgehaald.
sub	1..1	-	Formaat: "<id-systeem> <id>" Het ID van de gebruiker, of van een systeem, die uitgifte van dit access_token legitimeert. De claim kan bevatten: - Het BSN van de persoon die een interactie initieert m.b.t. haar eigen gegevens, of die een ander persoon hiertoe heeft gemachtigd - sub bevat dan de string "http://fhir.nl/fhir/NamingSystem/bsn <bsn>" - Het UZI-nummer van een zorgverlener - sub bevat dan de string "http://fhir.nl/fhir/NamingSystem/uzi-nr-pers <UZI-nummer>" - Het appID van het systeem (indien het request zonder tussenkomst van een gebruiker is ingestuurd) - sub bevat dan de string "http://fhir.nl/fhir/NamingSystem/uzi-nr-sys <app-id>"
role	0..1	-	Formaat: "<codesysteem> <rolcode>" De rolcode van de gebruiker die uitgifte van dit access_token legitimeert. De claim kan bevatten: - De rolcode die hoort bij een persoon, ofwel "http://fhir.nl/fhir/NamingSystem/aorta-rolcode P" - De UZI-rolcode van een zorgverlener, ofwel "http://fhir.nl/fhir/NamingSystem/uzi-rolcode <UZI-rolcode>" Verplicht indien de sub claim is gevuld met een ID van een persoon.

Claim	Cardinaliteit	Vaastewarde	Toelichting
act	0..1	-	De act claim bevat een aantal subclaims en wordt opgenomen wanneer iets of iemand handelt namens een ander persoon. Zie ook RFC 8693 ¹²¹ voor voorbeelden.
act.sub	1..1	-	Formaat: "<id-systeem> <id>" Het ID van de gebruiker of van het systeem die handelt namens de persoon, die is opgenomen in de sub claim. De claim kan bevatten: • Het BSN van een gemachtigd persoon die gegevens van een ander persoon opvraagt - sub bevat dan de string "http://fhir.nl/fhir/NamingSystem/bsn <bsn>" • Het UZI-nummer van een zorgverlener of van een medewerker van een zorginstelling - sub bevat dan de string "http://fhir.nl/fhir/NamingSystem/uzi-nr-pers <UZI-nummer>" • Het appID van het systeem (indien het request zonder tussenkomst van een gebruiker is ingestuurd) - sub bevat dan de string "http://fhir.nl/fhir/NamingSystem/aorta-app-id <app-id>"
acr	1..1	-	De Authentication Context Class Reference. Geeft informatie over het niveau waarop de sub, of indien aanwezig, de act.sub van het token is geauthenticeerd. Mogelijke waarden, zoals gespecificeerd binnen SAML¹²² zijn: • "urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport" (bijvoorbeeld DigiD-basis) • "urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract" (bijvoorbeeld DigiD-midden) • "urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard" (bijvoorbeeld DigiD-substantieel) • "urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI" (bijvoorbeeld UZI-pas of DigiD-hoog) • "urn:oasis:names:tc:SAML:2.0:ac:classes:X509" (servercertificaat)

121. <https://datatracker.ietf.org/doc/html/rfc8693#section-4.1>

122. <http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf>

Claim	Cardinaliteit	Vaastewarde	Toelichting
attest	1..1	-	Informatie over op welke grondslag of grondslagen dit token is gebaseerd. Het betreft een door spatie gescheiden set van strings. Mogelijk waarden: "MAP" - het Medisch Autorisatie Protocol is toegepast. "TR" - toestemming van patiënt is vastgelegd in een toegelaten toestemmingsregister. "MedMij" - het token is uitgeven n.a.v. een conform MedMij afgegeven toestemmingsverklaring. "BRON" - toestemming is, door de patiënt of diens vertegenwoordiger, vastgelegd bij de bronhoudende zorgaanbieder zelf, en is daarom nog niet getoetst. "CNST" - toestemming mag door de bronhoudende zorgaanbieder worden verondersteld te zijn verkregen, bijvoorbeeld t.b.v. een verwijzing van de patiënt - deze is vastgelegd in een consent_token, en het juiste gebruik van dit token voor het ontvangen request is reeds getoetst. "LOG" - specifieke autorisatieregels m.b.t. de toegangslog zijn toegepast. "ACT/VWI" - specifieke autorisatieregels m.b.t. toegang tot ACT/VWI-entries zijn toegepast. Een voorbeeld van een attest claim is "MAP TR", waarmee dan wordt aangeduid dat het MAP is getoetst en dat toestemming is vastgelegd en getoetst in een toegelaten toestemmingsregister.
nbf	1..1	-	nbf bevat het tijdstip van uitgifte van dit token (aantal seconden sinds 1970-01-01T0:0:0Z gemeten in UTC).
exp	1..1	-	Wordt gevuld met de expiration time van het MedMij access_token of met de expiration time van het AORTA transactietoken naar aanleiding waarvan dit AORTA access_token wordt uitgegeven.
aud	1..1	-	Formaat: ["<applID>", "<applID>"] De aud van het token bevat de set van applID's van alle GBx-applicaties, die deze interactie gaan ontvangen. Deze GBZ-applicaties vallen altijd onder één organisatie. Een applID heeft het formaat: "urn:oid:2.16.840.1.113883.2.4.6.6.<applicatie-id>". Aan iedere GBx-applicatie die is aangesloten op AORTA wordt een eigen <applicatie-id> toegekend.
scope	1..1	-	Voor de juiste vulling zie tekst onder deze tabel.

Claim	Cardinaliteit	Vaastewarde	Toelichting
patient	0..1	-	Formaat: "<id-systeem> <id>" Het BSN van de patiënt, d.w.z. de persoon waarop de gegevens, die worden uitgewisseld, betrekking hebben. patient bevat de string "http://fhir.nl/fhir/NamingSystem/bsn¹²³<bsn>". De verwachting is weliswaar dat hier altijd BSN's gecommuniceerd gaan worden. Het id-systeem is hier toegevoegd om consistent te blijven met de sub claim en om eventueel ook eigen patient-ID's van een zorgaanbieder te kunnen ondersteunen. Verplicht gevuld bij patiëntgebonden interacties.
client_id	1..1	-	Formaat: "urn:oid:2.16.840.1.113883.2.4.6.6.<applicatie-id>" Dit attribuut bevat informatie over de partij die als resource client mag optreden en daarvoor dit token mag gebruiken. Wanneer een interactie door RB VnC wordt geïnitieerd bij een resource server, dan bevat de client_id claim het applID van de Resource Broker VnC component. Wanneer een interactie door RB ZA-in wordt geïnitieerd bij een andere Resource Broker component (bijv. RB ACT) dan bevat de client_id claim het applID van de Resource Broker ZA-in component.
_vrb	0..1	-	De _vrb claim bevat, in een aantal subclaims, VZVZ Resource Broker specifieke informatie over de afhandeling van interacties. Een resource server (GBZ-applicatie) mag deze claim desgewenst negeren. Deze claim is slechts aanwezig wanneer een interactie, via RB VnC, wordt geïnitieerd bij een resource server.
_vrb._vrb_auid	1..1	-	Het applID van de Resource Broker VnC component. Formaat: "urn:oid:2.16.840.1.113883.2.4.6.6.<applicatie-id>".
_vrb._vrb_client_id	1..1	-	Het applID van de Resource Broker MedMij-in component of van de Resource Broker ZA-in component, die jegens de Resource Broker VnC component optreedt als resource client. Formaat: "urn:oid:2.16.840.1.113883.2.4.6.6.<applicatie-id>".
_vrb._vrb_ion	1..1	-	Een kenmerk van de organisatie die die het request heeft geïnitieerd (de "initiating organisation name"). In de MedMij use case gaat het om de OAuthclientOrganisatienaam (naam van het PGO), zoals opgenomen in de MedMij OCL. In de ZA-ZA use case gaat het om de URA (formaat: "urn:oid:2.16.528.1.1007.3.3.<URA>").
ver	1..1	2.0	De versie van de tokendefinitie die wordt gehanteerd.

123. <http://fhir.nl/fhir/NamingSystem/bsn%7C>

AOF.TS.AAT.500.v2

De scope claim van het token wordt als volgt gevuld, waarbij verschillende scope-onderdelen door een spatie van elkaar worden gescheiden:

Gegevensdiens t / Interactie	Vulling van scope	Toevoeging op scope bij interactie vanuit MedMij	Toevoeging op scope bij interactie vanuit AORTA
Gegevensdiens t / Interactie	Vulling van scope	Toevoeging op scope bij interactie vanuit MedMij	Toevoeging op scope bij interactie vanuit AORTA
Verzamelen Afspraken 2.0	patient/Appointment.read	medmij.gegevensdiens.47	nog niet beschikbaar
Verzamelen Basisgegevens zorg 3.0	patient/Patient.read patient/Coverage.read patient/Consent.read patient/Condition.read patient/Observation.read patient/NutritionOrder.read patient/Flag.read patient/AllergyIntolerance.read patient/MedicationStatement.read patient/MedicationRequest.read patient/MedicationDispense.read patient/DeviceUseStatement.read patient/Immunization.read patient/Procedure.read patient/Encounter.read patient/ProcedureRequest.read patient/ImmunizationRecommendation.read patient/DeviceRequest.read patient/Appointment.read	medmij.gegevensdiens.48	aorta.contentcode.BGZOPV
Verzamelen Basisgegevens GGZ 2.0	patient/Patient.read patient/Coverage.read patient/Consent.read patient/Condition.read patient/Observation.read patient/CarePlan.read patient/Procedure.read patient/DiagnosticReport.read patient/CareTeam.read	medmij.gegevensdiens.50	nog niet beschikbaar
Verzamelen Documenten 3.0	patient/DocumentManifest.read patient/DocumentReference.read patient/Binary.read	medmij.gegevensdiens.51	nog niet beschikbaar
Delen Meetwaarden vitale functies 2.0	patient/Observation.write	medmij.gegevensdiens.53	nog niet beschikbaar

Gegevensdiens t / Interactie	Vulling van scope	Toevoeging op scope bij interactie vanuit MedMij	Toevoeging op scope bij interactie vanuit AORTA
Gegevensdiens t / Interactie	Vulling van scope	Toevoeging op scope bij interactie vanuit MedMij	Toevoeging op scope bij interactie vanuit AORTA
Verzamelen Meetwaarden vitale functies 2.0	patient/Observation.read	medmij.gegevensdiens.52	nog niet beschikbaar
Verzamelen verwijzen naar vragenlijsten 2.0	patient/Task.read	medmij.gegevensdiens.59	nog niet beschikbaar
Delen antwoorden op vragenlijsten 2.0	patient/Task.write patient/QuestionnaireResponse.write	medmij.gegevensdiens.60	nog niet beschikbaar
\$is-allowed	patient\$is-allowed	-	n.v.t.
Interacties m.b.t. het actualiteitsregister en de verwijzindex	patient/DocumentManifest.write of patient/DocumentManifest.read of patient\$delete-dossier	n.v.t.	-

Gegevensdiens t / Interactie	Vulling van scope	Toevoeging op scope bij interactie vanuit MedMij	Toevoeging op scope bij interactie vanuit AORTA
Gegevensdiens t / Interactie	Vulling van scope	Toevoeging op scope bij interactie vanuit MedMij	Toevoeging op scope bij interactie vanuit AORTA
Interacties m.b.t. de toegang slog (RB- logging)	patient/AuditEvent.read	n.v.t.	-
Patiëntgebonden workflow interacties	patient/Task.write of patient/Task.read	-	-
Niet-patiëntgebonden workflow interacties	user/Task.write of user/Task.read	n.v.t.	-

Met een access_token wordt aan de ontvanger bewezen dat aan een gegeven subject bepaalde toegangsrechten zijn verstrekt.

10.3.1.2 MedMij Access token

10.3.1.2.1 Inhoud en formaat van het MedMij access_token

AOF.TS.MAT.100.v1

Het MedMij access_token is een JWT, die bestaat uit een header, een payload en een signature, waarbij gebruik wordt gemaakt van [JWS Compact Serialization](https://tools.ietf.org/html/rfc7515#section-3.1)¹²⁴.

AOF.TS.MAT.150.v1

De header van het token bevat de volgende attributen:

Claim	Vaste waarde	Toelichting
alg	RS256	
typ	mat+JWT	"mat" is een afkorting voor MedMij access_token
kid	-	The identifier of the key-pair used to sign this JWT

AOF.TS.MAT.200.v1

Het access_token wordt op basis van RS256 (RSA Signature met SHA-256), digitaal ondertekend met de private key van de Autorisatie Server. De signature wordt geplaatst over de header en de payload.

AOF.TS.MAT.300.v1

Het access_token bevat de volgende payload:

Claim	Vaste waarde	Toelichting
jti	-	Unieke ID van het token
ver	1.0	De versie van de tokendefinitie die wordt gehanteerd
iss	-	HTTPS-URL van de Autorisatie Server voor deze versie van het MedMij afsprakenstelsel (interfaceversie)
exp	-	Gelijk aan de waarde van <i>expires_in</i> in het <i>access token response</i> bericht

124. <https://tools.ietf.org/html/rfc7515#section-3.1>

Claim	Vaste waarde	Toelichting
scope	-	Gelijk aan de <i>scope</i> in het <i>access token response</i> bericht. Wanneer een <i>access_token</i> wordt gegenereerd t.b.v. een interne <i>\$is-allowed operation</i> tussen Autorisatie Server en Resource Broker, dan wordt de <i>scope</i> gevuld met • <i>\$is-allowed/</i> • gevolgd door de <i>scope</i> in het <i>access token response</i> bericht Bijvoorbeeld: "<i>\$is-allowed/eenofanderezorgaanbieder~42</i>"

10.3.2 AORTA SAML tokens

AORTA SAML tokens spelen een cruciale rol in de authenticatie en autorisatie binnen het Landelijk Schakelpunt (LSP). Ze zorgen ervoor dat zorgaanbieders en zorgverleners veilig toegang kunnen krijgen tot patiëntgegevens binnen de AORTA-architectuur.

AORTA SAML tokens zijn SAML 2.0 Assertions die digitale waarborgen bieden over de identiteit en rechten van een gebruiker of systeem. Deze waarborgen worden uitgegeven en ondertekend door een Identiteitsprovider (IdP), een systeem van een organisatie of gebruiker die verantwoordelijk is voor de uitgegeven waarborgen die in de assertion (waarborg) worden benoemd. De waarborgen zijn cryptografisch verifieerbaar.

10.3.2.1 Waarborgen

De waarborgen in een SAML token kunnen onderverdeeld worden in de volgende typen:

- **Identiteitswaarborg:** Bevestigt de identiteit van de gebruiker of het systeem van een organisatie.
 - Attributen: *Subject NameID*, *UZI-nummer*, *URA*, *BSN*, ...
- **Authenticatiewaarborg:** Geeft aan hoe de gebruiker is geauthenticeerd.
 - Attributen: *Authenticatieniveau* (bv. *eIDAS hoog*), *gebruikte authenticatiemethode* (bv. *smartcardPKI* of *X.509 certificaat*)
- **Autorisatiewaarborg:** Bevat de toegangsrechten en bevoegdheden van de gebruiker.
 - Attributen: *Rolcode*, *Mandaat (welke handelingen toegestaan zijn)*, *Scope (welke gegevens toegankelijk zijn)*
- **Organisatiewaarborg:** Bevestigt de organisatie waaraan de gebruiker is gekoppeld.
 - Attributen: *Zorgaanbieder (URA)*, *Organisatie-ID*, *Locatie*
- **Contextuele waarborg:** Bevat extra informatie over de transactie of sessie.
 - Attributen: *Tijdstempel*, *Geldigheidsduur*, *Sessie-ID*

De waarborgen in het SAML-token worden gevalideerd door de dienstverlener (SP) die toegang tot het LSP verleent. De dienstverlener of poortwachter tot het LSP is de XSG. Deze bepaalt op basis van de SAML Assertions of een gebruiker toegang krijgt tot de gevraagde informatie.

De Identiteitsprovider in de AORTA-architectuur speelt hierbij een cruciale rol in de authenticatie en autorisatie en is direct gekoppeld aan de verschillende typen uitgegeven certificaten. De IdP gebruikt

de certificaten, die o.a. op de UZI-passen staan, om de identiteit en rechten van zorgverleners, zorgmedewerkers op naam en systemen van zorgaanbieders te verifiëren en te waarborgen binnen het LSP. Dit onderscheid is nodig omdat *zorgverleners*, *zorgmedewerkers* op naam en *systemen* van zorgaanbieders elk een andere rol en verantwoordelijkheden hebben binnen de AORTA-architectuur en het Landelijk Schakelpunt (LSP).

We hebben de volgende SAML Assertions, die verschillende waarborgen bevatten.

- **Transactietoken.** Bevat waarborgen over de transactie context, de identiteit van de gebruiker, authenticatiemiddel, rol en zorgaanbieder.
- **Mandaattoken.** Bevat waarborgen over de identiteit, rol en zorgaanbieder welke *zorgverlener* het mandaat heeft uitgegeven. Alleen *zorgverleners* geven een mandaat.
- **Inschrijftoken.** Bevat waarborgen over de identiteit, rol en zorgaanbieder welke *zorgmedewerker* of *zorgverlener* de BSN verificatie van een patiënt heeft uitgevoerd.

Transactietoken ondertekend met	Mandaattoken ondertekend met	Inschrijftoken ondertekend met	Valide
UZI server-certificaat	Zorgverlenerspas	Niet	Nee
UZI server-certificaat	Zorgverlenerspas	Zorgverlenerspas	Ja
UZI server-certificaat	Zorgverlenerspas	Medewerkerspas op naam	Ja
UZI server-certificaat	Zorgverlenerspas	ZORG-ID Mobiel	Ja
UZI server-certificaat	Zorgverlenerspas	ZORG-ID Smartcard	Nog in ontwikkeling.
UZI server-certificaat	Medewerkerspas op naam	Zorgverlenerspas	Nee
Medewerkerspas op naam	Zorgverlenerspas	Niet	Nee
Medewerkerspas op naam	Zorgverlenerspas	Zorgverlenerspas	Ja
Medewerkerspas op naam	Zorgverlenerspas	Medewerkerspas op naam	Ja
Medewerkerspas op naam	Zorgverlenerspas	ZORG-ID Mobiel	Ja
ZORG-ID Smartcard	Zorgverlenerspas	Zorgverlenerspas	Nog in ontwikkeling

Transactietoken ondertekend met	Mandaattoken ondertekend met	Inschrijftoken ondertekend met	Valide
Medewerkerspas op naam	Medewerkerspas op naam	Zorgverlenerspas	Nee
Zorgverlenerspas	Niet nodig	Niet nodig	Ja

1. Indien het transactietoken door het *systeem van een zorgaanbieder* wordt ondertekend MOET er ook een mandaattoken en een inschrijftoken als waarborg meegestuurd worden.
2. Indien het transactietoken door een *zorgmedewerker op naam* wordt ondertekend MOET er ook een mandaattoken en een inschrijftoken als waarborg meegestuurd worden.
3. Alleen een *zorgverlener* mag een mandaattoken ondertekenen als waarborg.
4. Het inschrijftoken mag zowel door een *zorgmedewerker op naam* als door een *zorgverlener* ondertekend worden.
5. Het *systeem van een zorgaanbieder* mag geen inschrijftoken ondertekenen als waarborg.

10.3.2.2 Vertrouwensniveaus

Verskillende vertrouwensniveaus zijn gebaseerd op de mate van zekerheid die nodig is voor authenticatie en identificatie van gebruikers, en zijn afgeleid van de kaders zoals de NEN7510, eIDAS en de architectuur van AORTA.

Hieronder een samengesteld overzicht van vertrouwensniveaus gericht op het LSP.

1. Vertrouwensniveau: **Laag**

- **Toepassing:** Toegang tot informatie met beperkte risico's of niet-zorginhoudelijke gegevens (bijvoorbeeld systeemstatus of algemene berichten).
- **Identiteitsvaststelling:** Zelf aangemelde gegevens, minimale verificatie. Voor Nederlandse ingezetenen betreft dit de Basisregistratie Personen (BRP).
- **Authenticatie:** één factorauthenticatie, zoals gebruikersnaam en wachtwoord.
- **Beveiligingseisen:** Basismaatregelen, zoals TLS-versleuteling.
- **Risico:** Geschikt voor toepassingen waarbij een lage mate van zekerheid volstaat.

2. Vertrouwensniveau: **Midden**

- **Toepassing:** Zorginhoudelijke gegevens waarvoor enige mate van zekerheid over de identiteit van de gebruiker vereist is, bijvoorbeeld bij inzage door zorgverleners.
- **Identiteitsvaststelling:** Identiteitsverificatie op basis van een erkend middel zoals ZORG-ID Smart of een UZI-servercertificaat.
- **Authenticatie:** twee factorauthenticatie (2FA), bijvoorbeeld:
 - Gebruikersnaam + wachtwoord én een SMS-code.
 - UZI-servercertificaat (voor server-naar-servercommunicatie).

- **Beveiligingseisen:** Versleuteling (bijvoorbeeld PKI-overheid-certificaten) en controle op herkomst en integriteit van gegevens. Er moet sprake zijn van dynamische authenticatie. Dit betekent dat de (cryptografische) gegevens voor de authenticatie veranderen bij ieder gebruik.
- **Risico:** Voor toepassingen waarbij vertrouwelijkheid en integriteit essentieel zijn, zoals het opvragen van patiëntinformatie door zorgmedewerkers als ze geautoriseerd zijn of mandaat hebben.

3. Vertrouwensniveau: **Hoog**

- **Toepassing:** Kritieke interacties zoals het versturen van voorschriften, autoriseren van behandelingen, of toegang tot gevoelige patiëntgegevens.
- **Identiteitsvaststelling:** Tenminste éénmaal fysieke identiteitscontrole bij registratie, bijvoorbeeld een UZI-pas gekoppeld aan het BIG-register om **zorgverleners** te identificeren en te verifiëren.
- **Authenticatie:** Sterke authenticatie, zoals:
 - UZI-pas (PKI-overheid-certificaten).
- **Beveiligingseisen:** Gebruik van digitale handtekeningen en encryptie met hoge sterkte, logging van alle transacties.
- **Risico:** Voor toepassingen waar maximale zekerheid vereist is vanwege juridische of veiligheidsrisico's.

Zorgmedewerkers zijn doorgaans niet geregistreerd in het BIG-register. Zij kunnen echter ook een UZI-pas krijgen voor toegang tot zorginformatiesystemen, maar *zonder de koppeling* aan het *BIG-register*. Hun pas wordt wel gebruikt voor authenticatie en autorisatie, maar hebben niet dezelfde bevoegdheden als zorgverleners die in het BIG-register staan.

Belangrijke documenten en standaarden voor vertrouwensniveaus:

1. **NEN7510 & NEN7512:** Richtlijnen voor informatiebeveiliging in de zorg.
2. **eIDAS-verordening:** Internationale standaard voor vertrouwensniveaus.
3. **AORTA-architectuur:** Specifieke kaders voor interoperabiliteit binnen de zorg.
4. **VZVZ-specificaties:** Documentatie van het LSP, inclusief eisen voor UZI-passen en servercertificaten.

10.3.2.3 De opbouw van een SAML assertion

Een **SAML (Security Assertion Markup Language) assertion** is een XML-gebaseerd beveiligingstoken dat informatie bevat over een gebruiker en zijn of haar rechten binnen een bepaald systeem. SAML assertions worden vaak gebruikt bij federatieve authenticatie en autorisatieprocessen.

Een SAML assertion bestaat uit verschillende componenten:

1. **Header (Issuer & Metadata)**
 - De entiteit (zorgaanbieder) die de waarborgen heeft uitgegeven.
 - Geeft aan of de assertion ondertekend is en welke cryptografische algoritmes zijn gebruikt.

2. Subject

- Bevat informatie over de gebruiker (zorgverlener, zorgaanbieder of patiënt) waarvoor de waarborg is uitgegeven.
- Kan een unieke identifier bevatten, zoals een UZI-nummer of BSN.
- Kan een authenticatiemethode specificeren, zoals authenticatie met een smartcard.

3. Conditions

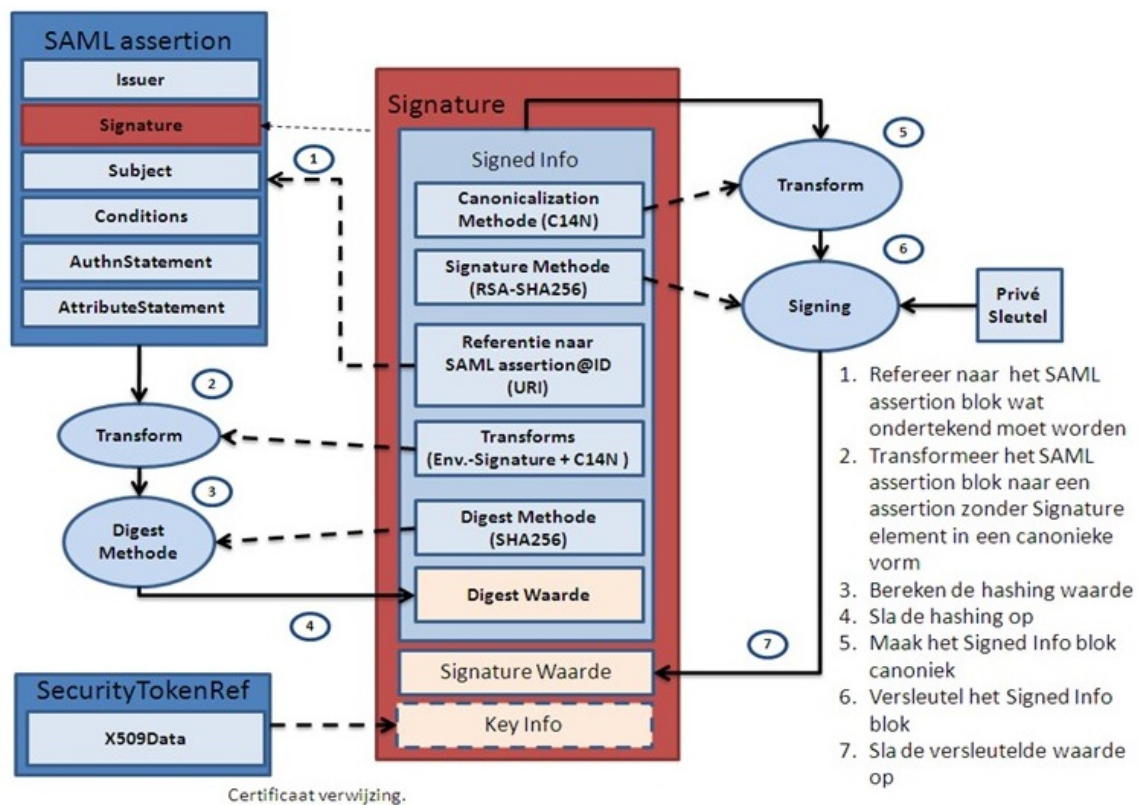
- Definieert de geldigheidsduur van de assertion (bijvoorbeeld van `NotBefore` tot `NotOnOrAfter`).
- Kan beperkingen bevatten, zoals een beperking tot een bepaalde doelgroep of systeem.

4. Statements

- **Authentication Statement:** Beschrijft de authenticatie van de gebruiker, inclusief de manier waarop de gebruiker is geauthenticeerd en tijdstip van authenticatie.
- **Attribute Statement:** Beschrijft kenmerken over de waarborg, zoals UZI-nummer, beroepsgroep, interactie, scope, etc.

5. Signature (Digitale Handtekening)

- De digitale handtekening om integriteit en authenticiteit te waarborgen van de uitgegeven waarborgen. Het wordt ondertekend met de privé-sleutel van de uitgever, die de ontvanger vervolgens kan verifiëren met de publieke sleutel van de uitgever.



1 Signed SAML assertion



Informatie, velden, elementen of attributen die in de SAML assertion beschreven zijn, zijn **obsolete** wanneer het **verouderd en niet langer aanbevolen** is voor gebruik in *nieuwe implementaties*, maar mogelijk nog wel wordt ondersteund voor *backward compatibility*.

Dit betekent:

- Het **kan nog aanwezig zijn in bestaande systemen**, maar wordt niet meer actief ontwikkeld of verbeterd.
- Het **kan in de toekomst worden verwijderd**, waardoor afhankelijkheid ervan wordt afgeraden.
- Nieuwe implementaties **moeten het niet meer gebruiken**, en bestaande systemen worden aangemoedigd om te migreren naar een alternatief.

10.3.2.4 GBZ AORTA_Auth_IH_Inschrijftoken

- **IH inschrijftoken**

Datum: 1 februari 2025

Publicatie: v8.4.0.0

10.3.2.4.1 Inleiding inschrijftoken

10.3.2.4.1.1 Doel en scope

Dit document heeft tot doel een handleiding te geven voor de implementatie van het koppelvlak tussen het goed beheerde Zorgsystemen (GBZ) en het landelijk schakelpunt (LSP) voor wat betreft de toe te passen technieken voor de authenticatie van zorgverleners en medewerkers.

10.3.2.4.1.2 Doelgroep voor dit document

Dit document is bedoeld voor softwareontwikkelaars van goed beheerde zorgsystemen en het LSP, die op grond van de HL7v3 communicatiestandaard en op grond van dit document berichten willen uitrusten met het SAML inschrijftoken. Het SAML inschrijftoken is met name vereist bij gebruik van een conditionele query.

Daarnaast wordt in dit document het plaatsen van de digitale handtekening besproken (zie ook [IH tokens generiek]).

10.3.2.4.1.3 Documenthistorie

Versie	Datum	Omschrijving
v8.1.0.0	21-juli-2019	Initieel document.
v8.1.1.0	4-februari-2020	INI-9137: MessageID WID/SBV-controle verwijderen uit inschrijftoken
v8.1.1.0	11-maart-2020	INI-9169: Inschrijftoken is 1.5 jaar geldig ondanks geldigheid certificaat
v8.2.0.0	1-oktober-2020	INI-9355: Aanpassingen doorgevoerd t.b.v. werkprocesondersteuning: • Uitvoerder optioneel gemaakt; • BSN validatietijd mag timestamp zijn van aanmaken inschrijftoken; • SubjectConfirmationData verplicht gesteld; *
8.2.0.1	14-november-2021	Inschrijftoken op basis van inscannen WID
8.3.0.0	9-februari-2022	De controle "De Issuer uit het inschrijftoken (URA) dient overeen te komen met de waarde van het attribuut "Zorgaanbieder" uit het scantoken" verwijderd om het gebruik van het scantoken bij een andere zorgaanbieder toe te staan.
8.3.0.1	6-februari-2024	Inschrijftoken o.b.v. UZI-pas of Scantoken verlengen via ZORG-ID Smart.
8.3.0.2	4-september-2024	Kleine aanpassing op @AuthnInstant en "Uitvoerder" bij verlenging van Inschrijftoken.
8.4.0.0	2025	Inschrijftoken o.b.v. ZORG-ID Smartcard.

10.3.2.4.2 Het SAML inschrijftoken

In de zorgsector is veilige en betrouwbare identificatie van patiënten essentieel voor correcte gegevensuitwisseling en toegangscontrole. Een **SAML inschrijftoken** speelt hierin een cruciale rol. Het dient als een cryptografisch ondertekend bewijs dat een patiënt is geïdentificeerd en ingeschreven bij een zorgaanbieder.

Het SAML inschrijftoken is gebaseerd op een **XML-gebaseerde SAML assertion** (Security Assertion Markup Language). Deze assertion bevat een verklaring over de identificatie van de patiënt en wordt gebruikt om deze bewering op een veilige en gestandaardiseerde manier over te brengen tussen zorgsystemen. Hierdoor kunnen partijen binnen het zorgnetwerk de inschrijving van een patiënt verifiëren zonder directe heridentificatie.

Het SAML token wordt gegenereerd door een zorgverlener of zorgmedewerker en ondertekend met een **geldig authenticiteitscertificaat** dat zich bevindt op een **authenticatiemiddel** zoals een **UZI-pas**, **ZORG-ID Smartcard** of **ZORG-ID Mobiel**. Dit certificaat garandeert de herkomst en betrouwbaarheid van het token, waardoor zorgsystemen kunnen controleren dat de patiënt correct is ingeschreven.

Een Inschrijftoken is maximaal **1,5 jaar (18 maanden)** geldig. Na deze periode kan het worden vernieuwd zonder dat de patiënt opnieuw fysiek hoeft te worden geïdentificeerd. Dit verlengingsproces maakt gebruik van het oorspronkelijke token of een eerder uitgevoerde **WID-scan** (Wet op de Identificatieplicht), wat de administratieve lasten voor zowel zorgverleners als patiënten verlaagt.

Door het gebruik van SAML inschrijftokens en de onderliggende **SAML assertions** wordt de uitwisseling van medische gegevens veiliger en efficiënter, met een solide balans tussen toegankelijkheid en privacybescherming binnen het zorgdomein.

In dit hoofdstuk wordt de inhoud van het SAML inschrijftoken besproken. Het SAML inschrijftoken bevat de, binnen een zorgorganisatie, gevalideerde BSN en is ondertekend door een zorgverlener of medewerker. Alle XML voorbeelden in het document dienen door de betrokken partijen tijdens het bouwen van de uitwisseling getest, en waar nodig, in samenspraak met VZVZ aangepast te worden voor een juiste optimale werking.

10.3.2.4.2.1 Structuur

Het SAML inschrijftoken is een afgegeven SAML assertion met betrekking tot de gevalideerde BSN die gebruikt wordt bij berichtauthenticatie voor het landelijk EPD. Het SAML inschrijftoken is ondertekend met behulp van een smartcard (UZI-pas of ZORG-ID Smartcard) van een zorgverlener of medewerker of m.b.v. het authenticiteit certificaat van de medewerker op naam die uitgegeven is door ZORG-ID. Er wordt gebruik gemaakt van SAML v2.0 [SAML Core].

Het UZI-register en ZORG-ID hebben als doel zorgaanbieders bij elektronische communicatie en toegang tot gegevens uniek te identificeren. Zowel het UZI-register als ZORG-ID koppelt hiertoe op unieke wijze de fysieke identiteit aan een elektronische identiteit en legt deze vast in authenticiteit certificaten. Deze certificaten en de hierbij behorende cryptografische sleutels worden vastgelegd op de smartcard. Bij het UZI-register heet dit de 'UZI-pas' en bij ZORG-ID heeft dit de 'ZORG-ID Smartcard'.

Het gebruik van OID in SAML-assertions.

Een **OID** (Object Identifier) is een unieke identificatie die wordt gebruikt om objecten of entiteiten te identificeren binnen verschillende technische systemen, met name in de wereld van cryptografie,

certificaatbeheer, netwerken en softwareontwikkeling. OID's worden vaak gebruikt om standaardconfiguraties, waarden, of zelfs certificaatattributen te identificeren, zoals algoritmen, protocollen en sleutelomgevingen.

Een OID bestaat uit een reeks niet-negatieve gehele getallen, gescheiden door punten (bijv. **2.16.840.1.113883.2.4.3.111** VZVZ service centrum). Volgens de ITU-T X.690-standaard (die ASN.1 BER/DER-codering definieert) en ISO/IEC 9834-1:

Elk getal in de reeks moet zonder voorloopnullen worden weergegeven.

Bijvoorbeeld, **2.16.84.01** is ongeldig, terwijl **2.16.840.1** correct is.

Dit voorkomt ambiguïteit en zorgt voor een eenduidige representatie van OIDs in verschillende systemen.

OID's die worden gebruikt in SAML-assertions moet in het volgende formaat worden opgenomen, ongeacht of het een HL7v3- of FHIR-client is:

- `"urn:IIroot:"<OID voor het betreffende ID-stelsel>":IIext:"<gehanteerde ID binnen dit stelsel>`, bijvoorbeeld `"urn:IIroot:"2.16.528.1.1007.3.3":IIext:"<URA>`

Belangrijk hierbij is dat de <URA> een unieke identificatiecode is voor zorgverleners en gekoppeld is aan het **UZI-register**.



Obsoleete OID formaat

Het volgende OID formaat is **Obsoleete**.

`"urn:oid:"<OID voor het betreffende ID-stelsel>". "<gehanteerde ID binnen dit stelsel>`

bijvoorbeeld

`"urn:2.16.528.1.1007.3.3."<URA>`

10.3.2.4.2.2 Assertion

De assertion heeft de volgende structuur (de waarden die in het token gebruikt worden zijn fictief):

Element / @Attribute	0..1	Omschrijving
@ID	1	Unieke identificatie van de Assertion
@Version	1	Versie van het SAML Protocol. Vaste waarde moet zijn 2.0

Element / @Attribute	0. .1	Omschrijving
@IssuInstant	1	Tijdstip van uitgifte van de Assertion.
Issuer	1	De URA van de zorgaanbieder organisatie waarbinnen de face to face controle heeft plaatsgevonden of waar het inschrijftoken wordt verlengd of waar het WID is ingescand in combinatie met een F2F controle.
@NameQualifier	0	Niet gebruiken
@SPNameQualifier	0	Niet gebruiken
@Format	1	Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"
@SPPProviderID	0	Niet gebruiken
Signat ure	1	Bevat de handtekening over de assertion zoals gezet met behulp van de smartcard van de zorgverlener (Z) of de smartcard van de medewerker op naam(N). De handtekening dient geplaatst te zijn met behulp van het authenticatie certificaat op de smartcard. De handtekening kan ook gezet zijn met het authenticiteit certificaat van de medewerker die uitgegeven is door ZORG-ID. Bij verlenging van het inschrijftoken wordt alleen gebruik gemaakt van het authenticiteit certificaat van de medewerker op naam die uitgegeven is door ZORG-ID.
Subject	1	BSN van de patiënt waarvan de BSN gevalideerd is.
BaseID	0	Niet gebruiken
NameID	1	Bevat de gevalideerde BSN.
Encrypte dID	0	Niet gebruiken
SubjectC onfirmati on	1	Moet aanwezig zijn.

Element / @Attribute	0. .1	Omschrijving
@Method	1	'urn:oasis:names:tc:SAML:2.0:cm:sender-vouches'
SubjectConfirmationData	1	Bevat Keyinfo
@Recipient	0	Niet gebruiken
@NotOnOrAfter	0	Niet gebruiken
@InResponseTo	0	Niet gebruiken
@NotBefore	0	Niet gebruiken
@Address	0	Niet gebruiken
KeyInfo	1	Bevat de X509 Issuer.serial van de medewerkerspas of zorgverlener smartcard of het publieke deel van het door ZORG-ID aangemaakte authenticiteit certificaat.
Conditions	1	Moet aanwezig zijn.
@NotBefore	1	Moet aanwezig zijn.
@NotOnOrAfter	1	Moet aanwezig zijn. Mag maximaal 1,5 jaar (18 maanden) na @NotBefore liggen.
Condition	0	Niet gebruiken
AudienceRestriction	1	Moet aanwezig zijn

Element / @Attribute	0..1	Omschrijving
Audience	1..*	Bij AORTA/LSP en AoF: <code>urn:IIroot:2.16.840.1.113883.2.4.6.6:IItext:1</code> (1 is de applicatie-id van de ZIM) Bij MITZ <code>"urn:oid:2.16.840.1.113883.2.4.3.111.2.1"</code> (is MITZ) WIJZIGINGSVOORSTEL: De verschillende Audience samenvoegen en er <code><saml:Audience>urn:generic:audience</saml:Audience></code> van maken.
ProxyRestriction	0	Niet gebruiken
Advice	0	Niet gebruiken
AuthnStatement	1	Moet aanwezig zijn
@AuthnInstant	1	Tijdstip van BSN validatie bij een nieuw inschrijftoken. Dit mag t.b.v. het werkproces ook de 'timestamp' zijn van het moment van aanmaken van het inschrijftoken of het tijdstip van inscannen van het WID. Bij een verlenging van een inschrijftoken wordt het originele tijdstip van BSN validatie overgenomen uit de oorspronkelijke inschrijftoken.
@SessionIndex	0	Niet gebruiken
AuthnContext	1	Moet aanwezig zijn
AuthnContextClassRef	1	<code>urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI</code> of <code>urn:oasis:names:tc:SAML:2.0:ac:classes:X509</code> (Deze is ondertekend via ZORG-ID Mobiel)
AttributeStatement	1	Moet aanwezig zijn
Attribute	1	Moet aanwezig zijn.

Element / @Attribute	0..1	Omschrijving
@Name	1	Vaste waarde: "Uitvoerder"
Attribute Value	1	De smartcard van de zorgverlener of medewerker die het token heeft ondertekend of de Common Name van het meegestuurd authenticiteit certificaat van ZORG-ID indien het scantoken gegenereerd is door ZORG-ID.
Attribute	0..1	Alleen aanwezig indien het een nieuw inschrijftoken op basis van een ingescand WID betreft.
@Name	0..1	Vaste waarde "Scantoken"
Attribute Value	0..1	Het scantoken Base64 gecodeerd. Voor het Scantoken zie AORTA_Auth_IH_Scantoken
Attribute	0..1	Alleen aanwezig indien het een inschrijftoken wordt <i>verlengd op basis van een origineel inschrijftoken</i> aangemaakt op basis van een smartcard van een zorgverlener of medewerker of op basis van een eerdere scantoken op basis van het authenticiteit certificaat van de uitvoerende medewerker uit ZORG-ID.
@Name	0..1	Vaste waarde "Verlengingstoken"
Attribute Value	0..1	Het originele inschrijftoken ondertekend op basis van een smartcard of het eerdere WID-scantoken op basis van het authenticiteit certificaat van de uitvoerende zorgverlener/medewerker uit ZORG-ID dat verlengd gaat worden, wordt Base64 gecodeerd. Als er al een origineel inschrijftoken in het "Verlengingstoken" aanwezig is en het inschrijftoken opnieuw verlengd moet worden, dan wordt het bestaande "Verlengingstoken" uit het inschrijftoken hergebruikt voor het nieuwe inschrijftoken.

N.B.: bovenstaande tabel bevat de meest gebruikte elementen van SAML assertions en is derhalve niet volledig. Voor niet genoemde elementen geldt: Niet gebruiken.

10.3.2.4.2.3 Namespaces

Het SAML inschrijftoken die gebruikt wordt bij berichtauthenticatie maakt gebruik van de volgende namespaces. De prefixen zijn *niet normatief* maar worden in dit document als voorbeelden gebruikt.

Tabel AORTA.STK.t3300 – Namespaces

Prefix	Namespace URI

ds	http://www.w3.org/2000/09/xmldsig#
saml	urn:oasis:names:tc:SAML:2.0:assertion
wss	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd



Bij het gebruik van de namespace-prefixes is het van belang deze na het ondertekenen niet meer te veranderen, dit maakt de digitale handtekening ongeldig.

10.3.2.4.2.4 Inhoud

De volgende paragrafen beschrijven de verschillende kenmerken en beveiligingsgerelateerde gegevens die het SAML inschrijftoken onderscheiden, zoals in [IH tokens generiek] beschreven is.

```
<saml:Assertion ... xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
```

Het SAML inschrijftoken begint met het Assertion element en een verwijzing naar de XML SAML namespace voor SAML 2.0 assertions. De attributen behorende bij het Assertion element wordt in [paragraaf 2.4.1](#)¹²⁵ Uniekheid beschreven.

Uniekheid

```
ID="token_dd1c1f96-f0b0-4026-a978-4d724c0a0a4f"
IssueInstant="2009-06-24T11:47:34Z"
Version="2.0">
```

De volgende attributen van het SAML assertion element maken van de SAML assertion een uniek gegeven, uitgegeven door de verzender van het bericht. Het attribuut ID identificeert op een unieke wijze de assertion. De waarde moet *mondiaal uniek* zijn voor AORTA berichten, zodat bij samenvoegen van meerdere XML bestanden (in een HL7v3 batch of anderszins) de waarde uniek blijft.

125. <https://vzvz.atlassian.net/wiki/spaces/A8/pages/85000380/Het+SAML+inschrijftoken#HetSAMLinschrijftoken-Uniekheid>

Het wordt aanbevolen een UUID (Universally Unique Identifier) te gebruiken. Bij het gebruik van andere vormen is er een kans, hoe klein ook, dat een ID samenvalt met een ID gemaakt volgens een andere methode van een andere leverancier).



Een ID in XML mag niet met een cijfer beginnen. Bij het gebruik van een UUID is het dus aan te raden een prefix te gebruiken, welke met een letter of underscore ('_') begint.

Het attribuut IssueInstant is een tijdsmoment van uitgifte van de SAML assertion. De tijdswaarde is gecodeerd in UTC. Het attribuut Version is de gebruikte SAML versie van de SAML assertion. De aanduiding voor de versie van SAML gedefinieerd in deze specificatie is "2.0".

Afzender

```
<saml:Issuer>
  <!-- De Issuer verwijst naar de organisatie waarbinnen de BSN validatie heeft
  plaats gevonden.-->
  urn:IIroot:2.16.528.1.1007.3.3:IItext:12345678
</saml:Issuer>
```

De URA wordt uitgedrukt met behulp van een URN (Uniform Resource Name). De URN is opgebouwd uit:

"urn:IIroot:"<OID voor UZI organisatielids>":IItext:"<URA>

De URN string is opgebouwd uit een IIroot en een IIext. "II" staat voor het HL7v3 datatype Instance Identifier. Om de namespace in URN uniek te krijgen is II als prefix voor de root en ext geplaatst. URA's worden uitgedrukt als een id onder het identificatiesysteem "2.16.528.1.1007.3.3". De URA wordt toegekend door het UZI-register. Stel dat de URA de waarde "12345678" heeft, dan ziet de URN er als volgt uit:

urn:IIroot:2.16.528.1.1007.3.3:IIext:12345678

Onderwerp

```
<saml:Subject>
  <saml:NameID>
    950052413
  </saml:NameID>
  <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:sender-vouches ">
    </saml:SubjectConfirmation>
</saml:Subject>
```

De Subject verwijst naar de door de zorgverlener/medewerker gevalideerde BSN. De BSN validatie dient plaatsgevonden te hebben

1) Aan de balie door:

- Een face to face controle van de patient en diens Wettelijk Identiteits Document (WID)
- Een controle van de geldigheid van het WID bij SBV-Z
- Een controle van de correctheid van het BSN bij SBV-Z

2) Door inlezen van de chip uit het WID waarbij:

- De echtheid van het WID wordt gecontroleerd
- De BSN wordt uitgelezen uit de chip of, bij paspoorten uitgegeven na 1 augustus 2021, de BSN QR code wordt gelezen.

3) Het subject en de daarbij behorende BSN overnemen uit het oorspronkelijke inschrijftoken dat verlengd gaat worden.

Vervolgens moet de SubjectConfirmation nog toegevoegd worden:

```
<saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:sender-vouches" ">
</saml:SubjectConfirmation>
```

Geldigheid

```
<saml:Conditions
  NotBefore="2009-06-24T11:47:34Z"
  NotOnOrAfter="2010-12-24T11:47:34Z">
```

Het attribuut *NotBefore* is de tijd waarop de SAML assertion geldig wordt. *NotBefore* moet altijd op of na de aanvang van de geldigheidsdatum van het certificaat (waarmee het inschrijftoken is getekend) liggen.



Wordt een bericht met een inschrijftoken ontvangen voor *NotBefore* is aangevallen, dan **moet** dit bericht geweigerd worden.

Het attribuut *NotOnOrAfter* is de tijd waarop de SAML assertion vervalst. *NotOnOrAfter* mag na het verstrijken van de geldigheid van het authenticiteit certificaat (waarmee het inschrijftoken is getekend) liggen.



Wordt een bericht met een inschrijftoken ontvangen op of nadat *NotOnOrAfter* is verstreken, dan **moet** dit bericht geweigerd worden.

Deze tijd is als bovenstaande tijd geformatteerd. Het maximaal toegestane verschil tussen *NotBefore* en *NotOnOrAfter* is anderhalf jaar.



De geldigheidsduur van een inschrijftoken (*NotOnOrAfter* minus *NotBefore*) kan langer zijn dan de geldigheidsduur van het authenticiteit certificaat waarmee het token wordt getekend.

Indien het authenticiteit certificaat waarmee het inschrijftoken is getekend op de CRL is geplaatst, dan dient het inschrijftoken niet geweigerd te worden door het LSP. Het is op de CRL niet inzichtelijk om welke reden een authenticiteit certificaat op de CRL is geplaatst. Dit kunnen uiteenlopende redenen zijn zoals een verloren pas of een intrekking van een BIG-registratie. Om het zorgproces niet te frustreren wordt deze controle procesmatig opgepakt door Security Management.

Echter, bij het ondertekenen van het inschrijftoken moet er een geldig authenticiteit certificaat gebruikt worden. Indien bij ondertekening van het inschrijftoken het authenticiteit certificaat al op de CRL is geplaatst, dan dient het inschrijftoken wel geweigerd te worden.



Indien het authenticiteit certificaat vóór ondertekening van het inschrijftoken op de CRL is geplaatst, dan dient het inschrijftoken geweigerd te worden door het LSP.



Indien het authenticiteit certificaat na ondertekening van het inschrijftoken op de CRL is geplaatst, dan dient het inschrijftoken niet geweigerd te worden.

Het inperken van bepaalde partijen (AudienceRestriction) waarvoor de assertion bedoeld is wordt beschreven in [paragraaf 2.4.5](#)¹²⁶ Ontvanger.

Ontvanger

```
<saml:AudienceRestriction>
  <!-- Root en extensie van de ZIM -->
  <saml:Audience>urn:IIroot:2.16.840.1.113883.2.4.6.6:IIext:1</saml:Audience>
</saml:AudienceRestriction>
```

126. <https://vzvz.atlassian.net/wiki/spaces/A8/pages/85000380/Het+SAML+inschrijftoken#HetSAMLinschrijftoken-Ontvanger>

In de AudienceRestriction wordt beschreven aan wie de SAML assertion is gericht. In ieder geval dient de ZIM als audience voor te komen (llex:1). Meerdere Audience elementen is toegestaan.

Voor de <Audience> parameter is gekozen voor URN. De URN string is opgebouwd uit een lroot en een llex. "l" staat voor het HL7v3 datatype Instance Identifier. Om de namespace in URN uniek te krijgen is l als prefix voor de root en ext geplaatst.

AORTA Applicatie-id's worden uitgedrukt als een id onder het identificatiesysteem "2.16.840.1.113883.2.4.6.6". Het correcte applicatie-id voor de GBZ-applicatie wordt toegekend bij aansluiting op de AORTA. Stel dat dit "300" zou zijn, dan ziet de URN er als volgt uit:
urn:llroot:2.16.840.1.113883.2.4.6.6:llex:300

Authenticatie

Een authenticatiemiddel wordt gedefinieerd als een middel waarmee de identiteit van een gebruiker wordt geverifieerd voordat toegang tot een systeem of dienst wordt verleend. Bijvoorbeeld een smartcard koppelt een fysieke identiteit (zorgverlener of medewerker) aan een elektronische identiteit.

```
<saml:AuthnStatement
  AuthnInstant="2009-06-24T11:47:34"
  SessionIndex="token_2.16.528.1.1007.3.3.1234567.1_0123456789">
```

Het subject, de gevalideerde BSN, in de SAML assertion is geauthentiseerd door middel van een authenticatiemiddel van de uitvoerende zorgverlener/medewerker.

Als de zorgverlener/medewerker de smartcard (UZI-pas f ZORG-ID Smartcard) heeft gebruikt als authenticatiemiddel wordt de AuthContextClassRef SmartcardPKI:

```
<saml:AuthnContext>
  <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI</
saml:AuthnContextClassRef>
</saml:AuthnContext>
```

Als de zorgverlener/medewerker ZORG-ID Mobiel als authenticatiemiddel heeft gebruikt wordt de AuthContextClassRef X509:

```
<saml:AuthnContext>
  <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:X509</saml:AuthnContextClassRef>
</saml:AuthnContext>
```

Binnen de gebruikte applicatie beveiligingsstandaarden is er sprake van verschillende vertrouwensniveaus.

Binnen de SAML-specificatie geeft men een authenticatie-context (*AuthnContext*) mee die de context van het gebruikte authenticatiemiddel aangeeft. Hiervoor zijn een aantal contexten gespecificeerd, zie [SAMLAuthnContext], die gebruikt worden als referentiekader voor de communicatie tussen de ZIM en andere componenten zoals GBZ applicaties.

Uitgaande van de beveiligingsniveaus van GBZ, zorgverlener/medewerker en smartcard wordt het "urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI" of "urn:oasis:names:tc:SAML:2.0:ac:classes:X509" beveiligingsniveau gehanteerd om het AORTA vertrouwensniveau midden voor zorgverleners weer te geven.

```
</saml:AuthnStatement>
```

Afsluiting authentication statement.

Attributen

```
<saml:AttributeStatement>
```

De volgorde van de attributen in het AttributeStatement is niet relevant. Er mogen geen andere attributen opgenomen worden in het AttributeStatement dan hier beschreven is.

Uitvoerder

```
<saml:Attribute Name="Uitvoerder">
  <saml:AttributeValue>123456789</saml:AttributeValue>
```

```
</saml:Attribute>
```

Het attribuut Uitvoerder bevat het UZI-nummer van de zorgverlener en medewerker op naam die de BSN validatie heeft uitgevoerd en het token heeft ondertekend. Indien deze nog niet bekend is bij het aanmaken van het inschrijftoken, dan kan dit veld leeg gelaten worden. Vanuit het authenticiteit certificaat waarmee het token is ondertekend, kan dan worden afgeleid wat het UZI-nummer van de ondertekenaar was. Voor de zorgverlener en de medewerker op naam is het UZI-nummer uniek gekoppeld aan de natuurlijk persoon.

Indien het scantoken is gegenereerd door Zorg-ID, dan kan dit attribuut ook de Common Name (CN) van het authenticiteit certificaat waarmee het token is ondertekend bevatten.

Bijvoorbeeld:

```
<saml:AttributeValue>Jan Test:91000001</saml:AttributeValue>
```

In dit voorbeeld zijn de volgende waarden te vinden:

Jan Test: Voornaam Achternaam

91000001: Uniek nummer`. Start van 91000000 en hoger.

Scantoken

```
<saml:Attribute Name="Scantoken">
  <saml:AttributeValue xsi:type="base64Binary">
    Hier het scantoken base64 gecodeerd.
  </saml:AttributeValue>
</saml:Attribute>
```

Het attribuut Scantoken bevat het Scantoken Base64 gecodeerd. Voor de opbouw van het Scantoken wordt verwezen naar [AORTA_Auth_IH_Scantoken]. Dit attribuut dient alleen aanwezig (en gevuld) te zijn als het gehele inschrijftoken ondertekend is met het identiteitscertificaat van ZORG-ID.

Verlengingstoken

```

<saml:Attribute Name="Verlengingstoken">

  <saml:AttributeValue xsi:type="base64Binary">

    Hier het originele inschrijftoken base64 gecodeerd.

  </saml:AttributeValue>

</saml:Attribute>

```

Het attribuut Verlengingstoken bevat het originele Inschrijftoken o.b.v. de smartcard of het scantoken op basis van het authenticiteit certificaat van de uitvoerende medewerker uit ZORG-ID, Base64 gecodeerd. Voor de opbouw van het scantoken wordt verwezen naar [AORTA_Auth_IH_Scantoken]. Het attribuut Verleningstoken dient alleen aanwezig (en gevuld) te zijn als het gehele inschrijftoken ondertekend is met het authenticiteit certificaat van ZORG-ID.

Tenslotte wordt het attributen statement blok afgesloten met

```

</saml:AttributeStatement>

```

10.3.2.4.2.5 Algoritmes

Om de integriteit en onweerlegbaarheid van het SAML inschrijftoken te waarborgen wordt een XML Signature geplaatst, zoals beschreven in [IH tokens generiek]. Na plaatsen van de XML Signature kan de ontvanger, met gebruikmaking van het persoonsgebonden authenticiteit certificaat van de verzender en de CA certificaten zoals verstrekt door het UZI-register of ZORG-ID, onomstotelijk vaststellen dat het SAML inschrijftoken ondertekend is met de privé sleutel behorend bij het gebruikte certificaat van de zorgmedewerker.

De XML Signature van het SAML inschrijftoken die gebruikt wordt bij berichtauthenticatie met behulp van de smartcard maakt gebruik van de volgende algoritmes, zoals beschreven in [IH tokens generiek]:

- Voor het berekenen van de hashwaarde wordt SHA-256 gebruikt.
- Voor de digitale handtekening in AORTA wordt gebruik gemaakt van een RSA handtekening over een SHA-256 digest.



Omdat de XML Signature onderdeel is van het SAML inschrijftoken en in het SAML inschrijftoken geplaatst wordt, moet er een "enveloped-signature" transformatie uitgevoerd worden die de Signature tags uit het SAML inschrijftoken verwijderd gevolgd door een "exc-c14n transformatie" (zie ook [SAML Core] §5.4.3 en §5.4.4).

10.3.2.4.2.6 Opbouw

De headers

Eerst wordt het SAML inschrijftoken – het <saml:Assertion ...> element aangemaakt en gevuld met die elementen, zoals beschreven in [paragraaf 2.4](#)¹²⁷Inhoud.

```
<saml:Assertion
  ID="token_2.16.528.1.1007.3.3.1234567.1_0123456789"
  IssueInstant="2009-06-24T11:47:34Z"
  Version="2.0"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
  ... Zie paragraaf 2.4 Inhoud ...
</saml:Assertion>
```

Het XML Signature blok is onderdeel van het SAML inschrijftoken. Het XML Signature blok komt na het <saml:Issuer> element. Na de Signature volgt de rest van de inhoud van de assertion.

```
<saml:Assertion
  ID="token_2.16.528.1.1007.3.3.1234567.1_0123456789"
  IssueInstant="2009-06-24T11:47:34Z"
  Version="2.0"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
  <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
    urn:IIroot:?:IIext:?
  </saml:Issuer>
```

127. <https://vzvz.atlassian.net/wiki/spaces/A8/pages/85000380/Het+SAML+inschrijftoken#HetSAMLinschrijftoken-Inhoud>

```

<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:SignedInfo>
    ...
  </ds:SignedInfo>
  <ds:SignatureValue>Wuwn...5e4=</ds:SignatureValue>
  <ds:KeyInfo>
    <wss:SecurityTokenReference>
      <ds:X509Data>
        ...
      </ds:X509Data>
    <wss:SecurityTokenReference>
    </ds:KeyInfo>
  </ds:Signature> ...
  ... Zie paragraaf 2.3 Inhoud ...
</saml:Assertion>

```

Indien de Signature aangemaakt wordt moet niet meer met de strings (saml:Assertion en SignedInfo) gemanipuleerd worden, maar ze moeten octet-voor-octet overgenomen worden in het bericht. Strikt genomen is het toegestaan wijzigingen aan te brengen die door canonicalisatie bij de ontvanger weer opgeheven worden, maar wanneer de digitale handtekening door middel van strings wordt opgebouwd, is het een foutgevoelige handeling.

Lange Base 64 waarden zijn afgekort. Wederom kan dit als strings worden behandeld, waarbij drie waarden vervangen moeten worden.

Deze drie waarden worden ingevuld:

- Neem het SignedInfo blok op.
- Neem de SignatureValue op.
- Neem certificaatgegevens in het KeyInfo blok op, in de vorm van een verwijzing (X509IssuerSerial).



Wanneer een bericht een SAML assertion bevat, moet dat bericht precies één bijbehorende digitale handtekening bevatten.

Het maken van de XML Signature uit strings levert de SAML assertion op met daarin de Signature.

Plaats van het SAML token en de digitale handtekening

Het SAML inschrijftoken met daarin de digitale handtekening wordt in het WS-Security SOAP Header gezet. Op het <wss:Security> element **moet** een soap:mustUnderstand="1" vlag opgenomen worden, die aangeeft dat de ontvanger dit security element **moet** verwerken en een soap:actor="<http://www.aortarelease.nl/actor/zim>" die aangeeft dat de ZIM dit security element verwerkt.

```
<soap:Header xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">

...

<wss:Security xmlns:wss=
  "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
  soap:actor="http://www.aortarelease.nl/actor/zim" soap:mustUnderstand="1">

  <saml:Assertion ... >

    <saml:Issuer>...</saml:Issuer>

    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

      <ds:SignedInfo>

        ...

      </ds:SignedInfo>

      <ds:SignatureValue>Wuwn...5e4=</ds:SignatureValue>

      <ds:KeyInfo>

        <ds:X509Data>

          ...

        </ds:X509Data>

      </ds:KeyInfo>

    </ds:Signature>

    ... Zie paragraaf 2.3 Inhoud ...

  </saml:Assertion ... >

</wss:Security>
```



```
</soap:Header>
```

10.3.2.4.3 Certificaten Inschrijftoken

10.3.2.4.3.1 Te gebruiken certificaat en attributen UZI

De UZI-pas kent een aantal modellen:

Tabel AORTA.STK.t3210 – UZI pastype

Naam UZI-pastype	Codering Pastype
Zorgverlenerpas	Z
Medewerkerpas op naam	N
Medewerkerpas niet op naam	M
Servercertificaat	S

De UZI-pas die gebruikt wordt voor het ondertekenen van een inschrijftoken moet een zorgverlener- of een medewerkerspas op naam zijn. Hoewel het pastype gecodeerd is opgenomen in het authenticiteit certificaat (in het subjectAltName attribuut), dient een applicatie op basis van de uitgevende CA vast te stellen wat het pastype van de UZI-pas is.

De signature wordt gezet met de sleutel voor authenticiteit (keyUsage=digitalSignature, hexadecimaal 0x80).

De attributen in het authenticiteit certificaat worden gegeven in de vorm van een Distinguished Name (DN), zie [IH tokens generiek].

De waarden van deze attributen voor de relevante UZI-passen zijn:

Tabel AORTA.STK.t3220 – DN attributen van zorgverlenerspas

Attribuut	Omschrijving	Waarde

CN	Issuer.commonName	<i>Derde generatie:</i> UZI-register Zorgverlener CA G3 Voor mogelijke volgende generaties wordt verwezen naar het UZI-register: https://www.uziregister.nl/
O	Issuer.organisationName	agentschap Centraal Informatiepunt Beroepen Gezondheidszorg
C	Issuer.countryName	NL

	De issuer.commonName verschilt per 'generatie' UZI-passen. Het is mogelijk dat verschillende 'generatie' UZI-passen door elkaar worden gebruikt. Daarom dient de Issuer DN dynamisch afgeleid te worden uit het gebruikte authenticatie certificaat.

Tabel AORTA.STK.t3230 – DN attributen van medewerkerpas op naam van de UZI-pas

Attribuut	Omschrijving	Waarde
CN	Issuer.commonName	<i>Derde generatie:</i> UZI-register Medewerker op naam CA G3 Voor mogelijke volgende generaties wordt verwezen naar het UZI-register: https://www.uziregister.nl/
O	Issuer.organisationName	agentschap Centraal Informatiepunt Beroepen Gezondheidszorg
C	Issuer.countryName	NL

Tabel AORTA.STK – DN attributen van medewerkerpas op naam van de ZORG-ID Smartcard

Attribuut	Omschrijving	Waarde
CN	Issuer.commonName	ZORG-ID Token CA
O	Issuer.organisationName	ZORG-ID
C	Issuer.countryName	NL

Extensions	OID	2.16.840.1.113883.2.4.3.111.20.5
proofValue	Cryptografisch bewijs om herkomst van een credential te verifiëren	z58.....ktZ

Om de digitale handtekening bij het LSP te verifiëren, moet de ontvanger over de bijbehorende publieke sleutel beschikken, zie [IH tokens generiek].

Voor verificatie is gekozen een verwijzing naar het authenticiteit certificaat mee te zenden; de ontvanger moet deze dan met bijvoorbeeld het LDAP protocol ophalen in de directory van het UZI-register of ZORG-ID.

Zie voor de verdere beschrijving van de passen [UZI pas].

Noot: uiteraard mogen in het testtraject alleen UZI-testpassen gebruikt worden. Het gebruik hiervan wordt verder niet uitgewerkt in deze handleiding. De werking is identiek.

Te gebruiken authenticiteit certificaat en attributen

ZORG-ID geeft unieke authenticiteit certificaten uit, gebaseerd op X.509, aan medewerkers. De waarden van de properties voor deze authenticiteit certificaten zijn:

Tabel ZORG-ID – properties van de authenticiteit certificaat

Property	Omschrijving	Waarde
Name	Authenticiteit certificaat van een medewerker	Person certificate
Subject DN	Onderwerp aan wie dit authenticiteit certificaat is uitgegeven. Volgende velden zijn gebruikt: • Common Name (CN) • Country C	CN=Voornaam Achternaam:ZIDnummer C=NL
Issuer DN	Uitgever van het authenticiteit certificaat. Volgende velden zijn gebruikt: - CommonName (CN) - Organisatie (O) - Country (C)	CN=ZORG-ID Person CA O=ZORG-ID C=NL

De CommonName van het Subject DN wordt ingevuld als AttributeValue bij het attribuut “Uitvoerder” in het inschrijftoken als dit door ZORG-ID wordt aangemaakt of wordt verlengd.

Zie voor de verdere beschrijving [UZI pas](#)¹²⁸

10.3.2.4.4 Referenties inschrijftoken

10.3.2.4.4.1 Bijlage A Referenties

Referentie	Document	Versie
[IH tokens generiek]	GBx AORTA_Auth_IH_Security_tokens_generiek (see page 435)	8.3.0.0
[Transactietoken]	GBZ AORTA_Auth_IH_Berichtauthenticatie_Transactietoken (see page 399)	8.3.0.0
[Mandaattoken]	AORTA_Auth_IH_Mandaattoken (see page 475)	8.3.0.0
[Scantoken]	ZORG-ID AORTA_Auth_IH_Scantoken_en_WID_token (see page 508)	8.3.0.0
[SAMLAuthnContext]	Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0 http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf	2.0 15-mrt-2005
[SAML Core]	SAML v2.0 Core Specification https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf	2.0 15-mrt-2005
[SAML Profiles]	Profiles for the OASIS Security Assertion Markup Language (SAML) v2.0 http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf	2.0 15-mrt-2005
[SAML Token]	SAML Token Profile http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SAMLSAMLTokenProfile.pdf	1.1 01-feb-2006
[UZI pas]	CA model, Pasmodel, Certificaat- en CRL-profielen, Agentschap CIBG www.uziregister.nl ¹²⁹	9.6 26 april 2019

128. <https://vzvz.atlassian.net/wiki/pages/createpage.action?spaceKey=A8&title=UZI+pas>

[PKI Design]	Describes the design of the PKI of ZORG-ID and provides a backbone for the Identity Security	1.8 24-dec-2024
[JWT]	RFC 7519 JSON Web Token (JWT) https://www.rfc-editor.org/rfc/rfc7519	Mei 2015
[JWS]	RFC 7515 JSON Web Signature (JWS) https://www.rfc-editor.org/rfc/rfc7515	Mei 2015
[JWA]	RFC 7518 JSON Web Algorithms (JWA) https://www.rfc-editor.org/rfc/rfc7518	Mei 2015

10.3.2.4.5 Token afhandeling inschrijftoken

10.3.2.4.5.1 Verificatie van het bericht

Het is belangrijk vast te stellen dat de velden in het SAML inschrijftoken een correcte waarde hebben en geldig ondertekend zijn. Wanneer dit niet zou gebeuren, kan een kwaadwillende met een gestolen token nog steeds gegevens opvragen van bv. ieder willekeurig Burgerservicenummer.

De ontvanger controleert of de WS-Security SOAP Header voor hem bestemd is, zie soap attribuut actor.

Het SAML inschrijftoken wordt door de ontvanger uit de WS-Security SOAP Header gehaald indien de WS-Security SOAP Header voor de ontvanger bestemd is en dat de ontvanger deze moet verwerken. Bij gebruik van het SAML inschrijftoken moet de ontvanger controleren of:

- De aanduiding voor de versie van SAML gedefinieerd is op "2.0", zie [Uniekheid \(see page 382\)](#) ;
- De juiste organisatielD is opgenomen die deze assertion heeft gecreëerd en de gebruiker heeft geauthentiseerd, zie [Afzender \(see page 383\)](#). Het zorgaanbiederID in het token dient overeen te komen met de zorgaanbiederID in het bericht. Tevens dient de zorgaanbiederID overeen te komen met:
 - De URA van het transactietoken
 - De URA uit het mandaattoken
- Het BSN uit het Subject zie [Onderwerp \(see page 383\)](#) overeenkomt met het BSN uit het transactietoken en het BSN uit het HL7-bericht;
- De Assertion correct is ondertekend door de Signature te valideren met het gerefereerde certificaat.
- Het gebruikte certificaat waarmee de ondertekening heeft plaatsgevonden geldig was ten tijde van de ondertekening.

129. <http://www.uziregister.nl/>

- Indien het certificaat op de CRL is geplaatst, dan dient dit plaats te hebben gevonden nadat het token gegenereerd en ondertekend is.
- De relevante certificaatketen te valideren op geldigheid.
- De geldigheidsperiode van het token, zie [Geldigheid \(see page 384\)](#) , niet langer is dan 1,5 jaar;
- Het bericht ontvangen is binnen de geldigheidsperiode van het token, zie [Geldigheid \(see page 384\)](#) ;
- De afnemer van het SAML inschrijftoken (audience) minimaal de ZIM is, zie [Ontvanger \(see page 385\)](#) ;
- De zorgverlener/zorgmedewerker is geauthentiseerd via het voor gedefinieerde authenticatiemiddel, de SmartCardPKI, zoals beschreven in [Authenticatie \(see page 386\)](#) ;
- Alleen die attributen zijn gedefinieerd, die zijn beschreven in [Attributen \(see page 387\)](#) ;
- Indien het inschrijftoken ondertekend is met een UZI certificaat: de attribuutwaarde van Uitvoerder overeenkomt met het UZI-nummer van het gerefereerde certificaat, zie [Attributen \(see page 387\)](#) ;
- Indien het inschrijftoken ondertekend is met het authenticiteit certificaat van ZORG-ID Mobile CA (CA) dienen de volgende extra controles plaats te vinden:
 - Het attribuut Scantoken dient aanwezig te zijn met hierin het Base64 gecodeerde scantoken
 - Het scantoken dient gedecodeerd en vervolgens gevalideerd te worden, zie [[Scantoken](#)¹³⁰].
 - Het verleningstoken dient gedecodeerd en vervolgens gevalideerd te worden, indien het attribuut Verlengingstoken aanwezig is.
 - Het subject uit het inschrijftoken (BSN) dient overeen te komen met de waarde van het subject uit het scantoken.
 - De AuthnInstant uit het inschrijftoken (DatumTijd) dient overeen te komen met de waarde van het AuthnInstant attribuut uit het scantoken.
 - De attribuutwaarde van Uitvoerder overeenkomt met de Common Name van het meegestuurde certificaat, zie [Attributen \(see page 387\)](#)
- Indien het inschrijftoken ondertekend is met het authenticiteit certificaat van ZORG-ID Token CA (CA) dienen de volgende extra controles plaats te vinden:
 - Van het gebruikte certificaat moet het extensie bewijs (proofValue) gecontroleerd worden dat dit met een geldige UZI-medewerkerspas op naam is gebeurd ten tijde van de ondertekening.
 - De proofValue extensie heeft de volgende OID: 2.16.840.1.113883.2.4.3.111.20.5 (Custom Extension copied Certificate)
 - De proofValue is een JSON Web Token dat uit drie delen bestaat:
`header.payload.signature`
 - Om het bewijs te controleren, moet uit het header element `x5c` , het X.509 certificaat geëxtraheerd worden, met Base64, waar vervolgens de publieke sleutel gehaald wordt.

130. <https://vzvz.atlassian.net/wiki/x/v4ltN>

- Gebruik de publieke sleutel om de JWT-handtekening te valideren met de algoritme die uit het header element `alg` is vastgelegd.
- Controleer of het geëxtraheerde certificaat ondertekend is door de vertrouwde CA (Certificate Authority)
- Decodeer de payload met Base64.
- Controleer de claims uit de payload, met die van het authenticiteit certificaat van ZORG-ID Token CA:
 - "ura"
 - "uziNumber"
 - "roleCode"
- Het inschrijftoken mag meerdere malen gebruikt worden.
- Het tokenID dient in de log van de ZIM opgenomen te worden.
- Als aan één van de bovenstaande condities niet is voldaan, moet het bericht door de ontvanger geweigerd worden en een SOAP foutmelding aan het verzendende systeem afgegeven worden, zie foutafhandeling in [IH tokens generiek].
- Als wel aan alle condities is voldaan, wordt het HL7v3 bericht verder verwerkt.

10.3.2.5 GBZ AORTA_Auth_IH_Berichtauthenticatie_Transactietoken

- **IH Berichtauthenticatie Transactietoken**

Datum: 1 februari 2025

Publicatie: V8.4.0.0

10.3.2.5.1 Inleiding transactietoken

10.3.2.5.1.1 Doel en scope

Dit document heeft tot doel een handleiding te geven voor de implementatie van het koppelvlak tussen het goed beheerde Zorgsystemen (GBZ) en het landelijk schakelpunt (LSP) voor wat betreft de toe te passen technieken voor de authenticatie van zorgverleners en medewerkers.

10.3.2.5.1.2 Doelgroep voor dit document

Dit document is bedoeld voor softwareontwikkelaars van goed beheerde zorgsystemen en het LSP, die op grond van de HL7v3 communicatiestandaard en op grond van dit document berichten willen uitrusten met het SAML transactietoken. Daarnaast wordt het plaatsen van de digitale handtekening besproken (zie ook [IH tokens generiek]).

10.3.2.5.1.3 Documenthistorie

Versie	Datum	Omschrijving
v8.0.2.0	31-januari-2018	Initieel document.
v8.0.3.0	15-nov-2018	Opgenomen in publicatie 8.0.3.0
v8.1.0.0	26-juni-2019	INI-8877: Aanpassing ten behoeve van de conditionele query
V8.1.0.0	13-september-2019	INI-9019: Optioneel gebruik BSN
V8.1.1.0	30-januari-2020	In hoofdstuk 3.1 verduidelijkt hoe om te gaan met het ondertekenen met een server certificaat.
V8.1.1.0	30-januari-2020	Op verschillende plekken in het document aangescherpt dat er ook ondertekend kan worden met een UZI-servercertificaat.
V8.2.0.0	22-juli-2020	Controle op overseer in hoofdstuk 4.1 aangepast.
V8.4	2025	Transactietoken o.b.v. ZORG-ID Smartcard.

10.3.2.5.1.4 Legenda

Deze implementatiehandleiding gebruikt de volgende symbolen:

	Let op! Dit is een aandachtspunt. Een opmerking die de aandacht vestigt op een bepaald opvallend aspect.
	Dit is een 'open issue' of 'known issue'. Een kwestie die nog open ligt voor discussie, maar onderkend is.
	Dit is een frequently asked question (FAQ) met antwoord.

10.3.2.5.2 Het SAML transactietoken

In dit hoofdstuk wordt de inhoud en het gebruik van het **SAML-transactietoken** besproken, zoals dat wordt toegepast bij berichtauthenticatie met behulp van een gekwalificeerd persoonscertificaat of servercertificaat. Het **SAML-transactietoken** is een XML-gebaseerde **SAML-assertion** die dient als bewijs (assertion) van de authenticatie en identificatie van een zorgverlener, medewerker, of organisatie.

Het token speelt een cruciale rol in het beveiligen van gegevensuitwisselingen tussen zorginformatiesystemen en het Landelijk Schakelpunt (LSP), en ondersteunt de integriteit en betrouwbaarheid van transacties in de zorg. Het is specifiek ontworpen om te voldoen aan de eisen voor gegevensbescherming en privacy, zoals vastgelegd in de NEN7510- en NEN7518-normen.

Alle XML voorbeelden in het document dienen door de betrokken partijen tijdens het bouwen van de uitwisseling getest, en waar nodig, in samenspraak met VZVZ aangepast te worden voor een juiste optimale werking.

De **SAML-transactietoken** wordt gebruikt bij verschillende koppelvlakken, zoals:

- **AORTA/LSP:** Goed Beheerd Zorgsysteem (GBZ) – het Landelijk SchakelPunt (LSP)
- **Mitz:** Toestemmingsbeheer en
- **AoF:** Aorta on FHIR (RESTful API's)

Hierbij worden de volgende transport mechanismes gebruikt:

- **WSS (Web Service Security) SOAP-berichtenprofiel**
 - Dit profiel faciliteert het veiligstellen en uitwisselen van authentieke SOAP-berichten tussen een Goed Beheerd Zorgsysteem (GBZ) en het LSP.
 - Het token wordt gebruikt om de afzender te authentifieren en het bericht te autoriseren.
- **FHIR RESTful-interacties**

- Voor omgevingen die gebruikmaken van (FHIR) REST-API's, zoals in **AORTA on FHIR**, wordt de SAML-assertion meegegeven in de HTTP-header, bijvoorbeeld in een `Authorization` header.
- Hier wordt vaak gebruik gemaakt van een combinatie van **SAML** en **JWT** (JSON Web Token) voor compatibiliteit met moderne infrastructuren.
- **SAML assertion via HTTP-payload**
 - Hier wordt de SAML-assertion in de body van een HTTP-verzoek opgenomen, als onderdeel van een JSON- of XML-structuur, bv in een JSON payload: `"samlAssertion": "<Base64-encoded-SAML-assertion>"`

Voor het verkrijgen van het SAML-transactietoken en het aanbieden van dit token aan systemen worden de volgende profielen gebruikt:

- Het gebruik van het SAML transactietoken (security token) in het kader van het WSS SOAP berichten profiel voor het veilig stellen en uitwisseling van authentieke SOAP berichten.
- Het gebruik van het SAML transactietoken (security token) in het kader AORTA on FHIR berichten profiel voor het veilig stellen en uitwisseling van authentieke FHIR berichten.

De profielen worden in de volgende paragrafen verder uitgewerkt.

10.3.2.5.2.1 Het gebruik van OID in SAML-assertions.

Een **OID** (Object Identifier) is een unieke identificatie die wordt gebruikt om objecten of entiteiten te identificeren binnen verschillende technische systemen, met name in de wereld van cryptografie, certificaatbeheer, netwerken en softwareontwikkeling. OID's worden vaak gebruikt om standaardconfiguraties, waarden, of zelfs certificaatattributen te identificeren, zoals algoritmen, protocollen en sleutelomgevingen.

Een OID bestaat uit een reeks niet-negatieve gehele getallen, gescheiden door punten (bijv. **2.16.840.1.113883.2.4.3.111** VZVZ service centrum). Volgens de ITU-T X.690-standaard (die ASN.1 BER/DER-codering definieert) en ISO/IEC 9834-1:

Elk getal in de reeks moet zonder voorloopnullen worden weergegeven.

Bijvoorbeeld, **2.16.84.01** is ongeldig, terwijl **2.16.840.1** correct is.

Dit voorkomt ambiguïteit en zorgt voor een eenduidige representatie van OIDs in verschillende systemen.

Kenmerken van een OID:

1. **Uniciteit:** OID's zijn wereldwijd uniek en worden vaak beheerd door officiële organisaties zoals ISO (International Organization for Standardization), IETF (Internet Engineering Task Force), of specifieke standaardorganisaties.
2. **Hiërarchische structuur:** OID's volgen een hiërarchische structuur, waarbij elk segment van het nummer verwijst naar een specifieke subcategorie of entiteit. Dit maakt het mogelijk om complexe structuren van objecten te representeren.
3. **Gebruik in certificaten:** OID's worden veel gebruikt in digitale certificaten en cryptografie. Bijvoorbeeld, een OID kan worden gebruikt om het type algoritme te identificeren in een digitale handtekening of om de extensies van een certificaat te definiëren.

4. **Gebruik in LDAP en andere protocollen:** In LDAP (Lightweight Directory Access Protocol) en andere netwerksystemen worden OID's gebruikt om attributen of objectklassen te identificeren.

OID's die worden gebruikt in SAML-assertions moet in het volgende formaat worden opgenomen, ongeacht of het een HL7v3- of FHIR-client is:

- `"urn:IIroot:"<OID voor het betreffende ID-stelsel>":IIext:"<gehanteerde ID binnen dit stelsel> , bijvoorbeeld`
`"urn:IIroot:"2.16.528.1.1007.3.3":IIext:"<URA>`

Belangrijk hierbij is dat de <URA> hier een unieke identificatiecode is voor zorgverleners en gekoppeld is aan het **UZI-register**.



Obsoleete OID formaat

Het volgende OID formaat is **Obsoleete**.

`"urn:oid:"<OID voor het betreffende ID-stelsel>". "<gehanteerde ID binnen dit stelsel>`

`bijvoorbeeld`

`"urn:2.16.528.1.1007.3.3."<URA>`

10.3.2.5.2.2 Structuur

Het SAML transactietoken is een afgegeven SAML-assertion die gebruikt wordt bij berichtauthenticatie met behulp van een gekwalificeerd persoonscertificaat of servercertificaat. Er wordt gebruik gemaakt van SAML v2.0 [SAML Core].

Het UZI-register en ZORG-ID hebben als doel zorgaanbieders bij elektronische communicatie en toegang tot gegevens uniek te identificeren. Zowel het UZI-register als ZORG-ID koppelt hiertoe op unieke wijze de fysieke identiteit aan een elektronische identiteit en legt deze vast in authenticiteit certificaten. Deze certificaten en de hierbij behorende cryptografische sleutels worden vastgelegd op de **smartcard**.

Bij het UZI-register heet dit de '**UZI-pas**' en bij ZORG-ID heet dit de '**ZORG-ID Smartcard**'.

SAML-assertion

De SAML-assertion heeft de volgende structuur (de waarden die in het token gebruikt worden zijn fictief):

Element/@Attribute	Cardinaliteit	Omschrijving	Vaste waarde
@ID	1..1	Unieke identificatie van de SAML-assertion. Een ID in XML mag NIET met een cijfer beginnen. Bij het gebruik van een UUID is het aan te raden een prefix te gebruiken, welke met een letter of underscore ('_') begint.	
@Version	1..1	Versie van het SAML Protocol.	"2.0"
@IssueInstant	1..1	Tijdstip van uitgifte van de SAML-assertion. De tijds waarde is gecodeerd in UTC (Universal Time Coordinated). UTC wordt gebruikt als referentie voor tijd over de hele wereld, en het vormt de basis voor de tijdzones. De UTC wordt weergegeven in het ISO 8601 formaat.	
Issuer	1..1	Bevat het OrganisatielD van de zendende applicatie. Hiervoor wordt de URA (UZI-Register Abonneenummer) gebruikt voor identificatie en authenticatie van zorgaanbieders in elektronische communicatie binnen de zorg. De OrganisatielD wordt uitgedrukt met behulp van een URN (Uniform Resource Name) omdat deze een organisatie formeel identificeert, zonder deze fysiek te lokaliseren. De URN string is opgebouwd uit een Iroot en een Iext. "II" staat voor het HL7v3 datatype Instance Identifier. Om de namespace in URN uniek te krijgen is II als prefix voor de root en ext geplaatst. "urn:IIroot:"2.16.528.1.1007.3.3":IExt:"<URA>"	
Issuer.@NameQualifier	0	Niet gebruiken	
Issuer.@SPNameQualifier	0	Niet gebruiken	

Element/@Attribute	Card inalit eit	Omschrijving	Vaste waarde
Issuer.@Format	1..1	Geeft aan dat de inhoud van het element de identifier is van een entiteit die SAML-gebaseerde diensten levert (zoals een SAML-autoriteit, een requester of responder) of deelneemt aan SAML-profielen (zoals een serviceprovider die het browser-SSO-profiel ondersteunt). Een dergelijke identifier kan worden gebruikt in het <Issuer>-element om de afzender van een SAML-verzoek, -antwoord of -assertion te identificeren, of in het <NameID>-element om uitspraken te doen over systeemiteiten die SAML-verzoeken, -antwoorden en -assertions kunnen afgeven. Het kan ook worden gebruikt in andere elementen en attributen die bedoeld zijn om een systeemiteit te identificeren in verschillende protocoluitwisselingen.	<code>"urn:oasis:names:tc:SAML:2.0:nameid-format:entity"</code>
Issuer.@SPPProviderID	0	Niet gebruiken	
Signature	1..1	Een XML-handtekening die de responder authenticceert en de integriteit van het bericht garandeert. AORTA/LSP en AoF: Bevat de handtekening over de SAML-assertion zoals gezet met behulp van de smartcard van de zorgverlener (Z) of de smartcard van de medewerker op naam(N). Alleen in het geval van een conditionele query mag de handtekening ook gezet worden met het servercertificaat (S) van de applicatie. MITZ: Bevat de handtekening over de SAML-assertion zoals gezet met behulp van het PKlo-servercertificaat van de Issuer. De handtekening dient geplaatst te zijn met behulp van een ander servercertificaat dan waarmee de TLS-sessie wordt opgezet.	

Element/@Attribute	Cardinaliteit	Omschrijving	Vaste waarde
Subject	1..1	AORTA/LSP en AoF: De zorgverlener/medewerker die zich authenticiseert. MITZ: Bevat de OrganisatieID van de zendende applicatie (zie Issuer)	
Subject.BaseID	0	Niet gebruiken	
Subject.NameID	0..1	AORTA/LSP en AoF: Bevat zowel het UZI-nummer van de geauthentiseerde zorgverlener/medewerker alsmede diens rolcode. Alleen in het geval van de conditionele query, waarmee de handtekening met een servercertificaat wordt geplaatst, MOET dit veld leeggelaten worden. MITZ: De handtekening wordt gezet met een server certificaat en MOET leeggelaten worden. WIJZIGINGSVOORSTEL: Is bij het gebruik van een server certificaat, zoals bij MITZ, de URA te plaatsen, zodat de <i>zorgaanbieder</i> geïdentificeerd kan worden.	
Subject.EncryptedID	0	Niet gebruiken	
Subject.SubjectConfirmation	1..1	Moet aanwezig zijn	
Subject.SubjectConfirmation@Method	1..1	Het Subject-element is verplicht en bij een naam identifier (NameID) gebruiken we een subjectbevestiging gebaseerd op bewijs van bezit van een sleutel. Ook als er geen naam identifier gebruikt wordt.	"urn:oasis:names:tc:SAML:2.0:cm:holder-of-key"
Subject.SubjectConfirmation.SubjectConfirmationData	0	Niet gebruiken	
Subject.SubjectConfirmation.SubjectConfirmationData@Recipient	0	Niet gebruiken	

Element/@Attribute	Card inalit eit	Omschrijving	Vaste waarde
Subject.SubjectConfirmation.SubjectConfirmationData@NotOnOrAfter	0	Niet gebruiken	
Subject.SubjectConfirmation.SubjectConfirmationData@InResponseTo	0	Niet gebruiken	
Subject.SubjectConfirmation.SubjectConfirmationData@NotBefore	0	Niet gebruiken	
Subject.SubjectConfirmation.SubjectConfirmationData@Address	0	Niet gebruiken	
Subject.SubjectConfirmation.SubjectConfirmationData.ds:KeyInfo.X509Data	1..1	Het element KeyInfo is onderdeel van het XML Signature schema. SAML vereist niet het gebruik van het KeyInfo element en legt geen beperkingen op aan het gebruik ervan. Het element KeyInfo bevat informatie over het certificaat en de daarbij behorende sleutel die is gebruikt voor het zetten van de digitale handtekening over de SAML-assertion. Het element KeyInfo.X509Data bevat certificaatinformatie in X.509-indeling. AORTA/LSP, AoF en MITZ: In dit geval bevat het de X.509 Issuer.Serial Number van de smartcard van de medewerker of het servercertificaat. In alle X.509 versies moet het serienummer uniek zijn voor elk certificaat dat door een specifieke CA wordt uitgegeven (zoals vermeld in RFC 5280).	
Conditions	1..1	Moet aanwezig zijn. Dit zijn de voorwaarden die MOETEN worden geëvalueerd bij het beoordelen van de geldigheid van en/of het gebruik van de SAML-assertion.	

Element/@Attribute	Cardinaliteit	Omschrijving	Vaste waarde
Conditions @NotBefore	1..1	Moet aanwezig zijn. Geeft het vroegste tijdstip aan waarop de SAML-assertion geldig is. De tijdwaarde wordt gecodeerd in UTC.	
Conditions @NotOnOrAfter	1..1	Moet aanwezig zijn. Specificeert het moment waarop de SAML-assertion is verlopen. De tijdwaarde wordt gecodeerd in UTC. AORTA/LSP en AoF: - Mag maximaal 90 minuten na @NotBefore liggen. MITZ: - Mag maximaal 10 minuten na @NotBefore liggen. WIJZIGINGSVOORSTEL: voor beide koppelvlakken: 90 minuten gebruiken.	
Conditions .Condition	0	Niet gebruiken	
Conditions .AudienceRestriction	1..1	Moet aanwezig zijn. Geeft aan dat de SAML-assertion gericht is aan een specifiek publiek.	
Conditions .AudienceRestriction.Audience	1..1	Bij AORTA/LSP en AoF: urn:IIroot:2.16.840.1.113883.2.4.6.6:IIext:1 (1 is de applicatie-id van de ZIM) Bij MITZ "urn:oid:2.16.840.1.113883.2.4.3.111.2.1" (is MITZ) WIJZIGINGSVOORSTEL: De verschillende Audience samenvoegen en er <saml:Audience>urn:generic:audience</saml:Audience> van maken.	<pre><saml:Audience> urn:IIroot:2.16.840.1.113883.2.4.6.6:IIext:1 </saml:Audience> <saml:Audience> urn:oid:2.16.840.1.113883.2.4.3.111.2.1 </saml:Audience></pre>

Element/@Attribute	Card inalit eit	Omschrijving	Vaste waarde
Conditions.ProxyRestriction	0	Niet gebruiken	
Conditions.Advice	0	Niet gebruiken	
AuthnStatement	1..1	Moet aanwezig zijn. Beschrijft een verklaring van de SAML-autoriteit waarin wordt bevestigd dat het subject van de verklaring op een specifieke manier op een bepaald moment is geauthentiseerd. Verklaringen die <AuthnStatement> -elementen bevatten, MOETEN een <Subject> -element bevatten.	
AuthnStatement@AuthnInstant	1..1	Geeft het tijdstip aan waarop de authenticatie (van de gebruiker of applicatie) heeft plaatsgevonden. De tijdwaarde wordt gecodeerd in UTC.	
AuthnStatement@SessionIndex	0	Niet gebruiken	
AuthnStatement.AuthnContext	1..1	Moet aanwezig zijn. De context die door de authenticerende autoriteit is gebruikt tot en met het authenticatie-evenement dat tot deze verklaring heeft geleid. Bevat een verwijzing naar een authenticatiecontextklasse, een verklaring van de authenticatiecontext of een verwijzing naar een verklaring, of beide. Raadpleeg de specificatie van de Authentication Context [SAMLAuthnCxt] voor een volledige beschrijving van informatie over de authenticatiecontext.	

Element/@Attribute	Cardinaliteit	Omschrijving	Vaste waarde
AuthnStatement .AuthnContext.AuthnContextClassRef	1..1	In het AuthnRequest wordt in het element AuthnContextClassRef het minimaal vereiste <i>betrouwbaarheidsniveau</i> meegegeven. Om de betrouwbaarheidsniveaus in de berichten mee te geven bevat het element AuthnContext een van de volgende declarations. • Laag: "urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport " • Midden: "urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract " • Substantieel: "urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard " of "urn:oasis:names:tc:SAML:2.0:ac:classes:X509 " • Hoog: "urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI " De aanbieder moet controleren of het betrouwbaarheidsniveau in de ontvangen SAML-assertion voldoet aan het minimaal gevraagde betrouwbaarheidsniveau.	Ingeval van ondertekening met smartcard: "urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI " Ingeval van ondertekening met UZI-server certificaat: "urn:oasis:names:tc:SAML:2.0:ac:classes:X509 "
AttributeStatement	1..1	Moet aanwezig zijn. Beschrijft een verklaring van de SAML-autoriteit waarin wordt bevestigd dat het subject van de verklaring is gekoppeld aan de gespecificeerde attributen. Verklaringen die <code><AttributeStatement></code> -elementen bevatten, MOETEN een <code><Subject></code> -element bevatten.	

Element/@Attribute	Cardinaliteit	Omschrijving	Vaste waarde
AttributeStatement.Attribute	0..1	Moet aanwezig zijn indien bericht aan één patiënt is gerelateerd.	
AttributeStatement.Attribute@Name	1..1	Vaste waarde "patientIdentifier" of de oude waarde "burgerServiceNummer" wat door MITZ ondersteund wordt.	"patientIdentifier" of "burgerServiceNummer"
AttributeStatement.Attribute.Attribute Value	0..1	ID van de patiënt (BSN, hash van BSN of COA nummer). Verplicht bij patiëntgebonden interacties. Anders afwezig. Formaat van een patientIdentifier: "urn:IIroot:"2.16.840.1.113883.2.4.6.3":IIext:"<BSN>" Formaat van een hash van een patientIdentifier: "urn:IIroot:"2.16.840.1.113883.2.4.3.111.4":IIext:"<BSN>" Formaat van een COA nummer: "urn:IIroot:"2.16.840.1.113883.2.4.3.111.6":IIext:"<BSN>" Let op! Indien "burgerServiceNummer" wordt gebruikt als attribuut, dan zal de root OID niet zijn opgenomen in de attribuutwaarde, maar slechts het BSN.	
AttributeStatement.Attribute	0..1	Moet aanwezig zijn bij AORTA/LSP en AoF	
AttributeStatement.Attribute@Name	1..1	Vaste waarde: "messageldRoot"	"messageldRoot"
AttributeStatement.Attribute.Attribute Value	1..1	De waarde van de messageldRoot bijvoorbeeld: "2.16.840.1.113883.2.4.3.111.15.4" (AORTA RequestID)	
AttributeStatement.Attribute	0..1	Moet aanwezig zijn bij AORTA/LSP en AoF	

Element/@Attribute	Cardinaliteit	Omschrijving	Vaste waarde
AttributeStatement.Attribute@Name	1..1	Vaste waarde: "messageIdExt"	"messageIdExt"
AttributeStatement.Attribute.Attribute Value	1..1	Het MessageId van het bericht. Dit is de waarde van het requestId dat zal worden meegestuurd in de AORTA-ID HTTP header.	
AttributeStatement.Attribute	0..1	Moet aanwezig zijn bij AORTA/LSP en AoF	
AttributeStatement.Attribute@Name	1	Vaste waarde: "InteractionId"	"InteractionId"
AttributeStatement.Attribute.Attribute Value	1	Het InteractionId van het Bericht (het extension-element).	
AttributeStatement.Attribute	0..1	Moet aanwezig zijn bij de Generieke Query van AORTA/LSP en AoF	
AttributeStatement.Attribute@Name	1	Vaste waarde: "contextCodeSystem"	"contextCodeSystem"
AttributeStatement.Attribute.Attribute Value	0..1	"2.16.840.1.113883.2.4.3.111.15.1" (AORTA Contextcodes)	"2.16.840.1.113883.2.4.3.111.15.1"
AttributeStatement.Attribute	0..1	Moet aanwezig zijn bij de Generieke Query van AORTA/LSP en AoF	
AttributeStatement.Attribute@Name	1..1	Vaste waarde: "contextCode". De contextcode die aanduidt binnen welke (zorg)toepassing de (FHIR)-interactie word geïnitieerd.	"contextCode"
AttributeStatement.Attribute.Attribute Value	0..1	De contextcode uit de Generieke query. bijv. "BGZ", of "MEDGEGTOT".	
AttributeStatement.Attribute	0..1	De scope waarop het transactietoken betrekking heeft. Wordt bij AoF gebruikt.	
AttributeStatement.Attribute@Name	1..1	"scope"	"scope"

Element/@Attribute	Cardinaliteit	Omschrijving	Vaste waarde
AttributeStatement.Attribute.Attribute Value	1..1	Bijvoorbeeld: • patient/Patient.s (verzamelen BGZ) • patient/Observation.s (verzamelen meetwaarden) • ...	
AttributeStatement.Attribute	0..1	Moet aanwezig zijn indien gebruik gemaakt is van een mandaat	
AttributeStatement.Attribute@Name	1	Vaste waarde: "autorisatieregel/context"	"autorisatieregel/context"
AttributeStatement.Attribute.Attribute Value	0..1	URI waar de autorisatieregel/context gevonden kan worden waarbinnen het mandaat gegeven wordt. Moet aanwezig zijn indien gebruik gemaakt is van een mandaat. Lokaal is vastgelegd dat een bepaald mandaat daadwerkelijk door een mandaatverlener is toegekend aan een bepaald persoon/systeem.	
AttributeStatement.Attribute	0..1	Moet aanwezig zijn indien gebruikt wordt binnen AORTA infrastructuur (AORTA/LSP en AoF)	
AttributeStatement.Attribute@Name	1..1	Vaste waarde: "applicationID"	"applicationID"
AttributeStatement.Attribute.Attribute Value	0..1	AORTA ApplicatieID van de (GBx) applicatie Formaat van een applicatie-id: "urn:IIroot:"2.16.840.1.113883.2.4.6.6":IIext:"<applicatie-id>"	
AttributeStatement.Attribute	0..1	De versie van de tokendefinitie die wordt gehanteerd. Geïntroduceerd bij AoF. Verplicht bij gebruik van deze versie van het token (Feature versie >= 2.1).	

Element/@Attribute	Cardinaliteit	Omschrijving	Vaste waarde
AttributeStatement.Attribute@Name	1..1	Vaste waarde: "tokenVersion"	"tokenVersion"
AttributeStatement.Attribute.Attribute Value	1..1	Formaat: "<major versie>.<minor versie>", conform semver.	

N.B.: bovenstaande tabel bevat de meest gebruikte elementen van SAML assertions en is derhalve niet volledig. Voor niet genoemde elementen geldt: Niet gebruiken.

10.3.2.5.2.3 Namespaces

Het SAML transactietoken die gebruikt wordt bij berichtauthenticatie maakt gebruik van de volgende namespaces. De prefixen zijn niet normatief maar worden in dit document als voorbeelden gebruikt.

Tabel AORTA.STK.t3300 – Namespaces

Prefix	Namespace URI
ds	http://www.w3.org/2000/09/xmldsig#
saml	urn:oasis:names:tc:SAML:2.0:assertion
wss	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd

	Bij het gebruik van de namespace-prefixes is het van belang deze na het ondertekenen niet meer te veranderen, dit maakt de digitale handtekening ongeldig.

10.3.2.5.2.4 Inhoud

De volgende paragrafen beschrijven de verschillende kenmerken en beveiliging gerelateerde gegevens die het SAML transactietoken onderscheiden, zoals in [IH tokens generiek] beschreven is.

```
<saml:Assertion ... xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
```

Het SAML transactietoken begint met het Assertion element en een verwijzing naar de XML SAML namespace voor SAML 2.0 assertions. De attributen behorende bij het Assertion element wordt in [paragraaf 2.3.1](#)¹³¹ Uniekheid beschreven.

Uniekheid

```
ID="token_ dd1c1f96-f0b0-4026-a978-4d724c0a0a4f"

IssueInstant="2009-06-24T11:47:34Z"

Version="2.0">
```

De volgende attributen van het SAML assertion element maken van de SAML assertion een uniek gegeven, uitgegeven door de verzender van het bericht. Het attribuut ID identificeert op een unieke wijze de assertion. De assertion mag slechts eenmalig als token gebruikt worden. De waarde moet *mondiaal uniek* zijn voor AORTA berichten, zodat bij samenvoegen van meerdere XML bestanden (in een HL7v3 batch of anderszins) de waarde uniek blijft.

Het wordt aanbevolen een UUID (Universally Unique Identifier) te gebruiken. Bij het gebruik van andere vormen is er een kans, hoe klein ook, dat een ID samenvalt met een ID gemaakt volgens een andere methode van een andere leverancier).



Een ID in XML mag niet met een cijfer beginnen. Bij het gebruik van een UUID is het dus aan te raden een prefix te gebruiken, welke met een letter of underscore ('_') begint.

Het attribuut IssueInstant is een tijdsmoment van uitgifte van de SAML assertion. De tijdswaarde is gecodeerd in UTC. Het attribuut Version is de gebruikte SAML versie van de SAML assertion. De aanduiding voor de versie van SAML gedefinieerd in deze specificatie is "2.0".

Afzender

```
<saml:Issuer>
```

131. <https://vzvz.atlassian.net/wiki/spaces/AORTA84/pages/879593488/Het+SAML+transactietoken#HetSAMLtransactietoken-Uniekheid>

```

<!-- De Issuer verwijst naar de organisatie van waaruit het totale bericht verstuurd
wordt.-->

    urn:IIroot:2.16.528.1.1007.3.3:IIext:12345678

</saml:Issuer>

```

De URA wordt uitgedrukt met behulp van een URN (Uniform Resource Name). De URN is opgebouwd uit:

"urn:IIroot:"<OID voor UZI organisatielids>".IIext:"<URA>

De URN string is opgebouwd uit een IIroot en een IIext. "II" staat voor het HL7v3 datatype Instance Identifier. Om de namespace in URN uniek te krijgen is II als prefix voor de root en ext geplaatst.

URA's worden uitgedrukt als een id onder het identificatiesysteem "2.16.528.1.1007.3.3". De URA wordt toegekend door het UZI-register. Stel dat de URA de waarde "12345678" heeft, dan ziet de URN er als volgt uit:

urn:IIroot:2.16.528.1.1007.3.3:IIext:12345678

Onderwerp

```

<saml:Subject>
  <saml:NameID>
    123456789:01.015
  </saml:NameID>
  <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:holder-of-key">
    <saml:SubjectConfirmationData>
      <saml:KeyInfo>
        <ds:X509Data>
          <ds:X509IssuerSerial>

```



```

        <ds:X509IssuerName>CN=...,...,O=...,C=NL</ds:X509IssuerName>

        <ds:X509SerialNumber>...834756977854956...</ds:X509SerialNumber>

    </ds:X509IssuerSerial>

</ds:X509Data>

</saml:KeyInfo>

</saml:SubjectConfirmationData>

</saml:SubjectConfirmation>

</saml:Subject>

```

De Subject verwijst naar het UZI-nummer van de zorgverlener/medewerker die de assertion heeft gegenereerd in combinatie met de rolcode van diezelfde zorgverlener/medewerker gescheiden door een dubbele punt (:). Voor de zorgverlener en de medewerker op naam is het UZI-nummer uniek gekoppeld aan de natuurlijk persoon.

Alleen in het geval van een conditionele query (een query die automatisch door het systeem verstuurd wordt) mag het nameID-element leeg gelaten worden.

In het geval van een conditionele query dient tevens een Mandaattoken [Mandaattoken] en een Inschrijftoken [Inschrijftoken] in het bericht opgenomen te zijn.

Vervolgens moet de SubjectConfirmation / SubjectConfirmationData / KeyInfo nog toegevoegd worden. Deze KeyInfo dient te verwijzen naar het certificaat waarmee het token ondertekend is.

Voor een beschrijving van de opbouw van de KeyInfo wordt verwezen naar [hoofdstuk 4.4.3 \(see page 455\)](#) Certificaatverwijzingen in document [IH tokens generiek].

Geldigheid

```

saml:Conditions

    NotBefore="2009-06-24T11:47:34Z"

```

```
NotOnOrAfter="2009-06-24T11:52:34Z">
```

Het attribuut *NotBefore* is de tijd waarop de SAML assertion geldig wordt. Dit hoeft niet de tijd te zijn waarop het bericht is aangemaakt. Het is mogelijk *NotBefore* in de toekomst te zetten, en het bericht na deze tijd pas te verzenden.



Wordt een bericht ontvangen voor *NotBefore* is aangevallen, dan **moet** dit bericht geweigerd worden.

Het attribuut *NotOnOrAfter* is de tijd waarop de SAML assertion vervalt.



Wordt een bericht ontvangen op of nadat *NotOnOrAfter* is verstreken, dan **moet** dit bericht geweigerd worden.

Deze tijd is als bovenstaande tijd geformatteerd. Richtlijn voor het verschil tussen *NotBefore* en *NotOnOrAfter* is 5 minuten. Het maximaal toegestane verschil is 90 minuten. Dit maximum dient voor berichten die niet direct, maar bijvoorbeeld 's nachts verzonden worden, of kort voor de aanvang van een consult, zodat er iets ruimere mogelijkheden voor batchgewijze processen zijn. Het wordt sterk aanbevolen de SAML assertion direct (binnen 5 minuten) te gebruiken voor berichten die verzonden worden (dus terwijl de zorgverlener of medewerker achter diens computer zit). Het gaat immers om het voorkomen van misbruik van onderschepte tokens, en 5 minuten is meer dan voldoende om de hele keten van vraag tot antwoord te doorlopen.



De geldigheidsduur van een token (*NotOnOrAfter* minus *NotBefore*) mag niet langer dan 90 minuten zijn. Wordt een bericht ontvangen waarin deze geldigheidsduur overschreden is, dan **moet** dat bericht geweigerd worden, ook al is het tijdstip *NotOnOrAfter* nog niet verstreken.

Het inperken van bepaalde partijen (AudienceRestriction) waarvoor de assertion bedoeld is wordt beschreven in [paragraaf 2.3.5](#)¹³² Ontvanger.

132. <https://vzvz.atlassian.net/wiki/spaces/AORTA84/pages/879593488/Het+SAML+transactietoken#HetSAMLtransactietoken-Ontvanger>

De subelementen OneTimeUse en ProxyRestriction worden niet gebruikt binnen het <Conditions> element bij berichtauthenticatie met behulp van de smartcard, gebaseerd op PKI.

Ontvanger

```
<saml:AudienceRestriction>

  <!-- Root en extensie van de ZIM -->

  <saml:Audience>urn:IIroot:2.16.840.1.113883.2.4.6.6:IIext:1</saml:Audience>

</saml:AudienceRestriction>
```

In de AudienceRestriction wordt beschreven aan wie de SAML assertion is gericht. De waarden in de elementen zijn (voorlopig) vaste waarden. Voor de <Audience> parameter is (ook) gekozen voor URN, zie voor opbouw [paragraaf 2.3.2](#)¹³³ Afzender.

Authenticatie

```
<saml:AuthnStatement

  AuthnInstant="2009-06-24T11:47:34"

  SessionIndex="token_2.16.528.1.1007.3.3.1234567.1_0123456789">
```

Het subject, een zorgverlener of medewerker, in de SAML assertion is geauthenticeerd door middel van een authenticatiemiddel op een gegeven moment.

```
<saml:AuthnContext>

  <saml:AuthnContextClassRef>
```

133. <https://vzvz.atlassian.net/wiki/spaces/AORTA84/pages/879593488/Het+SAML+transactietoken#HetSAMLtransactietoken-Afzender>

```
urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI

</saml:AuthnContextClassRef>

</saml:AuthnContext>
```

Als het transactietoken ondertekend is met het servercertificaat dan dient de `AuthnContextClassRef` de waarde `urn:oasis:names:tc:SAML:2.0:ac:classes:X509` te krijgen .

Binnen de gebruikte applicatie beveiligingsstandaarden is er sprake van verschillende vertrouwensniveaus.

Binnen de SAML-specificatie geeft men een authenticatie-context (*AuthnContext*) mee die de context van het gebruikte authenticatiemiddel aangeeft. Hiervoor zijn een aantal contexten gespecificeerd, zie [SAMLAuthnContext], die gebruikt worden als referentiekader voor de communicatie tussen de ZIM en andere componenten zoals GBZ applicaties.

```
</saml:AuthnStatement>
```

Afsluiting authentication statement.

Attributen

```
<saml:AttributeStatement>
```

De volgende attributen zijn gegevens uit het HL7v3 bericht die met de authenticatie meegetekend worden. Dit zijn kopieën van gegevens die elders in hetzelfde HL7v3 bericht voorkomen. De volgorde van de attributen in het `AttributeStatement` is niet relevant. Er mogen geen andere attributen opgenomen worden in het `AttributeStatement` dan hier beschreven is.

InteractionId

```
<saml:Attribute Name="interactionId">
  <saml:AttributeValue>QURX_IN990011NL</saml:AttributeValue>
</saml:Attribute>
```

Het attribuut `interactionId` wordt altijd meegetekend. De `interactionId` geeft een directe relatie met het berichttype. Dit attribuut meesturen verhindert veel soorten aanvallen, bijvoorbeeld het token van een query kapen en proberen deze te hergebruiken voor het afhandelen van verzoeken van patiënten en hun vertegenwoordigers om inzage te verkrijgen in de verwijzindex.

contextCode

```
<saml:Attribute Name="contextCodeSystem">
  <saml:AttributeValue>2.16.840.1.113883.2.4.3.111.15.1</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="contextCode">
  <saml:AttributeValue>KZDI</saml:AttributeValue>
</saml:Attribute>
```

In het geval er sprake is van een opvraag op basis van een context dient ook de `contextCode` meegetekend te worden. Dit is in principe alleen het geval bij de generiekeQueryZorggegevens. Bij deze generieke query is het trigger event niet meer voldoende om de intentie van de verzender aan te geven, aangezien deze altijd gelijk is. Door het toevoegen van de `contextCode` wordt deze intentie wel weer expliciet gemaakt. De codes zijn te vinden in het vocab bestand 2.16.840.1.113883.2.4.3.111.15.1.xml.

messageld

```
<saml:Attribute Name="messageIdRoot">
```

```

    <saml:AttributeValue>2.16.528.1.1007.3.3.1234567.1</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute Name="messageIdExt">
    <saml:AttributeValue>0123456789</saml:AttributeValue>
  </saml:Attribute>

```

De Attributen messageIdRoot en messageIdExt vormen een uniek gegeven, uitgegeven door de verzender van het HL7v3-bericht. De combinatie van de attribuutwaarden messageIdRoot en messageIdExt moeten gelijk zijn aan het uiteindelijk gebruikte HL7v3 message.Id.

burgerServiceNummer

```

<saml:Attribute Name="burgerServiceNummer">
  <saml:AttributeValue>950052413</saml:AttributeValue>
</saml:Attribute>

```

Voor berichten die betrekking hebben op een enkele patiënt, wordt het burgerServiceNummer (BSN) van de patiënt opgenomen. Dit maakt ook weer vele aanvallen onmogelijk, namelijk gegevens van een andere patiënt proberen op te vragen. Dit geldt voor alle berichten die betrekking hebben op één en niet meer dan één patiënt.

Het BSN in het token moet overeenkomen met het BSN in het bericht. In het geval er sprake is van een voorlooptoken in het bericht, dan dient deze ook overgenomen te worden in het token.

Voor berichten die geen betrekking hebben op een persoon waarvan het burgerServiceNummer bekend is, wordt het burgerServiceNummer weggelaten. Hierbij zijn twee situaties te onderscheiden:

- Logistieke berichten; het bericht betreft géén informatie gerelateerd tot een specifieke patiënt;
- Medische berichten; het bericht betreft medische informatie gerelateerd tot een specifieke patiënt(en), maar waarvan het BSN niet bekend is. In de implementatiehandleiding van een

zorgtoepassing zal bij de betreffende interactie expliciet benoemd staan, dat een patiëntidentificatie niet voorkomt of optioneel is.

autorisatieregel/context

Alleen indien gebruik gemaakt wordt van een mandaat dient het volgende attribuut toegevoegd te worden:

```
<saml:Attribute Name="autorisatieregel/context">

  <saml:AttributeValue>https://goedbeheerddziekenhuis/autorisatieregels/
  medicatiecontext/v2 </saml:AttributeValue>

</saml:Attribute>
```

In het voorbeeld is voor een URL gekozen.

applicationID

Indien het transactietoken gebruikt wordt binnen de AORTA infrastructuur is het applicatieID verplicht:

```
<saml:Attribute Name="applicationID">

<!-- Applicatie-id van de GBZ-applicatie, zoals toegekend bij aansluiting.-->

<saml:AttributeValue>urn:IIroot:2.16.840.1.113883.2.4.6.6:IIext:? </
saml:attributeValue>

</saml:Attribute>
```

Het applicatie-id van de afzender die deze SAML assertion heeft gecreëerd en de gebruiker authenticceert. De Issuer wordt uitgedrukt met behulp van een URN (Uniform Resource Name). De URN is opgebouwd uit:

"urn:llroot:"<OID voor AORTA Applicatie-id's>":llex:"<applicatie-id GBZ>

De URN string is opgebouwd uit een llroot en een llex. "ll" staat voor het HL7v3 datatype Instance Identifier. Om de namespace in URN uniek te krijgen is ll als prefix voor de root en ext geplaatst.

AORTA Applicatie-id's worden uitgedrukt als een id onder het identificatiesysteem "2.16.840.1.113883.2.4.6.6". Het correcte applicatie-id voor de GBZ-applicatie wordt toegekend bij aansluiting op de AORTA. Stel dat dit "300" zou zijn, dan ziet de URN er als volgt uit:

urn:llroot:2.16.840.1.113883.2.4.6.6:llex:300

attributeStatement blok

Het attributen statement blok ziet er dan bijvoorbeeld zo uit (de volgorde van de attributen is niet relevant):

```
<saml:AttributeStatement>

  <saml:Attribute Name="interactionId">

    <saml:AttributeValue>QURX_IN990011NL</saml:AttributeValue>

  </saml:Attribute>

  <saml:Attribute Name="messageIdRoot">

    <saml:AttributeValue>2.16.528.1.1007.3.3.1234567.1</saml:AttributeValue>

  </saml:Attribute>

  <saml:Attribute Name="messageIdExt">

    <saml:AttributeValue>0123456789</saml:AttributeValue>

  </saml:Attribute>

  <saml:Attribute Name="burgerServiceNumber">

    <saml:AttributeValue>950052413</saml:AttributeValue>

  </saml:Attribute>

  <saml:Attribute Name="autorisatieregel/context">
```



```

    <saml:AttributeValue>https://goedbeheerdziekenhuis/autorisatieregels/
    medicatiecontext/v2</saml:AttributeValue>

  </saml:Attribute>

  <saml:Attribute Name="applicationID">

    <saml:AttributeValue>urn:IIroot:2.16.840.1.113883.2.4.6.6:IIext:300

    </saml:AttributeValue>

  </saml:Attribute>

</saml:AttributeStatement>

```

Tenslotte wordt het attributen statement blok afgesloten met

```
</saml:AttributeStatement>
```

10.3.2.5.2.5 Algoritmes

Om de integriteit en onweerlegbaarheid van het SAML transactietoken te waarborgen wordt een XML Signature geplaatst, zoals beschreven in [IH tokens generiek]. Na plaatsen van de XML Signature kan de ontvanger, met gebruikmaking van het persoons- of organisatiegebonden authenticiteit certificaat van de verzender en de CA certificaten gebaseerd op PKI, onomstotelijk vaststellen dat het SAML transactietoken ondertekend is met de privé sleutel behorend bij het gebruikte authenticiteit certificaat van de zorgmedewerker of de organisatie.

De XML Signature van het SAML transactietoken die gebruikt wordt bij berichtauthenticatie met behulp van een authenticiteit certificaat, gebaseerd op PKI, maakt gebruik van de volgende algoritmes, zoals beschreven in [IH tokens generiek]:

- Voor het berekenen van de hashwaarde wordt SHA-256 gebruikt.
- Voor de digitale handtekening in AORTA wordt gebruik gemaakt van een RSA handtekening over een SHA-256 digest.



Omdat de XML Signature onderdeel is van het SAML transactietoken en in het SAML transactietoken geplaatst wordt, moet er een "enveloped-signature" transformatie uitgevoerd worden die de Signature tags uit het SAML transactietoken verwijderd gevolgd door een "exc-c14n transformatie" (zie ook [SAML Core] §5.4.3 en §5.4.4).

10.3.2.5.2.6 Opbouw

De headers

Eerst wordt het SAML transactietoken – het <saml:Assertion ...> element aangemaakt en gevuld met die elementen, zoals beschreven in [paragraaf 2.3](#)¹³⁴Inhoud.

```
<saml:Assertion
  ID="token_2.16.528.1.1007.3.3.1234567.1_0123456789"
  IssueInstant="2009-06-24T11:47:34Z"
  Version="2.0"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
  ... Zie paragraaf 2.3 Inhoud ...
</saml:Assertion>
```

Het XML Signature blok is onderdeel van het SAML transactietoken. Het XML Signature blok komt na het <saml:Issuer> element. Na de Signature volgt de rest van de inhoud van de assertion.

```
<saml:Assertion
  ID="token_2.16.528.1.1007.3.3.1234567.1_0123456789"
  IssueInstant="2009-06-24T11:47:34Z"
```

134. <https://vzvz.atlassian.net/wiki/spaces/AORTA84/pages/879593488/Het+SAML+transactietoken#HetSAMLtransactietoken-Inhoud>

```

Version="2.0"

xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">

<saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">

    urn:IIroot:?:IIext:?

</saml:Issuer>

<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

    <ds:SignedInfo>

        ...

    </ds:SignedInfo>

    <ds:SignatureValue>Wuwn...5e4=</ds:SignatureValue>

    <ds:KeyInfo>

        <ds:X509Data>

            <X509IssuerSerial>

                <X509IssuerName>CN=De Auteur CA,0=Nictiz,C=NL</X509IssuerName>

                <X509SerialNumber>359724...41160195</X509SerialNumber>

            </X509IssuerSerial>

        </ds:X509Data>

    </ds:KeyInfo>

</ds:Signature> ...

... Zie paragraaf 2.3 Inhoud ...

</saml:Assertion>

```

Indien de Signature aangemaakt wordt moet niet meer met de strings (saml:Assertion en SignedInfo) gemanipuleerd worden, maar ze moeten octet-voor-octet overgenomen worden in het bericht. Strikt genomen is het toegestaan wijzigingen aan te brengen die door canonicalisatie bij de ontvanger weer opgeheven worden, maar wanneer de digitale handtekening door middel van strings wordt opgebouwd, is het een foutgevoelige handeling.

Lange Base 64 waarden zijn in het voorbeeld afgekort. Wederom kan dit als strings worden behandeld, waarbij drie waarden vervangen moeten worden.

Deze drie waarden worden ingevuld:

- Neem het SignedInfo blok op.
- Neem de SignatureValue op.
- Neem certificaatgegevens in het KeyInfo blok op, in de vorm van een verwijzing (X509IssuerSerial).



Wanneer een bericht een SAML assertion bevat, moet dat bericht precies één bijbehorende digitale handtekening bevatten.

Het maken van de XML Signature uit strings levert de SAML assertion op met daarin de Signature.

Plaats van het SAML token en de digitale handtekening

Het SAML transactietoken met daarin de digitale handtekening wordt in het WS-Security SOAP Header gezet. Op het <wss:Security> element **moet** een soap:mustUnderstand="1" vlag opgenomen worden, die aangeeft dat de ontvanger dit security element **moet** verwerken en een soap:actor="<http://www.aortarelease.nl/actor/zim>" die aangeeft dat de ZIM dit security element verwerkt.

```
<soap:Header xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  ...
  <wss:Security xmlns:wss=
    "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
    soap:actor="http://www.aortarelease.nl/actor/zim" soap:mustUnderstand="1">
    <saml:Assertion ... >
      <saml:Issuer>...</saml:Issuer>
      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
          ...
        </ds:SignedInfo>
        <ds:SignatureValue>Wuwn...5e4=</ds:SignatureValue>
```

```

    <ds:KeyInfo>
      <ds:X509Data>
        ...
      </ds:X509Data>
    </ds:KeyInfo>
  </ds:Signature>
... Zie paragraaf 2.3 Inhoud ...
  </saml:Assertion ... >
</wss:Security>
</soap:Header>

```

10.3.2.5.3 Certificaten transactietoken

10.3.2.5.3.1 Te gebruiken certificaat en attributen

De smartcard certificaat, gebaseerd op PKI, kent een aantal modellen:

Tabel AORTA.STK.t3210 – UZI pastype

Naam UZI-pastype/certificaat	Codering Pastype/certificaat
Zorgverlenerpas	Z
Medewerkerpas op naam	N
Medewerkerpas niet op naam	M
Servercertificaat	S

De smartcard of het certificaat die gebruikt wordt voor het ondertekenen van een transactietoken moet een zorgverlener pas, een medewerker pas op naam zijn of een servercertificaat. Hoewel het pastype gecodeerd is opgenomen in het authenticiteit certificaat (in het subjectAltName attribuut), dient een applicatie op basis van de uitgevende CA vast te stellen wat het pastype van de UZI-pas is.

Indien gebruik gemaakt wordt van een servercertificaat, dan geldt het volgende: een GBZ dient voor transportbeveiliging bij voorkeur een ander servercertificaat te gebruiken dan voor berichtauthenticatie. Dit is met name van toepassing wanneer ondertekening niet via een zelfde key-store verloopt dan dat van de TLS-verbinding. De verschillende certificaten horen daarbij in verschillende componenten ondergebracht te zijn in de architectuur van het XIS.

De signature wordt gezet met de sleutel voor authenticiteit (keyUsage=digitalSignature, hexadecimaal 0x80).

De attributen in het authenticiteit certificaat worden gegeven in de vorm van een Distinguished Name (DN), zie [IH tokens generiek].

De waarden van deze attributen voor de relevante UZI-certificaten zijn:

Tabel AORTA.STK.t3220 – DN attributen van UZI-certificaten

Attribuut	Omschrijving	Waarde
CN	Issuer.commonName	<i>Derde generatie:</i> UZI-register Zorgverlener CA G3 Voor mogelijke volgende generaties wordt verwezen naar het UZI-register: https://www.uziregister.nl/
O	Issuer.organisationName	agentschap Centraal Informatiepunt Beroepen Gezondheidszorg
C	Issuer.countryName	NL

Tabel AORTA.STK – DN attributen van ZORG-ID certificaten, gebaseerd op PKI

Attribuut	Omschrijving	Waarde
CN	Issuer.commonName	ZORG-ID Token CA
O	Issuer.organisationName	ZORG-ID
C	Issuer.countryName	NL

Extensions	OID	2.16.840.1.113883.2.4.3.111.20.5
proofValue	Cryptografisch bewijs om herkomst van een credential te verifiëren	z58.....ktZ

	De issuer.commonName verschilt per 'generatie' UZI-passen. Het is mogelijk dat verschillende 'generatie' UZI-passen door elkaar worden gebruikt. Daarom dient de Issuer DN dynamisch afgeleid te worden uit het gebruikte authenticatiecertificaat.

Om de digitale handtekening bij het LSP te verifiëren, moet de ontvanger over de bijbehorende publieke sleutel beschikken, zie [IH tokens generiek].

Voor verificatie is gekozen een verwijzing naar het authenticiteit certificaat mee te zenden; de ontvanger moet deze dan met bijvoorbeeld het LDAP protocol ophalen in de directory van het UZI-register of ZORG-ID.

Zie voor de verdere beschrijving van de passen [UZI pas].

Noot: uiteraard mogen in het testtraject alleen UZI-testpassen en UZI-testcertificaten gebruikt worden. Het gebruik hiervan wordt verder niet uitgewerkt in deze handleiding. De werking is identiek.

10.3.2.5.4 Token afhandeling transactietoken

10.3.2.5.4.1 Verificatie van het bericht

Het is belangrijk vast te stellen dat de velden in het SAML transactietoken overeenstemmen met die van het bericht voor de gegevensuitwisseling en geldig ondertekend zijn. Wanneer dit niet zou gebeuren, kan een kwaadwillende met een gestolen token nog steeds gegevens opvragen van bv. ieder willekeurig Burgerservicenummer.

De ontvanger controleert of de WS-Security SOAP Header voor hem bestemd is, zie soap attribuut actor.

Het SAML transactietoken wordt door de ontvanger uit de WS-Security SOAP Header gehaald indien de WS-Security SOAP Header voor de ontvanger bestemd is en dat de ontvanger deze moet verwerken. Bij gebruik van het SAML transactietoken moet de ontvanger controleren of:

- Het attribuut ID van het Assertion element een unieke waarde heeft, welke slechts eenmalig gebruikt mag worden, zie [Uniekheid \(see page 415\)](#);
- De aanduiding voor de versie van SAML gedefinieerd is op "2.0", zie [Uniekheid \(see page 415\)](#) ;
- De juiste organisatielD is opgenomen die deze assertion heeft gecreëerd en de gebruiker heeft geauthenticeerd, zie [Afzender \(see page 415\)](#). Het zorgaanbiederID in het token dient overeen te komen met de zorgaanbiederID in het bericht;
- Indien Conditionele Query (token is ondertekend met een certificaat met certificaattype "S"): de NameID van het Subject is wel aanwezig maar leeg, zie [Onderwerp \(see page 416\)](#); Tevens dient er een mandaattoken en inschrijftoken aanwezig te zijn;
- In overige gevallen: Het UZI-nummer en rolcode van het authenticatie certificaat, gebruikt voor de ondertekening van de Assertion, overeenkomt met de NameID van het Subject en met de authorOrPerformer in het bericht zie [Onderwerp \(see page 416\)](#);
- De Assertion correct is ondertekend door de Signature te valideren met het gerefereerde authenticatie certificaat.
- Het gebruikte certificaat en de relevante certificaatketen te valideren op geldigheid, inclusief revocatie.
- Het bericht ontvangen is binnen de geldigheidsperiode van het token, zie [Geldigheid \(see page 417\)](#) ;
- De afnemer van het SAML transactietoken (audience) de ZIM is, zie [Ontvanger \(see page 419\)](#);
- Indien gebruik gemaakt is van een mandaat, dan dient er een getekend mandaattoken te zijn opgenomen in de SOAP-header (zie [Mandaattoken]). Het attribuut "autorisatieregel/context" dient identiek te zijn aan het overeenkomstige attribuut in het mandaattoken. Daarnaast dient de organisatielD in beide tokens overeen te komen.
- Indien geen Conditionele Query: De zorgverlener/zorgmedewerker is geauthenticeerd via het voorgedefinieerde authenticatiemiddel, de SmartCardPKI, zoals beschreven in [Authenticatie](#) ;
- Indien Conditionele Query: Het systeem is geauthenticeerd via het voorgedefinieerde authenticatiemiddel, Het X509 servercertificaat, zoals beschreven in [Authenticatie \(see page 419\)](#) ;
- Alleen die attributen zijn gedefinieerd, die zijn beschreven in [Attributen \(see page 420\)](#) ;
- De attribuutwaarde van interactionId overeenkomt met *het extension-element* van het HLv3 bericht, zie [Attributen \(see page 420\)](#) ;
- In het geval van een generieke query dient er een contextcode te zijn opgenomen. De contextcode dient overeen te komen met de contextcode in het bericht, zie [Attributen \(see page 420\)](#) ;.
- De attribuutwaarden van messageIdRoot en messageIdExt overeenkomt met de gebruikte HL7v3 [message.id](#)¹³⁵, zie [Attributen \(see page 420\)](#) ;
- Indien de interactie patient-specifiek is: de attribuutwaarde van burgerServiceNummer overeenkomt met het BSN in het HL7v3 bericht ofwel dat de gegevens in het bericht daadwerkelijk betrekking hebben op de persoon, zie [Attributen \(see page 420\)](#) . De volgende situaties zijn hierbij te onderscheiden:

135. <http://message.id>

- Wel BSN in token en in bericht; er is sprake van een goedsituatie indien BSN overeenkomt. Indien dat niet het geval is, is er sprake van een foutsituatie;
- Wel BSN in token en niet in het bericht; er is sprake van een foutsituatie;
- Geen BSN in token en wel in bericht; er is sprake van een foutsituatie;
- Geen BSN in token en geen BSN in het bericht; er is sprake van een goedsituatie.
- Indien het token gebruikt wordt binnen de AORTA infrastructuur moet de juiste applicatieID zijn vastgelegd die deze assertion heeft gecreëerd en de gebruiker heeft geauthenticeerd. Het applicatieID dient overeen te komen met de Message/sender/device/id in de transmission wrapper van het HL7v3 bericht;
- Indien het inschrijftoken ondertekend is met het authenticiteit certificaat van ZORG-ID Token CA (CA) dienen de volgende extra controles plaats te vinden:
 - Van het gebruikte certificaat moet het extensie bewijs (proofValue) gecontroleerd worden dat dit met een geldige UZI-medewerkerspas op naam is gebeurd ten tijde van de ondertekening.
 - De proofValue extensie heeft de volgende OID: 2.16.840.1.113883.2.4.3.111.20.5 (Custom Extension copied Certificate)
 - De proofValue is een JSON Web Token dat uit drie delen bestaat:
`header.payload.signature`
 - Om het bewijs te controleren, moet uit het header element `x5c`, het X.509 certificaat geëxtraheerd worden, met Base64, waar vervolgens de publieke sleutel gehaald wordt.
 - Gebruik de publieke sleutel om de JWT-handtekening te valideren met de algoritme die uit het header element `alg` is vastgelegd.
 - Controleer of het geëxtraheerde certificaat ondertekend is door de vertrouwde CA (Certificate Authority)
 - Decodeer de payload met Base64.
 - Controleer de claims uit de payload, met die van het authenticiteit certificaat van ZORG-ID Token CA:
 - "ura"
 - "uziNumber"
 - "roleCode"

Als aan één van de bovenstaande condities niet is voldaan, moet het bericht door de ontvanger geweigerd worden en een SOAP foutmelding aan het verzendende systeem afgegeven worden, zie foutafhandeling in [IH tokens generiek].

Als wel aan alle condities is voldaan, wordt het bericht verder verwerkt.

10.3.2.5.5 Referenties transactietoken

10.3.2.5.5.1 Bijlage A Referenties

Referentie	Document	Versie
[IH tokens generiek]	AORTA_Auth_IH_Security_tokens_generiek (see page 465)	8.3.0.0
[Mandaattoken]	GBZ AORTA_Auth_IH_Mandaattoken (see page 475)	8.3.0.0
[Inschrijftoken]	GBZ AORTA_Auth_IH_Inschrijftoken (see page 373)	8.3.0.0
[SAMLAuthnContext]	Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0 http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf	2.0 15-mrt-2005
[SAML Core]	SAML v2.0 Core Specification https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf	2.0 15-mrt-2005
[SAML Profiles]	Profiles for the OASIS Security Assertion Markup Language (SAML) v2.0 http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf	2.0 15-mrt-2005
[SAML Token]	SAML Token Profile http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SAMLTOKENProfile.pdf	1.1 01-feb-2006
[UZI pas]	CA model, Pasmodel, Certificaat- en CRL-profielen, Agentschap CIBG www.uziregister.nl ¹³⁶	4.1 september 2010
[PKI Design]	Describes the design of the PKI of ZORG-ID and provides a backbone for the Identity Security	1.8 24-dec-2024
[JWT]	RFC 7519 JSON Web Token (JWT) https://www.rfc-editor.org/rfc/rfc7519	Mei 2015

136. <http://www.uziregister.nl/>

[JWS]	RFC 7515 JSON Web Signature (JWS) https://www.rfc-editor.org/rfc/rfc7515	Mei 2015
[JWA]	RFC 7518 JSON Web Algorithms (JWA) https://www.rfc-editor.org/rfc/rfc7518	Mei 2015

10.3.2.6 GBx AORTA_Auth_IH_Security_tokens_generiek

- **IH Security tokens generiek**

Datum: 1 februari 2025
Publicatie: V8.4.0.0

10.3.2.6.1 Inleiding Security tokens generiek

10.3.2.6.1.1 Doel en scope

Dit document legt de basis voor de verschillende beveiligingsimplementatie handleidingen waarin security tokens voor specifieke toepassing concreet beschreven worden. Dit document beschrijft wat security tokens zijn, wat het doel is van security tokens en hoe security tokens in de AORTA-architectuur worden ingezet.

Dit document is normatief, behalve de hoofdstukken en paragrafen waarin wordt aangegeven dat ze informatief zijn.

10.3.2.6.1.2 Doelgroep voor dit document

Dit document is bedoeld voor softwareontwikkelaars van XIS'en.

De lezer wordt verondersteld kennis te hebben van [XML], [Namespaces], [SOAP], [HTTP], [WSDL] en [IH Transport].

10.3.2.6.1.3 Documenthistorie

Versie	Datum	Omschrijving
6.10.0.0	12-okt-2011	RfC 36422: SHA-256 in tokenauthenticatie. Voor het berekenen van hashwaarden wordt SHA-1 òf SHA-256 gebruikt. RfC 46142: SOAP Headers van tokens worden uitgebreid met soap:actor. RfC 46183: soap:actor moet zijn gbx ipv gbz. Verwijzing naar [IH Transport] opgenomen en tekst in Par 6.1 aangepast.
6.11.0.0	12-okt-2012	Ongewijzigde herpublicatie als onderdeel van AORTA-Infrastructuur v6.11
8.0.1.0	15-mei-2017	RfC 65898 en RfC 36422 SHA1 delen van AORTA_Auth_IH_Berichtauthenticatie_UZI.doc bijwerken met SHA256 en bij voorbeelden SHA256 in IH Security tokens generiek toegelicht.
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-20 17	RfC 76206: SSL verwijderen
8.0.3 .0	15- nov-20 18	Opgenomen in publicatie 8.0.3.0
8.1.0 .0	1- aug-20 19	INI-8877: Conditionele query
8.1.0 .0	1- aug-20 19	INI-8811: Loggen UZI-CertificaatID
8.2.0 .0	7- okt-202 0	Opgenomen in publicatie 8.2.0.0
8.4.0 .0	2025	Uitbreiding op Security tokens n.a.v. ZORG-ID CA (Certificate Authority). De CA speelt een cruciale rol in de digitale beveiliging, met name in de PKI.

10.3.2.6.1.4 Legenda

Deze implementatiehandleiding gebruikt de volgende symbolen:

	Let op! Dit is een aandachtspunt. Een opmerking die de aandacht vestigt op een bepaald opvallend aspect.
	Dit is een 'open issue' of 'known issue'. Een kwestie die nog open ligt voor discussie, maar onderkend is.
	Dit is een frequently asked question (FAQ) met antwoord.

10.3.2.6.2 Kaders en uitgangspunten

10.3.2.6.2.1 Externe normen en kaders

Op het gebied van beveiliging in de zorg zijn verschillende normen en wetten van kracht, zowel op Europees als Nederlands niveau. De NEN 7510-norm is de Nederlandse norm voor informatiebeveiliging in de zorg en is van toepassing op alle zorgaanbieders.

Bij de uitwisseling van informatie in de zorg speelt de wetgeving een belangrijke rol. Een uitgebreide behandeling hiervan valt buiten de reikwijdte van dit document, echter de Wet gebruik burgerservicenummer in de zorg (Wbsn-z) wordt hier kort benoemd.

De Wbsn-z (sinds 2008) regelt dat in alle berichtgevingen tussen zorgaanbieders onderling het *burgerservicenummer* (BSN) aanwezig **moet** zijn om persoonsverwisseling en daardoor medische fouten te voorkomen. Een burgerservicenummer mag door de zorgaanbieder worden geregistreerd nadat de betrokkene zich heeft gelegitimeerd met een wettelijk identificatiedocument.

10.3.2.6.2.2 Relatie met AORTA-principes en –beslissingen

In dit hoofdstuk worden de architectuurprincipes weergegeven waaraan de AORTA-document moet voldoen.

Architectuurprincipe AORTA.ALG.p1010: aan aangesloten zorgsystemen worden uitsluitend eisen gesteld die noodzakelijk zijn voor veilige gestandaardiseerde uitwisseling van gegevens.

Architectuurprincipe AORTA.ALG.p1020: voor toegang tot patiëntgegevens moeten zorgverleners persoonlijk worden *geïdentificeerd* en *geauthenticeerd*

10.3.2.6.2.3 Namespaces

Wanneer in dit document in voorbeeld fragmenten niet gedeclareerde namespace prefixes worden gebruikt, worden de volgende namespaces bedoeld.

Prefix	Namespace URI
ao	http://www.aortarelease.nl/805/
ds	http://www.w3.org/2000/09/xmldsig#
soap	http://schemas.xmlsoap.org/soap/envelope/
wsu	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd
wss	" http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd "
saml	urn:oasis:names:tc:SAML:2.0:assertion

10.3.2.6.2.4 Namespaces

De volgende namespaces worden gebruikt in de security header. De prefixen zijn niet normatief maar worden in dit document als voorbeelden gebruikt.

Tabel AORTA.STK.t3140 - Namespaces

Prefix	Namespace URI
soap	http://schemas.xmlsoap.org/soap/envelope/
ds	http://www.w3.org/2000/09/xmldsig#
saml	urn:oasis:names:tc:SAML:2.0:assertion
wss	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd
ao	http://www.aortarelease.nl/805/

	In XML mag een prefix veranderd worden (mits consequent toegepast). Na ondertekening kan dit echter niet meer, dit zou de handtekening ongeldig maken.

}

10.3.2.6.3 Het security token

Dit hoofdstuk is niet normatief.

Berichten die worden uitgewisseld binnen AORTA kunnen worden uitgerust met ondertekende security tokens om de integriteit, authenticiteit en onweerlegbaarheid ervan te waarborgen.

Een security token is opgebouwd uit de volgende componenten:

- verzameling authentieke kenmerken met de daarbij behorende waarden,
- een digitale handtekening,
- randvoorwaarden zoals transformaties, matchingregels, certificaten, etc.

Een security token is niet op te stellen zonder de privé sleutel waarmee het security token wordt ondertekend.

Een security token kan op verschillende manieren worden gebruikt:

- Het security token is aan één of door één entiteit uitgegeven (persoon, machine, etc.) en dient voor bepaalde (authenticatie, autorisatie of logging) doeleinden. Het security token bevat informatie over de afzender en bevat bepaalde kenmerken over een gegeven onderwerp.
- Het security token geeft het recht (autorisatie) om een bepaalde activiteit uit te voeren. Het security token wordt gekoppeld aan interacties.

Voor AORTA zijn voor de verschillende actoren (zorgverleners, patiënten, klantenloketmedewerkers, etc.) rollen gedefinieerd die bepaalde interacties kunnen uitvoeren. Voor elk van deze rollen zijn

verschillende soorten tokens gedefinieerd waarmee een actor met een voorgedefinieerde rol voor verdere actie en afhandeling bij het landelijk schakelpunt kunnen aanmelden. De volgende soorten tokens worden binnen AORTA toegepast:

- Een authenticatietoken waarmee de identiteit van een persoon of object wordt vastgesteld en gekoppeld aan uitgewisselde gegevens ([IH BA Trans]);
- Een inschrijftoken waarmee gegarandeerd wordt dat een patiënt d.m.v. een gevalideerd BSN is ingeschreven bij een bepaalde zorgaanbieder door een specifieke medewerker ([IH Inschrijf]);
- Een mandaattoken waarmee een mandaterende zorgverlener een set gegevens elektronisch ondertekend om onweerlegbaar zijn autorisaties over te kunnen dragen aan een gemandateerde ([IH Man]).

Opbouw

Het security token bevat een aantal basiskensmerken en beveiligingsgerelateerde gegevens. Het security token inclusief digitale handtekening mag dan zonder de privé sleutel niet na te maken zijn, het is wel te kopiëren. Gekopieerde tokens kunnen opnieuw gebruikt of misbruikt worden voor andere acties. De volgende basiskensmerken en beveiligingsgerelateerde gegevens horen bij het security token:

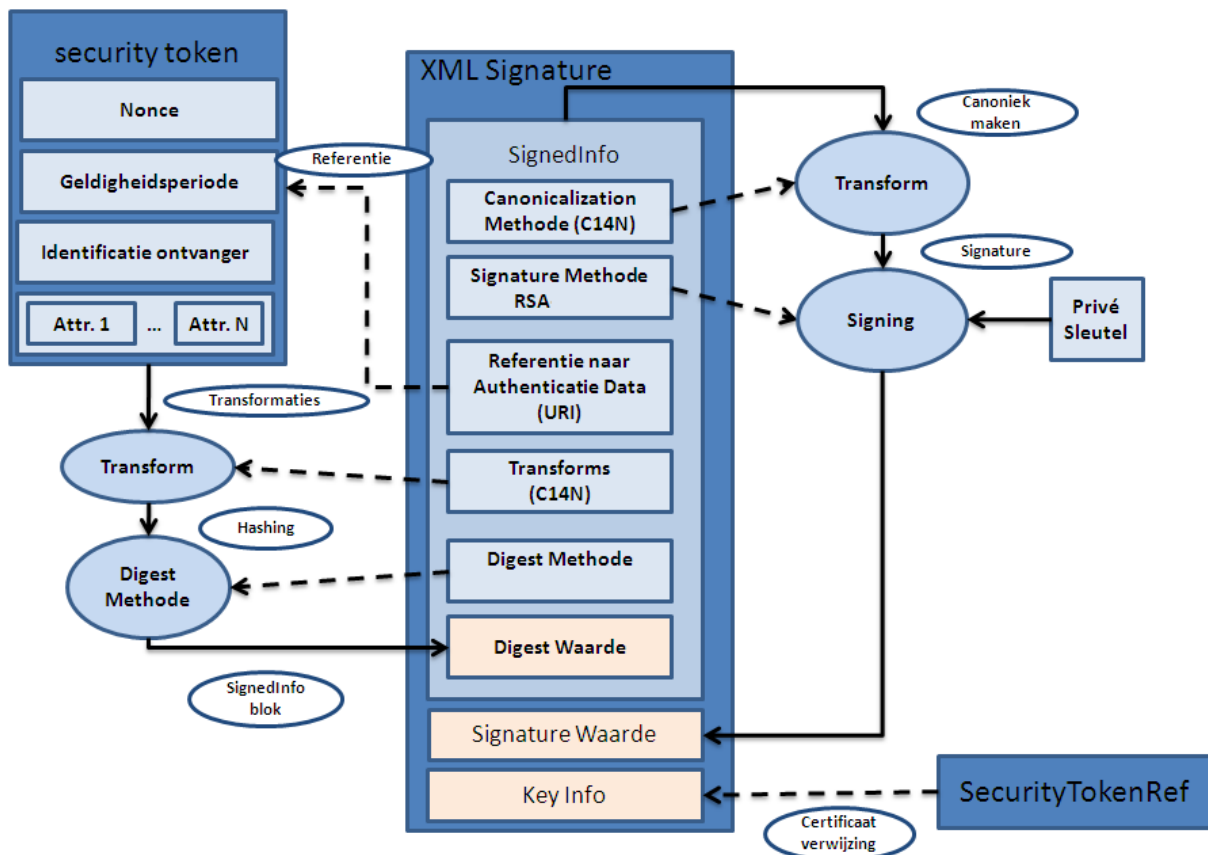
- Uniekheid. Per toepassing moet aangegeven worden of het security token *mondiaal uniek* identificeerbaar moet zijn. Dit kan worden gerealiseerd door een nonce (**N**umber used **O**NCE) in het bericht te stoppen.
- Onderwerp. Het security token heeft een onderwerp waarover de uitgewisselde (beveiligingsgerelateerde) gegevens gaan. Het onderwerp wordt uniek geïdentificeerd en gebruikt bij dialogen tussen partijen (bijvoorbeeld: authenticiteit van een bericht vaststellen op basis van een bericht-id).
- Geldigheid. Elk security token voldoet aan bepaalde condities en geldigheidsvoorwaarden.
- Afzender. De afzender of leverende partij van het security token. Het token bevat een unieke identificatie van de afzender.
- Ontvanger. Afnemer of gebruiker van het security token. Het token bevat een unieke identificatie van de ontvanger. Het doel hiervan is dat de ontvanger de uniciteit van de nonce moet kunnen controleren en de mogelijkheid van hergebruik van een security token bij derden moet worden voorkomen. Echter bij ongeadresseerde verzendingen waarbij het security token wordt gebruikt, is de ontvanger niet bekend.
- Authenticatie. Geeft aan binnen welke authenticatie-context het security token gebruikt wordt als referentiekader voor communicatie tussen de afzender en de ontvanger van het token. De authenticatie-context kan informatie bevatten over de actuele authenticatie methode (bijvoorbeeld de "sterkte" van het gebruikte authenticatiemiddel).
- Middel waarmee het onderwerp in het security token is geauthenticeerd (SAML definieert de details van meer dan 20 verschillende authenticatie methodes).
- Attributen. Aanvullende (essentiële) attributen die een sterkere relatie leggen tussen het bericht en het security token.

Afhankelijk van het type security token, worden bovenstaande componenten in het security token impliciet dan wel expliciet vastgelegd. De componenten worden als aparte paragrafen per beveiligingsimplementatie handleiding verder uitgewerkt.

10.3.2.6.4 Digitaal tekenen

10.3.2.6.4.1 Inleiding

Om de integriteit te waarborgen wordt (een subset van) het security token ondertekend met behulp van XML Signature. De ontvanger kan dan onomstotelijk vaststellen dat het security token ondertekend is met de privé sleutel behorend bij het certificaat van de verzender.



Figuur 1: Security token met (SHA1) XML Signature

10.3.2.6.4.2 Inhoud van de XML Signature

De XML Signature bij het security token ziet er als volgt uit (de lange Base 64 strings zijn fictieve waarden en afgekort):

```
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
```

```

<ds:SignedInfo>
  <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
  <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha256" />
  <ds:Reference URI="#security_token_Nonce">
    <ds:Transforms>
      <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature" />
      <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
    </ds:Transforms>
    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmlenc#sha256" />
    <ds:DigestValue>xx5...Gus2g</ds:DigestValue>
  </ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>bULmRGKBlhyPbumKDxrrT...SigWaarde</ds:SignatureValue>
<ds:KeyInfo>
  <!-- KEYINFO bevat informatie over gebruikte certificaat -->
</ds:KeyInfo>
</ds:Signature>

```

Er volgt nu een bespreking van alle XML Signature elementen.

Het <Signature> element

```
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
```

De XML Signature begint met het Signature blok en een verwijzing naar de XML Signature namespace. Het Signature blok kan onderdeel zijn van het security token of refereert naar het security token.

Het <SignedInfo> element

```
<ds:SignedInfo>
```

Vervolgens komt het SignedInfo blok. Dit blok bevat de gegevens die daadwerkelijk getekend worden.

Het <CanonicalizationMethod> element

```
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
```

Het SignedInfo blok zelf moet in de juiste canonieke vorm gebracht worden. Voor de digitale handtekening wordt het Exclusive XML Canonicalization zonder comments gebruikt [EXCC14N]. Deze vorm van canoniek maken, gaat goed om met namespaces van XML documenten die ingebed zijn in andere documenten.

Aangezien het security token wordt samengevoegd met het onderliggend bericht, dat weer is ingebed in een SOAP envelop, is het gebruik van Exclusive XML Canonicalization verplicht.

Het <SignatureMethod> element

```
<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
```

De methode van tekenen. Voor de digitale handtekening wordt gebruik gemaakt van een RSA handtekening over een digest. Voor de gebruikte algoritmes zie 4.3.

Het <Reference> element

```
<ds:Reference URI="#security_token_Nonce">
```

Een referentie naar het token dat getekend is. De referentie is een placeholder en de waarde die wordt overgenomen in een relatieve URI (dus voorzien van een "#" als prefix) moet globaal uniek zijn (i.v.m. het samenvoegen van mogelijk meerdere security tokens in een enkel document).

Het <Transforms> element

```
<ds:Transforms>
  <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
</ds:Transforms>
```

Er worden een aantal transforms gedaan over het token. De minimale set van transforms is de exclusieve canonicalisatie.

Het <DigestMethod> element

```
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmlenc#sha256"/>
```

Van het canonieke SignedInfo blok van het token wordt een digest berekend. Het gebruik van SHA256 of hoger DigestMethod wordt voor eerste implementatie voorgeschreven.

Het <DigestValue> element

```
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmlenc#sha256" / (see page 441)>
```

Van het canonieke SignedInfo blok van het token wordt een digest berekend. Het gebruik van SHA256 of hoger DigestMethod wordt voor eerste implementatie voorgeschreven.

Het <SignatureValue> element

```
<ds:SignatureValue>bULmRGKBIhyPbumKDxrrT...SiGWaarde</ds:SignatureValue>
```

Over (de canonieke vorm van) het SignedInfo blok wordt een digest berekend waarover een RSA handtekening gezet wordt. Dit volgens de methode zoals vermeld in de eerder vermelde SignatureMethod. De waarde van de RSA handtekening wordt met Base 64 gecodeerd en opgenomen in de XML Signature. De handtekening is dus niet over het token zelf, maar over een digest van een SignedInfo blok, waarin een digest van het token staat.

Het <KeyInfo> element

```
<ds:KeyInfo>
  <!-- KEYINFO bevat informatie over gebruikte certificaat -->
</ds:KeyInfo>
```

Het <KeyInfo> -element wordt gebruikt in XML Signature (XMLDSIG) om informatie te verstrekken over de cryptografische sleutel die verband houdt met een digitale handtekening. Het doel van dit element is om de verificatie van de handtekening mogelijk te maken. Het kan een verscheidenheid aan informatie bevatten, afhankelijk van de specifieke toepassing en vereisten. Een belangrijk element die gedefinieerd is binnen <KeyInfo> is de X.509-certificaatinformatie, het <X509Data> -element, die wordt gebruikt om de sleutel te valideren. Dit element kan sub-elementen bevatten zoals het <X509Certificate>- en <X509IssuerSerial>- element.

Verdere uitleg over <KeyInfo> en <X509Data> wordt nader toegelicht in [paragraaf 4.4 Certificaten](#),.

```
</ds:Signature>
```

Einde van de XML Signature.

10.3.2.6.4.3 Algoritmes

Voor ieder security token bestaat er een aparte beveiligingsimplementatie handleiding in AORTA. Een dergelijke handleiding specificeert welke algoritmes voor dat specifieke token toegestaan zijn.

Voor het berekenen van hashwaarden wordt het door NCSC als “goed” beoordeelde SHA algoritme gebruikt. Voor de digitale handtekening wordt RSA (asymmetrische encryptie algoritme) gebruikt.

In de XML Signature wordt tweemaal gerefereerd aan deze waarden. Eenmaal voor het <SignatureMethod> element en eenmaal voor <DigestMethod> element. In deze elementen wordt een subset gebruikt van de URI's zoals gespecificeerd in [XMLSECURI]:

Tabel AORTA.STK.t3100 - Algoritmes

Functie	Algoritme	URI (voorbeeld)
Signatur e	RSA+SHA-512 of SHA-384 of SHA-256	<SignatureMethod Algorithm="http://www.w3.org/2000/09/ xmldsig#rsa"/>
Digest	SHA-512 of SHA-384 of SHA-256	<DigestMethod Algorithm="http://www.w3.org/2000/09/ xmldsig#"/>
Signatur e	RSA+SHA-256	<SignatureMethod Algorithm="http://www.w3.org/2001/04/ xmldsig-more#rsa-sha256"/>
Digest	SHA-256	<DigestMethod Algorithm="http://www.w3.org/2001/04/ xmlenc#sha256"/>

10.3.2.6.4.4 Certificaten

Voor ieder security token bestaat er een aparte beveiligingsimplementatie handleiding in AORTA. Een dergelijke handleiding specificeert welke certificaten zijn toegestaan en hoe deze opgenomen worden in het bericht.

Een certificaat koppelt de identiteit van een actor aan een publieke sleutel. Alleen de houder van het certificaat beschikt over de privé sleutel en kent de toegangscode tot het authenticatiemiddel.

Een vertrouwde partij (*trusted third party*) geeft certificaten uit. Deze partij wordt de uitgever (*issuer*) genoemd. Om aan te tonen dat deze uitgever daadwerkelijk het certificaat heeft uitgegeven, ondertekent de uitgever het certificaat met zijn privé sleutel. Controle van deze ondertekening kan plaatsvinden door deze te controleren tegen de publieke sleutel in het certificaat van de uitgever. De controle moet voor de gehele keten een keer plaatsvinden tot aan het vertrouwde (root) certificaat.

Daarna kan dit (nu ook vertrouwde) certificaat opgenomen worden in de softwareomgeving.

De volgende CA's (*Certificate Authority*) spelen een belangrijke rol in AORTA:

- PKIoverheid. PKIoverheid heeft eigen CA's. Deze vallen allen onder de Root CA van de Staat der Nederlanden. Daaronder is een opdeling in verschillende domeinen, onder andere één voor burgers en één voor overheid en bedrijven (organisaties). De huidige hiërarchie (G2) worden certificaten ondertekend met SHA-256 en worden langere sleutels gebruikt. Deze hiërarchie wordt de tweede generatie (G2, Niet te verwarren met de G2 van het UZI-register, deze sluit aan

bij de **eerste** generatie van PKI-overheid.) genoemd. PKI-overheid is in 2017 over gegaan op een nieuwe hiërarchie, de derde generatie G3. Zie informatie op de Logius website.

- UZI-register van het CIBG. Het UZI-register is een intermediate CA onder PKI-overheid. Het CIBG is een uitvoeringsorganisatie van het ministerie van VWS, welke een programma voert met diverse CA's voor de zorgsector. Zij voeren dit uit onder de PKI-overheid richtlijnen en hiërarchie. Het CIBG treedt hierbij zowel als Register Authority als Certificate Authority op. Er worden certificaten (voor zorgverleners, medewerkers op naam, medewerkers niet op naam en voor servers verstrekt voor gebruik in de Zorgsector. In de certificaten van zowel UZI-passen als – server- certificaten wordt de identiteit van de houder, het UZI-nummer en aanverwante informatie opgenomen. Er zijn momenteel twee generaties (G2 en G21) van UZI-register CA's in gebruik. De G21 generatie CA's zijn ondertekend met SHA-256 en sluit aan bij G2 van PKI-overheid. Voor de derde generatie UZI-certificaten, zie informatie op de UZI-register website.
- (NIEUW 8.3.0.0) ZORG-ID Token. Het ZORG-ID Token certificaat is een intermediate CA onder ZORG-ID. Deze certificaten worden gebruikt bij de ZORG-ID Smartcard om zorgmedewerkers te kunnen authenticeren.

De gangbare *technische vorm* van certificaten zijn X.509 versie 3 certificaten. X.509v3 is een specificatie van de ITU, zie [X509]. In een X.509 certificaat zijn technische en organisatorische kenmerken opgenomen en wordt er een koppeling gelegd tussen de identiteit van een actor en een publieke sleutel. Verder is het mogelijk om naast standaard attributen extra kenmerken in het certificaat op te nemen, die door de uitgever als X.509v3 extensies in het certificaat worden gezet.

Tabel AORTA.STK.t3110 – X.509v3 attributen

Attribuut	Betekenis
Serial number	Een serie nummer van het certificaat. Het betreft een serie nummer van de uitgevende CA. Dit nummer moet uniek zijn per <i>issuer</i> , maar hoeft niet opend te zijn.
Signature Algorithm	Dit geeft aan met welk cryptografisch algoritme dit certificaat door de uitgever is ondertekend.
Issuer	Dit geeft de DN (Distinguished Name) van de uitgever van het certificaat aan. Dit geeft ook gelijk aan wie dit certificaat heeft ondertekend. Deze komt overeen met het subject in het CA certificaat van de uitgever.
Validity	Met twee datums wordt het interval aangegeven, waarbinnen het certificaat geldig is. De tijd is normaal opgegeven in UTC, tenzij een expliciete tijdzone is opgenomen.
Subject	De DN van de houder aan wie het certificaat behoort. Dit geeft de identiteit aan, die aan de publieke sleutel is gekoppeld.

Subject Public Key Info	Dit bevat de benodigde informatie over de publieke sleutel. Het beschrijft het algoritme voor de sleutel (bv. RSA) en de specifieke numerieke delen van die sleutel.
Signature	Dit bevat de ondertekening van het certificaat. Deze wordt gedaan door de uitgever, en kan worden gecontroleerd met de publieke sleutel in het certificaat van de uitgever.

Zoals eerder vermeld, wordt in de certificaten van zowel UZI-passen, smartcards als –server-certificaten de identiteit van de houder opgenomen. Dit gebeurt in de subjectAltName extensie als een otherName, met een vaste indeling.

De waarde hierin is een ASN.1 IAString met een OID (Object Identifier) van 2.5.5.5. De string heeft de volgende vaste notatie:

<OID CA>-<versie-nr>-<UZI-nr>-<pastype>-<Abonnee-nr>-<rol>-<AGB-code>

Tabel AORTA.STK.t3120 – X.509v3 extensie subjectAltName.otherName

Veld	Betekenis
OID CA	Dit is de OID van de CA en wijzigt niet per generatie en is generiek per type pas. Voor een complete lijst, zie [UZI CA Model].
versie-nr	1 voor alle UZI-register certificaten.
UZI-nr	Het UZI-nummer.
Pastype	Een codering met 1 karakter. Voor het type certificaat, of pastype, bestaan een aantal standaard waarden: Z (Zorgverlener), N (Medewerker op naam), M (Medewerker niet op naam) en S (Servercertificaat).
Abonnee-nr	Voor UZI passen is dit het URA (UZI-Register Abonnee) nummer.
Rol	Aanduiding van een medisch beroep. Wanneer er geen rol is (servers, medewerkers) wordt op het certificaat rolcode 00.000 gebruikt.
AGB-code	De AGB-code van de abonnee (zorgaanbieder) van deze server. Deze wordt binnen AORTA niet gebruikt.

De UZI-pas of smartcard die gebruikt wordt voor het ondertekenen van het security token moet een zorgverlener- of een medewerkerspas op naam zijn. Hoewel het pastype gecodeerd is opgenomen in

het certificaat (in het subjectAltName attribuut), dient een applicatie op basis van de uitgevende CA vast te stellen wat het pastype van de UZI-pas of smartcard is. De OID van de CA wijzigt niet per generatie.

Tabel AORTA.STK.txxx – X.509v3 extensie 2.16.840.1.113883.2.4.3.111.20.5 (Custom Extension copied Certificate)

Veld	Betekenis

proof

Het bewijs is een **JSON Web Token (JWT)**, een compact en URL-vriendelijk mechanisme dat wordt gebruikt om informatie veilig tussen twee partijen over te dragen in **JSON-formaat**.

Een JWT bestaat uit drie delen, gescheiden door puntjes (.):

1. Header:

- Bevat metadata over de token, zoals:
 - `typ` : Het type token (JWT)
 - `alg` : Het gebruikte signatuur algoritme (bijvoorbeeld `RS256` voor **RSA met SHA-256**)
 - `x5c` : Een verwijzing naar het publieke certificaat (non-repudiation) waarmee de handtekening kan worden geverifieerd
 - `iat` : Tijdstip van ondertekening

2. Payload:

- Bevat de **claims**, oftewel verklaringen over de entiteit (de zorgmedewerker). De volgende claims worden vastgelegd:
 - `ura` : het abonneenummer van de zorgaanbieder
 - `uziNumber` : het unieke identificatienummer van de zorgverlener
 - `roleCode` : de functionele rol van de zorgmedewerker

3. Signature:

- De token wordt **digitaal ondertekend** om de integriteit te waarborgen. Dit gebeurt als volgt:
 - De **header** en **payload** worden **Base64URL-encoded**
 - Beide worden samengevoegd en met de **privésleutel** (uit de UZI-, PKIO-pas, Zorg-ID Smartcard of ZORG-ID Mobiel) ondertekend
 - De gegenereerde handtekening wordt als derde deel toegevoegd

Het uiteindelijke JWT ziet er als volgt uit:

`xxxxx.yyyyy.zzzzz`

Waarbij:

- `xxxxx` = Base64URL-encoded header
- `yyyyy` = Base64URL-encoded payload
- `zzzzz` = Base64URL-encoded digitale handtekening

Gebruik van X.509-certificaten

- Het certificaat bevat de **publieke sleutel** die wordt gebruikt om de JWT-handtekening te **verifiëren**.
- De bijbehorende **privésleutel** bevindt zich op de **UZI-pas, PKIO-pas, ZORG-ID Smartcard of ZORG-ID Mobiel** en wordt gebruikt om de JWT te **ondertekenen**.

X.509 KeyUsage vereisten

De smartcard moet een certificaat bevatten met de juiste **X.509 keyUsage-extensie**, zoals:

- `digitalSignature` (voor ondertekening)
- `nonRepudiation` (voor niet-afwijzing)

Tabel AORTA.STK.t3130 – X.509v3 extensie keyUsage

Naam	Sleuteltype (KeyUsage)	Hexa decimaal gebruik
authenticiteitscertificaat	digitalSignature De naamgeving van deze keyUsage is verwarrend. De term "digital signature" verwijst naar de gebruikte techniek, die wordt gebruikt voor authenticatie en digitale handtekeningen. De term "non-repudiation" verwijst naar de functionaliteit die met de digitale handtekening wordt geboden." Een (verouderde) opvatting is, dat een certificaat voor elektronische handtekeningen beide bits op moet hebben staan. In PKI standaarden ter uitwerking van de Europese richtlijnen voor elektronische handtekeningen van o.a. PKI-overheid is dit niet echter toegestaan, om ondubbelzinnig duidelijk te maken dat een handtekeningcertificaat niet voor "gewone" authenticatiedoeleinden gebruikt mag worden.	0x80
handtekeningcertificaat	NonRepudiation	0x40



Elk security token dient getekend te worden met het juiste certificaat. Dit wordt verder in de verschillende beveiligingsimplementatie handleidingen beschreven.



De ontvanger van het security token dient te controleren of het certificaat met de juiste keyUsage gebruikt is.



De ontvanger dient te controleren of het certificaat door de juiste CA is uitgegeven en geldig is ondertekend. De keten dient gecontroleerd te worden tot een vertrouwd certificaat (bijvoorbeeld een root certificaat van het UZI-register waarvan de keten eerder vertrouwd is).



De ontvanger dient te controleren of het certificaat niet verlopen of ingetrokken is, inclusief de certificaten in de keten tot een vertrouwd certificaat.

Om de handtekening te verifiëren, moet de ontvanger over de bijbehorende publieke sleutel beschikken. De ondertekenaar kan deze op verschillende manieren aan de ontvanger ter beschikking stellen:

1. door het certificaat met de publieke sleutel mee te zenden als binaire security token (BinarySecurityToken) of als sleutel informatie (keyInfo).
2. door een verwijzing naar het certificaat mee te zenden; de ontvanger moet deze dan met bijvoorbeeld het LDAP protocol ophalen.

De opties worden in de volgende paragrafen in detail verder uitgewerkt. De eerste optie maakt de ontvanger flexibel. Als namelijk de afzender met een nieuw certificaat komt, hoeft de ontvanger niet zijn administratie voor zijn certificaten (store) bij te werken. De tweede optie heeft als voordeel dat de grootte van de berichten kleiner is.

Afhankelijk van de toepassing van het security token, wordt voor een optie gekozen.

In het testtraject worden testpassen gebruikt. Het gebruik hiervan wordt verder niet uitgewerkt in deze handleiding. De opbouw en werking is identiek, al staat de hiërarchie los van PKI-overheid.

Certificaat meezenden als BinarySecurityToken

```
<wss:Security ...>

  <wss:BinarySecurityToken

    wsu:Id="signing-cert"

    ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-
profile-1.0#X509v3"

    EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-
security-1.0#Base64Binary">MIIFd...PZaIvdgX0Q==

  </wss:BinarySecurityToken>

  <Signature ...>

    <SignedInfo ...>...</SignedInfo>

    <SignatureValue>...</SignatureValue>

    <KeyInfo>
```

```

    <wss:SecurityTokenReference>

        <wss:Reference URI="#signing-cert" ValueType="http://docs.oasis-open.org/wss/
2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" />

    </wss:SecurityTokenReference>

</KeyInfo>

</Signature>

</wss:Security>

```

Een bespreking per punt:

<wss:Security ...>

Bovenstaand is de WSS Security header.

```

<wss:BinarySecurityToken

    wsu:Id="signing-cert"

    ValueType=http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-
profile-1.0#X509v3

    EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-
security-1.0#Base64Binary">MIIFd...PZaIvdgX0Q==

</wss:BinarySecurityToken>

```

Bij het opnemen van het certificaat wordt een BinarySecurityToken element opgenomen met het hele certificaat in Base 64 codering. De wsu:Id moet matchen met de referentie later, maar de invulling is verder vrij. Wel moet deze waarde uniek zijn binnen het gehele document, aangezien het een ID is. De waarden voor ValueType en EncodingType zijn vast en verplicht.

```

<Signature ...>

```

```
<SignedInfo ...>...</SignedInfo>

<SignatureValue>...</SignatureValue>
```

De Signature zoals beschreven.

```
<KeyInfo>

  <wss:SecurityTokenReference>
```

De KeyInfo, met een verwijzing naar het BinarySecurityToken met het certificaat.

```
<wss:Reference URI="#signing-cert" ValueType="http://docs.oasis-open.org/wss/
2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" />
```

De verwijzing in de URI moet kloppen met de wsu:Id in het BinarySecurityToken element. ValueType is vast en verplicht.

```
</wss:SecurityTokenReference>

</KeyInfo>

</Signature>

</wss:Security>
```

Afsluiting van de elementen.

Certificaat meezenden als KeyInfo

```

<wss:Security ...>

...

<Signature ...>

  <SignedInfo ...>...</SignedInfo>

  <SignatureValue>...</SignatureValue>

  <KeyInfo>

    <X509Data>

      <!-- Het certificaat -->

      <X509Certificate>MIIFd...PZaIvdgX0Q==</X509Certificate>

    </X509Data>

  </KeyInfo>

</Signature>

</wss:Security>

```

Een bespreking per punt:

```

<wss:Security ...>

```

Bovenstaand is de WSS Security header.

```

<Signature ...>

  <SignedInfo>...</SignedInfo>

  <SignatureValue>...</SignatureValue>

```

De Signature zoals beschreven. De Signature en het daarbij gebruikte certificaat met de publieke sleutel kan als KeyInfo in het security token geïntegreerd zijn.

```

<KeyInfo>

  <X509Data>

    <!-- Het certificaat -->

    <X509Certificate>MIIFd...PZaIvdgX0Q==</X509Certificate>

  </X509Data>

</KeyInfo>

```

De KeyInfo, met het hele X509 certificaat in Base 64 codering.

```

</Signature>

</wss:Security>

```

Afsluiting van de elementen.

Certificaatverwijzingen

Bij het opnemen van een verwijzing naar het certificaat, wordt de volgende constructie opgenomen.

```

<KeyInfo>

  <wss:SecurityTokenReference>

    <X509Data xmlns="http://www.w3.org/2000/09/xmldsig#">

      <X509IssuerSerial>

        <X509IssuerName>CN=De Auteur CA, O=Nictiz, C=NL</X509IssuerName>

        <X509SerialNumber>359724...41160195</X509SerialNumber>

```

```

        </X509IssuerSerial>

    </X509Data>

    <RetrievalMethod
        URI="ldap://ldap.voorbeeld.nl/cn=CA,o=ZORG-ID,c=NL"
        Type="http://www.w3.org/2000/09/xmldsig#X509Data"
    />

    </wss:SecurityTokenReference>

</KeyInfo>

```

Een bespreking per punt:

```

<KeyInfo>

    <wss:SecurityTokenReference>

```

Het begin van de certificaatverwijzing. <KeyInfo> valt in de eerder gedeclareerde namespace van XML Signatures. <SecurityTokenReference> valt onder de WSS namespace, zie [paragraaf 2.4. \(see page 438\)](#)

```

<X509Data xmlns="http://www.w3.org/2000/09/xmldsig#">

```

De certificaatverwijzing zelf zit weer in de namespace van XML Signatures.

```

<X509IssuerSerial>

```


Begin van de certificaatgegevens.

```
<X509IssuerName>CN=De Auteur CA,O=Nictiz,C=NL</X509IssuerName>
```

De DN (Distinguished Name) van de CA (Certificate Authority). Dit geeft ook gelijk aan wie dit certificaat heeft ondertekend. Deze komt overeen met het subject in het CA certificaat van de uitgever. De attributen die in een DN van een security token zitten zijn CN (CommonName), O (OrganizationName) en C (CountryName), in die volgorde. De attributen worden van de waarden gescheiden door een = teken, van elkaar gescheiden met komma's en opgenomen zonder spaties, met uitzondering van de spaties in de waarden zelf, zoals beschreven in [LDAP]. De attribuutwaarden van een DN worden per CA verder in de verschillende beveiligingshandleidingen uitgewerkt.

```
<X509SerialNumber>359724...41160195</X509SerialNumber>
```

Het decimale serialNumber van het certificaat, conform [X509CRL]. Het betreft een serie nummer van de uitgevende CA. Dit nummer is uniek per issuer, maar hoeft niet oplopend te zijn.

```
</X509IssuerSerial>

</X509Data>
```

Afsluiten van de X509Data elementen

```
<RetrievalMethod

  URI="ldap://ldap.voorbeeld.nl/cn=ZORG-ID Token CA,o=ZORG-ID,c=NL"
  Type="http://www.w3.org/2000/09/xmldsig#X509Data"

/>
```

Een <RetrievalMethod>, is een *optioneel* element en kan worden gebruikt om te verwijzen naar een externe bron, zoals een LDAP-server, waar de certificaatgegevens (zoals de CA of serie nummer van het certificaat) kan worden opgehaald. Het element bevat een `URI`-attribuut dat de locatie aangeeft en een optioneel `Type`-attribuut om het type gegevens te specificeren.

- `URI`
 - Beschrijft de locatie van de LDAP-bron waar de gegevens kunnen worden opgehaald.
 - Structuur:
 - `ldap://` : Geeft aan dat LDAP als protocol wordt gebruikt.
 - `ldap.voorbeeld.nl`¹³⁷: De hostnaam of het IP-adres van de LDAP-server.
 - `cn=ZORG-ID Token CA` : De Distinguished Name (DN) van het object in de LDAP-directory. Hier wordt verwezen naar een specifiek CA.
 - `o=ZORG-ID, c=NL` : De organisatie en het land in de LDAP-directorystructuur.
- `Type` (optioneel)
 - Beschrijft het type gegevens dat wordt opgehaald.
 - Voor een X.509-certificaat gebruik je:
<http://www.w3.org/2000/09/xmlsig#X509Data>.

```
</wss:SecurityTokenReference>

</KeyInfo>
```

Afsluiting van de elementen.

}

10.3.2.6.5 Opbouw van de security header

WS-Security is een OASIS standaard en biedt een normatief raamwerk voor de beveiliging van het berichtenverkeer aan. Voor het toepassen van WS-Security, moet er een SOAP Header in de SOAP Envelope worden opgenomen. Deze SOAP Header omvat de WS-Security informatie en de XML Signature.

137. <http://ldap.example.com>

```

<soap:Envelope ...>
  <soap:Header ...>
    <wss:Security ...>
      <!-- Security header-->

      ...

    </wss:Security>
  </soap:Header >

</soap:Body >

  <!--HL7v3 (payload)-->
  ...

</soap:Body >
</soap:Envelope >

```

10.3.2.6.5.1 Plaats van het security token

Voor ieder type security token bestaat er een aparte beveiligingsimplementatie handleiding in AORTA. Een dergelijke handleiding specificeert waar het security token in het bericht geplaatst wordt.

Zie de WS-Security profielen X.509 Certificaat Token en SAML Token.

```

<wss:Security ...>
  <wss:BinarySecurityToken>
    <!--X.509 certificaat als security token-->
  </wss:BinarySecurityToken >

  ...

  <saml:Assertion ...>
    <!-- SAML Assertion als security token-->
  </saml:Assertion >

  ...
</wss:Security>

```

10.3.2.6.5.2 Plaats van de digitale handtekening

Digitale handtekeningen worden in de WS-Security SOAP Header gezet. Eén of meerdere digitale handtekeningen kunnen onderdeel zijn van het security token.



Wanneer een bericht uitgerust is met een security token, *moet* dat bericht minimaal één bijbehorende digitale handtekening bevatten om de integriteit en de onweerlegbaarheid van het security token te waarborgen.

```
<soap:Header ...>

...

<wss:Security ...>

  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

    <ds:SignedInfo>

      ...

    </ds:SignedInfo>

    <ds:SignatureValue>Wuwn...5e4=</ds:SignatureValue>

    <ds:KeyInfo>

      ...

    </ds:KeyInfo>

  </ds:Signature>

</wss:Security>

</soap:Header>
```

10.3.2.6.6 Afhandeling van het security token

10.3.2.6.6.1 Bestemming en verwerking

WS-Security informatie kan voor verschillende bestemmingen (GBx'en en ZIM) bedoeld zijn. In [IH Transport] wordt uitleg gegeven over het gebruik van de bestemming en verwerking attributen. In [IH Transport] wordt aangegeven welke soap:actor attributen gebruikt moeten worden per bestemming.

Het volgende blok is een implementatievoorbeeld van de bestemming en verwerking van WS-Security.

```

<soap:Header ...>

...

<wss:Security xmlns:wss=
    "http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd"
    soap:actor="http://www.aortarelease.nl/actor/zim" soap:mustUnderstand="1">
    ...
</wss:Security>
</soap:Header>

```

Er is één WS-Security header per bestemming. Er zijn dus maximaal twee WS-Security headers: één voor de ZIM, één voor het GBx. Een security header kan meer dan één security token bevatten. De security header gericht aan de ZIM wordt bij voorkeur vóór de security header van een GBZ geplaatst; daarmee kunnen ze verwerkt worden in de volgorde waarin ze nodig zijn.

10.3.2.6.6.2 Verificatie en controle

In de verschillende beveiligingsimplementatie handleidingen in AORTA en in [IH Transport] worden aanvullende voorwaarden gesteld i.h.k.v. verificatie en controle.



De WBSN-z regelt dat voor berichten die betrekking hebben op een persoon waarvan het burgerservicenummer (BSN) bekend is, het BSN als gegeven in het security token op te nemen.

Bij ontvangst van het security token dient de ontvanger de volgende controles uit te voeren:

- voldoet de XML Signature aan de eisen die er in [XMLSIG] aan gesteld worden;
- voldoet het security token aan de eisen die er in dit document aan gesteld worden;
- valideert de signature over het security token conform de eisen die er in dit document aan gesteld worden;
- is het gebruikte certificaat correct getekend, evenals de certificaten tot een vertrouwd certificaat;
- is het gebruikte certificaat geldig, niet verlopen en niet ingetrokken;

- als het gebruikte certificaat afkomstig is van "ZORG-ID Token CA" dan controle uitvoeren van de proof-extensie in het certificaat of deze overeenkomen met de verwachte waarden.
- is er een match tussen het bericht en de claims in het security token conform de eisen die de (zorg)toepassing daaraan stelt.

Indien één van de controles niet bevestigd wordt, wordt een SOAP fout gegenereerd, zie [paragraaf 6.3](#)¹³⁸ Foutafhandeling. Indien een SOAP fout wordt gegenereerd *mag* het bericht door de ontvangende partij verder verwerkt worden wanneer de betreffende toepassing dat vereist.

10.3.2.6.6.3 Foutafhandeling

De volgende SOAP fouten zijn van toepassing bij security tokens. Op de eerste SOAP foutmelding na, zijn ze onderdeel van WS-Security.

Tabel AORTA.STK.t3150

Omschrijving (faultstring)	Faultcode
Er is een (WS-Security) header aanwezig die niet bekend is, maar met mustUnderstand = "1". In dit geval moet deze Fault gegenereerd worden.	soap:MustUnderstand
An unsupported token was provided	wss:UnsupportedSecurityToken
An unsupported signature or encryption algorithm was used	wss:UnsupportedAlgorithm
An error was discovered processing the <wss:Security> header	wss:InvalidSecurity
An invalid security token was provided	wss:InvalidSecurityToken
The security token could not be authenticated or authorized	wss:FailedAuthentication
The signature or decryption was invalid	wss:FailedCheck
Referenced security token could not be retrieved	wss:SecurityTokenUnavailable
The message has expired	wss:MessageExpired

138. <https://vzvz.atlassian.net/wiki/spaces/AORTA84/pages/879593320/Afhandeling+van+het+security+token#Afhandelingvanhetsecuritytoken-Foutafhandeling>

De volgende foutmeldingen worden daar aan toegevoegd.

Tabel AORTA.STK.t3160

Omschrijving (faultstring)	Faultcode
Authenticatietoken en bericht stemmen niet overeen	ao:AuthTokenMessageMismatch
Authenticatietoken is niet valide of compleet	ao:AuthTokenInvalid
Authenticatietoken buiten geldigheidsduur ontvangen	ao:ExpirationTimeError
Nonce is reeds gebruikt	ao:NonceRejected
Proof Extension Invalid	ao:ProofInvalid

De volgende statuscodes (URI referenties) worden door SAML onderkend en geretourneerd [SAML Core].

Een statuscode is een Uniforme Resource Name (URN) en is als volgt opgebouwd:

"urn:"<Namespace Identifier>":"<Name Specific String>

Voorbeeld:

"urn:oasis:names:tc:SAML:2.0:status:Success"

In de <statuscode> tabel AORTA.STK.t3170 wordt alleen de omschrijving en de specifieke string (<Name Specific String>) getoond. <StatusDetail> kan daarnaast gebruikt worden om een specifieke leesbare melding te retourneren (zie [SAML Core]).

Tabel AORTA.STK.t3170

Omschrijving	Name Specific String
The request could not be performed due to an error on the part of the requester.	Requester

The request could not be performed due to an error on the part of the SAML responder or SAML	Responder
The SAML responder could not process the request because the version of the request message was incorrect.	VersionMismatch
The responding provider was unable to successfully authenticate the principal.	AuthnFailed
The specified authentication context requirements cannot be met by the responder.	NoAuthnContext
The SAML responder or SAML authority is able to process the request but has chosen not to respond.	RequestDenied
The SAML responder or SAML authority does not support the request.	RequestUnsupported
The SAML responder cannot process any requests with the protocol version specified in the request.	RequestVersionDeprecated
The SAML responder cannot process the request because the protocol version specified in the request message is a major upgrade from the highest protocol version supported by the responder.	RequestVersionTooHigh
The SAML responder cannot process the request because the protocol version specified in the request message is too low.	RequestVersionTooLow
The resource value provided in the request message is invalid or unrecognized.	ResourceNotRecognized
The response message would contain more elements than the SAML responder is able to return.	TooManyResponses
The responding provider does not recognize the principal specified or implied by the request.	UnknownPrincipal
The SAML responder cannot properly fulfill the request using the protocol binding specified in the request.	UnsupportedBinding

10.3.2.6.6.4 Loggen

Per security token wordt bepaald wat er gelogd moet worden door het LSP. Dit is opgenomen in de IH's van de verschillende tokens. In ieder geval dient van elk op het LSP binnenkomend token die getekend is door een PKI(o) certificaat, het certificaatID van hetPKI(o) certificaat gelogd te worden.

10.3.2.6.7 Referenties security tokens generiek

10.3.2.6.7.1 Bijlage A Referenties

Referentie	Document	Versie
[BSP]	Basic Security Profile Version 1.0, Final. www.ws-i.org ¹³⁹	1.0 30- mrt-200 7
[EXCC14N]	Exclusive XML Canonicalization, Version 1.0, W3C Recommendation, 18 July 2002, http://www.w3.org/TR/xml-exc-c14n/	1.0 18- juli-200 2
[HTTP]	RFC 2616 Hypertext Transfer Protocol -- HTTP/1.1 http://www.ietf.org	1.1
[IH Transport]	Implementatiehandleiding berichttransport	8.3.0.0
[LDAP]	Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names, IETF, Juni 2006, http://www.ietf.org/rfc/rfc4514.txt	juni-20 08
[MIME]	Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies, www.ietf.org/rfc/rfc2045.txt ¹⁴⁰	
[Namespaces]	Namespaces in XML 1.0 (Second Edition) www.w3.org/TR/xml-names/ ¹⁴¹	1.0
[SAML Binding]	Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS Standard, March 2005 http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf	2.0 mrt-200 5
[SAML Core]	Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS Standard, March 2005 http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf	2.0 mrt-200 5
[SAML Profiles]	Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS Standard, March 2005 http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf	2.0 mrt-200 5

139. <http://www.ws-i.org>

140. <http://www.ietf.org/rfc/rfc2045.txt>

141. <http://www.w3.org/TR/xml-names/>

[SAML Security]	Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS Standard, March 2005 http://docs.oasis-open.org/security/saml/v2.0/saml-sec-consider-2.0-os.pdf	2.0 mrt-2005
[SOAP]	Simple Object Access Protocol (SOAP) 1.1 http://www.w3.org/TR/SOAP	1.1
[UZI CA Model]	CA Model, Pasmodel, Certificaat- en CRL-profielen Zorg CSP. http://www.uziregister.nl/ https://www.uziregister.nl/overhetuziregister/hierarchie-productieomgeving ¹⁴²	7.0 16 jan 2014
[WSDL]	Web Services Description Language (WSDL) 1.1, W3C Note, 15 March 2001, http://www.w3.org/TR/wsdl	15- mrt-2001
[WSS]	Web Services Security: SOAP Message Security 1.0, OASIS Standard Specification, March 2004 http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf	mrt-2004
[WS SAML Token Profile]	Web Service Security: SAML Token Profile 1.1 http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SAMLSecurityProfile.pdf	1- feb-2006
[WS Soap Message Security]	WSS: SOAP Message Security 1.1 http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SOAPMessageSecurity.pdf	1- feb-2006
[WS Trust]	WS-Trust 1.4 http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/os/ws-trust-1.4-spec-os.pdf	2- feb-2009
[WSX509]	Web Services Security X.509 Certificate Token Profile 1.0, OASIS Standard Specification, March 2004 http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0.pdf	mrt-2004
[X509]	Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks, Recommendation X.509, 08-2005 http://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.509-200508-!!!PDF-E&type=items	aug-2005
[X509CRL]	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile http://www.ietf.org/rfc/rfc3280.txt	apr-2002

142. <http://www.uziregister.nl/>

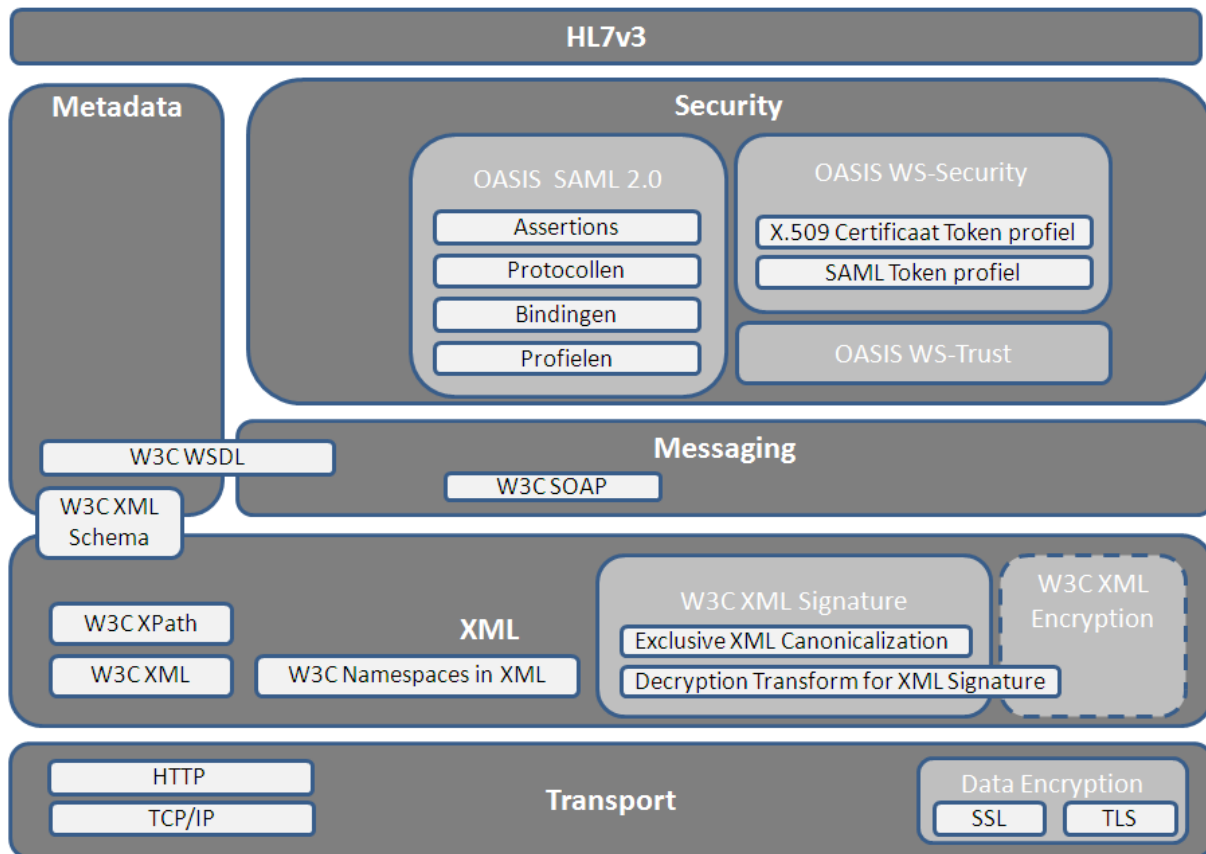
[XML]	Extensible Markup Language (XML) 1.0, W3C Recommendation, Fourth Edition, 16 August 2007 http://www.w3.org/TR/xml	16-aug-2007
[XMLEC14N]	W3C Recommendation, "Canonical XML Version 1.0," 15 March 2001 http://www.w3.org/TR/xml-c14n	15-mrt-2001
[XMLSECURI]	Additional XML Security Uniform Resource Identifiers (URIs) http://www.ietf.org/rfc/rfc4051.txt	
[XMLESIG]	XML-Signature Syntax and Processing (Seconde Edition), W3C Recommendation, 12 February 2002 http://www.w3.org/TR/xmldsig-core/	10-juni-2008
[XPATh]	W3C Recommendation, "XML Path Language", 16 November 1999 http://www.w3.org/TR/xpath/	16-nov-1999
[IH BA Trans]	Implementatiehandleiding Berichtauthenticatie Transactietoken (see page 399)	8.4.0.0
[IH Inschrijf]	Implementatiehandleiding Inschrijftoken (see page 373)	8.4.0.0
[IH Mandaat]	Implementatiehandleiding Mandaattoken (see page 475)	8.3.0.0
[JWT]	RFC 7519 JSON Web Token (JWT) https://www.rfc-editor.org/rfc/rfc7519	Mei 2015
[JWS]	RFC 7515 JSON Web Signature (JWS) https://www.rfc-editor.org/rfc/rfc7515	Mei 2015
[JWA]	RFC 7518 JSON Web Algorithms (JWA) https://www.rfc-editor.org/rfc/rfc7518	Mei 2015

10.3.2.6.8 Technologieën en standaarden

10.3.2.6.8.1

Bijlage B Technologieën en standaarden

Deze bijlage geeft een overzicht van de gebruikte technologieën en standaarden en beschrijft die profielen die nodig zijn om berichten van securitytokens te voorzien, voor de uitwisseling van beveiligingsgerelateerde informatie tussen vertrouwde partijen en die voldoen aan de eisen van authenticiteit.



Figuur 2: Technologieën en standaarden

XML Signature

XML Signature [XMLESIG] beschrijft de mogelijkheid om XML documenten of delen hiervan te ondertekenen. Een deel van de XML wordt gesigneerd (als tekst) en de signature wordt als XML bestand (Signature element) toegevoegd aan het XML document.

XML Canonicalization

XML Canonicalization [XMLEC14N] (kortweg C14N genaamd) is een methode om ervoor te zorgen dat XML altijd in dezelfde syntactische vorm aanwezig is. Met XML is het mogelijk dat software "onderweg" de vorm aanpast. Zo is in XML bijvoorbeeld per definitie `<tag></tag>` equivalent aan `<tag></tag>`. Voor een signature is dit echter niet hetzelfde. Met C14N wordt een XML uitdrukking in een canoneke vorm gebracht. Daarna kan dan op eenduidige wijze de signature gegenereerd worden. De ontvanger kan dan ook vóór het verifiëren van de ondertekening de canoneke vorm genereren, zodat het juiste – canoneke – document wordt vergeleken met de signature.

Er zijn twee vormen van canonek maken: Inclusive en Exclusive [EXCC14N]. De tweede vorm is de meest gebruikte voor Web Services. Het verschil tussen Inclusive en Exclusive Canonicalization zit in de wijze waarop namespace declaraties worden meegenomen. Bij Inclusive Canonicalization worden namespace declaraties uit een inkapselend document gewoon meegenomen: dat betekent dat de

signature verandert wanneer een document ingekapseld wordt. Dat maakt Inclusive Canonicalization ongeschikt voor ingekapselde documenten, zoals een HL7v3 bericht in een SOAP Envelope. Daarmee is Exclusive Canonicalization de gebruikte optie voor AORTA.

Voorbeeld van een bericht vóór het canoniek maken:

```
<?xml version="1.0" encoding="UTF-8"?>

<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">

  <soap:Body>

    <MFMT_IN002101 xmlns="urn:hl7-org:v3"

      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

      xsi:schemaLocation="urn:hl7-org:v3 ../schemas/MFMT_IN002101.xsd">

      <id extension="34234" root="2.16.528.1.1007.3.2.700222.1"/>

      <creationTime value="20040417161000"/>

      <versionCode code="NictizEd2005-0kt"/>

      <interactionId extension="MFMT_IN002101" root="2.16.840.1.113883.1.6"/>

      <profileId root="2.16.840.1.113883.2.4.3.11.1" extension="810"/>

      <processingCode code="P"/>

      <processingModeCode code="T"/>

      <acceptAckCode code="AL"/>

    </MFMT_IN002101>

  </soap:Body>

</soap:Envelope>
```

Hetzelfde bericht canoniek, exclusive zonder commentaar:

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">

  <soap:Body>
```

```

<MFMT_IN002101 xmlns="urn:hl7-org:v3" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xsi:schemaLocation="urn:hl7-org:v3 ../schemas/MFMT_IN002101.xsd">

  <id extension="34234" root="2.16.528.1.1007.3.2.700222.1"></id>

  <creationTime value="20040417161000"></creationTime>

  <versionCode code="NictizEd2005-0kt"></versionCode>

  <interactionId extension="MFMT_IN002101" root="2.16.840.1.113883.1.6"></
interactionId>

  <profileId extension="810" root="2.16.840.1.113883.2.4.3.11.1"></profileId>

  <processingCode code="P"></processingCode>

  <processingModeCode code="T"></processingModeCode>

  <acceptAckCode code="AL"></acceptAckCode>

```

Te zien valt dat:

- de XML declaratie is verwijderd;
- attributen per element alfabetisch zijn gesorteerd;
- namespace declaraties voor een element in lexicografische volgorde eerder komen dan andere attributen van dat element;
- lege elementen een eind-tag krijgen.

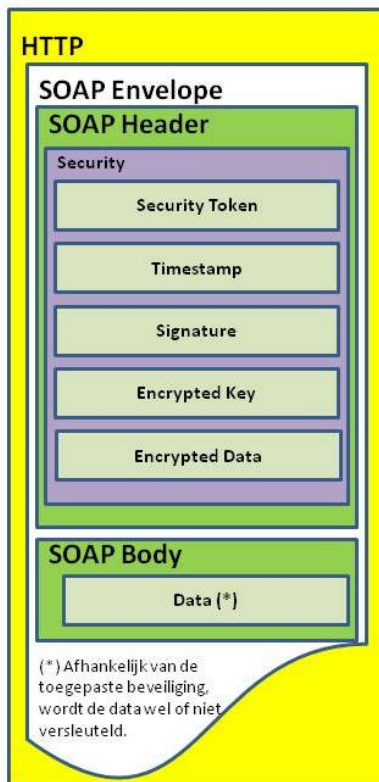
Whitespace – spaties, tabs, regeleindes – zijn significant in XML. XML is immers begonnen als opmaaktaal voor documenten, en in een document is whitespace relevant.

Canoniek maken laat de whitespace dus ongemoeid, behalve newlines die bij canoniek als een linefeed worden opgenomen.

WS-Security

Web Services Security (WS-Security) is een OASIS (Organization for the Advancement of Structured Information Standards) standaard die de integriteit, authenticiteit en vertrouwelijkheid van gegevens op *bericht niveau* garandeert (en koppelt daardoor de beveiliging los van het gebruikte communicatie kanaal).

WS-Security biedt tevens een mechanisme voor het gebruik van WS-Security tokens om deze aan berichten te koppelen. In WS-Security is een WS-Security token een XML structuur met beveiligingsgegevens. Omdat WS-Security geen specifieke type WS-Security tokens vereist, gebruiken we in de rest van dit document de term "security token" voor "WS-Security token".



Figuur 3: SOAP bericht met WS-Security

WS-Security voegt zijn gegevens toe aan de SOAP header door een <Security> element te definiëren waarbinnen een aantal beveiligingsaspecten worden geregeld, zoals:

- Vertrouwelijkheid. Berichten kunnen (deels) versleuteld worden. Hiervoor wordt de XML Encryption (W3C) specificatie geïmplementeerd.
- Integriteit. Berichten kunnen digitaal ondertekend worden zodat zowel de zendende als de ontvangende partij ervan zijn verzekerd dat de inhoud niet door derden is gewijzigd. Hiervoor wordt de XML Signature specificatie (W3C) geïmplementeerd.
- Geldigheidsduur. Berichten kunnen voor een bepaalde duur geldig en bruikbaar zijn.
- Authenticatie en autorisatie. In de SOAP header(s) kunnen verschillende type WS-Security tokens gebruikt worden, zoals:
 - gebruikersnaam en wachtwoord van een gebruiker in tekstformaat;
 - X.509 certificaat voor de authenticatie van gebruikers;
 - SAML Assertion (bewering) over entiteiten.

WS-Security kent diverse profielen die het gebruik van de verschillende security tokens (WS-Security tokens) beschrijft en hoe deze in de SOAP header geplaatst moeten worden.

In de volgende paragrafen wordt WS-Trust als uitbreiding van WS-Security besproken en de WS-Security profielen X.509 Certificaat Token en SAML Token.

Er zijn twee versies van WS-Security, 1.0 [WSS] en 1.1 [WS Soap Message Security], verschenen in 2004 respectievelijk 2006. De 1.1-specificatie benadrukt verbeteringen aan "security token" ondersteuning, berichtbijlagen en het beheer van rechten.

WS-Trust

WS-Trust [WS Trust] is eveneens een OASIS standaard en definieert uitbreidingen op WS-Security voor het verkrijgen en valideren van security tokens en voor het vormgeven van trust relaties. De reden voor het bestaan van WS-Trust is dat WS-Security alleen niet goed schaal in een complexe omgeving, zoals AORTA.

Indien er meerdere applicaties bestaan, verdeeld over verschillende security domeinen is het moeilijk om security tokens op de juiste manier te verkrijgen en te valideren. WS-Trust voorziet in een ontkoppelpunt voor het valideren van security tokens en het uitgeven of transformeren van deze security tokens in een bepaalde vorm (bijvoorbeeld een SAML token uit het ene domein transformeren in een SAML token uit een ander domein). Dit ontkoppelpunt heet "Security Token Service" (STS).

Binnen AORTA wordt gebruik gemaakt van WS-Trust 1.4.

509 Certificate Token Profile

Dit profiel [WSX509] beschrijft het gebruik van X.509 certificaat als "security token" in WS-Security. Dit profiel definieert de opties voor het invoegen van een X.509 certificaat en gerelateerde gegevens. Hiervan zijn voor ons relevant:

- 509 certificaat in binaire vorm (geserialiseerd na Base64 encoding)
- Verwijzing naar X.509 certificaat aan de hand van de naam van de uitgevende CA en het serienummer van het certificaat binnen die CA (X509IssuerSerial).

Binnen AORTA wordt gebruik gemaakt van WS-Security X.509 profiel 1.0.

SAML Token Profile

Dit profiel [WS SAML Token Profile] beschrijft het invoegen van SAML assertions als "security token" in WS-Security voor SAML v2.0. Hiervan is van belang hoe de SAML assertion in de header geplaatst moet worden:

- Attaching Security Tokens met SAML v2.0

10.3.2.6.8.2 SAML

Security Assertion Markup Language (SAML) [SAML Core] is een op XML gebaseerde OASIS standaard voor de uitwisseling van beveiligingsgerelateerde informatie.

De uitwisseling van de beveiligingsgerelateerde informatie gebeurt op basis van assertions. Een assertion is een uitspraak of bewering van een vertrouwde autoriteit (partij die verantwoordelijk is voor de waarmerking van die uitspraak) over een gebruiker en wordt door de Service Provider (partij die een applicatie of bron beschikbaar stelt voor de gebruiker) gebruikt om te bepalen of de gebruiker toegang mag krijgen tot een opgevraagde dienst of informatie. Uitspraken die een assertion kunnen bevatten zijn op te delen in een drietal categorieën:

- **Authenticatie uitspraken:** Deze uitspraken vertellen iets over het feit of de gebruiker zijn identiteit eerder succesvol kenbaar heeft gemaakt bij een Identity Provider. Voorbeelden van authenticatie assertions zijn: "Dit is arts X" en "Op datum D en tijdstip T heeft patiënt Y zich geauthenticeerd bij DigiD".
- **Autorisatie uitspraken:** Een dergelijke uitspraak vertelt tot welke delen van aangeboden diensten en/of informatie een gebruiker toegang heeft. In dit geval vertrouwt de dienstverlener volledig op de Identity Provider voor fijnmazige afscherming van de dienst, in plaats van zelf autorisatie bepalingen te maken. Een voorbeeld van een autorisatie uitspraak: "Patiënt P heeft toegang tot dossier D". Voor patiëntauthenticatie wordt geen gebruik gemaakt van deze uitspraken.
- **Attribuut uitspraken:** Een attribuut uitspraak geeft aan wat de kenmerken van een gebruiker zijn, zoals die bekend zijn bij een Identity Provider. Een voorbeeld van een attribuut uitspraak: "Patiënt P heeft burgerServiceNummer 123456789".

Verder beschrijft de SAML standaard onder andere:

- Verschillende mechanismen (protocollen) voor het opvragen en het verkrijgen van assertions, authenticatie verzoek, artifacts, name identifiers en logout verzoek [SAML Core];
- Bindingen met transport protocollen zoals HTTP en SOAP [SAML Binding];
- Standaard manieren (profielen) voor gebruik van SAML [SAML Profiles]

SAML heeft de WS-Security standaard geadopteerd. Met behulp van het SAML Token profile is het mogelijk om één of meerdere assertions als "security token" in SOAP berichten mee te sturen en digitaal te ondertekenen.

Binnen AORTA wordt gebruik gemaakt van HTTP over TLS-verbindingen met NCSC beveiligingsniveau "goed" om de vertrouwelijkheid van de assertions te waarborgen [SAML Security].

In de volgende paragrafen worden SAML2.0 profielen [SAML Profiles] beschreven, met referenties aan de OASIS SAML 2.0 specificaties.

SSO (Single Sign-On) Profile

Het Single Sign-On profiel (SSO) [SAML Profiles] is een SAML profiel dat aangeeft hoe gebruik te maken van het SAML authenticatie vraag en antwoord protocol in combinatie met verschillende SAML-bindings, zoals SOAP en HTTP. De communicatie bij authenticatie gaat tussen een Identity Provider (partij die verantwoordelijk is voor de waarmerking van de gebruiker) en een Service Provider (partij die een applicatie of bron beschikbaar stelt voor de gebruiker).

Voor het SSO profiel zijn de volgende twee aspecten van belang:

1. Bepalen of de berichten door de Identity Provider of door de Service Provider worden geïnitieerd.
2. Bepalen welke binding er gebruikt wordt voor de berichtuitwisseling tussen Identity Provider en Service Provider.

Het eerste aspect heeft te maken met waar de gebruiker start met het SSO proces voor de berichtuitwisseling. SAML ondersteunt twee algemene berichtstromen ter ondersteuning van het SSO proces. Binnen AORTA initieert de Service Provider het SSO profiel.

Het tweede aspect heeft te maken met de verschillende SAML bindingen (HTTP, SOAP of Artefact), die gebruikt worden tussen het uitwisselen van informatie tussen de Identity Provider en de Service Provider. Binnen AORTA maken we gebruik van Artefacts, die op SOAP/HTTP gebaseerd zijn.

Voor het SSO profiel zijn de volgende twee SAML berichten van belang; een verificatieverzoek bericht van de Service Provider naar een Identity Provider en het antwoord daarop dat van de Identity Provider naar de Service Provider wordt verzonden.

Artifact Resolution Profile

Het Artefact Resolution profiel [SAML Profiles] is een SAML profiel dat aangeeft hoe gebruik te maken van SAML artefacten in combinatie met SAML-bindings. De communicatie vindt plaats tussen de artefact opvrager (Service Provider) en de artefact resolution service (Identity Provider).

De artefact opvrager initieert het profiel door een vraag over een artefact naar de artefact resolution service te versturen. De artefact resolution service reageert hierop door (altijd) antwoord op de vraag te geven.

Een SAML artefact is een klein gestructureerd data object van een vast formaat dat verwijst naar een groter SAML protocol bericht [SAML Binding], bijvoorbeeld een SAML assertion. Een SAML artefact wordt in URL ingebed en overgebracht via een HTTP-bericht.

}

10.3.2.7 GBZ AORTA_Auth_IH_Mandaattoken

- **IH Mandaattoken**

Datum: 1 mei 2022
Publicatie: V8.3.0.0

10.3.2.7.1 Inleiding mandaattoken

10.3.2.7.1.1 Doel en scope

Dit document betreft een specificatie van het mandaattoken. Het betreft hier een mandaattoken voor gebruik bij communicatie tussen het goed beheerde Zorgsystemen (GBZ) en het landelijk schakelpunt (LSP).

10.3.2.7.1.2 Doelgroep voor dit document

Dit document is bedoeld voor softwareontwikkelaars van goed beheerde zorgsystemen en het LSP, die op grond van de HL7v3 communicatiestandaard en op grond van dit document berichten willen uitrusten met het SAML mandaattoken. Daarnaast wordt het plaatsen van de digitale handtekening besproken (zie ook [IH tokens generiek]).

10.3.2.7.1.3 Documenthistorie

Versie	Datum	Omschrijving	
V8.0.2.0	31-januari-2018		Initieel document.
V8.0.3.0	1-juli-2018		INI-8462 ¹⁴³ : Plaatsing Mandaattoken naast het Transactietoken
V8.0.3.0	1-jan-2019		INI-8769: Verduidelijken <security>-header
V8.0.3.0	1-jan-2019		INI-8771: Aanpassen controle geldigheid Mandaattoken
V8.0.3.0	1-jan-2019		INI-8754: Uitbreiden voorbeeld m.b.t. verwijzing naar certificaatgegevens en verwijzing naar het juiste certificaat met keyUsage non-repudiation (0x40)
V8.2.0.0	7-okt-2020		Controle op overseer in hoofdstuk 5.1 aangepast.

10.3.2.7.2 Het SAML mandaattoken

In dit hoofdstuk wordt de inhoud van het SAML mandaattoken besproken die bij mandatering en de berichtauthenticatie met behulp van de UZI-pas wordt gebruikt. Het SAML mandaattoken bevat informatie over de mandaatgever in relatie tot de gemandateerde zorgmedewerker. Het SAML

143. <https://vzvz.atlassian.net/browse/INI-8462>

mandaattoken is een op XML gebaseerd SAML assertion en heeft tot doel de *assertions* (bewijs van een bewering) over te brengen tussen partijen.

Alle XML voorbeelden in het document dienen door de betrokken partijen tijdens het bouwen van de uitwisseling getest, en waar nodig, in samenspraak met VZVZ aangepast te worden voor een juiste optimale werking.

Voor het verkrijgen van het SAML mandaattoken en het aanbieden van dit token aan het LSP worden de volgende profielen gebruikt:

- Het gebruik van het SAML mandaattoken (security token) in het kader van het WSS SOAP berichten profiel voor het veilig stellen en uitwisseling van authentieke SOAP berichten.

Dit profiel raakt het koppelvlak:

- goed beheerd zorgsysteem (GBZ) – het landelijk schakelpunt (LSP)

Dit profiel wordt in de volgende paragrafen verder uitgewerkt.

10.3.2.7.2.1 Structuur

Het SAML mandaattoken is een afgegeven SAML assertion die gebruikt wordt bij mandatering en berichtauthenticatie met behulp van de UZI-pas binnen AORTA. Er wordt gebruik gemaakt van SAML v2.0 [SAML Core].

Assertion

De assertion heeft de volgende structuur (de waarden die in het token gebruikt worden zijn fictief):

Element/ @Attribu te	0. .1	Omschrijving
@ID	1	Unieke identificatie van de Assertion
@Version	1	Versie van het SAML Protocol. Vaste waarde moet zijn 2.0
@IssueIns tant	1	Tijdstip van registratie van het mandaat.
Issuer	1	De zorgverlener die het mandaat afgeeft.
@NameQ ualifier	0	Niet gebruiken

Element/ @Attribute	0. .1	Omschrijving
@SPNameQualifier	0	Niet gebruiken
@Format	1	Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"
@SPProviderID	0	Niet gebruiken
Signature	1	Bevat de handtekening over de assertion zoals gezet met behulp van de UZI pas van de zorgverlener die het mandaat verleent (de mandaterende). De handtekening dient geplaatst te zijn met behulp van het handtekening-certificaat op de pas.
Subject	1	Bevat de Organisatie (URA) waarbinnen het mandaat geldig is. Let op: Indien dit veld gevuld wordt bij het uitlezen van de UZI pas, dan zal dit veld in het geval van gastgebruik niet de juiste URA bevatten. Er wordt aanbevolen dit veld met de URA uit het gebruikte servercertificaat te vullen.
BaseID	0	Niet gebruiken
NameID	1	Bevat de URA
EncryptedID	0	Niet gebruiken
SubjectConfirmation	1	Moet aanwezig zijn
@Method	1	'urn:oasis:names:tc:SAML:2.0:cm:sender-vouches'
SubjectConfirmationData	0	Niet gebruiken
@Recipient	0	Niet gebruiken
@NotOnOrAfter	0	Niet gebruiken
@InResponseTo	0	Niet gebruiken

Element/ @Attribute	0. .1	Omschrijving
@NotBefore	0	Niet gebruiken
@Address	0	Niet gebruiken
KeyInfo	0	Niet gebruiken
Conditions	1	Moet aanwezig zijn
@NotBefore	1	Moet aanwezig zijn.
@NotOnOrAfter	1	Moet aanwezig zijn.
Condition	0	Niet gebruiken
Audience Restriction	1	Moet aanwezig zijn
Audience	1	Bij AORTA/LSP en AoF: <code>urn:IIroot:2.16.840.1.113883.2.4.6.6:IIext:1</code> (1 is de applicatie-id van de ZIM) Bij MITZ "urn:oid:2.16.840.1.113883.2.4.3.111.2.1" (is MITZ) Obsolete: Bij de verzendende GBZ-applicatie <code>urn:IIroot:2.16.840.1.113883.2.4.6.6:IIext:<AppId></code> (is de verzendende GBZ-applicatie) WIJZIGINGSVOORSTEL: De verschillende Audience samenvoegen en er <code><saml:Audience>urn:generic:audience</saml:Audience></code> van maken.
ProxyRestriction	0	Niet gebruiken
Advice	0	Niet gebruiken

Element/ @Attribute	0. .1	Omschrijving
AuthnStatement	0	Niet gebruiken
AttributeStatement	1	Moet aanwezig zijn
Attribute	1	Moet aanwezig zijn
@Name	1	Vaste waarde: "autorisatieregel/context"
AttributeValue	1	URI waar de autorisatieregel/context gevonden kan worden waarbinnen het mandaat gegeven wordt.

N.B.: bovenstaande tabel bevat de meest gebruikte elementen van SAML assertions en is derhalve niet volledig. Voor niet genoemde elementen geldt: Niet gebruiken.

10.3.2.7.2.2 Namespaces

Het SAML mandaattoken maakt gebruik van de volgende namespaces. De prefixen zijn niet normatief maar worden in dit document als voorbeelden gebruikt.

Tabel AORTA.STK.t3300 – Namespaces

Prefix	Namespace URI
ds	http://www.w3.org/2000/09/xmldsig#
saml	urn:oasis:names:tc:SAML:2.0:assertion
wss	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd

	Bij het gebruik van de namespace-prefixes is het van belang deze na het ondertekenen niet meer te veranderen, dit maakt de digitale handtekening ongeldig.

10.3.2.7.2.3 Inhoud

De volgende paragrafen beschrijven de verschillende kenmerken en beveiligingsgerelateerde gegevens die het SAML mandaattoken onderscheiden, zoals in [IH tokens generiek] beschreven is.

```
<saml:Assertion ... xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
```

Het SAML mandaattoken begint met het Assertion element en een verwijzing naar de XML SAML namespace voor SAML 2.0 assertions. De attributen behorende bij het Assertion element wordt in [paragraaf 2.3.1](#)¹⁴⁴ Uniekheid beschreven.

Uniekheid

```
ID="token_2.16.528.1.1007.3.3.1234567.1_0123456789"

IssueInstant="2009-06-24T11:47:34Z"

Version="2.0">
```

De volgende attributen van het SAML assertion element maken van de SAML assertion een uniek gegeven, uitgegeven door de verzender van het bericht. Het attribuut ID identificeert op een unieke wijze de assertion. De assertion mag meerdere malen als token gebruikt worden. De waarde moet *mondiaal uniek* zijn voor AORTA berichten, zodat bij samenvoegen van meerdere XML bestanden (in een HL7v3 batch of anderszins) de waarde uniek blijft.

Het wordt aanbevolen een UUID (Universally Unique Identifier)[\[1\]](#) te gebruiken. Bij het gebruik van andere vormen is er een kans, hoe klein ook, dat een ID samenvalt met een ID gemaakt volgens een andere methode van een andere leverancier).

144. <https://vzvz.atlassian.net/wiki/spaces/A8/pages/85000374/Het+SAML+mandaattoken#HetSAMLmandaattoken-Uniekheid>



Een ID in XML mag niet met een cijfer beginnen. Bij het gebruik van een UUID is het dus aan te raden een prefix te gebruiken, welke met een letter of underscore ('_') begint.

[1] Zie het RfC4122 opgesteld door het IETF: A Universally Unique Identifier (UUID) URN Namespace

Het attribuut IssuedInstant is een tijdstip van uitgifte van de SAML assertion, in andere woorden: het tijdstip van ondertekening. De tijdswaarde is gecodeerd in UTC. Het attribuut Version is de gebruikte SAML versie van de SAML assertion. De aanduiding voor de versie van SAML gedefinieerd in deze specificatie is "2.0".

Afzender

```
<saml:Issuer>
  123456789:01.015
</saml:Issuer>
```

De Issuer verwijst naar de UZI van de zorgverlener/medewerker die het mandaat registreert (de mandaatgever) in combinatie met de rolcode van diezelfde zorgverlener/medewerker gescheiden door een dubbele punt (:).

Onderwerp

```
<saml:Subject>
  <saml:NameID>
    urn:IIroot:2.16.528.1.1007.3.3:IIext:12345678
  </saml:NameID>
  <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:sender-vouches">
  </saml:SubjectConfirmation>
</saml:Subject>
```

De Subject verwijst naar de organisatie waarbinnen het mandaat geldig is.

De URA wordt uitgedrukt met behulp van een URN (Uniform Resource Name). De URN is opgebouwd uit:

"urn:llroot:"<OID voor UZI organisatielids>":llex:"<URA>

De URN string is opgebouwd uit een llroot en een llex. "ll" staat voor het HL7v3 datatype Instance Identifier. Om de namespace in URN uniek te krijgen is ll als prefix voor de root en ext geplaatst.

URA's worden uitgedrukt als een id onder het identificatiesysteem "2.16.528.1.1007.3.3". De URA wordt toegekend door het UZI-register. Stel dat de URA de waarde "12345678" heeft, dan ziet de URN er als volgt uit:

urn:llroot:2.16.528.1.1007.3.3:llex:12345678

Vervolgens moet de SubjectConfirmation nog toegevoegd worden:

```
<saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:sender-vouches">
  </saml:SubjectConfirmation>
```

Geldigheid

```
<saml:Conditions
  NotBefore="2009-06-24T11:47:34Z"
  NotOnOrAfter="2009-09-24T11:47:34Z">
```

Het attribuut *NotBefore* is de tijd waarop de SAML assertion geldig wordt. Dit hoeft niet de tijd te zijn waarop het mandaat is aangemaakt. Het is mogelijk *NotBefore* in de toekomst te zetten. *NotBefore* moet altijd op of na de aanvang van de geldigheidsdatum van het certificaat (waarmee het mandaat is getekend) liggen.



Wordt een bericht met een mandaat ontvangen wordt voor *NotBefore* is aangevallen, dan **moet** dit bericht geweigerd worden.

Het attribuut *NotOnOrAfter* is de tijd waarop de SAML assertion vervalst. *NotOnOrAfter* moet altijd voor het verstrijken van de geldigheid van het certificaat (waarmee het mandaat is getekend) liggen.



Wordt een bericht met een mandaat ontvangen wordt op of nadat *NotOnOrAfter* is verstreken, dan **moet** dit bericht geweigerd worden.

Deze tijd is als bovenstaande tijd geformatteerd. Richtlijn voor het verschil tussen *NotBefore* en *NotOnOrAfter* is niet vastgesteld.



De geldigheidsduur van een mandaattoken (*NotOnOrAfter* minus *NotBefore*) kan nooit langer zijn dan de geldigheidsduur van het handtekeningcertificaat waarmee het token wordt getekend.

Indien het certificaat waarmee het mandaat is getekend op de CRL is geplaatst, dan dient het mandaattoken niet geweigerd te worden door het LSP. Het is op de CRL niet inzichtelijk om welke reden een certificaat op de CRL is geplaatst. Dit kunnen uiteenlopende redenen zijn zoals een verloren pas of een intrekking van een BIG-registratie. Om het zorgproces niet te frustreren wordt deze controle procesmatig opgepakt door Security Management.

Echter, bij het ondertekenen van het mandaattoken moet er een geldig certificaat gebruikt worden. Indien bij ondertekening van het mandaattoken het certificaat al op de CRL is geplaatst, dan dient het mandaattoken wel geweigerd te worden.



Indien het certificaat vóór ondertekening van het mandaattoken op de CRL is geplaatst, dan dient het mandaattoken geweigerd te worden door het LSP.



Indien het certificaat na ondertekening van het mandaattoken op de CRL is geplaatst, dan dient het mandaattoken niet geweigerd te worden.

Het inperken van bepaalde partijen (AudienceRestriction) waarvoor de assertion bedoeld is wordt beschreven in [paragraaf 2.3.5](#)¹⁴⁵ Ontvanger.

De subelementen OneTimeUse en ProxyRestriction worden niet gebruikt binnen het <Conditions> element bij het mandaattoken.

Ontvanger

In de AudienceRestriction wordt beschreven aan wie de SAML assertion is gericht. Aangezien het mandaattoken bedoeld is voor gebruik door een verzendende applicatie en bedoeld is om door de ZIM begrepen te worden, worden er binnen de AudienceRestriction twee Audience elementen opgenomen, één voor de ZIM en één voor de verzendende GBZ-applicatie.

Het applicatie-id binnen de AudienceRestriction wordt uitgedrukt met behulp van een URN (Uniform Resource Name). De URN is opgebouwd uit:

"urn:llroot:"<OID voor AORTA Applicatie-id's>":llex:"<applicatie-id GBZ>

De URN string is opgebouwd uit een llroot en een llex. "ll" staat voor het HL7v3 datatype Instance Identifier. Om de namespace in URN uniek te krijgen is ll als prefix voor de root en ext geplaatst.

AORTA Applicatie-id's worden uitgedrukt als een id onder het identificatiesysteem "2.16.840.1.113883.2.4.6.6". Het correcte applicatie-id voor het GBZ wordt toegekend bij aansluiting op de AORTA. Stel dat dit "300" zou zijn, dan ziet de URN er als volgt uit:

urn:llroot:2.16.840.1.113883.2.4.6.6:llex:300

De volledige AudienceRestriction wordt dan:

145. <https://vzvz.atlassian.net/wiki/spaces/A8/pages/85000374/Het+SAML+mandaattoken#HetSAMLmandaattoken-ontvanger>

```

<saml:AudienceRestriction>

  <!-- Root en extensie van de ZIM -->

  <saml:Audience>urn:IIroot:2.16.840.1.113883.2.4.6.6:IIext:1</saml:Audience>

  <!-- Root en extensie van de Applicatie -->

  <saml:Audience>urn:IIroot: 2.16.840.1.113883.2.4.6.6:IIext:300</saml:Audience>

</saml:AudienceRestriction>

```

Attributen

```

<saml:AttributeStatement>

```

Het volgende attribuut betreft aanvullende gegevens met betrekking tot het mandaat. Er mogen geen andere attributen opgenomen worden in het AttributeStatement dan hier beschreven is.

```

<saml:Attribute Name="autorisatieregel/context">

  <saml:AttributeValue>https://goedbeheerdziekenhuis/autorisatieregels/
medicatiecontext/v2</saml:AttributeValue>

</saml:Attribute>

```

Via de URI dient de lokale autorisatieregel en/of de context opgehaald te kunnen worden waarbinnen het mandaat is uitgegeven. In het voorbeeld is voor een URL gekozen.

Tenslotte wordt het attributen statement blok afgesloten met

```
</saml:AttributeStatement>
```

10.3.2.7.2.4 Algoritmes

Om de integriteit en onweerlegbaarheid van het SAML mandaattoken te waarborgen wordt een XML Signature geplaatst, zoals beschreven in [IH tokens generiek]. Na plaatsen van de XML Signature kan de ontvanger, met gebruikmaking van de publieke sleutel van het UZI handtekening-certificaat van de verzender onomstotelijk vaststellen dat de getekende SAML assertion ondertekend is met de privé sleutel behorend bij het gebruikte UZI handtekening-certificaat van de UZI-pas van de zorgverlener.

De publieke sleutel van het UZI handtekening-certificaat bevindt zich in de LDAP van het UZI-register.

De XML Signature van het SAML mandaattoken die gebruikt wordt bij berichtauthenticatie met behulp van de UZI-pas maakt gebruik van de volgende algoritmes, zoals beschreven in [IH tokens generiek]:

- Voor het berekenen van de hashwaarde wordt SHA-256 gebruikt.
- Voor de digitale handtekening in AORTA wordt gebruik gemaakt van een RSA handtekening over een SHA-256 digest.



Omdat de XML Signature onderdeel is van het SAML mandaattoken en in het SAML mandaattoken geplaatst wordt, moet er een "enveloped-signature" transformatie uitgevoerd worden die de Signature tags uit het SAML authenticatietoken verwijderd gevolgd door een "exc-c14n transformatie" (zie ook [SAML Core] §5.4.3 en §5.4.4).

10.3.2.7.2.5 Opbouw

De headers

Eerst wordt het SAML mandaattoken – het <saml:Assertion ...> element aangemaakt en gevuld met die elementen, zoals beschreven in [paragraaf 2.3](#)¹⁴⁶Inhoud.

146. <https://vzvz.atlassian.net/wiki/spaces/A8/pages/85000374/Het+SAML+mandaattoken#HetSAMLmandaattoken-Inhoud>

```

<saml:Assertion
  ID="token_2.16.528.1.1007.3.3.1234567.1_0123456789"
  IssueInstant="2009-06-24T11:47:34Z"
  Version="2.0"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
  ... Zie paragraaf 2.3 Inhoud ...
</saml:Assertion>

```

Het XML Signature blok is onderdeel van het SAML mandaattoken. Het XML Signature blok komt na het <saml:Issuer> element.

```

<saml:Assertion
  ID="token_2.16.528.1.1007.3.3.1234567.1_0123456789"
  IssueInstant="2009-06-24T11:47:34Z"
  Version="2.0"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
  <saml:Issuer>
    123456789:01.015
  </saml:Issuer>
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
      ...
    </ds:SignedInfo>
    <ds:SignatureValue>Wuwn...5e4=</ds:SignatureValue>
    <ds:KeyInfo>
      <ds:X509Data>

```



```

    <X509IssuerSerial>

      <X509IssuerName>CN=De Auteur CA,O=Nictiz,C=NL</X509IssuerName>

      <X509SerialNumber>359724...41160195</X509SerialNumber>

    </X509IssuerSerial>

  </ds:X509Data>

</ds:KeyInfo>

</ds:Signature> ...

... Zie paragraaf 2.3 Inhoud ...

</saml:Assertion>

```

Indien de Signature aangemaakt wordt mogen de strings (saml:Assertion en SignedInfo) inhoudelijk niet meer gewijzigd worden. Ze moeten octet-voor-octet overgenomen worden in het bericht. Strikt genomen is het toegestaan wijzigingen aan te brengen die door canonicalisatie bij de ontvanger weer opgeheven worden, maar wanneer de digitale handtekening door middel van strings wordt opgebouwd, is het een foutgevoelige handeling.

Lange Base 64 waarden zijn in het voorbeeld afgekort. Wederom kunnen dit als strings worden behandeld, waarbij drie waarden vervangen moeten worden.

Deze drie waarden worden ingevuld:

- Neem het SignedInfo blok op.
- Neem de SignatureValue op.
- Neem certificaatgegevens in het KeyInfo blok op.



Wanneer een bericht een SAML assertion bevat, moet dat bericht precies één bijbehorende digitale handtekening bevatten.



Voor mandaattokens mag er niet meer dan één SAML assertion voorkomen met de gegevens van een daarbij behorende X.509 certificaat als KeyInfo.

Het maken van de XML Signature uit strings levert de SAML assertion op met daarin de Signature.

Plaats van het SAML token en de digitale handtekening

Het SAML authenticatietoken met daarin de digitale handtekening wordt in het WS-Security SOAP Header gezet. Deze dient altijd te bestaan als aparte SAML-assertion naast het Transactietoken [IH Transactietoken].

Het mandaattoken dient tezamen met het transactietoken ([IH transactietoken]) in het zelfde security-element opgenomen te zijn conform de [IH tokens generiek] hoofdstuk 5.1.

10.3.2.7.3 Compliance

Bij het opstellen van dit document is onder andere gekeken naar de volgende specificaties:

IHE XUA

Binnen het Integrating the Healthcare Enterprise (IHE) Cross Enterprise User Authentication (XUA) profiel wordt in transactie ITI-40 Provide X-user Assertion de SAML-assertion beschreven.

Idensys

In het Nederlandse Afsprakenstelsel Elektronische Toegangsdiensten wordt binnen de interface specificatie tussen HerkenningsMakelaar en de Dienstverlener de Assertion van de Herkenningsmakelaar beschreven. Idensys maakt gebruik van vergelijkbare SAML elementen met uitzondering van het SubjectID welke, binnen Idensys, wordt weergegeven door een encryptedID.

10.3.2.7.4 Certificaten mandaattoken

10.3.2.7.4.1 Te gebruiken certificaat en attributen

Voor het tekenen van het Mandaattoken wordt het **handtekening**certificaat van de persoonlijke UZI-pas gebruikt. Dit certificaat bevat een RSA publieke sleutel. Met de privé sleutel wordt de digitale handtekening gegenereerd. Voor de technische context en het feitelijk genereren van de digitale handtekening met een UZI-pas wordt verwezen naar respectievelijk [Bijlage B \(see page 600\)](#) en [Bijlage C \(see page 604\)](#) uit het document IH Berichtauthenticatie met UZI-Pas [UZI berichttoken] met dien verstande dat in het mandaattoken dus het **handtekening**certificaat^[1] wordt gebruikt in plaats van het in de bijlagen vermelde authenticatiecertificaat.

Om de digitale handtekening bij de ZIM te verifiëren, moet de ontvanger over de bijbehorende publieke sleutel beschikken, zie [IH tokens generiek]. Voor verificatie is gekozen door een verwijzing naar het handtekeningcertificaat in het SAML mandaattoken als KeyInfo mee te zenden; de ontvanger moet deze dan met bijvoorbeeld het LDAP protocol ophalen, zie ook [IH tokens generiek].

^[1] Technisch dus het certificaat met keyUsage non-repudiation (0x40).

10.3.2.7.5 Token afhandeling mandaattoken

10.3.2.7.5.1 Verificatie van het mandaattoken

Het is belangrijk vast te stellen dat de velden in het SAML mandaattoken overeenstemmen met die in het transactietoken en geldig ondertekend zijn. Wanneer dit niet zou gebeuren, kan een kwaadwillende met een gestolen mandaattoken nog steeds gegevens opvragen.

Het SAML mandaattoken wordt door de ontvanger uit het transactietoken gehaald indien aanwezig. Bij gebruik van het SAML mandaattoken moet de ontvanger controleren of:

- De aanduiding voor de versie van SAML gedefinieerd is op "2.0", zie [Uniekheid \(see page 481\)](#) ;
- De URA, weergegeven door de NameID van het Subject, moet overeenkomen met de URA binnen het transactietoken en de URA uit het servercertificaat waarmee de TLS-verbinding is opgezet, zie [Onderwerp \(see page 482\)](#) ;
- Het bericht ontvangen is binnen de geldigheidsperiode van het token, zie [Geldigheid \(see page 483\)](#) ;
- De Assertion correct is ondertekend door de Signature te valideren met het gerefereerde handtekening certificaat.
- Het certificaat waarmee de ondertekening heeft plaatsgevonden geldig was ten tijde van de ondertekening.
- De juiste afzender (issuer) is vastgelegd die deze assertion heeft gecreëerd en ondertekend, zie [Afzender \(see page 482\)](#). De UZI en rolcode dienen overeen te komen met de bijbehorende waarden uit het UZI-certificaat van de mandaatgever. Die waarden dienen tevens overeen te komen met de Overseer in het HL7v3 bericht;
- De afnemers van het SAML mandaattoken (audience) de ZIM en de verzendende applicatie zijn, zie [Ontvanger \(see page 485\)](#) ;
- De als audience opgenomen applicatie moet geregistreerd zijn bij de URA uit het Subject.
- Alleen die attributen zijn gedefinieerd, die zijn beschreven in [Attributen \(see page 486\)](#);
- Indien Conditionele Query: de overseer in het HL7-bericht moet gelijk zijn aan het eerste gedeelte van de issuer (UZI) in het mandaattoken. Tevens dient het tweede gedeelte van de issuer (de rolcode) in het mandaattoken vergeleken te worden met de rolcode van de overseer in het HL7 bericht;

Het mandaattoken mag meerdere malen gebruikt worden. Het attribuut 'autorisatieregel/context' kan niet door de ZIM gecontroleerd worden maar dient wel in de log van de ZIM opgenomen te worden.

Als aan één van de bovenstaande condities niet is voldaan, moet het bericht door de ontvanger geweigerd worden en een SOAP foutmelding aan het verzendende systeem afgegeven worden, zie foutafhandeling in [IH tokens generiek].

Als wel aan alle condities is voldaan, wordt het HL7v3 bericht verder verwerkt.

10.3.2.7.6 Referenties mandaattoken

10.3.2.7.6.1 Bijlage A Referenties

Referentie	Document	Versie
[IH tokens generiek]	Implementatiehandleiding security tokens generiek (see page 435)	8.3.0.0
[IH transactietoken]	GBZ AORTA_Auth_IH_Berichtauthenticatie_Transactietoken (see page 399)	8.3.0.0
[SAMLAuthnContext]	Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0 http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf	2.0 15- mrt-2005
[SAML Core]	SAML v2.0 Core Specification https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf	2.0 15- mrt-2005
[SAML Profiles]	Profiles for the OASIS Security Assertion Markup Language (SAML) v2.0 http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf	2.0 15- mrt-2005
[SAML Token]	SAML Token Profile http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SAMLTOKENProfile.pdf	1.1 01- feb-2006
[UZI pas]	CA model, Pasmodel, Certificaat- en CRL-profielen, Agentschap CIBG www.uziregister.nl ¹⁴⁷	4.1 september 2010

10.3.2.8 GBZ AORTA_Auth_IH_Contracttoken

10.3.2.8.1 Inleiding contracttoken

10.3.2.8.1.1 Doel en scope

Dit document heeft tot doel een handleiding te geven voor de implementatie van het koppelvlak tussen twee partijen die onderling een contract willen afsluiten voor wat betreft de toe te passen technieken

¹⁴⁷ <http://www.uziregister.nl/>

voor de authenticatie van beide partijen. Partij A (de contractnemer) stuurt hierbij een request voor een concept-contracttoken naar partij B (de te contracteren partij). Partij B neemt gegevens over uit het request, stelt het concept contract op, ondertekend dit en stuurt het terug naar partij A. Partij A neemt het gehele concept contracttoken op in het uiteindelijke contracttoken, ondertekend dit en stuurt het contracttoken terug naar partij B. Met behulp van dit token mag partij B handelen namens partij A. Indien het Uitwisselsysteem een register van tokens bijhoudt dient partij A het contracttoken tevens naar dit register te sturen.

Dit document beschrijft zowel het concept-contracttoken als het (definitieve) contracttoken.

10.3.2.8.1.2 Doelgroep voor dit document

Dit document is bedoeld voor softwareontwikkelaars van goed beheerde zorgsystemen, en het LSP, die op grond van de toegelaten berichtstandaarden en op grond van dit document berichten willen uitrusten met het contracttoken.

Daarnaast wordt in dit document het plaatsen van de digitale handtekening besproken (zie ook [IH tokens generiek]).

10.3.2.8.1.3 Documenthistorie

Versie	Datum	Omschrijving
8.3.0.0	1 nov 2023	Initieel document.
8.3.0.0	9 nov 2023	OrganisatielD gewijzigd in Subject Distinguished Name

10.3.2.8.2 Het SAML contracttoken

10.3.2.8.2.1 Structuur

Het SAML concept-contracttoken is een afgegeven SAML assertion van partij B met betrekking tot het af te sluiten contract tussen beide partijen. Het concept-contracttoken wordt in zijn geheel Base64 geëncodeerd toegevoegd aan het contracttoken die gebruikt wordt bij berichtauthenticatie voor het landelijk EPD. Het SAML concept-contracttoken is ondertekend met behulp van het server-certificaat (UZI of EV/OV) van partij B. Het SAML contracttoken is ondertekend met behulp van het server-certificaat (UZI of EV/OV) van partij A. Het contracttoken is qua structuur en inhoud vrijwel identiek aan het concept-contracttoken. Enige verschillen zijn:

- De issuer van het concept-contracttoken is de Subject Distinguished Name van partij B; de issuer van het contracttoken is de Subject Distinguished Name van partij A.
- Het subject is de Subject Distinguished Name van de tegenpartij, dus: in het concept-contracttoken de Subject Distinguished Name van partij A; in het contracttoken de Subject Distinguished Name van partij B
- Het contracttoken bevat (optioneel) een attribuut `_CTR_locatie`
- Het contracttoken bevat een attribuut `_Concept-contract_token`
- Het contracttoken bevat een attribuut `_AC`

- Beide tokens bevatten een attribuut `_FQDN`. Hierin is de FQDN van de tegenpartij opgenomen.

Dientengevolge kan overal waar in de hiernavolgende tekst concept-contracttoken vermeld staat ook contracttoken gelezen worden tenzij in de paragraaf duidelijk onderscheid gemaakt wordt.

10.3.2.8.2.2 Het request

Het request is een simpel XML bericht aan de te contracteren organisatie en bevat de Subject Distinguished Name van de contractnemer.

Noot: alhoewel het geen authenticatieverzoek betreft is het wel een verzoek om een SAML assertion. Hiermee wordt dus afgeweken van het zuivere SAML protocol.

Voorbeeld request:

```
<samlp:AuthnRequest
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
ID="identifier_1"
Version="2.0"
IssueInstant="2004-12-05T09:21:59Z"
AssertionConsumerServiceIndex="1">
<saml:Issuer>https://sp.example.com/SAML2</saml:Issuer>
<samlp:NameIDPolicy
AllowCreate="true"
Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"/>
<samlp:Subject>
<value>
Subject Distinguished Name A
</value>
</samlp:Subject>
</samlp:AuthnRequest>
```

10.3.2.8.2.3 Assertion

De SAML assertion heeft de volgende structuur (de waarden die in het token gebruikt worden zijn fictief):

Element/@Attribute	0..1	Omschrijving
@ID	1	Unieke identificatie van de Assertion
@Version	1	Versie van het SAML Protocol. Vaste waarde moet zijn 2.0
@IssueInstant	1	Tijdstip van uitgifte van de Assertion.

Element/@Attribute	0..1	Omschrijving
Issuer	1	Concept-contracttoken: De Subject Distinguished Name van de te contracteren partij (partij B). Contracttoken: De Subject Distinguished Name van de contractnemer (partij A)
@NameQualifier	0	Niet gebruiken
@SPNameQualifier	0	Niet gebruiken
@Format	1	Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"
@SPProviderID	0	Niet gebruiken
Signature	1	Beide tokens kunnen ondertekend worden door zowel een UZI-servercertificaat als een EV/OV servercertificaat. Concept-contracttoken: Bevat de handtekening over de assertion zoals gezet met behulp van het servercertificaat van partij B. Contracttoken: Bevat de handtekening over de assertion zoals gezet met behulp van het servercertificaat van partij A.
Subject	1	Subject Distinguished Name van de tegenpartij: concept-cotracttoken: Subject Distinguished Name van partij A; contracttoken: Subject Distinguished Name van partij B.
BaseID	0	Niet gebruiken
NameID	1	Bevat de Subject Distinguished Name.
EncryptedID	0	Niet gebruiken
SubjectConfirmation	1	Moet aanwezig zijn.
@Method	1	'urn:oasis:names:tc:SAML:2.0:cm:sender-vouches'
SubjectConfirmationData	1	Bevat Keyinfo
@Recipient	0	Niet gebruiken
@NotOnOrAfter	0	Niet gebruiken

Element/@Attribute	0..1	Omschrijving
@InResponseTo	0	Niet gebruiken
@NotBefore	0	Niet gebruiken
@Address	0	Niet gebruiken
KeyInfo	1	Voor beide tokens: Bevat het publieke deel van het X509 servercertificaat
Conditions	1	Moet aanwezig zijn.
@NotBefore	1	Moet aanwezig zijn.
@NotOnOrAfter	1	Moet aanwezig zijn. Mag maximaal 10 jaar na @NotBefore liggen.
Condition	0	Niet gebruiken
AudienceRestriction	1	Moet aanwezig zijn
Audience	1..*	Minimaal 1 element: urn:llroot:2.16.840.1.113883.2.4.6.6:lltext:1 (is de ZIM). Voor het concept-contracttoken tevens de urn naar de contractnemer (partij A). Meerdere audiences zijn toegestaan.
ProxyRestriction	0	Niet gebruiken
Advice	0	Niet gebruiken
AuthnStatement	1	Moet aanwezig zijn
@AuthnInstant	1	Tijdstip van aanmaak.
@SessionIndex	0	Niet gebruiken
AuthnContext	1	Moet aanwezig zijn
AuthnContextClassRef	1	urn:oasis:names:tc:SAML:2.0:ac:classes:X509
AttributeStatement	1	Moet aanwezig zijn

Element/@Attribute	0..1	Omschrijving
Attribute	0..1	Optioneel aanwezig; alleen in contracttoken.
@Name	1	Vaste waarde: “_CTR_locatie”
AttributeValue	0..1	De URL naar het Contracttokenregister
Attribute	1	Moet aanwezig zijn alleen in contracttoken.
@Name	1	Vaste waarde: “_Concept-contract_token”
AttributeValue	1	Base64 representatie van het WID_token
Attribute	1	Moet aanwezig zijn alleen in contracttoken.
@Name	1	Vaste waarde: “_AC”
AttributeValue	1	Bevat een X.509 Attribute certificate
Attribute	1	Moet aanwezig zijn in beide tokens
@Name	1	Vaste waarde: “_Scope”
AttributeValue	1	Bevat de scope (dienst) van het contract

N.B.: bovenstaande tabel bevat de meest gebruikte elementen van SAML assertions en is derhalve niet volledig. Voor niet genoemde elementen geldt: Niet gebruiken.

10.3.2.8.2.4 Namespaces

Het SAML concept-contracttoken die gebruikt wordt bij berichtauthenticatie maakt gebruik van de volgende namespaces. De prefixen zijn niet normatief maar worden in dit document als voorbeelden gebruikt.

Tabel AORTA.STK.t3300 - Namespaces

Prefix	Namespace URI
ds	http://www.w3.org/2000/09/xmldsig#
saml	urn:oasis:names:tc:SAML:2.0:assertion

Prefix	Namespace URI
samlp	urn:oasis:names:tc:SAML:2.0:protocol
wss	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd



Bij het gebruik van de namespace-prefixes is het van belang deze na het ondertekenen niet meer te veranderen, dit maakt de digitale handtekening ongeldig.

10.3.2.8.2.5 Inhoud

De volgende paragrafen beschrijven de verschillende kenmerken en beveiligingsgerelateerde gegevens die het SAML (concept-)contracttoken onderscheiden, zoals in [IH tokens generiek] beschreven is.

```
<saml:Assertion ... xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
```

Het SAML (concept-)contracttoken begint met het Assertion element en een verwijzing naar de XML SAML namespace voor SAML 2.0 assertions. De attributen behorende bij het Assertion element wordt in paragraaf 2.4.1 Uniekheid beschreven.

Uniekheid

```
ID="token_dd1c1f96-f0b0-4026-a978-4d724c0a0a4f"
IssueInstant="2009-06-24T11:47:34Z"
Version="2.0">
```

De volgende attributen van het SAML assertion element maken van de SAML assertion een uniek gegeven, uitgegeven door de verzender van het bericht. Het attribuut ID identificeert op een unieke wijze de assertion. De waarde moet *mondiaal uniek* zijn voor alle berichten, zodat bij samenvoegen van meerdere XML bestanden (in een HL7v3 batch of anderszins) de waarde uniek blijft.

Het wordt aanbevolen een UUID (Universally Unique Identifier) te gebruiken. Bij het gebruik van andere vormen is er een kans, hoe klein ook, dat een ID samenvalt met een ID gemaakt volgens een andere methode van een andere leverancier).



Een ID in XML mag niet met een cijfer beginnen. Bij het gebruik van een UUID is het dus aan te raden een prefix te gebruiken, welke met een letter of underscore ('_') begint.

Het attribuut *IssuedInstant* is een tijdstipmoment van uitgifte van de SAML assertion. De tijdswaarde is gecodeerd in UTC. Het attribuut *Version* is de gebruikte SAML versie van de SAML assertion. De aanduiding voor de versie van SAML gedefinieerd in deze specificatie is "2.0".

Afzender

```
<saml:Issuer>
  <!-- De Issuer verwijst naar de organisatie die het token heeft gegenereerd.-->
    VOORBEELD ziekenhuis ABC
</saml:Issuer>
```

In de issuer dient de Subject Distinguished Name uit het servercertificaat waarmee het token is ondertekend overgenomen te worden.

Onderwerp

```
<saml:Subject>
  <saml:NameID>
    VOORBEELD Vendor XYZ
  </saml:NameID>
  <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:sender-vouches ">
  </saml:SubjectConfirmation>
</saml:Subject>
```

De **Subject** verwijst naar de door de organisatorische (tegen) partij waarmee het contract afgesloten wordt. Dus voor de contractnemer de te contracteren partij; voor de contractgever de contractnemer.

Vervolgens moet de SubjectConfirmation nog toegevoegd worden:

```
<saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:sender-vouches ">
</saml:SubjectConfirmation>
```

Geldigheid

```
<saml:Conditions
  NotBefore="2009-06-24T11:47:34Z"
  NotOnOrAfter="2010-12-24T11:47:34Z">
```

Het attribuut *NotBefore* is de tijd waarop de SAML assertion geldig wordt. *NotBefore* moet altijd op of na de aanvang van de geldigheidsdatum van het certificaat (waarmee het concept-contracttoken is getekend) liggen.

-  Wordt een bericht met een concept-contracttoken ontvangen voor *NotBefore* is aangevangen, dan **moet** dit bericht geweigerd worden.

Het attribuut *NotOnOrAfter* is de tijd waarop de SAML assertion vervalst. *NotOnOrAfter* mag na het verstrijken van de geldigheid van het certificaat (waarmee het concept-contracttoken is getekend) liggen.

-  Wordt een bericht met een concept-contracttoken ontvangen op of nadat *NotOnOrAfter* is verstreken, dan **moet** dit bericht geweigerd worden.

Deze tijd is als bovenstaande tijd geformatteerd. Het maximaal toegestane verschil tussen *NotBefore* en *NotOnOrAfter* is tien jaar.

-  De geldigheidsduur van een concept-contracttoken (*NotOnOrAfter* minus *NotBefore*) kan langer zijn dan de geldigheidsduur van het identiteitscertificaat waarmee het token wordt getekend.

Bij het ondertekenen van het concept-contracttoken moet er een geldig certificaat gebruikt worden. Indien bij ondertekening van het concept-contracttoken het certificaat al op de CRL is geplaatst, dan dient het concept-contracttoken wel geweigerd te worden.

-  Indien het certificaat vóór ondertekening van het concept-contracttoken op de CRL is geplaatst, dan dient het concept-contracttoken geweigerd te worden door het LSP.

-  Indien het certificaat na ondertekening van het concept-contracttoken op de CRL is geplaatst, dan dient het concept-contracttoken niet geweigerd te worden.

Het inperken van bepaalde partijen (*AudienceRestriction*) waarvoor de assertion bedoeld is wordt beschreven in paragraaf 2.4.5 Ontvanger.

Ontvanger

```
<saml:AudienceRestriction>
  <!-- Root en extensie van de ZIM -->
  <saml:Audience>urn:IIroot:2.16.840.1.113883.2.4.6.6:IIext:1</saml:Audience>
</saml:AudienceRestriction>
```

In de `AudienceRestriction` wordt beschreven aan wie de SAML assertion is gericht. In ieder geval dient de ZIM als audience voor te komen (`IIext:1`). Meerdere Audience elementen is toegestaan.

Voor de `<Audience>` parameter is gekozen voor URN. De URN string is opgebouwd uit een `IIroot` en een `IIext`. "II" staat voor het HL7v3 datatype Instance Identifier. Om de namespace in URN uniek te krijgen is II als prefix voor de root en ext geplaatst.

AORTA Applicatie-id's worden uitgedrukt als een id onder het identificatiesysteem "2.16.840.1.113883.2.4.6.6". Het correcte applicatie-id voor de GBZ-applicatie wordt toegekend bij aansluiting op de AORTA. Stel dat dit "300" zou zijn, dan ziet de URN er als volgt uit:

```
urn:IIroot:2.16.840.1.113883.2.4.6.6:IIext:300
```

Authenticatie

```
<saml:AuthnStatement
  AuthnInstant="2009-06-24T11:47:34"
  SessionIndex="token_2.16.528.1.1007.3.3.1234567.1_0123456789">
```

Het subject, de contactpartij binnen het contract, in de SAML assertion is geauthenticeerd door middel van het X509 servercertificaat van de betreffende organisatie.

```
<saml:AuthnContext>
  <saml:AuthnContextClassRef
>urn:oasis:names:tc:SAML:2.0:ac:classes:X509</saml:AuthnContextClassRef>
</saml:AuthnContext>

</saml:AuthnStatement>
```

Afsluiting authentication statement.

Attributen

```
<saml:AttributeStatement>
```

De volgorde van de attributen in het `AttributeStatement` is niet relevant. Er mogen geen andere attributen opgenomen worden in het `AttributeStatement` dan hier beschreven is.

_CTR_locatie (optioneel, alleen in contracttoken)

```
<saml:Attribute Name="_CTR_locatie">
  <saml:AttributeValue>
```

```

    http://aorta-zorg.nl/contractregister
  </saml:AttributeValue>
</saml:Attribute>

```

Het attribuut `_CTR_locatie` geeft de locatie aan van een contractregister aan indien het uitwisselsysteem van zo een register gebruikt maakt. Binnen AORTA is dit:

```
http://aorta-zorg.nl/contractregister
```

Het attribuut is optioneel en dient alleen voor te komen in het contracttoken.

`_Concept-contract_token` (alleen in contracttoken)

```

<saml:Attribute Name="_Concept-contract_token">
  <saml:AttributeValue>
    Base64 representatie van het WID_token
  </saml:AttributeValue>
</saml:Attribute>

```

Het attribuut `WID_token` bevat de gehele SAML assertion van het concept-contract Base64 geëncodeerd.

`_FQDN` (beide tokens)

```

<saml:Attribute Name="_FQDN">
  <saml:AttributeValue>
    FQDN uit servercertificaat
  </saml:AttributeValue>
</saml:Attribute>

```

Het attribuut `_FQDN` bevat de FQDN uit het servercertificaat waarmee het token is ondertekend, dus van de issuer.

`_Scope` (beide tokens)

```

<saml:Attribute Name="_Scope">
  <saml:AttributeValue>
    urn:IIroot:2.16.840.1.113883.2.4.6.10:IIext:"<code>"
  </saml:AttributeValue>
</saml:Attribute>

```

Het attribuut `_Scope` bevat de code van de dienst waar het contract betrekking op heeft.

De lijst met diensten en bijbehorende codes wordt gemeenschappelijk bijgehouden en aangevuld.

De in het voorbeeld genoemde OID (2.16.840.1.113883.2.4.6.10) is fictief en dient nog nader vastgesteld te worden.

_AC (alleen in contracttoken)

```
<saml:Attribute Name="_AC">
  <saml:AttributeValue>
    Attribute certificate
  </saml:AttributeValue>
</saml:Attribute>
```

Het attribuut _AC bevat een, door de contractnemer gegenereerd, X.509 certificate een AttributeCertificate (AC)

Een AC heeft geen eigen sleutelpaar maar wordt ondertekend met het private certificate van de uitgever ervan. Bij wijze van trust wordt verwacht dat een AC-verifier de publieke sleutel heeft bijvoorbeeld door die eenmalig uit te wisselen.

Standaard attributen van een AC zijn:

- Version = v2
- Holder: De FQDN van de gecontracteerde
- Issuer: het issuerserial van de uitgever van het AC meer concreet: de issuerserial van het UZI-servercertificaat van de zorgverlener. Met dit certificaat moet het AC ondertekend worden. Indien geen UZI-partij, dan dient het publieke deel van het EV/OV servcertificaat eenmalig uitgewisseld te worden.
- Serialnumber: Uniek nummer gegenereerd door de uitgever (issuer)
- Validity period: Voorlopig vaststellen op 10 jaar?
- CRL: locatie waar de Certificate Revocation List gevonden kan worden
- De signature

Het certificaat waarmee het AC ondertekend is dient geldig te zijn (geweest) ten tijde van de ondertekening.

Het contract kan opgezegd worden door het AttributeCertificate op de CRL te plaatsen.

Tenslotte wordt het attributen statement blok afgesloten met

```
</saml:AttributeStatement>
```

attributeStatement blok

Het attributen statement blok ziet er dan bijvoorbeeld zo uit (de volgorde van de attributen is niet relevant):

```
<saml:AttributeStatement>
<saml:Attribute Name="_CTR_locatie">
  <saml:AttributeValue>
    http://aorta-zorg.nl/contractregister
  </saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="_Concept-contract_token">
  <saml:AttributeValue>
    Base64 representatie van het WID_token
  </saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="_FQDN">
  <saml:AttributeValue>
    FQDN uit servercertificaat
  </saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="_Scope">
  <saml:AttributeValue>
    urn:IIroot:2.16.840.1.113883.2.4.6.10:IIext:"<code>"
  </saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="_AC">
  <saml:AttributeValue>
    Attribute certificate
  </saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

10.3.2.8.2.6 Algoritmes

Om de integriteit en onweerlegbaarheid van het SAML concept-contracttoken te waarborgen wordt een XML Signature geplaatst, zoals beschreven in [IH tokens generiek]. Na plaatsen van de XML Signature kan de ontvanger, met gebruikmaking van het publieke deel van het servercertificaat, onomstotelijk vaststellen dat het SAML concept-contracttoken ondertekend is met de privé sleutel behorend bij het gebruikte servercertificaat van de te contracteren organisatie en dat het contracttoken ondertekend is met de privé sleutel van het servercertificaat van de contractnemer.

De XML Signature van het SAML concept-contracttoken die gebruikt wordt bij berichtauthenticatie met behulp van het identiteitscertificaat maakt gebruik van de volgende algoritmes, zoals beschreven in [IH tokens generiek]:

- Voor het berekenen van de hashwaarde wordt SHA-256 gebruikt.
- Voor de digitale handtekening in AORTA wordt gebruik gemaakt van een RSA handtekening over een SHA-256 digest.



Omdat de XML Signature onderdeel is van het SAML concept-contracttoken en in het SAML concept-contracttoken geplaatst wordt, moet er een "enveloped-signature" transformatie uitgevoerd worden die de Signature tags uit het SAML concept-contracttoken verwijderd gevolgd door een "exc-c14n transformatie" (zie ook [SAML Core] §5.4.3 en §5.4.4).

10.3.2.8.2.7 Opbouw

De headers

Eerst wordt het SAML concept-contracttoken – het `<saml:Assertion ...>` element aangemaakt en gevuld met die elementen, zoals beschreven in paragraaf 2.4 Inhoud.

```
<saml:Assertion
  ID="token_2.16.528.1.1007.3.3.1234567.1_0123456789"
  IssueInstant="2009-06-24T11:47:34Z"
  Version="2.0"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
... Zie paragraaf 2.4 Inhoud ...
</saml:Assertion>
```

Het XML Signature blok is onderdeel van het SAML concept-contracttoken. Het XML Signature blok komt na het `<saml:Issuer>` element. Na de Signature volgt de rest van de inhoud van de assertion.

```
<saml:Assertion
  ID="token_2.16.528.1.1007.3.3.1234567.1_0123456789"
  IssueInstant="2009-06-24T11:47:34Z"
  Version="2.0"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
<saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
  Subject Distinguished Name
</saml:Issuer>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:SignedInfo>
    ...
  </ds:SignedInfo>
  <ds:SignatureValue>Wuwn...5e4=</ds:SignatureValue>
  <ds:KeyInfo>
    <wss:SecurityTokenReference>
      <ds:X509Data>
        ...
      </ds:X509Data>
    <wss:SecurityTokenReference>
      </ds:KeyInfo>
  </ds:Signature> ...
... Zie paragraaf 2.3 Inhoud ...
</saml:Assertion>
```

Indien de Signature aangemaakt wordt moet niet meer met de strings (saml:Assertion en SignedInfo) gemanipuleerd worden, maar ze moeten octet-voor-octet overgenomen worden in het bericht. Strikt genomen is het toegestaan wijzigingen aan te brengen die door canonicalisatie bij de ontvanger weer opgeheven worden, maar wanneer de digitale handtekening door middel van strings wordt opgebouwd, is het een foutgevoelige handeling.

Lange Base 64 waarden zijn afgekort. Wederom kan dit als strings worden behandeld, waarbij drie waarden vervangen moeten worden.

Deze drie waarden worden ingevuld:

- Neem het SignedInfo blok op.
- Neem de SignatureValue op.
- Neem certificaatgegevens in het KeyInfo blok op, in de vorm van het volledige publieke certificaat (in het concept-contracttoken het servercertificaat van de te contracteren partij; in het contracttoken het servercertificaat van de contractnemer).



Wanneer een bericht een SAML assertion bevat, moet dat bericht precies één bijbehorende digitale handtekening bevatten.

Het maken van de XML Signature uit strings levert de SAML assertion op met daarin de Signature.

Plaats van het SAML token en de digitale handtekening

Het SAML concept-contracttoken met daarin de digitale handtekening wordt Base64-geëncodeerd in het attribuut “_Concept-contract_token” van het contracttoken gezet.

Het gehele contracttoken wordt ondertekend met het servercertificaat van de contractnemer.

10.3.2.8.3 Token afhandeling contracttoken

10.3.2.8.3.1 Verificatie van het bericht

Het is belangrijk vast te stellen dat de velden in het SAML concept-contracttoken en het SAML contracttoken een correcte waarde hebben en geldig ondertekend zijn. Wanneer dit niet zou gebeuren, kan een kwaadwillende met een gestolen token nog steeds gegevens opvragen van bv. ieder willekeurig burger servicenummer (BSN).

Controles op het concept-contracttoken

Het SAML concept-contracttoken wordt door de ontvanger uit het betreffende attribuut van het contracttoken gehaald, Base64 gedecodeerd en vervolgens gevalideerd.

Bij de validatie van het SAML concept-contracttoken moet de ontvanger controleren of:

- De aanduiding voor de versie van SAML gedefinieerd is op "2.0", zie paragraaf 2.4.1 Uniekheid;
- De juiste Subject Distinguished Name is opgenomen die deze assertion heeft gecreëerd en de gebruiker heeft geauthenticeerd, zie paragraaf 2.4.2 Afzender. De Subject Distinguished Name dient overeen te komen met de Subject Distinguished Name uit het servercertificaat.

- De Assertion correct is ondertekend door de Signature te valideren met het meegestuurde certificaat.
- Het gebruikte certificaat waarmee de ondertekening heeft plaatsgevonden geldig was ten tijde van de ondertekening.
- Indien het certificaat op de CRL is geplaatst, dan dient dit plaats te hebben gevonden nadat het token gegenereerd en ondertekend is.
- De relevante certificaatketen te valideren op geldigheid.
- De geldigheidsperiode van het token, zie paragraaf 2.4.4 Geldigheid, niet langer is dan 10 jaar;
- Het bericht ontvangen is binnen de geldigheidsperiode van het token, zie paragraaf 2.4.4 Geldigheid;
- De afnemer van het SAML concept-contracttoken (audience) minimaal de ZIM is, zie paragraaf 2.4.5 Ontvanger;
- Alleen die attributen zijn gedefinieerd, die zijn beschreven in paragraaf 2.4.7 Attributen;

Het tokenID dient in de log van de ZIM opgenomen te worden.

Controles op het contracttoken

Het SAML contracttoken wordt door de ontvanger gevalideerd.

Bij de validatie van het SAML contracttoken moet de ontvanger controleren of:

- De aanduiding voor de versie van SAML gedefinieerd is op "2.0", zie paragraaf 2.4.1 Uniekheid;
- De juiste Subject Distinguished Name is opgenomen die deze assertion heeft gecreëerd en de gebruiker heeft geauthenticeerd, zie paragraaf 2.4.2 Afzender. De Subject Distinguished Name dient overeen te komen met de Subject Distinguished Name uit het servercertificaat.
- De Assertion correct is ondertekend door de Signature te valideren met het meegestuurde certificaat.
- Het gebruikte certificaat waarmee de ondertekening heeft plaatsgevonden geldig was ten tijde van de ondertekening.
- Indien het certificaat op de CRL is geplaatst, dan dient dit plaats te hebben gevonden nadat het token gegenereerd en ondertekend is.
- De relevante certificaatketen te valideren op geldigheid.
- De geldigheidsperiode van het token, zie paragraaf 2.4.4 Geldigheid, niet langer is dan 10 jaar;
- Het bericht ontvangen is binnen de geldigheidsperiode van het token, zie paragraaf 2.4.4 Geldigheid;
- De afnemer van het SAML concept-contracttoken (audience) minimaal de ZIM is, zie paragraaf 2.4.5 Ontvanger;
- Alleen die attributen zijn gedefinieerd, die zijn beschreven in paragraaf 2.4.7 Attributen;
- Het AttributeCertificate geldig is, de bijbehorende CRL opgehaald kan worden en het AC niet op deze CRL staat.

Het tokenID dient in de log van de ZIM opgenomen te worden.

Controles tussen concept-contract token en contracttoken

Om te controleren dat het concept-contracttoken en het contracttoken daadwerkelijk bij elkaar horen dienen de volgende controles uitgevoerd te worden:

- De issuer uit het concept-contracttoken komt overeen met het subject van het contracttoken
- De issuer uit het contracttoken komt overeen met het subject van het concept-contracttoken
- De _Scope in beide tokens is identiek

Als aan één van de bovenstaande condities niet is voldaan, moet het contracttoken door de ontvanger geweigerd worden en een SOAP foutmelding aan het verzendende systeem afgegeven worden, zie foutafhandeling in [IH tokens generiek].

10.3.2.8.4 Referenties contracttoken

10.3.2.8.4.1 Bijlage A Referenties

Referentie	Document	Versie
[IH tokens generiek]	AORTA_Auth_IH_Security_tokens_generiek	8.2.0.0
[Inschrijftoken]	AORTA_Auth_IH_ Inschrijftoken	8.2.0.0
[SAMLAuthnContext]	Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0 http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf	2.0 15-mrt-2005
[SAML Core]	SAML v2.0 Core Specification https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf	2.0 15-mrt-2005
[SAML Profiles]	Profiles for the OASIS Security Assertion Markup Language (SAML) v2.0 http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf	2.0 15-mrt-2005
[SAML Token]	SAML Token Profile http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SAMLSAMLTokenProfile.pdf	1.1 01-feb-2006

10.3.2.9 ZORG-ID AORTA_Auth_IH_Scantoken_en_WID_token

- **IH Scantoken en WID token**

Datum: 1 Mei 2022

Publicatie: v8.3.0.0

10.3.2.9.1 Inleiding Scan en WID token

10.3.2.9.1.1 Doel en scope

Dit document heeft tot doel een handleiding te geven voor de implementatie van het koppelvlak tussen het Goed Beheerd Zorgsysteem (GBZ), ZORG-ID en het landelijk schakelpunt (LSP) voor wat betreft de toe te passen technieken voor de authenticatie van zorgverleners, medewerkers en burgers (patiënten).

10.3.2.9.1.2 Doelgroep voor dit document

Dit document is bedoeld voor softwareontwikkelaars van goed beheerde zorgsystemen, ZORG-ID en het LSP, die op grond van de toegelaten berichtstandaarden en op grond van dit document berichten willen uitrusten met het SAML scantoken. Het SAML scantoken is met name toepasbaar bij gebruik van de ZORG-ID app.

Daarnaast wordt in dit document het plaatsen van de digitale handtekening besproken (zie ook [IH tokens generiek]).

10.3.2.9.1.3 Documenthistorie

Versie	Datum	Omschrijving
8.3.0.0	11-november-2021	Initieel document.
8.3.0.0	09-februari-2022	Tekst bij figuur 1 aangepast
8.3.0.0	11-februari-2022	Enkele kleine tekstuele wijzigingen
8.3.0.0	31 maart 2022	Structuur wid_raw_data toegevoegd,

10.3.2.9.2 Het SAML Scan en WID token

In dit hoofdstuk wordt de inhoud van het SAML scantoken besproken. Het SAML scantoken bevat een geverifieerd BSN en is ondertekend door een zorgverlener/medewerker. Het SAML scantoken is een op XML gebaseerde SAML assertion en heeft tot doel de *assertions* (bewijs van een bewering) over te brengen tussen partijen.

Alle XML voorbeelden in het document dienen door de betrokken partijen tijdens het bouwen van de uitwisseling getest, en waar nodig, in samenspraak met VZVZ aangepast te worden voor een juiste optimale werking.

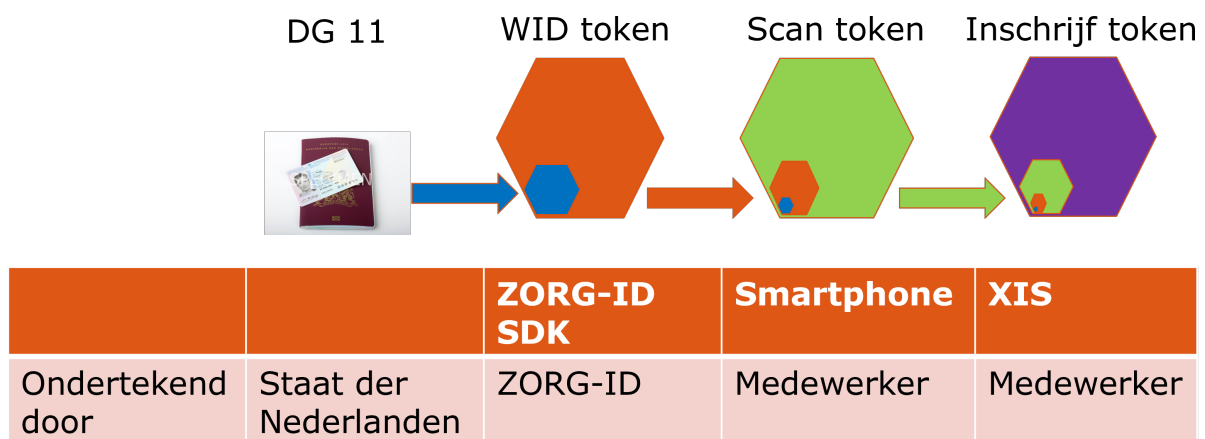
10.3.2.9.2.1 Structuur

Het SAML scantoken is een afgegeven SAML assertion met betrekking tot het, uit de chip van een ingescand Wettelijk Identificatie Document (WID) uitgelezen, BSN. Het scantoken wordt in zijn geheel Base64 geëncodeerd toegevoegd aan het inschrijftoken die gebruikt wordt bij berichtauthenticatie voor het landelijk EPD. Het SAML scantoken is ondertekend met behulp van het door ZORG-ID uitgegeven identiteitscertificaat van een zorgverlener/medewerker.

Het scantoken bevat op haar beurt een Base64 geëncodeerd attribuut waarin zich het WID_token bevindt. Het WID_token is de waarborg dat de WID data zijn verkregen middels ZORG-ID. Het WID token is qua structuur en inhoud vrijwel identiek aan het scantoken. Enige verschillen zijn:

- Het WID_token is ondertekend met het ZID servercertificaat
- Het WID_token heeft een extra attribuut met de Base64 geëncodeerde WID_raw_data

Dientengevolge kan overal waar in de hiernavolgende tekst 'scantoken' vermeld staat ook WID_token gelezen worden tenzij in de paragraaf duidelijk onderscheid tussen beide tokens gemaakt wordt.



Figuur 1 Structuur, Uitleg zie tekst

Figuur 1 representeert de uiteindelijke structuur. De door de scan uitgelezen datagroep 11, ondertekend door de staat der Nederlanden, wordt toegevoegd aan het WID token. Het WID token wordt ondertekend met ZORG-ID servercertificaat en toegevoegd aan het Scantoken. Het Scantoken wordt ondertekend met het identiteitscertificaat van de medewerker die de scan heeft gedaan en toegevoegd aan het inschrijftoken. Het Inschrijftoken wordt eveneens ondertekend met een ZORG-ID identiteitscertificaat.

Er wordt gebruik gemaakt van SAML v2.0 [SAML Core].

10.3.2.9.2.2 Assertion

De assertion heeft de volgende structuur (de waarden die in het token gebruikt worden zijn fictief):

Element/ @Attribute	0.. 1	Omschrijving
@ID	1	Unieke identificatie van de Assertion
@Version	1	Versie van het SAML Protocol. Vaste waarde moet zijn 2.0
@IssueInstant	1	Tijdstip van uitgifte van de Assertion.
Issuer	1	De URA van de organisatie waarbinnen de medewerker die de scan uitvoert werkzaam is.

Element/ @Attribute	0.. 1	Omschrijving
@NameQualifier	0	Niet gebruiken
@SPNameQualif ier	0	Niet gebruiken
@Format	1	Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"
@SPProviderID	0	Niet gebruiken
Signature	1	Scantoken: Bevat de handtekening over de assertion zoals gezet met behulp van het door Zorg-ID aangemaakte identiteitscertificaat van de medewerker die de scan uitvoert. WID_token: Bevat de handtekening over de assertion zoals gezet met behulp van het Zorg-ID servercertificaat.
Subject	1	BSN van de patient waarvan de BSN gevalideerd is.
BaseID	0	Niet gebruiken
NameID	1	Bevat de gevalideerde BSN.
EncryptedID	0	Niet gebruiken
SubjectConfirma tion	1	Moet aanwezig zijn.
@Method	1	'urn:oasis:names:tc:SAML:2.0:cm:sender-vouches'
SubjectConfirma tionData	1	Bevat Keyinfo
@Recipient	0	Niet gebruiken

Element/ @Attribute	0.. 1	Omschrijving
@NotOnOrAfter	0	Niet gebruiken
@InResponseTo	0	Niet gebruiken
@NotBefore	0	Niet gebruiken
@Address	0	Niet gebruiken
KeyInfo	1	Scantoken: Bevat het publieke deel van het X509 identiteitscertificaat WID token: Bevat het publieke deel van het ZORG-ID servercertificaat
Conditions	1	Moet aanwezig zijn.
@NotBefore	1	Moet aanwezig zijn.
@NotOnOrAfter	1	Moet aanwezig zijn. Mag maximaal 10 jaar na @NotBefore liggen.
Condition	0	Niet gebruiken
AudienceRestriction	1	Moet aanwezig zijn
Audience	1.. *	Minimaal 1 element: urn:llroot:2.16.840.1.113883.2.4.6.6:lltext:1 (is de ZIM). Meerdere audiences zijn toegestaan.
ProxyRestriction	0	Niet gebruiken
Advice	0	Niet gebruiken
AuthnStatement	1	Moet aanwezig zijn
@AuthnInstant	1	Tijdstip van BSN scan.

Element/ @Attribute	0.. 1	Omschrijving
@SessionIndex	0	Niet gebruiken
AuthnContext	1	Moet aanwezig zijn
AuthnContextClassRef	1	urn:oasis:names:tc:SAML:2.0:ac:classes:X509
AttributeStatement	1	Moet aanwezig zijn
Attribute	1	Moet aanwezig zijn.
@Name	1	Vaste waarde: "Zorgaanbieder"
AttributeValue	1	De URA van de zorgaanbieder waar de zorgverlener of medewerker in dienst is.
Attribute	1	Moet aanwezig zijn alleen in Scantoken.
@Name	1	Vaste waarde: "WID_token"
AttributeValue	1	Base64 representatie van het WID_token
Attribute	1	Moet aanwezig zijn alleen in het WID_token.
@Name	1	Vaste waarde: "WID_raw_data"
AttributeValue	1	Base64 representatie van de ingescande datagroep 11 van de chip van het WID inclusief het Document Security Object.

N.B.: bovenstaande tabel bevat de meest gebruikte elementen van SAML assertions en is derhalve niet volledig. Voor niet genoemde elementen geldt: Niet gebruiken.

10.3.2.9.2.3 Namespaces

Het SAML scantoken die gebruikt wordt bij berichtauthenticatie maakt gebruik van de volgende namespaces. De prefixen zijn niet normatief maar worden in dit document als voorbeelden gebruikt.

Tabel AORTA.STK.t3300 – Namespaces

Prefix	Namespace URI
ds	http://www.w3.org/2000/09/xmldsig#
saml	urn:oasis:names:tc:SAML:2.0:assertion
wss	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd



Bij het gebruik van de namespace-prefixes is het van belang deze na het ondertekenen niet meer te veranderen, dit maakt de digitale handtekening ongeldig.

10.3.2.9.2.4 Inhoud

De volgende paragrafen beschrijven de verschillende kenmerken en beveiligingsgerelateerde gegevens die het SAML scantoken onderscheiden, zoals in [IH tokens generiek] beschreven is.

```
<saml:Assertion ... xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
```

Het SAML scantoken begint met het Assertion element en een verwijzing naar de XML SAML namespace voor SAML 2.0 assertions. De attributen behorende bij het Assertion element wordt in [paragraaf 2.4.1](#)¹⁴⁸ Uniekheid beschreven.

Uniekheid

```
ID="token_dd1c1f96-f0b0-4026-a978-4d724c0a0a4f"
```

```
IssueInstant="2009-06-24T11:47:34Z"
```

148. <https://vzvz.atlassian.net/wiki/spaces/AORTA84/pages/879593947/Het+SAML+Scan+en+WID+token#HetSAMLScanenWIDtoken-Uniekheid>

```
Version="2.0">
```

De volgende attributen van het SAML assertion element maken van de SAML assertion een uniek gegeven, uitgegeven door de verzender van het bericht. Het attribuut ID identificeert op een unieke wijze de assertion. De waarde moet *mondiaal uniek* zijn voor AORTA berichten, zodat bij samenvoegen van meerdere XML bestanden (in een HL7v3 batch of anderszins) de waarde uniek blijft.

Het wordt aanbevolen een UUID (Universally Unique Identifier) te gebruiken. Bij het gebruik van andere vormen is er een kans, hoe klein ook, dat een ID samenvalt met een ID gemaakt volgens een andere methode van een andere leverancier).



Een ID in XML mag niet met een cijfer beginnen. Bij het gebruik van een UUID is het dus aan te raden een prefix te gebruiken, welke met een letter of underscore ('_') begint.

Het attribuut IssueInstant is een tijdstipmoment van uitgifte van de SAML assertion. De tijdswaarde is gecodeerd in UTC. Het attribuut Version is de gebruikte SAML versie van de SAML assertion. De aanduiding voor de versie van SAML gedefinieerd in deze specificatie is "2.0".

Afzender

```
<saml:Issuer>

  <!-- De Issuer verwijst naar de organisatie waarbinnen de BSN validatie heeft plaats
  gevonden.-->

  urn:IIroot:2.16.528.1.1007.3.3:IItext:12345678

</saml:Issuer>
```

De URA wordt uitgedrukt met behulp van een URN (Uniform Resource Name). De URN is opgebouwd uit:

"urn:llroot:"<OID voor UZI organisatielids>":llex:"<URA>

De URN string is opgebouwd uit een llroot en een llex. "ll" staat voor het HL7v3 datatype Instance Identifier. Om de namespace in URN uniek te krijgen is ll als prefix voor de root en ext geplaatst.

URA's worden uitgedrukt als een id onder het identificatiesysteem "2.16.528.1.1007.3.3". De URA wordt toegekend door het UZI-register. Stel dat de URA de waarde "12345678" heeft, dan ziet de URN er als volgt uit:

urn:llroot:2.16.528.1.1007.3.3:llex:12345678

Onderwerp

```
<saml:Subject>
  <saml:NameID>
    950052413
  </saml:NameID>
  <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:sender-vouches ">
  </saml:SubjectConfirmation>
</saml:Subject>
```

De Subject verwijst naar de door de zorgverlener/medewerker gevalideerde BSN. De BSN validatie dient plaatsgevonden te hebben door:

- inlezen van de chip uit het WID waarbij:
- De echtheid van het WID wordt gecontroleerd
- De BSN wordt uitgelezen uit de chip of, bij paspoorten uitgegeven na 1 augustus 2021, de BSN QR code wordt gelezen.

Vervolgens moet de SubjectConfirmation nog toegevoegd worden:

```
<saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:sender-vouches">

</saml:SubjectConfirmation>
```

Geldigheid

```
<saml:Conditions

  NotBefore="2009-06-24T11:47:34Z"

  NotOnOrAfter="2010-12-24T11:47:34Z">
```

Het attribuut *NotBefore* is de tijd waarop de SAML assertion geldig wordt. *NotBefore* moet altijd op of na de aanvang van de geldigheidsdatum van het certificaat (waarmee het scantoken is getekend) liggen.



Wordt een bericht met een scantoken ontvangen voor *NotBefore* is aangevallen, dan **moet** dit bericht geweigerd worden.

Het attribuut *NotOnOrAfter* is de tijd waarop de SAML assertion vervalst. *NotOnOrAfter* mag na het verstrijken van de geldigheid van het certificaat (waarmee het scantoken is getekend) liggen.



Wordt een bericht met een scantoken ontvangen op of nadat *NotOnOrAfter* is verstreken, dan **moet** dit bericht geweigerd worden.

Deze tijd is als bovenstaande tijd geformatteerd. Het maximaal toegestane verschil tussen *NotBefore* en *NotOnOrAfter* is tien jaar.



De geldigheidsduur van een scantoken (*NotOnOrAfter* minus *NotBefore*) kan langer zijn dan de geldigheidsduur van het identiteitscertificaat waarmee het token wordt getekend.

Indien het certificaat waarmee het scantoken is getekend op de CRL is geplaatst, dan dient het scantoken niet geweigerd te worden door het LSP. Het is op de CRL niet inzichtelijk om welke reden een certificaat op de CRL is geplaatst. Dit kunnen uiteenlopende redenen zijn zoals een verloren telefoon. Om het zorgproces niet te frustreren wordt deze controle procesmatig opgepakt door Security Management.

Echter, bij het ondertekenen van het scantoken moet er een geldig certificaat gebruikt worden. Indien bij ondertekening van het scantoken het certificaat al op de CRL is geplaatst, dan dient het scantoken wel geweigerd te worden.



Indien het certificaat vóór ondertekening van het scantoken op de CRL is geplaatst, dan dient het scantoken geweigerd te worden door het LSP.



Indien het certificaat na ondertekening van het scantoken op de CRL is geplaatst, dan dient het scantoken niet geweigerd te worden.

Het inperken van bepaalde partijen (AudienceRestriction) waarvoor de assertion bedoeld is wordt beschreven in [paragraaf 2.4.5](#)¹⁴⁹ Ontvanger.

Ontvanger

```
<saml:AudienceRestriction>

  <!-- Root en extensie van de ZIM -->

  <saml:Audience>urn:IIroot:2.16.840.1.113883.2.4.6.6:IIext:1</saml:Audience>
```

149. <https://vzvz.atlassian.net/wiki/spaces/AORTA84/pages/879593947/Het+SAML+Scan+en+WID+token#HetSAMLScanenWIDtoken-Ontvanger>

```
</saml:AudienceRestriction>
```

In de AudienceRestriction wordt beschreven aan wie de SAML assertion is gericht. In ieder geval dient de ZIM als audience voor te komen (llex:1). Meerdere Audience elementen is toegestaan.

Voor de <Audience> parameter is gekozen voor URN. De URN string is opgebouwd uit een llroot en een llex. "ll" staat voor het HL7v3 datatype Instance Identifier. Om de namespace in URN uniek te krijgen is ll als prefix voor de root en ext geplaatst.

AORTA Applicatie-id's worden uitgedrukt als een id onder het identificatiesysteem "2.16.840.1.113883.2.4.6.6". Het correcte applicatie-id voor de GBZ-applicatie wordt toegekend bij aansluiting op de AORTA. Stel dat dit "300" zou zijn, dan ziet de URN er als volgt uit:

```
urn:llroot:2.16.840.1.113883.2.4.6.6:llex:300
```

Authenticatie

```
<saml:AuthnStatement
  AuthnInstant="2009-06-24T11:47:34"
  SessionIndex="token_2.16.528.1.1007.3.3.1234567.1_0123456789">
```

Het subject, de gevalideerde BSN, in de SAML assertion is geauthenticeerd door middel van het X509 identiteitscertificaat van de uitvoerende zorgverlener/medewerker.

```
<saml:AuthnContext>
  <saml:AuthnContextClassRef
    >urn:oasis:names:tc:SAML:2.0:ac:classes:X509</saml:AuthnContextClassRef>
```



```
</saml:AuthnContext>
```

```
</saml:AuthnStatement>
```

Afsluiting authentication statement.

Attributen

```
<saml:AttributeStatement>
```

De volgorde van de attributen in het AttributeStatement is niet relevant. Er mogen geen andere attributen opgenomen worden in het AttributeStatement dan hier beschreven is.

Zorgaanbieder

```
<saml:Attribute Name="Zorgaanbieder">
  <saml:AttributeValue>
    urn:IIroot:2.16.528.1.1007.3.3:IIext:12345678
  </saml:AttributeValue>
</saml:Attribute>
```

Het attribuut Zorgaanbieder bevat de URA van de zorgaanbieder van de zorgverlener/medewerker die de BSN validatie heeft uitgevoerd en het token heeft ondertekend. Vanuit het certificaat waarmee het token is ondertekend, kan worden afgeleid wat het URA-nummer van de zorgaanbieder waar de ondertekenaar in dienst is.

De URA wordt uitgedrukt met behulp van een URN (Uniform Resource Name). De URN is opgebouwd uit:

"urn:llroot:"<OID voor UZI organisatielids>":llex:"<URA>

De URN string is opgebouwd uit een llroot en een llex. "ll" staat voor het HL7v3 datatype Instance Identifier. Om de namespace in URN uniek te krijgen is ll als prefix voor de root en ext geplaatst.

URA's worden uitgedrukt als een id onder het identificatiesysteem "2.16.528.1.1007.3.3". De URA wordt toegekend door het UZI-register. Stel dat de URA de waarde "12345678" heeft, dan ziet de URN er als volgt uit:

urn:llroot:2.16.528.1.1007.3.3:llex:12345678

WID_token (alleen in Scan_token)

```
<saml:Attribute Name="WID_token">
  <saml:AttributeValue>
    Base64 representatie van het WID_token
  </saml:AttributeValue>
</saml:Attribute>
```

Het attribuut WID_token bevat de gehele SAML assertion ondertekend met het ZID servercertificaat Base64 geëncodeerd.

WID_raw_data (alleen in WID_token)

```
<saml:Attribute Name="WID_raw_data">
  <saml:AttributeValue>
    Base64 representatie van de ingescande Datagroep 11
  </saml:AttributeValue>
</saml:Attribute>
```

```

    </saml:AttributeValue>
  </saml:Attribute>

```

Het attribuut WID_raw_data bevat de volledig ingescande datagroep 11 uit het WID. Het element is Base64 geëncodeerd.

Indien het element base64 gedecodeerd wordt is de structuur in JSON als volgt:

```

{
  "type": "3",
  "version": "1",
  "attributes":
  [
    {
      "dg11": "<dg11 value>"
    }
  ],
  "sod": "<sod value>"
}

```

Waarbij:

“dg11” de data uit datagroep 11 bevat en

“sod” het Document Security Object bevat.

attributeStatement blok

Het attributen statement blok ziet er dan bijvoorbeeld zo uit (de volgorde van de attributen is niet relevant):

```

<saml:AttributeStatement>

```

```

<saml:Attribute Name="Zorgaanbieder">
  <saml:AttributeValue>
    urn:IIroot:2.16.528.1.1007.3.3:IIext:12345678
  </saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="WID_token">
  <saml:AttributeValue>
    Base64 representatie van het WID_token
  </saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>

```

Tenslotte wordt het attributen statement blok afgesloten met

```

</saml:AttributeStatement>

```

10.3.2.9.2.5 Algoritmes

Om de integriteit en onweerlegbaarheid van het SAML scantoken te waarborgen wordt een XML Signature geplaatst, zoals beschreven in [IH tokens generiek]. Na plaatsen van de XML Signature kan de ontvanger, met gebruikmaking van het persoonsgebonden identiteits-certificaat van de verzender en de CA certificaten zoals verstrekt door ZORG-ID, onomstotelijk vaststellen dat het SAML scantoken ondertekend is met de privé sleutel behorend bij het gebruikte certificaat van de zorgmedewerker en dat het WID_token ondertekend is met de privé sleutel van het ZORG-ID servercertificaat.

De XML Signature van het SAML scantoken die gebruikt wordt bij berichtauthenticatie met behulp van het identiteitscertificaat maakt gebruik van de volgende algoritmes, zoals beschreven in [IH tokens generiek]:

- Voor het berekenen van de hashwaarde wordt SHA-256 gebruikt.
- Voor de digitale handtekening in AORTA wordt gebruik gemaakt van een RSA handtekening over een SHA-256 digest.



Omdat de XML Signature onderdeel is van het SAML scantoken en in het SAML scantoken geplaatst wordt, moet er een "enveloped-signature" transformatie uitgevoerd worden die de Signature tags uit het SAML scantoken verwijderd gevolgd door een "exc-c14n transformatie" (zie ook [SAML Core] §5.4.3 en §5.4.4).

10.3.2.9.2.6 Opbouw

De headers

Eerst wordt het SAML scantoken – het <saml:Assertion ...> element aangemaakt en gevuld met die elementen, zoals beschreven in [paragraaf 2.4](#)¹⁵⁰Inhoud.

```
<saml:Assertion
  ID="token_2.16.528.1.1007.3.3.1234567.1_0123456789"
  IssueInstant="2009-06-24T11:47:34Z"
  Version="2.0"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
  ... Zie paragraaf 2.4 Inhoud ...
</saml:Assertion>
```

Het XML Signature blok is onderdeel van het SAML scantoken. Het XML Signature blok komt na het <saml:Issuer> element. Na de Signature volgt de rest van de inhoud van de assertion.

150. <https://vzvz.atlassian.net/wiki/spaces/AORTA84/pages/879593947/Het+SAML+Scan+en+WID+token#HetSAMLScanenWIDtoken-Inhoud>

```

<saml:Assertion
  ID="token_2.16.528.1.1007.3.3.1234567.1_0123456789"
  IssueInstant="2009-06-24T11:47:34Z"
  Version="2.0"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
  <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
    urn:IIroot:?:IIext:?
  </saml:Issuer>
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
      ...
    </ds:SignedInfo>
    <ds:SignatureValue>Wuwn...5e4=</ds:SignatureValue>
    <ds:KeyInfo>
      <wss:SecurityTokenReference>
        <ds:X509Data>
          ...
        </ds:X509Data>
        <wss:SecurityTokenReference>
        </ds:KeyInfo>
      </ds:Signature> ...
    ... Zie paragraaf 2.3 Inhoud ...
  </saml:Assertion>

```

Indien de Signature aangemaakt wordt moet niet meer met de strings (saml:Assertion en SignedInfo) gemanipuleerd worden, maar ze moeten octet-voor-octet overgenomen worden in het bericht. Strikt genomen is het toegestaan wijzigingen aan te brengen die door canonicalisatie bij de ontvanger weer

opgeheven worden, maar wanneer de digitale handtekening door middel van strings wordt opgebouwd, is het een foutgevoelige handeling.

Lange Base 64 waarden zijn in het voorbeeld afgekort. Wederom kan dit als strings worden behandeld, waarbij drie waarden vervangen moeten worden.

Deze drie waarden worden ingevuld:

- Neem het SignedInfo blok op.
- Neem de SignatureValue op.
- Neem certificaatgegevens in het KeyInfo blok op, in de vorm van het volledige publieke certificaat (in het scantoken het identiteitscertificaat; in het WID-token het ZORG-ID servercertificaat).



Wanneer een bericht een SAML assertion bevat, moet dat bericht precies één bijbehorende digitale handtekening bevatten.

Het maken van de XML Signature uit strings levert de SAML assertion op met daarin de Signature.

1.2.2 Plaats van het SAML token en de digitale handtekening

Het SAML scantoken met daarin de digitale handtekening wordt Base64-geëncodeerd in het attribuut "Scantoken" van het inschrijftoken gezet.

Het SAML WID_token met daarin de digitale handtekening wordt Base64-geëncodeerd in het attribuut "WID_token" van het scantoken gezet.

De WID_raw_data met daarin de digitale handtekening wordt Base64-geëncodeerd in het attribuut "WID_raw_data" van het WID_token gezet.

10.3.2.9.3 Token afhandeling Scan en WID token

10.3.2.9.3.1 Token afhandeling

Verificatie van het bericht

Het is belangrijk vast te stellen dat de velden in het SAML scantoken een correcte waarde hebben en geldig ondertekend zijn. Wanneer dit niet zou gebeuren, kan een kwaadwillende met een gestolen token nog steeds gegevens opvragen van bv. ieder willekeurig burgerservicenummer.

Controles op het scantoken

Het SAML scantoken wordt door de ontvanger uit het betreffende attribuut van het inschrijftoken gehaald, Base64 gedecodeerd en vervolgens gevalideerd.

Bij de validatie van het SAML scantoken moet de ontvanger controleren of:

- De aanduiding voor de versie van SAML gedefinieerd is op "2.0", zie [Uniekheid \(see page 515\)](#) ;
- De juiste organisatielD (URA) is opgenomen die deze assertion heeft gecreëerd en de gebruiker heeft geauthenticeerd, zie [Afzender \(see page 516\)](#) .
- Het BSN uit het Subject zie [Onderwerp \(see page 517\)](#) overeenkomt met het BSN uit het inschrijftoken;
- De Assertion correct is ondertekend door de Signature te valideren met het meegestuurde certificaat.
- Het gebruikte certificaat waarmee de ondertekening heeft plaatsgevonden geldig was ten tijde van de ondertekening.
- Indien het certificaat op de CRL is geplaatst, dan dient dit plaats te hebben gevonden nadat het token gegenereerd en ondertekend is.
- De relevante certificaatketen te valideren op geldigheid.
- De geldigheidsperiode van het token, zie [Geldigheid \(see page 518\)](#) , niet langer is dan 10 jaar;
- Het bericht ontvangen is binnen de geldigheidsperiode van het token, zie [Geldigheid \(see page 518\)](#) ;
- De afnemer van het SAML scantoken (audience) minimaal de ZIM is, zie [Ontvanger \(see page 519\)](#) ;
- De zorgverlener/zorgmedewerker is geauthenticeerd via het voorgedefinieerde authenticatiemiddel, het X509 identiteitscertificaat, zoals beschreven in [Authenticatie \(see page 520\)](#);
- Alleen die attributen zijn gedefinieerd, die zijn beschreven in [Attributen \(see page 521\)](#) ;

Het scantoken mag meerdere malen gebruikt worden.

Het tokenID dient in de log van de ZIM opgenomen te worden.

Controles op het WID_token

Het SAML WID_token wordt door de ontvanger uit het betreffende attribuut van het scantoken gehaald, Base64 gedecodeerd en vervolgens gevalideerd.

Bij de validatie van het SAML WID_token moet de ontvanger controleren of:

- De aanduiding voor de versie van SAML gedefinieerd is op "2.0", zie [Uniekheid \(see page 515\)](#) ;
- De juiste organisatielD (URA) is opgenomen die deze assertion heeft gecreëerd en de gebruiker heeft geauthenticeerd, zie [Afzender \(see page 516\)](#) .

- Het BSN uit het Subject zie [Onderwerp \(see page 517\)](#) overeenkomt met het BSN uit het scantoken;
- De Assertion correct is ondertekend door de Signature te valideren met het meegestuurde certificaat.
- Het gebruikte certificaat waarmee de ondertekening heeft plaatsgevonden geldig was ten tijde van de ondertekening.
- Indien het certificaat op de CRL is geplaatst, dan dient dit plaats te hebben gevonden nadat het token gegenereerd en ondertekend is.
- De relevante certificaatketen te valideren op geldigheid.
- De geldigheidsperiode van het token, zie [Geldigheid \(see page 518\)](#) , niet langer is dan 10 jaar;
- Het bericht ontvangen is binnen de geldigheidsperiode van het token, zie [Geldigheid \(see page 518\)](#) ;
- De afnemer van het SAML WID_token (audience) minimaal de ZIM is, zie [Ontvanger \(see page 519\)](#) ;
- De waarde van @AuthnInstant binnen het AuthnStatement van het WID_token identiek is aan de waarde van @AuthnInstant binnen het AuthnStatement van het Scan_token
- Alleen die attributen zijn gedefinieerd, die zijn beschreven in [Attributen \(see page 521\)](#) ;

Controles op de WID_raw_data

Vooralsnog hoeven de WID_raw_data niet gevalideerd te worden.

Als aan één van de bovenstaande condities niet is voldaan, moet het inschrijftoken door de ontvanger geweigerd worden en een SOAP foutmelding aan het verzendende systeem afgegeven worden, zie foutafhandeling in [IH tokens generiek].

10.3.2.9.4 Referenties Scan en WID token

10.3.2.9.4.1 Bijlage A Referenties

Referentie	Document	Versie
[IH tokens generiek]	GBx AORTA_Auth_IH_Security_tokens_generiek (see page 435)	8.3.0.0
[Inschrijftoken]	AORTA_Auth_IH_ Inschrijftoken (see page 373)	8.3.0.0

[SAMLAuthnContext]	Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0 http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf	2.0 15- mrt-2005
[SAML Core]	SAML v2.0 Core Specification https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf	2.0 15- mrt-2005
[SAML Profiles]	Profiles for the OASIS Security Assertion Markup Language (SAML) v2.0 http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf	2.0 15- mrt-2005
[SAML Token]	SAML Token Profile http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SAMLTOKENProfile.pdf	1.1 01- feb-2006

10.3.2.10 GBP AORTA_Auth_IH_Berichtauthenticatie_DigiD

- **IH Berichtauthenticatie met DigiD**

Datum: 1 mei 2022

Publicatie: V8.3.0.0

10.3.2.10.1 Inleiding berichtauthenticatie DigiD

10.3.2.10.1.1 Doel en scope

Dit document heeft tot doel een handleiding te geven voor de implementatie van het koppelvlak tussen het goed beheerd patiënten portaal (GBP) en het landelijk schakelpunt (LSP) voor wat betreft de toe te passen technieken voor de authenticatie van patiënten.

Dit document specificeert het SAML (Security Assertion Markup Language) authenticatietoken voor patiënten die zich bij DigiD laten authenticeren.

10.3.2.10.1.2 Doelgroep voor dit document

Dit document is bedoeld voor softwareontwikkelaars van het goed beheerd patiënten portaal en het LSP, die op grond van de HL7v3 communicatiestandaard en op grond van dit document berichten willen uitrusten met het SAML authenticatietoken. Daarnaast wordt het plaatsen van de digitale handtekening besproken (zie ook [IH tokens generiek]).

10.3.2.10.1.3 Documenthistorie

Versie	Datum	Omschrijving
6.10.0.0	12 oktober 2011	RfC 46142: SOAP Headers van tokens worden uitgebreid met soap:actor.
6.11.0.1	29 januari 2013	Aanpassingen ten behoeve van DigiD v4.0 koppelvlak SAML
8.0.1.0	28 mei 2014	Geactualiseerd en mogelijkheid van DigiD om assertions te tekenen verwerkt
8.0.1.0	15 mei 2017	RfC 76206: SSL verwijderen
8.0.1.0	13 sep 2017	RfC 78296: Aanpassing KeyInfo veld in DigiD SAML assertion
8.0.2.0	31 januari 2018	RfC 76680: DigiD authenticatiesterktes uitbreiden
8.0.2.0	31 januari 2018	RfC 77951: Controle op SubjectConfirmation door LSP

8.0.3.0	1 juli 2018	INI-8527: Kleine aanpassingen m.b.t. authenticatiesterktes in hoofdstuk 2.3.6. en Bijlage B. Aanpassing referentie m.b.t. Logius koppelvakspecificatie DigiD. INI-8792: ZIM als audience in DigiD-token verwijderen
8.2.0.0	7-okt-2020	Opgenomen in publicatie 8.2.0.0

10.3.2.10.2 Het SAML authenticatietoken DigiD

In dit hoofdstuk wordt de inhoud van het gecreëerde SAML authenticatietoken van DigiD [DigiD Koppel] besproken, dat bij berichtauthenticatie voor patiënten wordt gebruikt. Het SAML authenticatietoken bevat informatie over de toegepaste authenticatie en identificatie van de patiënt. Het SAML authenticatietoken is een op XML gebaseerde SAML assertion en heeft tot doel de *assertions* (beweringen over authenticatie) over te brengen tussen partijen (service- en identity provider) die een vertrouwensrelatie hebben.

Alle XML voorbeelden in het document dienen door de betrokken partijen tijdens het bouwen van de uitwisseling getest, en waar nodig, in samenspraak met VZVZ aangepast te worden voor een juiste optimale werking.

Voor het verkrijgen van het SAML authenticatietoken en het aanbieden van dit token aan de ZIM worden de volgende profielen gebruikt:

- Een op Webrowsers gebaseerd profiel van het authenticatie verzoek protocol (Authentication Request Protocol) is gedefinieerd ter ondersteuning van Single Sign-On. Dit profiel raakt de koppelvakken:
- patiënt ondersteuning (PC) - goed beheerd patiëntenportaal (GBP)
- goed beheerd patiëntenportaal (GBP)- identity provider (neemt als vertrouwde autoriteit, de diensten van DigiD waar)

Dit profiel is niet normatief en is terug te vinden in [Bijlage B \(see page 545\)](#).

- Het gebruik van het SAML authenticatietoken (security token) in het kader van het WSS SOAP berichten profiel voor het veilig stellen en uitwisseling van authentieke SOAP berichten. Dit profiel raakt het koppelvak:
- goed beheerd patiëntenportaal (GBP) – het landelijk schakelpunt (LSP)

Dit profiel wordt in de volgende paragrafen verder uitgewerkt.

10.3.2.10.2.1 Structuur

Het SAML authenticatietoken is een door een vertrouwde Identity Provider (DigiD) gecreëerde SAML assertion die gebruikt wordt bij berichtauthenticatie van patiënten voor het LSP. DigiD ondertekent zowel de ArtifactResponse als de Assertion. De Assertion wordt vervolgens door het GBP als authenticatietoken in het bericht opgenomen.

Assertion

De assertion heeft de volgende structuur (de waarden die in het token gebruikt worden zijn fictief):

```
<saml:Assertion

  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
  Version="2.0"
  ID="_dc9f793e2811b86f8e5cdf43ab5fd47d1fe0e61c"
  IssueInstant="2012-12-20T18:50:27Z">
  <saml:Issuer>SamlIssuer</saml:Issuer>
  <saml:Subject>
    <saml:NameID>s00000000:12345678</saml:NameID>
    <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
      <saml:SubjectConfirmationData
        InResponseTo="_7afa6d9f9ff28ca9233ada1d9ec2aa1bd6c5ce49"
        Recipient="http://example.com/artifact_url"
        NotOnOrAfter="2012-12-20T18:52:27Z"/>
    </saml:SubjectConfirmation>
  </saml:Subject>
  <saml:Conditions
    NotBefore="2012-12-20T18:48:27Z"
    NotOnOrAfter="2012-12-20T18:52:27Z">
    <saml:AudienceRestriction>
      <saml:Audience>

        urn:IIroot:2.16.840.1.113883.2.4.6.6:IIext:1

      </saml:Audience>
    </saml:AudienceRestriction>
  </saml:Conditions>
  <saml:AuthnStatement
    SessionIndex="17"
    AuthnInstant="2012-12-20T18:50:27Z">
    <saml:SubjectLocality Address="127.0.0.1"/>
    <saml:AuthnContext>
      <saml:AuthnContextClassRef>
        urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract
      </saml:AuthnContextClassRef>
    </saml:AuthnContext>
  </saml:AuthnStatement>
</saml:Assertion>
```

10.3.2.10.2.2 Namespaces

Het door een vertrouwde Identity Provider afgegeven SAML authenticatietoken dat gebruikt wordt bij berichtauthenticatie, maakt gebruik van de volgende namespaces. De prefixen zijn niet normatief maar worden in dit document als voorbeelden gebruikt.

Tabel AORTA.STK.t3400 - Namespaces

Prefix	Namespace URI
ds	http://www.w3.org/2000/09/xmldsig#
ec	http://www.w3.org/2001/10/xml-exc-c14n#
saml	urn:oasis:names:tc:SAML:2.0:assertion



Bij het gebruik van de namespace-prefixes is het van belang deze na het ondertekenen niet meer te veranderen, dit maakt de digitale handtekening ongeldig.

10.3.2.10.2.3 Inhoud

De volgende paragrafen beschrijven de verschillende kenmerken en beveiligingsgerelateerde gegevens die het SAML authenticatietoken onderscheiden, zoals in [IH tokens generiek] beschreven is.

```
<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" ... >
```

Op de plaats van de drie punten (...) worden Uniekheidattributen opgenomen ten aanzien van de Assertion. Deze attributen worden beschreven in [paragraaf 2.3.1 \(see page 534\)](#) Uniekheid.

Uniekheid

```
<saml:Assertion
  Version="2.0"
```

```
ID="_dc9f793e2811b86f8e5cdf43ab5fd47d1fe0e61c"
```

```
IssueInstant="2012-12-20T18:50:27Z">
```

De attributen van het SAML assertion element maken van de afgegeven SAML assertion een uniek gegeven. Het attribuut ID identificeert op een unieke wijze de assertion. Het attribuut IssueInstant is een tijdstipmoment van uitgifte van de SAML assertion. De tijdswaarde is gecodeerd in UTC. Het attribuut Version is de gebruikte SAML versie van de SAML assertion. De aanduiding voor de versie van SAML gedefinieerd in deze specificatie is "2.0".

Onderwerp

```
<saml:Subject>
  <saml:NameID>s00000000:12345678</saml:NameID>
  <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
    <saml:SubjectConfirmationData

      InResponseTo="_7afa6d9f9ff28ca9233ada1d9ec2aa1bd6c5ce49"

      Recipient="http://example.com/artifact_url"

      NotOnOrAfter="2012-12-20T18:52:27Z"/>
  </saml:SubjectConfirmation>
</saml:Subject>
```

Het onderwerp <Subject> bij berichtauthenticatie met DigiD is een referentie naar een authenticatieverzoek van een patiënt dat door het goed beheerd patiëntenportaal is geïnitieerd. Het onderwerp bevat een uniek authenticatienummer, het <NameID> element.

DigiD neemt in het element <NameID> het sectoraal nummer op in het formaat <sectorcode>;<sectoraal nummer>

Indien de sectorcode de waarde 'S00000000' heeft, dan is het sectoraal nummer een BurgerServiceNummer.

Het InResponseTo attribuut en het Recipient attribuut in de bevestiging van het onderwerp <SubjectConfirmation> worden niet gebruikt door het LSP. Deze attributen worden echter wel opgenomen in de assertion.

Verder heeft de bevestiging van het onderwerp een geldigheidsduur (het NotOnOrAfter attribuut). De geldigheidsduur geeft de duur van een sessie aan tussen het goed beheerd patiëntenportaal en de identity provider (DigiD).

Voor deze bevestigingsmethode (het Method attribuut) moet de URN waarde "urn:oasis:names:tc:SAML:2.0:cm:bearer" (assertion drager) worden gebruikt.

Geldigheid

```
<saml:Conditions
  NotBefore="2012-12-20T18:48:27Z"
  NotOnOrAfter="2012-12-20T18:52:27Z">
  ...
</saml:Conditions>
```

Op de plaats van de drie punten (...) dient een AudienceRestriction te worden toegevoegd zoals beschreven in [paragraaf 2.3.5 \(see page 538\)](#) Ontvanger).

Het attribuut *NotBefore* is de tijd waarop de afgegeven SAML assertion geldig wordt.



Wordt een bericht ontvangen op of nadat *NotOnOrAfter* is verstreken, dan **moet** dit bericht geweigerd worden^[1].

^[1] Met de configuratie parameter "*ZIM-max-BSN-gracetijd*" van de ZIM kan de geldigheidstermijn van een SAML assertion vergroot worden waarbij de begintijd (*NotBefore*) vervroegd en de eindtijd (*NotOnOrAfter*) verlaat mag worden.

Het attribuut *NotOnOrAfter* is de tijd waarop de afgegeven SAML assertion vervalst.



Wordt een bericht ontvangen op of nadat *NotOnOrAfter* is verstreken, dan **moet** dit bericht geweigerd worden Met de configuratie parameter "*ZIM-max-BSN-gracetijd*" van de ZIM kan de geldigheidstermijn van een SAML assertion vergroot worden waarbij de begintijd (*NotBefore*) vervroegd en de eindtijd (*NotOnOrAfter*) verlaat mag worden. .

Aangezien DigiD deze waarden interpreteert als tijdstip van authenticatie wordt de geldigheidstermijn (d.i. de eindtijd *NotOnOrAfter*) opgehoogd met een "ZIM-max-BSN-gracetijd" van 15 minuten.

Het tijdsverschil tussen *NotOnOrAfter* en *NotBefore* bedraagt maximaal 4 minuten in DigiDv4.0-SAML. De tijden worden bepaald op het afgiftemoment van de assertion bij DigiD waarbij *NotBefore* de waarde afgiftemoment - 2 minuten en *NotOnOrAfter* de waarde afgiftemoment + 2 minuten krijgt.



De geldigheidsduur van een token (*NotOnOrAfter* minus *NotBefore*) mag niet langer dan 4 minuten zijn. Wordt een bericht ontvangen waarin deze geldigheidsduur overschreden is, dan **moet** dat bericht geweigerd worden, ook al is het tijdstip *NotOnOrAfter* nog niet verstreken.



Van het GBP wordt verwacht dat zij een timer bijhoudt die op het moment dat een gebruiker van het Portaal (de burger) via een redirect vanuit DigiD terugkeert in het LSP-portaal gestart moet worden en de gebruiker na 10 minuten (als de gebruiker op dat moment een nieuwe actie wil doen) weer terugstuurt naar DigiD voor herauthenticatie. Tevens dient het GBP op grond van deze timer een eventueel nog aanwezig *ArtifactResponse* token te verwijderen.

De subelementen *OneTimeUse* en *ProxyRestriction* worden niet gebruikt binnen het *<Conditions>* element bij Berichtauthenticatie met DigiD.

Afzender

```
<saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
  https://federatie.overheid.nl/aselectserver/server/
</saml:Issuer>
```

De afzender is de authenticatie autoriteit (DigiD) die de assertion heeft afgegeven en de patiënt heeft geauthenticeerd. De Issuer wordt in dit fictieve voorbeeld uitgedrukt met behulp van een URL.

Noot: In samenspraak met VZVZ en andere betrokken partijen kan het formaat en inhoud van de Issuer in de assertion heroverwogen worden, zie volgende opmerking.

De Issuer kan ook uitgedrukt worden met behulp van URN (Uniform Resource Name). De URN is opgebouwd uit:

"urn:IIroot:"<OID van het coderingssysteem>":IIext:"<extensie>

De URN string is opgebouwd uit een IIroot en een IIext. "II" staat voor Instance Identifier. Binnen AORTA is de IIroot een oid (Object Identifier), die een identificatie- of coderingssysteem weergeeft, en dat leidt in HL7v3 XML tot een element met twee attributen, een root met de uitgegeven codering en een extensie (ext). Om de namespace in URN uniek te krijgen is II als prefix voor de root en ext geplaatst.

Indien de keuze door de betrokken partijen gemaakt wordt om de Issuer als URN uit te drukken, moet de root en extensie door de GBP organisatie aangevraagd en geregeld worden.

Het goed beheerd patiëntenportaal past een TLS-sessie toe bij het opvragen van de assertion bij de identity provider.

Ontvanger

```
<saml:AudienceRestriction>
  <!-- Root en extensie van de ZIM en het patiëntenportaal -->

  <saml:Audience>urn:IIroot:2.16.840.1.113883.2.4.6.6:IIext:1</saml:Audience>
</saml:AudienceRestriction>
```

In de AudienceRestriction wordt beschreven aan welke ontvangende partijen (service providers) de SAML assertion is gericht. De waarden in de elementen zijn (voorlopig) vaste waarden. Voor de <Audience> parameter is (ook) gekozen voor URN, zie voor de opbouw van de URN [paragraaf 2.3.4 \(see page 537\)](#) Afzender.

Vooralsnog staat DigiD niet toe dat er meerdere audiences in het token worden teruggegeven. De root en extensie van de ZIM zullen niet zijn opgenomen in de assertion. Het LSP zal zo geconfigureerd moeten worden dat tokens waarbij als audience het patiëntenportaal is opgenomen ook toegelaten worden.

Authenticatie

```
<saml:AuthnStatement
```

```

SessionIndex="17"

AuthnInstant="2012-12-20T18:50:27Z">
...
</saml:AuthnStatement>

```

Op de plaats van de drie punten (...) worden de <SubjectLocality> en de <AuthnContext> toegevoegd zoals hieronder beschreven.

Het onderwerp (Subject), een patiënt, in de SAML assertion is geauthenticeerd doormiddel van een authenticatiemiddel op een gegeven moment.

```
<saml:SubjectLocality Address="127.0.0.1"/>
```

De SubjectLocality is gevuld met het IP-adres (Address attribuut) van de PC van de gebruiker en is onderdeel van het AuthnStatement. Deze wordt gebruikt om te verifiëren of de patiënt een vervolg verzoek vanaf hetzelfde IP-adres doet als zijn initiële verzoek tijdens het benaderen van het patiëntenportaal.



Bij communicatie tussen de computer van de patiënt en het patiëntenportaal mag het adres van de computer van de patiënt tijdens een sessie niet wijzigen. Bij wijziging van het adres (Address attribuut) tijdens de sessie in de SubjectLocality, wordt dit als malafide activiteit aangemerkt en wordt de sessie beëindigd en is herauthenticatie vereist.

```

<saml:AuthnContext>
  <saml:AuthnContextClassRef>

    urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract

  </saml:AuthnContextClassRef>
</saml:AuthnContext>

```

Binnen de SAML specificatie is het mogelijk om een authenticatie-context (*AuthnContext*) mee te geven die de context aangeeft van het gebruikte authenticatiemiddel. Binnen de SAML specificatie zijn een aantal contexten gespecificeerd, zie [SAML Authn Context], die gebruikt kunnen worden als

referentiekader voor communicatie tussen de ZIM en andere componenten zoals het goed beheerd patiëntenportaal.

Het LSP moet de volgende DigiD-betrouwbaarheidsniveau's ondersteunen:

- Basis[1]: "urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport";
- Burger krijgt toegang tot dienst met authenticatiesterkte 10 t/m 19;
- Midden: "urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract";
- Burger krijgt toegang tot dienst met authenticatiesterkte 20 t/m 24;
- Substantieel: "urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard";
- Burger krijgt toegang tot dienst met authenticatiesterkte 25 t/m 29;
- Hoog[2]: "urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI"
- Burger krijgt toegang tot dienst met authenticatiesterkte 30 en hoger.

Het LSP controleert op de geldigheid en correctheid van het DigiD-token.

[1] Het LSP ondersteunt geen diensten die gebruik maken van betrouwbaarheidsniveau basis.

[2] Het LSP ondersteunt geen diensten die gebruik maken van betrouwbaarheidsniveau hoog.

10.3.2.10.2.4 Algoritmes

Om de integriteit en onweerlegbaarheid van het SAML authenticatietoken te waarborgen wordt een XML Signature geplaatst, zoals beschreven in [IH tokens generiek]. Na plaatsen van de XML Signature kan de ontvanger, met gebruikmaking van het PKI-overheid-certificaat van de verzender onomstotelijk vaststellen dat de getekende SAML assertion ondertekend is met de privé sleutel behorend bij het gebruikte PKI-overheid-certificaat.

De XML Signature van het SAML authenticatietoken die gebruikt wordt bij berichtauthenticatie met behulp van DigiD maakt gebruik van de volgende algoritmes, zoals beschreven in [IH tokens generiek].

- Voor het berekenen van de hashwaarde wordt SHA-256 gebruikt.
- Voor de digitale handtekening in AORTA wordt gebruik gemaakt van een RSA handtekening over een SHA-256 digest.
- Omdat de XML Signature onderdeel is van het SAML authenticatietoken en in het SAML authenticatietoken geplaatst wordt, moet er een "enveloped-signature" transformatie uitgevoerd worden die de Signature tags uit het SAML authenticatietoken verwijderd.

10.3.2.10.2.5 Opbouw

Na authenticatie en toegangsverlening van een patiënt op het GBP moet het GBP er zorg voor dragen dat het SAML authenticatietoken wordt toegevoegd bij de berichten die van het GBP naar het landelijk schakelpunt worden verzonden.

Het SAML authenticatietoken – het <saml:Assertion ...> element is aangemaakt en gevuld met die elementen, zoals beschreven in de voorgaande paragrafen.

De digitale handtekening

Het XML Signature blok is onderdeel van het SAML authenticatietoken. Het XML Signature blok komt na het <saml:Issuer> element van de <saml:Assertion>.

```
<ds:Signature>
  <ds:SignedInfo>
    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" /
  >
    <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
    <ds:Reference URI="#_b2728a3aa52c4779c4c77ab8dd8a7dda604c94c7">
      <ds:Transforms>
        <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
          <ec:InclusiveNamespaces PrefixList="ds saml xs" />
        </ds:Transform>
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig#sha256" />
      <ds:DigestValue>675ga8KqGFqJSGgSJHzoVU+kgrlWqYLpTxJ28gWLPkQ=</
ds:DigestValue>
    </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue>ecXG...igg==</ds:SignatureValue>
  <ds:KeyInfo>
    <ds:KeyName>e37ee2522de410c633b3700835727ebf1834cd88</ds:KeyName>
  </ds:KeyInfo>
</ds:Signature>
```

Het certificaat waarmee de assertion is getekend is opgenomen in het X509Data element.

Het in het metadatatadocument gebruikte entity_id wordt gebruikt als Issuer in de Assertion.

Om van DigiD een ondertekende assertion te verkrijgen is het nodig dat de dienst aanbieder (het GBP) éénmalig in de uitwisseling van metadata van de dienst aanbieder met DigiD binnen het element <SPSSODescriptor> het attribuut WantAssertionsSigned op "true" zet.

```
<md:SPSSODescriptor WantAssertionsSigned="true"
  protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
```

Plaats van het SAML token in het SOAP bericht.

Het gehele SAML authenticatietoken met daarin de digitale handtekening worden in het WS-Security SOAP Header gezet.

Op het <wss:Security> element **moet** een soap:mustUnderstand="1" vlag opgenomen worden, die aangeeft dat de ontvanger dit security element **moet** verwerken en een soap:actor="<http://www.aortarelease.nl/actor/zim>"¹⁵¹ die aangeeft dat de ZIM dit security element verwerkt.

```
<soap:Header xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  ...
  <wss:Security xmlns:wss=
    "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
    soap:actor="http://www.aortarelease.nl/actor/zim" soap:mustUnderstand="1">
    <saml:Assertion ...>
```

151. <http://www.aortarelease.nl/actor/lsp>

```

<saml:Issuer>SamlIssuer</saml:Issuer>

<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:SignedInfo>
    ...
  </ds:SignedInfo>
  <ds:SignatureValue>Wuwn...5e4=</ds:SignatureValue>
  <ds:KeyInfo>
    <ds:KeyName>e37ee2522de410c633b3700835727ebf1834cd88</
ds:KeyName>
  </ds:KeyInfo>
</ds:Signature>
... Zie paragraaf 2.3 Inhoud ...
</saml:Assertion ...>
</wss:Security>
</soap:Header>
<soap:Body>
  ...
</soap:Body>

```

10.3.2.10.3 Certificaten berichtauthenticatie DigiD

10.3.2.10.3.1 Te gebruiken certificaat en attributen

Voor het tekenen van het SAML authenticatietoken wordt het authenticiteitcertificaat van de identity provider DigiD gebruikt. Dit certificaat bevat een RSA publieke sleutel. Met de privé sleutel wordt de digitale handtekening gegenereerd.

De attributen in het authenticiteitcertificaat worden gegeven in de vorm van een Distinguished Name (DN) en het serienummer, zie [IH tokens generiek].

De volgende attribuutwaarden zijn voorbeelden en moeten in samenspraak met VZVZ en ander betrokken partijen (zoals de certificaatdienstverlener) nog bepaald en vastgelegd worden.

Tabel AORTA.STK.t3410 – Certificaat attributen

Attribuut	Omschrijving	Waarde
CN	Subject.commonName	as.digid.nl
OU	Subject.organizationalUnitName	Digid
O	Subject.organizationName	Stichting ICTU
C	Subject.countryName	NL
Serienummer	SerialNumber. Wordt door de certificaatdienstverlener vastgelegd	PK070001000868195 (voorbeeld)

Om de digitale handtekening bij de ZIM te verifiëren, moet de ontvanger over de bijbehorende publieke sleutel beschikken, zie [IH tokens generiek]. Voor verificatie is gekozen door een verwijzing naar het authenticiteitscertificaat in het SAML authenticatietoken als KeyInfo mee te zenden; de ontvanger moet deze dan met bijvoorbeeld het LDAP protocol ophalen, zie ook [IH tokens generiek].

Noot: In samenspraak met VZVZ en andere betrokken partijen kan de keuze voor opnemen van een verwijzing naar het certificaat nog heroverwogen worden.

10.3.2.10.4 Token afhandeling berichtauthenticatie DigiD

10.3.2.10.4.1 Verificatie met het bericht

Het is belangrijk vast te stellen dat velden in het SAML authenticatietoken overeenstemmen met die in het HL7v3 bericht. Wanneer dit niet zou gebeuren, kan een kwaadwillende met een gestolen token nog steeds gegevens opvragen van bv. ieder willekeurig burgerservicenummer.

Voordat het GBP de berichten met de daarbij behorende SAML authenticatietoken doorstuurt naar de ZIM, voert het patiëntenportaal een aantal controles uit op de afgegeven SAML assertion. De controles die het GBP uitvoert staan beschreven in SSO verificatie, omdat deze controles buiten de scope van deze implementatie handleiding vallen.

Na controle door het GBP wordt de SAML assertion door het GBP in de WS-Security SOAP Header geplaatst voor verzending naar de ZIM.

De ontvanger controleert of de WS-Security SOAP Header voor hem bestemd is, zie soap attribuut actor.

Het SAML authenticatietoken wordt door de ontvanger uit de WS-Security SOAP Header gehaald indien de WS-Security SOAP Header voor de ontvanger bestemd is en dat de ontvanger deze moet verwerken. Bij gebruik van het SAML authenticatietoken moet de ontvanger controleren of de digitale handtekening over het SAML authenticatietoken geldig is:

- De aanduiding voor de versie van SAML gedefinieerd is op "2.0", zie [paragraaf 2.3.1 \(see page 534\)](#) Uniekheid;
- De verschillende attributen die bij de bevestiging van het onderwerp horen voldoen aan de daarvoor gestelde eisen, zie [paragraaf 2.3.2 \(see page 535\)](#) Onderwerp;
- Het sectoraal nummer een BSN aanduidt en dat het bijbehorende BSN identiek is aan het BSN in de payload van het HL7v3 bericht zie [paragraaf 2.3.2 \(see page 535\)](#) Onderwerp;
- Het bericht ontvangen is binnen de geldigheidsperiode van het token, zie [paragraaf 2.3.3 \(see page 536\)](#) Geldigheid;
- De juiste afzender is vastgelegd, die deze assertion heeft gecreëerd en de patiënt heeft geauthenticeerd, zie [paragraaf 2.3.4 \(see page 537\)](#) Afzender;
- De verschillende afnemers van de assertion (audience) benoemd zijn die dit token mogen ontvangen en verwerken, zie [paragraaf 2.3.5 \(see page 538\)](#) Ontvanger;
- De patiënt geauthenticeerd is door de authenticatie autoriteit (DigiD) op minimaal het voorgedefinieerde betrouwbaarheidsniveau ([paragraaf 2.3.6 \(see page 538\)](#)) voor het bijbehorende bericht;
- Controle of binnen het KeyInfo element de keyName en X509data zijn opgenomen;
- Alleen die attributen zijn gedefinieerd, die zijn beschreven in [paragraaf 2.3.7](#) Attributen

Als aan één van de bovenstaande condities niet is voldaan, moet het bericht door de ontvanger geweigerd worden en een SOAP foutmelding aan het verzendende systeem afgegeven worden, zie foutafhandeling in [IH tokens generiek].

Als wel aan alle condities is voldaan, wordt het HL7v3 bericht verder verwerkt.

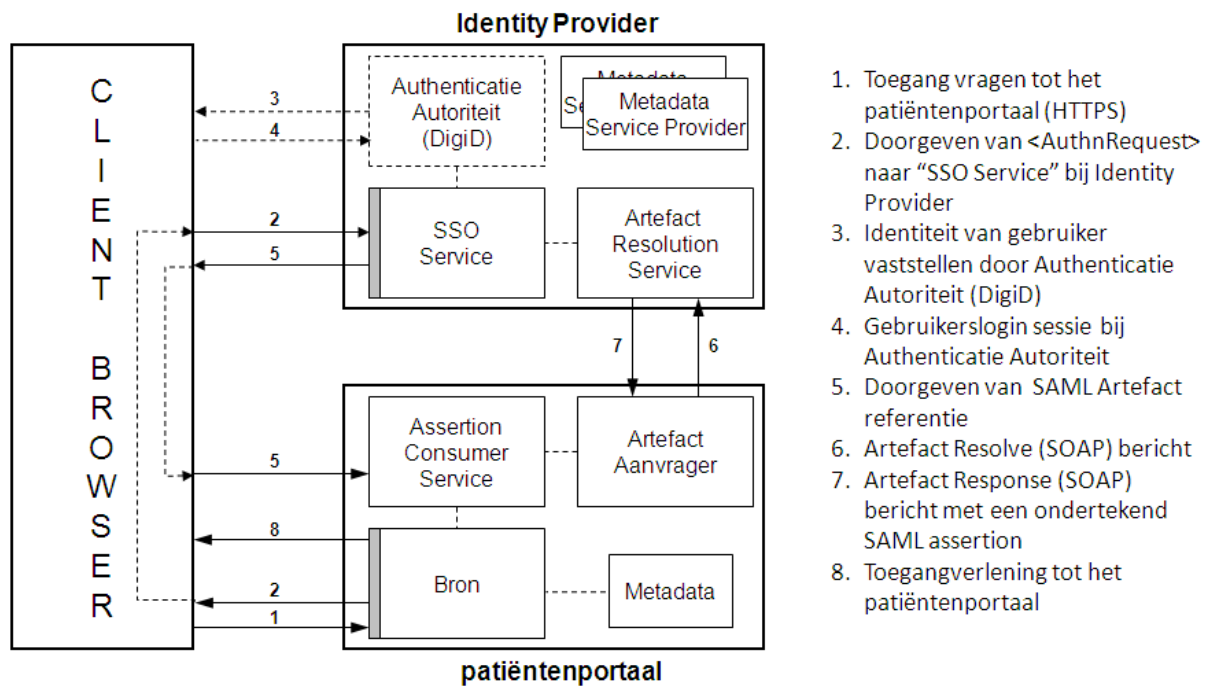
10.3.2.10.5 SSO (profiel, verificatie, meldingen)

10.3.2.10.5.1 Bijlage B Het SSO profiel

Het Single Sign-On profiel (SSO) is een SAML profiel dat aangeeft hoe gebruik te maken van het SAML authenticatie vraag en antwoord protocol in combinatie met verschillende SAML-bindings, zoals SOAP en HTTP. De communicatie bij authenticatie gaat tussen een Identity Provider (partij die verantwoordelijk is voor de waarmerking van de gebruiker) en een Service Provider (partij die een applicatie of bron beschikbaar stelt voor de gebruiker).

Noot: Het patiëntenportaal (GBP) vervult de rol van de Service Provider. De Identity Provider (IdP) wordt vervuld door DigiD.

Het volgende figuur illustreert het proces (stappen 1 t/m 8) voor de verwezenlijking van het SSO profiel. De stappen zijn in deze bijlage uitgewerkt.



Voorbeeld van configuratie waarden voor een fictieve testomgeving:

Entiteit	Waarde
Domein patiëntenportaal	" testportal.aorta-zorg.nl " ¹⁵²
Domein Identity Provider	" federatie.overheid.nl " ¹⁵³
Assertion Consumer Service	" https://testportal.aorta-zorg.nl:443/topa-prototype/saml/SSO " ¹⁵⁴
SSO Service	" https://federatie.overheid.nl/aselectserver/server/saml20_sso "

152. <http://testportal.aorta-zorg.nl>

153. <http://federatie.overheid.nl>

154. <https://testportal.aorta-zorg.nl/topa-prototype/saml/SSO>

Artefact Resolution Service	"https://federatie.overheid.nl/aselectserver/server/saml20_artifact"
Authenticatie Autoriteit	"https://federatie.overheid.nl/aselectserver/server"

Noot: Omdat niet *alle* internet browsers een ongelimiteerde URL ondersteunen, wordt er gebruik gemaakt van HTTP artefact binding (zie de pijlen 6 en 7 in bovenstaand figuur).

Stap 1: Het HTTP Request voor het patiëntenportaal

Een patiënt verzoekt via een cliënt (internet) browser toegang tot het patiëntenportaal (GBP). Dit is een standaard HTTP/TLS verzoek, hiervoor worden geen beperkingen opgelegd.

Stap 2: Het afgeven van een <AuthnRequest>

De 2^e stap is implementatie afhankelijk. Voor het authenticeren van burgers is DigiD de aangewezen authenticatie-autoriteit. Het patiëntenportaal stuurt de gebruiker via een HTTP-Redirect door naar een voorgedefinieerde Identity Provider waar de gebruiker wordt geauthenticeerd. Voor dit geval geeft het patiëntenportaal een <AuthnRequest> door. De <AuthnRequest> is van het complexe type AuthnRequestType dat afgeleid is van het abstracte complexe type RequestAbstractType. Zie voor alle SAML elementen en types [SAML Assertion Protocol].

De locatie van de "SSO Service", die binnen het Identity Provider domein actief is, wordt out-of-band doorgegeven met behulp van een SAML Metadata bestand. Dit bestand bevat tevens de publieke X509-certificaten voor de ondertekening en eventuele encryptie. Encryptie wordt vooralsnog niet gebruikt.

```
<md:IDPSSODescriptor ... >

<!-- Metadata van de SSO Service als onderdeel van de Identity Provider -->

  <md:SingleSignOnService WantAssertionsSigned="true"

    Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"

    Location="https://federatie.overheid.nl/aselectserver/server/saml20_sso"/>

  ...
```

```
</md:IDPSSODescriptor>
```

Het <SingleSignOnService> element is van het complexe type IndexedEndpointType en onderdeel van het <IDPSSODescriptor> element uit het metadata bestand dat een specifiek profiel (dienstverlening) reflecteert ter ondersteuning van het SSO profiel van de Identity Provider.

Het <SingleSignOnService> metadata element bestaat uit de volgende attributen:

Naam (@=attribuut)	Omschrijving	Vereist
@WantAssertionsSigned	Geeft aan dat, naast het gehele ArtefactResonse bericht, de assertion zelf ook ondertekend moet zijn	Ja
@Binding	Specificeert de binding dat door de "SSO Service" wordt ondersteund. De binding wordt via een URI geïdentificeerd. Bijvoorbeeld: "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect".	Ja
@Location	De locatie van de "SSO Service". Ook een URI attribuut.	Ja

Het patiëntenportaal initieert de SAML binding. In antwoord op het authenticatie verzoek wordt een antwoord aan het patiëntenportaal geleverd als onderdeel van de "SSO Service".

```
<?xml version="1.0" encoding="UTF-8"?>

<!-- Authenticatie verzoek via HTTP Redirect -->

<samlp:AuthnRequest AssertionConsumerServiceURL="https://testportal.aorta-zorg.nl:443/
topa-prototype/saml/SSO"

  Destination="https://federatie.overheid.nl/aselectserver/server/saml20_sso"

  ID="authntoken_2.16.528.1.1007.3.3.1234567.1_0123456789"

  IssueInstant="2009-06-24T11:46:53Z"

  ProviderName="testportal.aorta-zorg.nl"
```

```

Version="2.0"

xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">

<!-- Aanvrager van het authenticatie verzoek -->

  <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://
testportal.aorta-zorg.nl:443/topa-prototype/saml/SSO</saml:Issuer>

  <!-- Authenticatie-context -->

  <samlp:RequestedAuthnContext Comparison="exact">

    <saml:AuthnContextClassRef

xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract</saml:AuthnContextClassRef>

    </samlp:RequestedAuthnContext>

  <!-- Partijen waar toegang voor gevraagd wordt -->

  <saml:Conditions>

    <saml:AudienceRestriction>

      <saml:Audience>urn:IIroot:2.16.840.1.113883.2.4.6.6:IIext:1</saml:Audience>

<!-- Root en extensie van de ZIM -->

      <saml:Audience>urn:IIroot:?:IIext:?:</saml:Audience>

    </saml:AudienceRestriction>

  </saml:Conditions>

</samlp:AuthnRequest>

```

Het SAML authenticatie verzoek <AuthnRequest> bestaat uit verschillende attributen en elementen. De elementen worden in hiërarchische (top-down) volgorde beschreven en hebben de volgende betekenis:

Naam (@=attribuut)	Omschrijving	Ver eis t

@ID	Unieke identificatie van het (authenticatie) verzoek. De waarden van de ID-attribuut in een verzoek en de InResponseTo attribuut in het bijbehorende antwoord moeten overeenkomen.	Ja
@Version	De SAML versie van dit (authenticatie) verzoek. De aanduiding voor de versie van SAML gedefinieerd in deze specificatie wordt "2.0".	Ja
@IssuedInstant	Tijdstmoment van uitgifte van het (authenticatie) verzoek. De tijds waarde is gecodeerd in UTC.	Ja
@Destination	Een URI referentie waarnaar het (authenticatie) verzoek wordt verzonden, dit om malafide activiteiten te voorkomen. De ontvangende partij dient de URI verwijzing te controleren met de locatie waar het bericht is ontvangen. Indien dit niet overeenkomt, moet het bericht genegeerd en verwijderd worden.	Ne e
@AssertionConsumerServiceURL	Hiermee wordt aangegeven waar het antwoord van het (authenticatie) verzoek heen gestuurd moet worden, De responder moet ervoor zorgen dat de opgegeven waarde in feite verbonden is aan het verzoek.	Ne e
@ProviderName	Leesbare naam van de aanvrager van het (authenticatie) verzoek. Wordt gebruikt door de gebruiker van de Identity Provider.	Ja
saml:Issuer	Geeft de entiteit die het (authenticatie) verzoek heeft gegenereerd.	Ja
saml:Conditions	Via de condities kan de aanvrager van het (authenticatie) verzoek de geldigheid en/of gebruik van de verkregen assertion beperken. De responder <i>kan</i> wijzigingen of aanvullingen in de assertion invoeren als zij dit nodig acht aan de hand van de gegeven condities. Paragraaf 2.3.3 Geldigheid Geldigheid beschrijft kaders van de SAML condities waaraan het (authenticatie) verzoek moet voldoen	Ja
saml:Subject	De entiteit die het (authenticatie) verzoek genereert kan een <Subject> element toevoegen waarin het onderwerp van de verklaring(en) staat voor de ontvangende assertion. Dit element mag geen <SubjectConfirmation> elementen in het verzoek bevatten.	Ne e
samlp:RequestedAuthnContext	Specificeert in welke context de authenticatie statement wordt afgegeven, in antwoord op het (authenticatie) verzoek. Indien dit element aanwezig is, <i>moet</i> het antwoord een <AuthnContext> bevatten.	Ne e

<AuthnContext> (authenticatie-context) wordt gedefinieerd als de informatie, naast de authenticatie assertion zelf, dat een vertrouwde partij kan eisen voordat zij een besluit neemt over het afgeven van

een assertion. De authenticatie-context kan informatie bevatten over de actuele authenticatie methode (de "sterkte" van het gebruikte authenticatiemiddel) die gebruikt wordt.

Binnen de SAML specificatie zijn verschillende mogelijke authenticatie-contexten gespecificeerd die gebruikt kunnen worden als referentiekader voor de communicatie tussen de aanvrager en uitvoerder van het authenticatieverzoek. Dit moet met de software leverancier verder afgestemd worden, zie ook AuthnContextClassRef. Het <RequestedAuthnContext> element is van het complexe type RequestedAuthnContextType en bevat één of meerdere elementen en attributen. Zie ook [SAML Assertion Protocol] en [SAML Authn Context] voor de verschillende voorgedefinieerde context klassen voor authenticatie.

Naam (@=attribuut)	Omschrijving	Ver eis t
@Comparison	Specificeert welke vergelijkingsmethode gebruikt wordt om de gevraagde context klasse te evalueren. Standaard is de waarde "exact". Dit houdt in dat de inhoud van de authenticatie assertion exact moet matchen met tenminste een van de opgegeven authenticatie-context klassen. Andere mogelijke waarden zijn: "minimum", "maximum", of "better".	Ne e
saml:AuthnContextClassRef	Is een URI naar een voorgedefinieerde context klasse voor authenticatie, zie [SAML Authn Context]. De URI waarde die nu bij DigiD als voorbeeld wordt gebruikt is "urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport". De PasswordProtectedTransport klasse is van toepassing wanneer een opdrachtgever een authenticatie autoriteit een gebruiker laat verifiëren met een wachtwoord dialoog via een beveiligde sessie.	Ne e

Noot: DigiD kan verschillende authenticatiemiddelen hanteren om de identiteit van een gebruiker vast te stellen. Bij wijziging van de SAML contexten (saml:AuthnContextClassRef) kan de authenticatiesterkte wijzigen.

Noot: De huidige PasswordProtectedTransport heeft een te lage authenticatiesterkte en (AORTA) niveau voor patiënten die gebruik willen maken van het patiëntenportaal. In het [PvE VZVZ Portaal] staan de vereiste authenticatieniveau's benoemd.

Mogelijke authenticatieniveau's zijn hieronder opgenomen:

Authenticatieniveau (AORTA)	AuthnContextClassRef (SAML)	Comparison (SAML)	Authenticatiesterkte (DigiD)
Midden, waarbij een burger aan de hand van een wachtwoord en een tijdelijk eenmalige code, die hij per SMS ontvangt (per authenticatiepoging), authenticceert;	urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract	exact	20
AORTA vertrouwensniveau midden [1], gelijk aan het vorige niveau waarbij de burger eenmalig op zijn fysieke verschijning tegen zijn WID is geverifieerd (een zogeheten face2face controle)	urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract	better	22
Substantieel; gebruikers kunnen met de DigiD app een eenmalige controle uitvoeren op een paspoort, rijbewijs of identiteitskaart. Hierna is zijn of haar DigiD app geschikt om in te loggen op het niveau substantieel.	urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard	exact	25

Authenticatieniveau basis en hoog worden momenteel nog niet ondersteund.

Stap 3 en 4: Identificeren van een Gebruiker door de Identity Provider

De authenticatie-autoriteit bij de Identity Provider moet de identiteit van de gebruiker vast stellen. Het authenticatieverzoek hiertoe wordt gedaan door het patiëntenportaal die het element <RequestedAuthnContext> in het verzoek toevoegt. De authenticatie-autoriteit start een dialoog op met de gebruiker om deze te identificeren aan de hand van het <RequestedAuthnContext>, zie [SAML Authn Context] .

Eis: Voor bepaalde patiëntenportaalfunctionaliteit moet het authenticatieniveau of betrouwbaarheidsniveau door de authenticatie-autoriteit worden afgegeven zoals is opgenomen in de [PvE VZVZ portaal].

Stap 5: Het antwoord van de Identity Provider

Ongeacht of de identificatie van een patiënt door de Identity Provider wel of niet lukt, wordt er een antwoord naar het patiëntenportaal gestuurd in de vorm van een artefact. Het patiëntenportaal maakt gebruik van het artefact resolution profiel. Het patiëntenportaal maakt hierbij gebruik van een callback aanroep naar de Identity Provider, om het <Response> bericht met behulp van een SOAP binding over authenticatie op te halen. De locatie van de "Assertion Consumer Service" kan met behulp van metadata van het patiëntenportaal worden bepaald. De Identity Provider moet middelen hebben om vast te stellen dat deze locatie wordt gecontroleerd door het patiëntenportaal.

Het patiëntenportaal geeft aan welke SAML binding en specifieke "Assertion Consumer Service" gebruikt wordt voor het <AuthnRequest> bericht. De Identity Provider moet deze instellingen volgen.

Wanneer de authenticatie via de "SSO Service" van de Identity Provider succesvol verlopen is, wordt de gebruiker terug naar het patiëntenportaal gedirigeerd.

```
Redirect to https://aselectserver/server/saml20_assertion?
SAMLart=AAQAABhQELuXX%3D
```

Bovenstaand voorbeeld toont een SAML artefact referentie afgegeven door de "SSO Service" voor de "Assertion Consumer Service".

Stap 6: Het opvragen van een Artefact

Het patiëntenportaal maakt gebruik van het artefact resolution profiel, zie [SAML Profiles], om via een callback de <AuthnRequest> bericht te achterhalen waarin het uiteindelijke SAML authenticatie antwoord staat. Het artefact resolution profiel maakt gebruik van SOAP binding, wat ook in het SAML metadata bestand van de Identity Provider voor het patiëntenportaal is vastgelegd.

```
<md:IDPSSODescriptor ... >

  <md:ArtifactResolutionService

    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"

    Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"   Location="https://
federatie.overheid.nl/aselectserver/server/saml20_artifact"

    index="0"

    isDefault="true" />

  ...
```

```
</md:IDPSSODescriptor>
```

Het <ArtifactResolutionService> element is van het complexe type IndexedEndpointType en onderdeel van het <IDPSSODescriptor> element uit het SAML metadata bestand dat weer een specifiek profiel (dienstverlening) reflecteert ter ondersteuning van het SSO profiel van de Identity Provider.

Het <ArtifactResolutionService> element bestaat uit de volgende attributen en elementen:

Naam (@=attribuut)	Omschrijving	Vereist
@Binding	Specificeert de binding dat door de "Artefact Resolution Service" wordt ondersteund. De binding wordt via een URI geïdentificeerd. Bijvoorbeeld: "urn:oasis:names:tc:SAML:2.0:bindings:SOAP".	Ja
@Location	De locatie van de "Artefact Resolution Service". Ook een URI attribuut.	Ja
@index	Een unieke integer waarde die aan de "Artefact Resolution Service" wordt toegekend, waarnaar in het protocol bericht wordt verwezen.	Ja
@isDefault	Wordt gebruikt om een standaard (Artefact Resolution) Service aan te wijzen uit een geïndexeerde set van diensten.	Nee

Het patiëntenportaal stuurt een <ArtifactResolve> bericht met het gegeven <Artifact> referentie naar een "Artefact Resolution Service". De locatie van deze service kan weer met behulp van het SAML metadata bestand worden bepaald. Het opvragen van het artefact gebeurt via een beveiligde sessie met behulp van SOAP over HTTP.

```
<?xml version="1.0" encoding="UTF-8"?>

<soap11:Envelope xmlns:soap11="http://schemas.xmlsoap.org/soap/envelope/"

    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
```

```

    xmlns:saml="urn:oasis:names:tc:SAML:2.0:protocol">
<soap11:Body>

  <saml:ArtifactResolve

    ID="samlart_2.16.528.1.1007.3.3.1234567.1_0123456789"

    IssueInstant="2009-06-24T11:47:01Z"

    Version="2.0">

    <saml:Issuer

      Format="urn:oasis:names:tc:SAML:2.0:nameidformat:entity">https://
testportal.aorta-zorg.nl:443/topa-prototype/saml/SSO</saml:Issuer>

    <saml:Artifact>AAQAABhQELuXX=</saml:Artifact>

  </saml:ArtifactResolve>

</soap11:Body>
</soap11:Envelope>

```

Het <ArtifactResolve> element is van het complexe type ArtifactResolveType dat is afgeleid van RequestAbstractType en bestaat uit de volgende attributen en elementen:

Naam (@=attribuut)	Omschrijving	Vereist
@ID	Unieke identificatie van het Artefact verzoek. De waarde van het ID-attribuut in een verzoek en het InResponseTo attribuut in het bijbehorende antwoord moeten overeenkomen.	Ja
@IssueInstant	Tijdstipmoment van uitgifte van het Artefact verzoek. De tijds waarde is gecodeerd in UTC.	Ja

@Version	De versie van dit SAML Artefact verzoek. De aanduiding voor de versie van SAML gedefinieerd in deze specificatie wordt "2.0".	Ja
saml:Issuer	Geeft de entiteit die het Artefact verzoek doet.	Ja
samlp:Artifact	Artefact (referentie) waarde die de aanvrager heeft ontvangen en deze wenst te vertalen in het protocol boodschap die zij vertegenwoordigd. In dit geval is dat het antwoord op een authenticatie verzoek.	Ja

Eis: Er wordt bij een unieke artefact verzoek, maximaal één en eenmalig een artefact response bericht gegeven door de "Artefact Resolution Service", in antwoord op het verzoek.

Stap 7: De ArtifactResponse met de SAML assertion

Het uiteindelijke antwoord betreffende de authenticatie van een gebruiker staat in het <ArtifactResponse>. De "Artefact Resolution Service" geeft altijd een <Status> terug over de <ArtifactResponse>. De <ArtifactResponse> bevat de <Response> van de Identity Provider, of de identificatie en authenticatie van een gebruiker wel of niet gelukt is. Dit wordt ook weer met een <Status> aangegeven, maar dan voor de <Response>. Verder bevat de <Response> het uiteindelijke SAML assertion element <Assertion>.

```
<?xml version="1.0" encoding="UTF-8"?>

<soap11:Envelope xmlns:soap11="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">

  <soap11:Body>

    <samlp:ArtifactResponse

      Destination="Destination unknown"

      ID="_b2d765569da660eff830c352d5bb4da2"

      InResponseTo="samlart_2.16.528.1.1007.3.3.1234567.1_0123456789"

      IssueInstant="2009-06-24T11:47:05Z" Version="2.0">

      <saml:Issuer
```

```

    Format="urn:oasis:names:tc:SAML:2.0:nameidformat:entity">https://
testportal.aorta-zorg.nl:443/topa-prototype/saml/SSO</saml:Issuer>

    <samlp:Status>

        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>

    </samlp:Status>

    <samlp:Response ID="EE7E3DF7EBC86438"

        InResponseTo="authntoken_2.16.528.1.1007.3.3.1234567.1_0123456789"

        IssueInstant="2009-06-24T11:46:59Z" Version="2.0">

        <saml:Issuer

            Format="urn:oasis:names:tc:SAML:2.0:nameidformat:entity">https://
testportal.aorta-zorg.nl:443/topa-prototype/saml/SSO</saml:Issuer>

            <samlp:Status>

                <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>

            </samlp:Status>

            <saml:Assertion

                ID="__2c81606885bf79c716eb2c082a2249a5"

                IssueInstant="2009-06-24T11:46:59Z"

                Version="2.0"

                xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">

                    ...

            </saml:Assertion>

        </samlp:Response>

    </samlp:ArtifactResponse>

</soap11:Body>

</soap11:Envelope>

```

Het <ArtifactResponse> element is van het complexe type ArtifactResponseType dat een uitbreiding is van StatusResponseType en bestaat uit de volgende attributen en elementen:

Naam (@=attribuut)	Omschrijving	Vereist
@ID	Unieke identificatie van het antwoord van de "Artefact Resolution Service".	Ja
@Version	De aanduiding voor de SAML versie gedefinieerd in deze specificatie wordt "2.0".	Ja
@IssueInstant	Tijdstip van uitgifte van het antwoord. De tijds waarde is gecodeerd in UTC.	Ja
@InResponseTo	Moet de waarde bevatten die overeen komt met het ArtifactResolve@ID bericht.	Nee
saml:Issuer	Geeft de entiteit die het artefact verzoek heeft ingediend.	Nee
samlp:Status	Een code die de status van het desbetreffende verzoek weergeeft. Dit element heeft weer verplicht het samlp:StatusCode element in zich. Als het opvragen van het artefact geslaagd is, wordt de waarde "urn:oasis:names:tc:SAML:2.0:status:Success" teruggeven. Als het opvragen van het artefact niet geslaagd is wordt een foutcode gegenereerd, zie verder SSO meldingen voor de verschillende foutcodes.	Ja
samlp:Response	Het bericht element dat bestaat uit 0 of meerdere assertions die aan een (authenticatie) verzoek voldoen.	Nee

Het <Response> element is van het complexe type ResponseType en bevat de volgende elementen en attributen:

Naam (@=attribuut)	Omschrijving	Vereist
@ID	Unieke identificatie van het antwoord op het authenticatie verzoek.	Ja
@Version	De aanduiding voor de SAML versie gedefinieerd in deze specificatie wordt "2.0".	Ja
@IssueInstant	Tijdstip van uitgifte van het antwoord. De tijds waarde is gecodeerd in UTC.	Ja
@InResponseTo	Moet de waarde bevatten die overeen komt met het AuthnRequest@ID bericht.	Ja

saml:Issuer	Geeft de entiteit die het authenticatie verzoek heeft gegenereerd.	Ja
samlp:Status	Een code die de status van het desbetreffende verzoek weergeeft. Dit element heeft weer verplicht het samlp:Statuscode element in zich. Als het authenticatie verzoek geslaagd is, wordt de waarde "urn:oasis:names:tc:SAML:2.0:status:Success" teruggegeven. Als het authenticatie verzoek niet geslaagd is wordt een foutcode gegenereerd, zie verder SSO meldingen voor de verschillende foutcodes.	Ja
saml:Assertion	Dit type specificeert de basis informatie die gemeenschappelijk is voor alle afgegeven beweringen (assertion) door een vertrouwde partij of autoriteit.	Nee

Eis: Indien de samlp:Status $\neq$ "urn:oasis:names:tc:SAML:2.0:status:Success" moet er geen saml:Assertion element teruggegeven worden.

Het <Assertion> element is van het complexe type AssertionType. De opbouw en inhoud van het <Assertion> element wordt in paragraaf 2 Het SAML authenticatietoken besproken.

Het <Assertion> element valt in de gedeclareerde namespace van "urn:oasis:names:tc:SAML:2.0:assertion".

Eis: Indien er een Assertion wordt afgegeven **moet** de Identity Provider deze Assertion signeren in het daarvoor aangewezen Signature veld, zie paragraaf 2.4 Algoritmes.

Stap 8: Toegang verlening

Ter voltooiing van het SSO profiel, verwerkt het patiëntenportaal de <Response> en de daarbij behorende <Assertion>, en verleent of weigert hij de gebruiker of patiënt toegang tot het patiëntenportaal door antwoord te geven op het HTTP Request waarmee bij stap 1 werd begonnen.

De verleende <Assertion> is het lokaal geldig toegangsbewijs voor de patiënt om bepaalde handelingen te mogen uitvoeren op het patiëntenportaal, die in verbinding staat met de ZIM, die als (web)service fungeert waartussen beveiligde SOAP berichten worden uitgewisseld met behulp van SAML authenticatietokens.

Eis: De verleende assertion moet door het patiëntenportaal verwijderd worden na afloop van een TLS-sessie met het LSP respectievelijk na afloop van gebruik van de sessie door een patiënt of na het verstrijken van 15 minuten gerekend vanaf het afgiftemoment door DigiD.

10.3.2.10.5.2 **Bijlage C SSO verificatie**

Het goedbeheerde patiëntenportaal (GBP) moet voor elk bericht dat naar de ZIM doorgestuurd wordt een bijbehorende SAML authenticatietoken hebben. Deze tokens worden opgevraagd bij de Identity Provider (IdP) met behulp van een artefact referentie, zie stap 6 van Het SSO profiel. Het uiteindelijke antwoord van de IdP, een artefact response, bevat een SAML assertion over een patiënt, zie stap 7 van Het SSO profiel.

Voordat het GBP de assertion als SAML authenticatietoken gebruikt, moeten onderstaande controles uitgevoerd worden. Als het uiteindelijke antwoord van de IdP hieraan niet voldoet, mag de assertion niet gebruikt worden als SAML authenticatietoken tussen het GBP en het LSP.

De volgende controles moeten door het patiëntenportaal uitgevoerd worden:

- Controleer of het attribuut "InResponseTo" van het <ArtifactResponse> gelijk is aan de ID van het oorspronkelijke <ArtifactResolve> bericht;
- Controleer of het attribuut "InResponseTo" van het <Response> gelijk is aan de ID van het oorspronkelijke <AuthnRequest> bericht;
- Verifieer het attribuut "Issuer" van het <ArtifactResponse> element of die overeenkomt met de Assertion Consumer Service URL;
- Verifieer het attribuut "Status" van het <ArtifactResponse> element of die overeenkomt met de waarde "urn:oasis:names:tc:SAML:2.0:status:Success";
- Verifieer het attribuut "Issuer" van het <Response> element of die overeenkomt met de Assertion Consumer Service URL;
- Verifieer het attribuut "Status" van het <Response> element of die overeenkomt met de waarde "urn:oasis:names:tc:SAML:2.0:status:Success".

10.3.2.10.5.3 **Bijlage D SSO meldingen**

De volgende statuscodes (URI referenties) worden door SAML onderkend en geretourneerd binnen het SSO profiel waar van toepassing (De volgende tabel is deels overgenomen uit [SAML Assertion Protocol]).

De SAML meldingen worden alleen binnen het SSO profiel gebruikt. Dat wil zeggen dat de meldingen alleen voorkomen tussen het patiëntenportaal (GBP) en de Identity Provider (IdP).

Een statuscode is een Uniforme Resource Name (URN) en is als volgt opgebouwd:

"urn:"<Namespace Identifier>":"<Name Specific String>

Voorbeeld: "urn:oasis:names:tc:SAML:2.0:status:Success"

In de statuscode tabel wordt alleen de omschrijving en de specifieke string getoond.

Omschrijving	Namespace Specific String
The request could not be performed due to an error on the part of the requester.	Requester
The request could not be performed due to an error on the part of the SAML responder or SAML	Responder
The SAML responder could not process the request because the version of the request message was incorrect.	VersionMismatch
The responding provider was unable to successfully authenticate the principal.	AuthnFailed
The specified authentication context requirements cannot be met by the responder.	NoAuthnContext
The SAML responder or SAML authority is able to process the request but has chosen not to respond.	RequestDenied
The SAML responder or SAML authority does not support the request.	RequestUnsupported
The SAML responder cannot process any requests with the protocol version specified in the request.	RequestVersionDeprecated
The SAML responder cannot process the request because the protocol version specified in the request message is a major upgrade from the highest protocol version supported by the responder.	RequestVersionTooHigh
The SAML responder cannot process the request because the protocol version specified in the request message is too low.	RequestVersionTooLow
The resource value provided in the request message is invalid or unrecognized.	ResourceNotRecognized
The response message would contain more elements than the SAML responder is able to return.	TooManyResponses
The responding provider does not recognize the principal specified or implied by the request.	UnknownPrincipal
The SAML responder cannot properly fulfill the request using the protocol binding specified in the request.	UnsupportedBinding

[1] De AuthnContextClassRef is niet te onderscheiden van Authenticatieniveau midden. Hier dient rekening mee te worden gehouden bij de verwerking van het token. De service die dit authenticatieniveau vereist dient zodanig geconfigureerd te worden dat het de aanvullende maatregelen (F2F-token) ook controleert.

10.3.2.10.6 Referenties authenticatie DigiD

10.3.2.10.6.1 Bijlage A Referenties

Referentie	Document	Versie
[IH tokens generiek]	Implementatiehandleiding security tokens generiek (see page 435)	8.3.0.0
[SAML Assertion Protocol]	Assertion and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0 http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf	2.0 15 maart 2005
[SAML Authn Context]	Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0 http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf	2.0 15-mrt-2005
[SAML Profiles]	Profiles for the OASIS Security Assertion Markup Language (SAML) v2.0 http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf	2.0 15-mrt-2005
[SAML Token]	SAML Token Profile http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SAMLTOKENProfile.pdf	1.1 01-feb-2006
[WSS]	WS-Security SOAP Message Security http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SOAPMessageSecurity.pdf	1.1 01-feb-2006
[PvE VZVZ Portaal]	Programma van Eisen VZVZ Portaal	n.v.t.

[DigiD Koppel]	Koppelvlakspecificatie DigiD SAML Authenticatie https://www.logius.nl/fileadmin/logius/ns/diensten/digid/155/koppelvlakspecificaties/Koppelvlakspecificatie_ ¹⁵⁶ SAML_DigiD4_v3_3.pdf ¹⁵⁷	3.3 31- aug-2016

10.3.2.11 AORTA_Auth_IH_Berichtauthenticatie_PKIO

- **IH Berichtauthenticatie PKIO**

Datum: 1 mei 2022

Publicatie: V8.3.0.0

155. https://www.logius.nl/fileadmin/logius/ns/diensten/digid/koppelvlakspecificaties/Koppelvlakspecificatie_SAML_DigiD4_v3_3.pdf

156. https://www.logius.nl/fileadmin/logius/ns/diensten/digid/koppelvlakspecificaties/Koppelvlakspecificatie_SAML_DigiD4_v3_3.pdf

157. https://www.logius.nl/fileadmin/logius/ns/diensten/digid/koppelvlakspecificaties/Koppelvlakspecificatie_SAML_DigiD4_v3_3.pdf

10.3.2.11.1 Inleiding Berichtauthenticatie PKIO

10.3.2.11.1.1 Doel en scope

Dit document heeft tot doel een handleiding te geven voor de implementatie van het koppelvlak tussen het goed beheerd klantenloket (GBK) en het landelijk schakelpunt (LSP) voor wat betreft de toe te passen technieken voor de authenticatie van klantenloketmedewerkers.

10.3.2.11.1.2 Doelgroep voor dit document

Dit document is bedoeld voor softwareontwikkelaars van het goed beheerd klantenloket en het LSP, die op grond van de HL7v3 communicatiestandaard en op grond van dit document berichten willen uitrusten met het SAML authenticatietoken. Daarnaast wordt het plaatsen van de digitale handtekening besproken (zie ook [IH tokens generiek]).

10.3.2.11.1.3 Documenthistorie

Versie	Datum	Omschrijving
6.10.0.0	12-okt-2011	RfC 46142: SOAP Headers van tokens worden uitgebreid met soap:actor.
6.11.0.0	12-okt-2012	Ongewijzigde herpublicatie als onderdeel van AORTA-Infrastructuur v6.11
6.12.0.0	17-juni-2013	RfC 58592: Subject.organizationName gewijzigd naar Vereniging van Zorgaanbieders voor Zorgcommunicatie.
8.0.1.0	15-mei-2017	Opgenomen in publicatie 8.0.1.0
8.0.2.0	31-januari-2018	RfC 76680: Uitbreiding DigiD authenticatieniveaus
8.0.3.0	15-nov-2018	Opgenomen in publicatie 8.0.3.0
8.2.0.0	7-okt-2020	Opgenomen in publicatie 8.2.0.0

10.3.2.11.1.4 Legenda

Deze implementatiehandleiding gebruikt de volgende symbolen:

	Let op! Dit is een aandachtspunt. Een opmerking die de aandacht vestigt op een bepaald opvallend aspect.
	Dit is een 'open issue' of 'known issue'. Een kwestie die nog open ligt voor discussie, maar onderkend is.
	Dit is een frequently asked question (FAQ) met antwoord.

10.3.2.11.2 Het SAML authenticatietoken Berichtauthenticatie PKIO

In dit hoofdstuk wordt de inhoud van het SAML authenticatietoken besproken die bij berichtauthenticatie met behulp van de PKIO-pas wordt gebruikt. Het SAML authenticatietoken bevat informatie over de toegepaste authenticatie en identificatie van de klantenloketmedewerker en namens welke patiënt het verzoek wordt afgehandeld. Het SAML authenticatietoken is een op XML gebaseerd SAML assertion en heeft tot doel de *assertions* (bewijs van een bewering) over te brengen tussen partijen.

Alle XML voorbeelden in het document dienen door de betrokken partijen tijdens het bouwen van de uitwisseling getest, en waar nodig, in samenspraak met Nictiz aangepast te worden voor een juiste optimale werking.

Voor het verkrijgen van het SAML authenticatietoken en het aanbieden van dit token aan het LSP worden de volgende profielen gebruikt:

- Het gebruik van het SAML authenticatietoken (security token) in het kader van het WSS SOAP berichten profiel voor het veilig stellen en uitwisseling van authentieke SOAP berichten.

Dit profiel raakt het koppelvlak:

- goed beheerd klantenloket (GBK) – het landelijk schakelpunt (LSP)

Dit profiel wordt in de volgende paragrafen verder uitgewerkt.

10.3.2.11.2.1 Structuur

Het SAML authenticatietoken is een afgegeven SAML assertion die gebruikt wordt bij berichtauthenticatie met behulp van de PKIO-pas voor het landelijk EPD. Het SAML authenticatietoken heeft de volgende structuur (de waarden die in het token gebruikt worden zijn fictief):

```

<saml:Assertion
  ID="token_2.16.528.1.1007.3.3.1234567.1_0123456789"
  IssueInstant="2009-06-24T11:47:34Z"
  Version="2.0"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
  <!-- De partij (klantenloket applicatie) die deze assertion heeft gecreëerd, -->
  <!-- wordt als een OID gepresenteerd. Moet door de GBK organisatie geregeld worden --
  >
  <!-- Applicatie-id van de GBK-applicatie, zoals toegekend bij aansluiting. -->
  <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
    urn:IIroot:2.16.840.1.113883.2.4.6.6:IIext:?
  </saml:Issuer>
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    ...
  </ds:Signature>
  <!-- Het onderwerp -->
  <saml:Subject>
    <!-- Serienummer van persoonlijk certificaat van een medewerker-->
    <saml:NameID>urn:cert:35972415477696508790773831356241</saml:NameID>
  </saml:Subject>
  <!-- Geldigheidsduur en geldige toehoorder van de assertion -->
  <saml:Conditions
    NotBefore="2009-06-24T11:47:34Z"
    NotOnOrAfter="2009-06-24T11:52:34Z">
    <saml:AudienceRestriction>
      <!-- Root en extensie van de ZIM -->
      <saml:Audience>urn:IIroot:2.16.840.1.113883.2.4.6.6:IIext:1</saml:Audience>
    </saml:AudienceRestriction>
  </saml:Conditions>

```

```

<saml:AuthnStatement
  AuthnInstant="2009-06-24T11:47:34"
  SessionIndex="token_2.16.528.1.1007.3.3.1234567.1_0123456789">
  <!-- Authenticatiemiddel -->
  <saml:AuthnContext>
    <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI</
    saml:AuthnContextClassRef>
  </saml:AuthnContext>
</saml:AuthnStatement>

<!-- Overige HL7 attributen die ondertekend worden -->
<saml:AttributeStatement>
  <saml:Attribute Name="triggerEventId">
    <saml:AttributeValue>QRX_TE990011NL</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute Name="messageIdRoot">
    <saml:AttributeValue>2.16.528.1.1007.3.3.1234567.1</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute Name="messageIdExt">
    <saml:AttributeValue>0123456789</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute Name="burgerServiceNummer">
    <saml:AttributeValue>950052413</saml:AttributeValue>
  </saml:Attribute>
</saml:AttributeStatement>
</saml:Assertion>

```

10.3.2.11.2.2 Namespaces

Het SAML authenticatietoken die gebruikt wordt bij berichtauthenticatie met behulp van de PKIO-pas maakt gebruik van de volgende namespaces. De prefixen zijn niet normatief maar worden in dit document als voorbeelden gebruikt.

Tabel AORTA.STK.t3300 – Namespaces

Prefix	Namespace URI
ds	http://www.w3.org/2000/09/xmldsig#
saml	urn:oasis:names:tc:SAML:2.0:assertion
wss	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd



Bij het gebruik van de namespace-prefixes is het van belang deze na het ondertekenen niet meer te veranderen, dit maakt de digitale handtekening ongeldig.

10.3.2.11.2.3 Inhoud

De volgende paragrafen beschrijven de verschillende kenmerken en beveiligingsgerelateerde gegevens die het SAML authenticatietoken onderscheiden, zoals in [IH tokens generiek] beschreven is.

```
<saml:Assertion ... xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
```

Het SAML authenticatietoken begint met het Assertion element en een verwijzing naar de XML SAML namespace voor SAML 2.0 assertions. De attributen behorende bij het Assertion element wordt in [paragraaf 2.3.1 \(see page 568\)](#) Uniekheid beschreven.

Uniekheid


```
ID="token_2.16.528.1.1007.3.3.1234567.1_0123456789"

IssueInstant="2009-06-24T11:47:34Z"

Version="2.0">
```

De volgende attributen van het SAML assertion element maken van de SAML assertion een uniek gegeven, uitgegeven door de verzender van het bericht. Het attribuut ID identificeert op een unieke wijze de assertion. De waarde moet *mondiaal uniek* zijn voor AORTA berichten, zodat bij samenvoegen van meerdere XML bestanden (in een HL7v3 batch of anderszins) de waarde uniek blijft. De aanbevolen methode is:

- begin met de string "token" en een underscore "_"
- voeg hier de root van het HL7v3 [message.id](#)¹⁵⁸ aan toe
- voeg hier een underscore "_" aan toe
- voeg hier de extension van het HL7v3 [message.id](#)¹⁵⁹ aan toe
- bijvoorbeeld: token_2.16.528.1.1007.3.3.1234567.1_0123456789

Deze methode garandeert dat iedere waarde uniek is, ook wanneer meerdere HL7v3 berichten in een XML bestand worden samengevoegd. (De methode kan niet verplicht worden, omdat de extension van een [message.id](#)¹⁶⁰ niet numeriek hoeft te zijn, en het dus mogelijk is dat deze karakters bevat die in een XML ID niet toegestaan zijn. In dat geval dient een leverancier er zelf voor te zorgen een waarde te genereren die uniek is voor een AORTA bericht. Hierbij dient dan een UUID (Universally Unique Identifier) gebruikt te worden. Bij het gebruik van andere vormen is er een kans, hoe klein ook, dat een ID samenvalt met een ID gemaakt volgens een andere methode van een andere leverancier).

Het attribuut IssueInstant is een tijdstipmoment van uitgifte van de SAML assertion. De tijdswaarde is gecodeerd in UTC. Het attribuut Version is de gebruikte SAML versie van de SAML assertion. De aanduiding voor de versie van SAML gedefinieerd in deze specificatie is "2.0".

Onderwerp

```
<saml:Subject>

  <saml:NameID>

    urn:cert:35972415477696508790773831356241
```

158. <http://message.id>

159. <http://message.id>

160. <http://message.id>

```
</saml:NameID>

</saml:Subject>
```

Het Subject bevat identificerende gegevens van het systeem dat de transactie heeft geïnitieerd. Het subject bevat het serienummer van het authenticiteitcertificaat. Het Subject wordt als URN (Uniform Resource Name) genoteerd en wordt aan de hand van het PKI-overheid-certificaat gevalideerd. De URN is opgebouwd uit:

"urn:cert:"<serienummer authenticiteitcertificaat>

Het OID (Object Identifier) van het serienummer van het certificaat is een uniek identificerend kenmerk, binnen de context van een gegeven CA, en is onweerlegbaar terug te voeren naar de klantenloketmedewerker.

Geldigheid

```
<saml:Conditions

  NotBefore="2009-06-24T11:47:34Z"

  NotOnOrAfter="2009-06-24T11:52:34Z">
```

Het attribuut *NotBefore* is de tijd waarop de SAML assertion geldig wordt. Dit hoeft niet de tijd te zijn waarop het bericht is aangemaakt. Het is mogelijk *NotBefore* in de toekomst te zetten, en het bericht na deze tijd pas te verzenden.



Wordt een bericht ontvangen voor *NotBefore* is aangevangen, dan **moet** dit bericht geweigerd worden.

Het attribuut *NotOnOrAfter* is de tijd waarop de SAML assertion vervalt.



Wordt een bericht ontvangen op of nadat *NotOnOrAfter* is verstreken, dan **moet** dit bericht geweigerd worden.

Deze tijd is als bovenstaande tijd geformatteerd. Richtlijn voor het verschil tussen *NotBefore* en *NotOnOrAfter* is 5 minuten. Het wordt sterk aanbevolen de SAML assertion direct (binnen 5 minuten) te gebruiken voor berichten die verzonden worden (dus terwijl de klantenloketmedewerker achter diens computer zit). Het gaat immers om het voorkomen van misbruik van onderschepte tokens, en 5 minuten is meer dan voldoende om de hele keten van vraag tot antwoord te doorlopen.



De geldigheidsduur van een token (*NotOnOrAfter* minus *NotBefore*) mag niet langer dan 5 minuten zijn. Wordt een bericht ontvangen waarin deze geldigheidsduur overschreden is, dan **moet** dat bericht geweigerd worden, ook al is het tijdstip *NotOnOrAfter* nog niet verstreken.

Het inperken van bepaalde partijen (AudienceRestriction) waarvoor de assertion bedoeld is wordt beschreven in [paragraaf 2.3.5 \(see page 572\)](#) Ontvanger.

De subelementen OneTimeUse en ProxyRestriction worden niet gebruikt binnen het <Conditions> element bij berichtauthenticatie met behulp van de PKIO-pas.

Afzender

```
<!-- Applicatie-id van de GBK-applicatie, zoals toegekend bij aansluiting. -->
<!-- Root en extensie van het GBK, Moet GBK org. aanvragen en regelen. -->

urn:IIroot:2.16.840.1.113883.2.4.6.6:IIext:?

</saml:Issuer>
```

Het applicatie-id van de afzender die deze SAML assertion heeft gecreëerd en de gebruiker authenticceert. De Issuer wordt uitgedrukt met behulp van een URN (Uniform Resource Name). De URN is opgebouwd uit:

"urn:IIroot:"<OID voor AORTA Applicatie-id's>":IIext:"<applicatie-id GBK>

De URN string is opgebouwd uit een IIroot en een IIext. "II" staat voor het HL7v3 datatype Instance Identifier. Om de namespace in URN uniek te krijgen is II als prefix voor de root en ext geplaatst.

AORTA Applicatie-id's worden uitgedrukt als een id onder het identificatiesysteem "2.16.840.1.113883.2.4.6.6". Het correcte applicatie-id voor het GBK wordt toegekend bij aansluiting op de AORTA. Stel dat dit "300" zou zijn, dan ziet de URN er als volgt uit:

urn:IIroot:2.16.840.1.113883.2.4.6.6:IIext:300

Ontvanger

```
<saml:AudienceRestriction>
  <!-- Root en extensie van de ZIM -->
  <saml:Audience>urn:IIroot:2.16.840.1.113883.2.4.6.6:IIext:1</saml:Audience>
</saml:AudienceRestriction>
```

In de AudienceRestriction wordt beschreven aan wie de SAML assertion is gericht. De waarden in de elementen zijn (voorlopig) vaste waarden. Voor de <Audience> parameter is (ook) gekozen voor URN, zie voor opbouw [paragraaf 2.3.4 \(see page 571\)](#) Afzender.

Authenticatie

```
<saml:AuthnStatement
  AuthnInstant="2009-06-24T11:47:34"
  SessionIndex="token_2.16.528.1.1007.3.3.1234567.1_0123456789">
```

Het subject, een klantenloketmedewerker, in de SAML assertion is geauthenticeerd door middel van een authenticatiemiddel op een gegeven moment.

```
<saml:AuthnContext>
  <saml:AuthnContextClassRef
    >urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI</saml:AuthnContextClassRef>
</saml:AuthnContext>
```

Binnen de gebruikte applicatie beveiligingsstandaarden is er sprake van verschillende vertrouwensniveaus.

Binnen de SAML-specificatie geeft men een authenticatie-context (*AuthnContext*) mee die de context van het gebruikte authenticatiemiddel aangeeft. Hiervoor zijn een aantal contexten gespecificeerd, zie [SAMLAuthnContext], die gebruikt worden als referentiekader voor de communicatie tussen de ZIM en andere componenten zoals GBK applicaties.

Uitgaande van de beveiligingsniveaus van GBK, klantenloketmedewerker en PKIO-pas wordt het "urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI" beveiligingsniveau gehanteerd om het AORTA vertrouwensniveau midden voor klantenloketmedewerkers weer te geven.

```
</saml:AuthnStatement>
```

Einde van de gegevens voor de authenticatie conform de SAML specificatie.

Attributen

```
<saml:AttributeStatement>
```

De volgende attributen zijn gegevens uit het HL7v3 bericht die met de authenticatie meegetekend worden. Dit zijn kopieën van gegevens die elders in hetzelfde HL7v3 bericht voorkomen. De volgorde van de attributen in het AttributeStatement is niet relevant. Er mogen geen andere attributen opgenomen worden in het AttributeStatement dan hier beschreven is.

```
<saml:Attribute Name="triggerEventId">
  <saml:AttributeValue>QURX_TE990011NL</saml:AttributeValue>
</saml:Attribute>
```

Het attribuut TriggerEventId wordt altijd meegetekend. Het trigger event identificeert *de aanleiding voor het verzenden* van het bericht, en bepaalt dus de intentie van de verzender. Merk op dat het trigger event geen verplicht element in het HL7v3-bericht zelf is. Dit attribuut meesturen verhindert veel soorten aanvallen, bijvoorbeeld het token van een query kapen en proberen deze te hergebruiken voor het afhandelen van verzoeken van patiënten en hun vertegenwoordigers om inzage te verkrijgen in de verwijsindex. Het is ook mogelijk de interactionId te gebruiken: deze wijzigt echter tussen versies van berichten, het triggerEventId meestal niet, zodat een nieuwe versie van het bericht niet noodzakelijk wijzigingen voor het token tot gevolg heeft.

```
<saml:Attribute Name="messageIdRoot">
  <saml:AttributeValue>2.16.528.1.1007.3.3.1234567.1</saml:AttributeValue>
</saml:Attribute>

<saml:Attribute Name="messageIdExt">
  <saml:AttributeValue>0123456789</saml:AttributeValue>
</saml:Attribute>
```

De Attributen messageIdRoot en messageIdExt vormen een uniek gegeven, uitgegeven door de verzender van het HL7v3-bericht. De combinatie van de attribuutwaarden messageIdRoot en messageIdExt moeten gelijk zijn aan het uiteindelijk gebruikte HL7v3 message.Id.

```
<saml:Attribute Name="burgerServiceNummer">
  <saml:AttributeValue>950052413</saml:AttributeValue>
</saml:Attribute>
```

Voor berichten die betrekking hebben op een enkele patiënt, wordt het burgerServiceNummer (BSN) van de patiënt opgenomen. Dit maakt ook weer vele aanvallen onmogelijk, namelijk gegevens van een andere patiënt proberen op te vragen. Dit geldt voor alle berichten die betrekking hebben op één en niet meer dan één patiënt.

Het BSN in het token moet overeenkomen met het BSN in het bericht. In het geval er sprake is van een voorlooptuul in het bericht, dan dient deze ook overgenomen te worden in het token.

Voor berichten die geen betrekking hebben op een persoon waarvan het burgerServiceNummer bekend is, wordt het burgerServiceNummer weggelaten.

Het attributen statement blok ziet er dan bijvoorbeeld zo uit (de volgorde van de attributen is niet relevant):

```
<saml:Attribute Name="triggerEventId">
  <saml:AttributeValue>QURX_TE990011NL</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="messageIdRoot">
  <saml:AttributeValue>2.16.528.1.1007.3.3.1234567.1</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="messageIdExt">
  <saml:AttributeValue>0123456789</saml:AttributeValue>
```

```
</saml:Attribute>
```

Tenslotte wordt het attributen statement blok afgesloten met

```
</saml:AttributeStatement>
```

10.3.2.11.2.4 Algoritmes

Om de integriteit en onweerlegbaarheid van het SAML authenticatietoken te waarborgen wordt een XML Signature geplaatst, zoals beschreven in [IH tokens generiek]. Na plaatsen van de XML Signature kan de ontvanger, met gebruikmaking van het persoonsgebonden PKI-overheid-certificaat van de verzender en de CA certificaten zoals verstrekt door PKI-overheid, onomstotelijk vaststellen dat het SAML authenticatietoken ondertekend is met de privé sleutel behorend bij het gebruikte en meegezonden certificaat van de klantloketmedewerker.

De XML Signature van het SAML authenticatietoken die gebruikt wordt bij berichtauthenticatie met behulp van de PKIO-pas maakt gebruik van de volgende algoritmes, zoals beschreven in [IH tokens generiek]:

- Voor het berekenen van de hashwaarde wordt SHA-256 gebruikt.
- Voor de digitale handtekening in AORTA wordt gebruik gemaakt van een RSA handtekening over een SHA-256 digest.



Omdat de XML Signature onderdeel is van het SAML authenticatietoken en in het SAML authenticatietoken geplaatst wordt, moet er een "enveloped-signature" transformatie uitgevoerd worden die de Signature tags uit het SAML authenticatietoken verwijderd.

10.3.2.11.2.5 Opbouw

De headers

Eerst wordt het SAML authenticatietoken – het <saml:Assertion ...> element aangemaakt en gevuld met die elementen, zoals beschreven in [paragraaf 2.3 \(see page 568\)](#) Inhoud.


```

<saml:Assertion
  ID="token_2.16.528.1.1007.3.3.1234567.1_0123456789"
  IssueInstant="2009-06-24T11:47:34Z"
  Version="2.0"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
  ... Zie paragraaf 2.3 Inhoud ...
</saml:Assertion>

```

Het XML Signature blok is onderdeel van het SAML authenticatietoken. Het XML Signature blok komt na het <saml:Issuer> element.

```

<saml:Assertion
  ID="token_2.16.528.1.1007.3.3.1234567.1_0123456789"
  IssueInstant="2009-06-24T11:47:34Z"
  Version="2.0"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
  ... Zie paragraaf 2.3 Inhoud ...
  <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
    urn:IIroot:?:IIext:?
  </saml:Issuer>
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
      ...
    </ds:SignedInfo>
    <ds:SignatureValue>Wuwn...5e4=</ds:SignatureValue>
    <ds:KeyInfo>
      <ds:X509Data>

```

```

...
</ds:X509Data>

</ds:KeyInfo>

</ds:Signature> ...
</saml:Assertion>

```

Indien de Signature aangemaakt wordt moet niet meer met de strings (saml:Assertion en SignedInfo) gemanipuleerd worden, maar ze moeten octet-voor-octet overgenomen worden in het bericht. Strikt genomen is het toegestaan wijzigingen aan te brengen die door canonicalisatie bij de ontvanger weer opgeheven worden, maar wanneer de digitale handtekening door middel van strings wordt opgebouwd, is het een foutgevoelige handeling.

Lange Base 64 waarden zijn afgekort. Wederom kan dit als strings worden behandeld, waarbij drie waarden vervangen moeten worden.

Deze drie waarden worden ingevuld:

- Neem het SignedInfo blok op.
- Neem de SignatureValue op.
- Neem certificaatgegevens in het KeyInfo blok op.



Wanneer een bericht een SAML assertion bevat, moet dat bericht precies één bijbehorende digitale handtekening bevatten.



Voor authenticatie doeleinden mag er niet meer dan één SAML assertion voorkomen met een daarbij behorende X.509 certificaat als KeyInfo.

Het maken van de XML Signature uit strings levert de SAML assertion op met daarin de Signature.

Plaats van het SAML token en de digitale handtekening

Het SAML authenticatietoken met daarin de digitale handtekening wordt in het WS-Security SOAP Header gezet. Op het <wss:Security> element **moet** een soap:mustUnderstand="1" vlag opgenomen worden, die aangeeft dat de ontvanger dit security element **moet** verwerken en een soap:actor="<http://www.aortarelease.nl/actor/zim>" die aangeeft dat de ZIM dit security element verwerkt.

```
<soap:Header xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  ...
  <wss:Security xmlns:wss=
    "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
    soap:actor="http://www.aortarelease.nl/actor/zim" soap:mustUnderstand="1">
    <saml:Assertion ... >
    ... Zie paragraaf 2.3 Inhoud ...
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:SignedInfo>
        ...
      </ds:SignedInfo>
      <ds:SignatureValue>Wuwn...5e4=</ds:SignatureValue>
      <ds:KeyInfo>
        <ds:X509Data>
          ...
        </ds:X509Data>
      </ds:KeyInfo>
    </ds:Signature>
    <saml:Assertion ... >
  </wss:Security>
</soap:Header>
```

10.3.2.11.3 Certificaten Berichtauthenticatie PKIO

10.3.2.11.3.1 Te gebruiken certificaat en attributen

Voor het tekenen van het SAML authenticatietoken worden persoonsgebonden authenticiteitcertificaten uit de PKIoverheid hiërarchie gebruikt. Dit certificaat bevat een RSA publieke sleutel. Met de privé sleutel wordt de digitale handtekening gegenereerd.

De attributen in het authenticiteitcertificaat worden gegeven in de vorm van een Distinguished Name (DN) en het serienummer, zie [IH tokens generiek].

Tabel AORTA.STK.t3310 – Certificaat attributen

Attribuut	Omschrijving	Waarde
CN	Subject.commonName	<Volledige naam van de persoon, zie [CP PKIO] deel 3a>
OU	Subject.organizationalUnitName	Klantenloket
O	Subject.organizationName	Vereniging van Zorgaanbieders voor Zorgcommunicatie
C	Subject.countryName	C=NL <zie [CP PKIO] deel 3a>
Serienummer	SerialNumber. Wordt door de certificaatdienstverlener vastgelegd	<zie [CP PKIO] deel 3a>



De issuer.commonName verschilt per 'generatie' PKIO-passen.

De root en de domeinen die het door NCSC als "goed" beoordeelde SHA algoritme gebruiken, worden aangemerkt als G2, waarbij G staat voor generatie. De Issuer DN kan alleen dynamisch afgeleid worden uit het gebruikte authenticatie certificaat. De verschillende generaties PKIO-passen kunnen bij een klantenloket naast elkaar gebruikt worden.



Het serialNumber van het authenticiteitscertificaat van de pas wordt gebruikt in combinatie met de attributen O en OU om een klantenloketmedewerker te identificeren.

Om de digitale handtekening bij het LSP te verifiëren, moet de ontvanger over de bijbehorende publieke sleutel beschikken, zie [IH tokens generiek]. Voor verificatie is gekozen door het certificaat met de publieke sleutel mee te zenden in KeyInfo van het SAML authenticatietoken, zie ook [IH tokens generiek].

Noot: In samenspraak met Nictiz en andere betrokken partijen kan de keuze voor het meezenden van het certificaat nog heroverwogen worden.

Noot: In het testtraject worden ook PKIO-passen gebruikt.

10.3.2.11.4 Token afhandeling Berichtauthenticatie PKIO

10.3.2.11.4.1 Verificatie van het bericht

Het is belangrijk vast te stellen dat de velden in het SAML authenticatietoken overeenstemmen met die in het HL7v3 bericht en geldig ondertekend zijn. Wanneer dit niet zou gebeuren, kan een kwaadwillende met een gestolen token nog steeds gegevens opvragen van bv. ieder willekeurig burgerservicenummer.

De ontvanger controleert of de WS-Security SOAP Header voor hem bestemd is, zie soap attribuut actor.

Het SAML authenticatietoken wordt door de ontvanger uit de WS-Security SOAP Header gehaald indien de WS-Security SOAP Header voor de ontvanger bestemd is en dat de ontvanger deze moet verwerken. Bij gebruik van het SAML authenticatietoken moet de ontvanger controleren of:

- Het attribuut ID van het Assertion element op een unieke wijze het uiteindelijk gebruikte HL7v3 message.Id identificeert, zie [Uniekheid \(see page 568\)](#) ;
- De aanduiding voor de versie van SAML gedefinieerd is op "2.0", zie [Uniekheid \(see page 568\)](#) ;
- Het bericht ontvangen is binnen de geldigheidsperiode van het token, zie [Geldigheid \(see page 570\)](#) ;
- Het serienummer van het authenticatie certificaat overeenkomt met de NameID van het Subject, zie [paragraaf 2.3.2](#)¹⁶¹;
- De juiste afzender is vastgelegd die deze assertion heeft gecreëerd en de gebruiker heeft geauthenticeerd, zie [Afzender \(see page 571\)](#) ;
- De afnemer van het SAML authenticatietoken (audience) het LSP is, zie [Ontvanger \(see page 572\)](#) ;
- De klantenloketmedewerker is geauthenticeerd via het voorgedefinieerde authenticatiemiddel, de SmartCardPKI, zoals beschreven in [Authenticatie \(see page 572\)](#) ;
- Alleen die attributen zijn gedefinieerd, die zijn beschreven in [Attributen \(see page 573\)](#) ;

161. <https://vzvz.atlassian.net/wiki/pages/createpage.action?spaceKey=A8&title=v>

- De attribuutwaarde van TriggerEventId overeenkomt met het berichttype van het HLv3 bericht, zie [Attributen \(see page 573\)](#) ;
- De attribuutwaarden van messageIdRoot en messageIdExt overeenkomt met de gebruikte HL7v3 [message.id](#)¹⁶², zie [Attributen \(see page 573\)](#) ;
- De attribuutwaarde van burgerServiceNummer overeenkomt met het BSN in het HL7v3 bericht ofwel doordat de gegevens in het bericht daadwerkelijk betrekking hebben op de persoon, zie [Attributen \(see page 573\)](#);

Als aan één van de bovenstaande condities niet is voldaan, moet het bericht door de ontvanger geweigerd worden en een SOAP foutmelding aan het verzendende systeem afgegeven worden, zie foutafhandeling in [IH tokens generiek].

Als wel aan alle condities is voldaan, wordt het HL7v3 bericht verder verwerkt.

10.3.2.11.5 Referenties Berichtauthenticatie PKIO

Referentie	Document	Versie
[IH tokens generiek]	Implementatiehandleiding security tokens generiek (see page 435)	8.3.0.0
[SAMLAuthnContext]	Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0 http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf	2.0 15- mrt-2005
[CP PKIO]	Certificate Policies	3.0 25 januari 2011

10.3.2.12 AORTA_Auth_IH_Berichtauthenticatie_UZI

162. <http://message.id>

- **IH Berichtauthenticatie met de UZI-pas**

Datum: 1 mei 2022

Publicatie: V8.3.0.0

10.3.2.12.1 Inleiding Berichtauthenticatie UZI

10.3.2.12.1.1 Doel en scope

Dit document beschrijft op welke wijze berichten tussen een goed beheerd zorgsysteem (GBZ) en het landelijk schakelpunt (LSP) worden uitgerust met authenticatietokens.

Dit document specificeert het authenticatietoken voor zorgverleners en hun medewerkers dat wordt gemaakt met hun UZI-pas. Daarnaast wordt het plaatsen van de digitale handtekening besproken (zie ook [IH tokens generiek]).

10.3.2.12.1.2 Doelgroep voor dit document

Dit document is bedoeld voor softwareontwikkelaars van XIS'en.

10.3.2.12.1.3 Documenthistorie

Versie	Datum	Omschrijving

6.10. 0.0	12- okt-201 1	RfC 46142: SOAP Headers van tokens worden uitgebreid met soap:actor.
6.11. 0.0	12- okt-201 2	Ongewijzigde herpublicatie als onderdeel van AORTA-Infrastructuur v6.11
6.12. 0.0	4- okt-201 3	Bijlage technische context (gebruik UZI-pas) weer toegevoegd (zat in v6.0.5.0, maar verdwenen in v6.10)
8.0.1 .0	15- mei-20 17	RfC 52477: Uitwisseling op basis van bouwstenen.
8.0.1 .0	15- mei-20 17	RfC 65592: SHA1 encryptiemethoden verwijderd
8.0.1 .0	15- mei-20 17	RfC 65898 en RfC 36422 SHA1 delen van AORTA_Auth_IH_Berichtauthenticatie_UZI.doc bijwerken met SHA256. Voor nieuwe leveranciers is het gebruik van SHA256 als DigestMethod en als onderdeel van SignatureMethode verplicht. Verwijzingen naar G2 generatie UZI-certificaat hiërarchie verwijderd.
8.0.1 .0	15- mei-20 17	RfC 71719: PKIO/UZI certificaten gaan over naar de Public G3/Private G1 generatie.
8.0.1 .0	15- mei-20 17	RfC 76206: SSL verwijderen
8.0.3 .0	15- nov-20 18	Opgenomen in publicatie 8.0.3.0
8.2.0 .0	7- okt-202 0	Opgenomen in publicatie 8.2.0.0

10.3.2.12.1.4 Legenda

Deze implementatiehandleiding gebruikt de volgende symbolen:

	Let op! Dit is een aandachtspunt. Een opmerking die de aandacht vestigt op een bepaald opvallend aspect.
	Dit is een 'open issue' of 'known issue'. Een kwestie die nog open ligt voor discussie, maar onderkend is.
	Dit is een frequently asked question (FAQ) met antwoord.

10.3.2.12.2 Het SAML authenticatietoken Berichtauthenticatie UZI

In dit hoofdstuk wordt concreet de inhoud van het authenticatietoken besproken die bij berichtauthenticatie met behulp van de UZI-pas wordt gebruikt.

10.3.2.12.2.1 Structuur

Het authenticatietoken die gebruikt wordt bij berichtauthenticatie met behulp van de UZI-pas voor het landelijk EPD heeft de volgende structuur:

```
<signedData xmlns="http://www.aortarelease.nl/805/"
  xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
  wsu:Id="token_2.16.528.1.1007.3.3.1234567.1_0123456789">
  <authenticationData>
    <messageId>
      <root>2.16.528.1.1007.3.3.1234567.1</root>
      <extension>0123456789</extension>
    </messageId>
    <notBefore>20070128173600</notBefore>
    <notAfter>20070128174059</notAfter>
    <addressedParty>
      <root>2.16.840.1.113883.2.4.6.6</root>
```

```

    <extension>1</extension>

  </addressedParty>

</authenticationData>

<coSignedData>

  <triggerEventId>QURX_TE990011NL</triggerEventId>

  <patientId>

    <root>2.16.840.1.113883.2.4.6.3</root>

    <extension>012345672</extension>

  </patientId>

</coSignedData>

</signedData>

```

10.3.2.12.2.2 Namespaces

Het authenticatietoken die gebruikt wordt bij berichtauthenticatie met behulp van de UZI-pas maakt gebruik van de volgende namespaces. De prefixen zijn niet normatief maar worden in dit document als voorbeelden gebruikt.

Tabel AORTA.STK.t3200 – Namespaces

Prefix	Namespace URI
-	http://www.aortarelease.nl/805/
-	http://www.w3.org/2000/09/xmldsig#
soap	http://schemas.xmlsoap.org/soap/envelope/
wsu	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd

In de voorbeelden wordt voor de eenvoud gewerkt zonder namespace-prefixes, dus:

```
<signedData xmlns="http://www.aortarelease.nl/805/..."
```

in plaats van:

```
<ao:signedData xmlns:ao="http://www.aortarelease.nl/805/..."
```

Namespace prefixes mogen echter wel gebruikt worden, dus ontvangers moeten tokens met prefixes goed kunnen verwerken. Bij het gebruik van prefixes is het wel van belang deze na ondertekening niet meer te veranderen, dit maakt de digitale handtekening ongeldig.

```
<signedData xmlns="http://www.aortarelease.nl/805/"
  xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
  utility-1.0.xsd"
  wsu:Id="token_2.16.528.1.1007.3.3.1234567.1_0123456789">
```

Het token begint bij het <signedData> element. Het <signedData> element is geen HL7v3 element, maar gedefinieerd binnen deze specificatie.

De AORTA namespace "<http://www.aortarelease.nl/805/>" is verplicht en wordt als standaard namespace ingesteld voor de berichtauthenticatie met UZI-pas.

Een *Id* attribuut is verplicht (ook de hoofdletter I en kleine letter d). Voor het Id wordt de WS-Security 1.0 richtlijn van een Id in de wsu namespace gevolgd. De waarde van het wsu:Id attribuut moet uniek zijn in het hele XML bestand. De waarde moet *globaal uniek* zijn voor AORTA berichten, zodat bij samenvoegen van meerdere XML bestanden (in een HL7v3 batch of anderszins) de waarde uniek blijft.

10.3.2.12.2.3 Inhoud

```
<authenticationData>
```

De volgende paragrafen beschrijven de verschillende basis kenmerken en beveiligingsgerelateerde gegevens die het authenticatietoken onderscheiden, zoals in [IH tokens generiek] beschreven is.

Uniekheid

```
<messageId>

  <root>2.16.528.1.1007.3.3.1234567.1</root>

  <extension>0123456789</extension>

</messageId>
```

Een uniek gegeven, uitgegeven door de verzender van het bericht. Deze moet gelijk zijn aan het uiteindelijk gebruikte HL7v3 message.Id.

Geldigheid

```
<notBefore>20070128173600</notBefore>
```

De tijd waarop het authenticatietoken geldig wordt. Dit hoeft niet de tijd te zijn waarop het bericht is aangemaakt. Vaak zal het complete bericht pas later aangemaakt worden. In principe is het mogelijk *notBefore* in de toekomst te zetten, en het bericht na deze tijd pas te verzenden. Wordt een bericht ontvangen voor *notBefore* is aangevangen, dan **moet** dit bericht geweigerd worden.

De tijd moet doorgegeven worden als Coordinated Universal Time (UTC), volgens de ook in HL7v3 gebruikte ISO 8601 notatie. Deze notatie is YYYYMMDDHHMMSS, bijvoorbeeld "20080225134130" zonder tussenvoegsels als "T", ":" etc. Er wordt geen gebruik gemaakt van timezones, dus "20080225134130+1" is niet toegestaan. De verzender en ontvanger zijn verantwoordelijk voor het eventueel converteren van lokale tijd naar UTC, en dus daarbij rekening houden met zomer- en wintertijd. De precisie is in seconden.

```
<notAfter>20070128174059</notAfter>
```

De tijd waarop het authenticatietoken vervalst. Wordt een bericht ontvangen nadat *notAfter* is verstreken, dan **moet** dit bericht geweigerd worden. Deze tijd is als bovenstaande tijd geformatteerd. Het aanbevolen verschil tussen *notBefore* en *notAfter* is 5 minuten. Het maximaal toegestane verschil is 90 minuten. Dit maximum dient voor berichten die niet direct, maar bijvoorbeeld 's nachts verzonden worden, of kort voor de aanvang van een consult, zodat er iets ruimere mogelijkheden voor batchgewijze processen zijn. Het wordt sterk aanbevolen dat voor berichten die direct verzonden worden (dus terwijl de zorgverlener of medewerker achter diens computer zit) niet afgeweken wordt van de periode van vijf minuten. Het gaat immers om het voorkomen van misbruik van onderschepte tokens, en vijf minuten is meer dan voldoende om de hele keten van vraag tot antwoord te doorlopen.



De geldigheidsduur van een token (*notAfter* minus *notBefore*) mag niet langer dan 90 minuten zijn. Wordt een bericht ontvangen waarin deze maximale geldigheidsduur overschreden is, dan **moet** dat bericht geweigerd worden, ook al is het tijdstip *notAfter* nog niet verstreken.

Richtlijn: de beste geldigheidsduur van een token (*notAfter* minus *notBefore*) voor online bevraging is 5 minuten.

Ontvanger

```
<addressedParty>
  <root>2.16.840.1.113883.2.4.6.6</root>
  <extension>1</extension>
</addressedParty>
```

Het applicatie-id van het geadresseerde zorgsysteem, hier de ZIM. Het betreft hier het systeem waaraan het authenticatietoken gericht is; dat hoeft niet hetzelfde te zijn als het systeem waaraan het bericht zelf gericht is. De waarden in de elementen zijn (voorlopig) vaste waarden, omdat authenticatie alleen naar de ZIM geschiedt (behoudens testsituaties).

Attributen

```
<coSignedData>
```

Met de authenticatie meegetekende gegevens uit het bericht. Dit zijn kopieën van gegevens die ook in het bericht voorkomen. Deze zijn vooral wenselijk omdat de authenticatiegegevens op zich niet verhinderen dat het token met een ander bericht (met gelijk message-Id) wordt gebruikt.

```
<triggerEventId>QURX_TE990011NL</triggerEventId>
```

Merk op dat het trigger event geen verplicht element in het HL7v3-bericht zelf is. Het wordt echter altijd opgenomen in het token, omdat bij elke interactie een trigger event gespecificeerd is. De Trigger Event identificeert het *berichttype* uniek, en bepaalt dus de intentie van de verzender. Deze meesturen verhindert veel soorten aanvallen, bijv. een authenticatie van een medicatiequery kapen en pogen deze te hergebruiken voor het opvragen van een waarneemdossier. Het is ook mogelijk de interactionId te gebruiken: deze wijzigt echter tussen versies van berichten, het triggerEventId niet, zodat een nieuwe versie van het bericht geen wijzigingen voor het token tot gevolg heeft. De Trigger Events zijn te vinden in het vocab bestand 2.16.840.1.113883.1.6.xml.

```
<contextCode>
  <codeSystem>2.16.840.1.113883.2.4.3.111.15.1</codeSystem>
  <code>KZDI</code>
</contextCode>
```

In het geval er sprake is van een opvraag op basis van een context dient ook de contextCode meegetekend te worden. Dit is in principe alleen het geval bij de generiekeQueryZorggegevens. Bij deze generieke query is het trigger event niet meer voldoende om de intentie van de verzender aan te geven, aangezien deze altijd gelijk is. Door het toevoegen van de contextCode wordt deze intentie wel weer expliciet gemaakt. De codes zijn te vinden in het vocab bestand 2.16.840.1.113883.2.4.3.111.15.1.xml.

```

<patientId>

  <root>2.16.840.1.113883.2.4.6.3</root>

  <extension>012345672</extension>

</patientId>

```

Voor berichten die betrekking hebben op een enkele patiënt, wordt het burgerservicenummer van de patiënt opgenomen. Dit maakt ook weer vele aanvallen onmogelijk, namelijk gegevens van een andere patiënt proberen op te vragen. Dit geldt voor alle berichten die betrekking hebben op één en niet meer dan één patiënt; ook als het burgerservicenummer niet voorkomt in het bijbehorende schema. Het burgerservicenummer is te vinden in het patientId met root 2.16.840.1.113883.2.4.6.3.

Voor berichten die geen betrekking hebben op een persoon wordt het BSN weggelaten. Het hele coSignedData blok ziet er dan zo uit:

```

<coSignedData>

  <triggerEventId>QURX_TE990011NL</triggerEventId>

</coSignedData>

```

Tenslotte wordt het token afgesloten.

```

</signedData>

```

10.3.2.12.2.4 Algoritmes

Om de integriteit en onweerlegbaarheid van het authenticatietoken te waarborgen wordt een XML Signature geplaatst, zoals beschreven in [IH tokens generiek]. Na plaatsen van de XML Signature kan de ontvanger, met gebruikmaking van het persoonsgebonden UZI certificaat van de verzender, vaststellen dat het authenticatietoken ondertekend is met de privé sleutel behorend bij het gebruikte en meegezonden certificaat.

De XML Signature van het authenticatietoken die gebruikt wordt bij berichtauthenticatie met behulp van de UZI-pas maakt gebruik van de volgende algoritmes, zoals beschreven in [IH tokens generiek].

Voor het berekenen van de hashwaarde wordt SHA-256 gebruikt. Voor de digitale handtekening wordt RSA gebruikt.

10.3.2.12.2.5 Opbouw

De headers

Eerst wordt het token – het <signedData> element aangemaakt. Een voorbeeld:

```
<ao:authenticationTokens xmlns:ao="http://www.aortarelease.nl/805/" soap:actor="http://
www.aortarelease.nl/actor/zim" soap:mustUnderstand="1">

  <signedData ...>

    ... Het eerder gedefinieerd signedData blok ...

  </signedData>

</ao:authenticationTokens>
```

Vervolgens moet het XML Signature blok in een WSS 1.0 SOAP Header opgenomen worden. Een voorbeeld:

```
<wss:Security xmlns:wss="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd" soap:actor="http://www.aortarelease.nl/actor/zim"
soap:mustUnderstand="1">

  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">

    <SignedInfo ...>

      ...

    </SignedInfo>
```



```

    <SignatureValue>
        ...
    </SignatureValue>
    <KeyInfo>
        ...
    </KeyInfo>
</Signature>
</wss:Security>

```

Wanneer er met strings gewerkt wordt bij het zetten van de digitale handtekening, moet hier niet meer met de strings (signedData en SignedInfo) gemanipuleerd worden, maar ze moeten octet-voor-octet overgenomen worden in het bericht. Strikt genomen is het toegestaan wijzigingen aan te brengen die door canonicalisatie bij de ontvanger weer opgeheven worden, maar wanneer de digitale handtekening door middel van strings wordt opgebouwd, is het een foutgevoelige handeling.

Lange Base 64 waarden zijn afgekort. Wederom kan dit als strings worden behandeld, waarbij drie waarden vervangen moeten worden.

Deze drie waarden worden ingevuld:

- Neem het SignedInfo blok op.
- Neem de SignatureValue op.
- Neem certificaatgegevens in het KeyInfo blok op.

Canonicalisatie speelt alleen bij die XML code waarover een SHA digest wordt berekend of waarover RSA handtekeningen worden gezet. Het maken van de XML Signature uit strings levert dus twee blokken tekst op: de signedData en de Signature.

Plaats van het token

Het authenticatietoken wordt opgenomen in een SOAP Header.



Voor authenticatie doeleinden mag er niet meer dan één authenticatietoken voorkomen.

```
<soap:Header xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">

  <ao:authenticationTokens xmlns:ao="http://www.aortarelease.nl/805/"

    soap:actor="http://www.aortarelease.nl/actor/zim" soap:mustUnderstand="1">

      <signedData xmlns="http://www.aortarelease.nl/805/" xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
wsu:Id="token_2.16.528.1.1007.3.3.1234567.1_0123456789">

        <authenticationData>

          ...

        </authenticationData>

        <coSignedData>

          ...

        </coSignedData>

      </signedData>

    </ao:authenticationTokens>

    ...

  </soap:Header>
```

Het token – het <signedData> element – wordt opgenomen in het <authenticationTokens> element van de <soap:Header>. Dit is voor het geval er (in de toekomst) meerdere authenticatietokens in een bericht zouden kunnen voorkomen. Op het <authenticationTokens> element **moet** een soap:mustUnderstand="1" vlag opgenomen worden, die aangeeft dat de ontvanger deze header **moet** verwerken. Bij het <authenticationTokens> element **mag** met een soap:actor="<http://www.aortarelease.nl/actor/zim>"¹⁶³ worden aangegeven dat de ZIM deze header verwerkt.

163. <http://www.aortarelease.nl/actor/lsp>

Het declareren van de namespace "<http://www.aortarelease.nl/805/>" bij <signedData> is niet nodig: deze wordt overgeërfd van het bovenliggende element. Bij canonicalisatie zal bij de ontvanger de namespace teruggeplaatst worden voor controle van de digitale handtekening. Voor de duidelijkheid is de namespace declaratie hier tweemaal opgenomen.

Plaats van de digitale handtekening

De digitale handtekening wordt in een WS-Security 1.0 SOAP Header gezet. Op het <wss:Security> element **moet** een soap:mustUnderstand="1" vlag opgenomen worden, die aangeeft dat de ontvanger dit security element **moet** verwerken. Bij het <authenticationTokens> element **mag** met een soap:actor="<http://www.aortarelease.nl/actor/zim>¹⁶⁴" worden aangegeven dat de ZIM dit security element verwerkt.



Wanneer een bericht een authenticatietoken bevat, moet dat bericht precies één bijbehorende digitale handtekening bevatten.

De volgorde van beide headers (authenticatietoken en digitale handtekening) is niet relevant: zowel digitale handtekening vóór het token als token vóór de digitale handtekening zijn geldig.

```
<soap:Header xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  ...
  <wss:Security xmlns:wss=
    "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
    soap:actor="http://www.aortarelease.nl/actor/zim" soap:mustUnderstand="1">
    <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
      <SignedInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
        ...
      </SignedInfo>
      <SignatureValue>...</SignatureValue>
      <KeyInfo>
        <X509Data>
```

¹⁶⁴ <http://www.aortarelease.nl/actor/lsp>

```

...
</X509Data>

</KeyInfo>

</Signature>

</wss:Security>

</soap:Header>

```

10.3.2.12.3 Certificaten Berichtauthenticatie UZI

10.3.2.12.3.1 Te gebruiken certificaat en attributen

De UZI-pas kent een aantal modellen:

Tabel AORTA.STK.t3210 – UZI pastype

Naam UZI-pastype	Codering Pastype
Zorgverlenerpas	Z
Medewerkerpas op naam	N
Medewerkerpas niet op naam	M
Servercertificaat	S

De pas die gebruikt wordt voor het ondertekenen van een authenticatietoken moet een zorgverlenerpas of een medewerkerpas op naam zijn. Hoewel het pastype gecodeerd is opgenomen in het authenticiteitcertificaat (in het subjectAltName attribuut), dient een applicatie op basis van de uitgevende CA vast te stellen wat het pastype van de UZI-pas is.

De signature wordt gezet met de sleutel voor authenticiteit (keyUsage=digitalSignature, hexadecimaal 0x80).

De attributen in het authenticiteitcertificaat worden gegeven in de vorm van een Distinguished Name (DN), zie [IH tokens generiek].

De waarden van deze attributen voor de relevante UZI-passen zijn:

Tabel AORTA.STK.t3220 – DN attributen van zorgverlenerspas

Attribuut	Omschrijving	Waarde
CN	Issuer.commonName	SHA-2 generatie (G21): UZI-register Zorgverlener CA G21 Generatie Public G3: UZI-register Zorgverlener CA G3
O	Issuer.organisationName	SHA-2 generatie (G21): agentschap Centraal Informatiepunt Beroepen Gezondheidszorg Public G3/Private G1 generatie: CIBG
C	Issuer.countryName	NL

Tabel AORTA.STK.t3230 – DN attributen van medewerkerpas op naam

Attribuut	Omschrijving	Waarde
CN	Issuer.commonName	SHA-2 generatie (G21): UZI-register Medewerker op naam CA G21 Generatie Public G3: UZI-register Medewerker op naam CA G3

O	Issuer.organisationName	SHA-2 generatie (G21): agentschap Centraal Informatiepunt Beroepen Gezondheidszorg Public G3/Private G1 generatie: CIBG
C	Issuer.countryName	NL

Om de digitale handtekening bij het LSP te verifiëren, moet de ontvanger over de bijbehorende publieke sleutel beschikken, zie [IH tokens generiek].

Voor verificatie is gekozen een verwijzing naar het certificaat mee te zenden; de ontvanger moet deze dan met bijvoorbeeld het LDAP protocol ophalen in de directory van het UZI-register.

Zie voor de verdere beschrijving van de passen [UZI pas].

Noot: uiteraard mogen in het testtraject alleen UZI-testpassen gebruikt worden. Het gebruik hiervan wordt verder niet uitgewerkt in deze handleiding. De werking is identiek.

10.3.2.12.4 Token afhandeling Berichtauthenticatie UZI

10.3.2.12.4.1 Verificatie met het bericht

Bij ontvangst van een bericht met authenticatietoken moet het *ontvangende systeem* het token en de digitale handtekening daarover controleren (zie [IH tokens generiek]) en controleren of het token overeenstemt met het bericht. Deze twee onderwerpen van controle worden hieronder beschreven.

Bij ontvangst van een bericht haalt het ontvangende systeem het token uit de SOAP header. Het ontvangende systeem controleert of:

- Het gebruikte certificaat geldig is, zie [Certificaten \(see page 596\)](#) ;
- De messageld in het token overeen komt met de gebruikte HL7v3 message.Id in het bericht, zie [Uniekheid \(see page 588\)](#) ;
- Het bericht ontvangen is binnen de geldigheidsperiode van het token, zie [Geldigheid \(see page 588\)](#) ;
- Het token bestemd is voor het geadresseerde zorgsysteem, zie [Ontvanger \(see page 589\)](#) ;
- In het token het patientId staat, en dit patientId overeenkomt met het gebruikte HL7v3 patientId (indien in bericht aanwezig), zie [Attributen \(see page 589\)](#) ;
- In het token het triggerEventId staat, zie [Attributen \(see page 589\)](#)

Als aan één van bovenstaande condities niet is voldaan, wordt het bericht geweigerd en wordt een SOAP foutmelding aan het verzendende systeem gegeven, zie foutafhandeling in [IH tokens generiek]. Als wel aan alle condities is voldaan, wordt het HL7v3 bericht verder verwerkt.

	Als er geen authenticatietoken in de SOAP header is aangetroffen <i>kan</i> het HL7v3 bericht wel verder worden verwerkt, op voorwaarde dat voor de betreffende interactie het vertrouwensniveau "laag" is toegestaan.

Naast de controle van het token moeten bij het bericht een aantal gegevens worden vastgehouden die verderop worden gebruikt voor inhoudelijke controle van het bericht:

- Authenticatietoken aanwezig (ja/nee);
- UZI-nummer van de afzender van het bericht (afkomstig uit het certificaat van de afzender);
- URA-nummer van het systeem dat het bericht heeft verstuurd (afkomstig uit het servercertificaat van dat systeem, die onderdeel is van gegevens van de TLS sessie).

10.3.2.12.5 Referenties Berichtauthenticatie UZI

Referentie	Document	Versie
[AETSDK]	Software Developers Kit beschikbaar gesteld door AET Europe B.V. Geeft toelichting bij de PKCS#11 stappen die nodig zijn voor het ondertekenen van een authenticatie 'challenge'. http://www.uziregister.nl ¹⁶⁵	
[IH tokens generiek]	Implementatiehandleiding security tokens generiek (see page 435)	8.3.0.0
[EXCC14N]	Exclusive XML Canonicalization, Version 1.0, W3C Recommendation	1.0 18-juli-2002
[MIME]	Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies http://www.ietf.org/rfc/rfc2045.txt	

¹⁶⁵. <http://www.uziregister.nl/>

[UZI pas]	CA Model, Pasmodel, Certificaat- en CRL-profielen Zorg CSP. http://www.uziregister.nl/ https://www.uziregister.nl/overhetuziregister/hierarchie-productieomgeving	7.0 16 jan 2014

10.3.2.12.6 Bijlage B Technische context (gebruik UZI-pas)

10.3.2.12.6.1 Inleiding

Voor realisatie van de cryptografische beveiligingsfuncties wordt binnen AORTA gebruik gemaakt van de Private Key Infrastructuur (PKI) die geboden wordt door het UZI-register. Het UZI-register verstrekt smartcards (UZI-passen) aan zorgverleners en medewerkers van zorgaanbieders. De UZI-pas bevat X.509 certificaten voor authenticatie, vertrouwelijkheid en elektronische handtekeningen en de bijbehorende private keys. Bij zogenaamde Medewerkerpassen niet op naam ontbreekt het handtekeningcertificaat, maar deze pas is binnen AORTA niet bruikbaar.

De UZI-pas is een smartcard. Deze bevat een NXP microprocessor, operating systeem (NXP JCOP) en de nodige (Java Card) programmatuur om kleine programma's te kunnen draaien. Zie [UZITS] voor details. De smartcard ondersteunt het RSA algoritme voor public/private key cryptografie, het door NCSC als "goed" beoordeelde SHA algoritme voor hashing en AES algoritmen voor symmetrische versleuteling.

De smartcard kan benaderd worden via de meegeleverde SafeSign middleware van AET. Zie voor actuele versies van de software:

<http://www.uziregister.nl/uzipas/gebruikuzipas/paszonderabonneenummer/>

<http://www.uziregister.nl/ondersteuning/handleidingeneninstallatie/>

Het UZI-register ondersteunt deze middleware op Windows; Linux (SuSe en RedHat distributie) en MacOS X operating systeem[1].

10.3.2.12.6.2 Application Programming Interfaces voor benadering UZI-pas

De AET middleware biedt twee interfaces om de smartcard te benaderen:

1. De [PKCS#11] interface. Dit is een leveranciers onafhankelijke standaard API -ook wel Cryptoki genoemd- voor cryptografische modules om cryptografische informatie te benaderen (certificaten, sleutels) en om cryptografische functies aan te roepen die op deze modules worden uitgevoerd (zoals het ondertekenen van data). Deze interface is platformonafhankelijk en wordt voor de UZI-pas ondersteund op Windows, Linux en MacOS.
2. [MSCrypto] MS CryptoAPI is een microsoftstandaard en biedt een API om cryptografische functies aan te roepen die door een zogenaamde Cryptographic Service Provider worden uitgevoerd.

Naast verschil in platformondersteuning is een belangrijk verschil het abstractieniveau:

- PKCS#11 is een API die specifiek is ontwikkeld voor smartcards en andere hardware modules. Deze biedt tot in detail inzicht in de stappen die uitgevoerd worden en de objecten op de UZI-pas die benaderd worden. Dit geeft de ontwikkelaar meer controle over het gebruik van de UZI-pas.
- MS CryptoAPI is een interface op een hoger abstractieniveau en is niet 'smartcard aware'. Er worden crypto functies aangeroepen, maar de programmeur hoeft daarbij niet te weten dat sommige functies in specifieke hardware uitgevoerd worden (zoals het signen van data op de UZI-pas zelf).

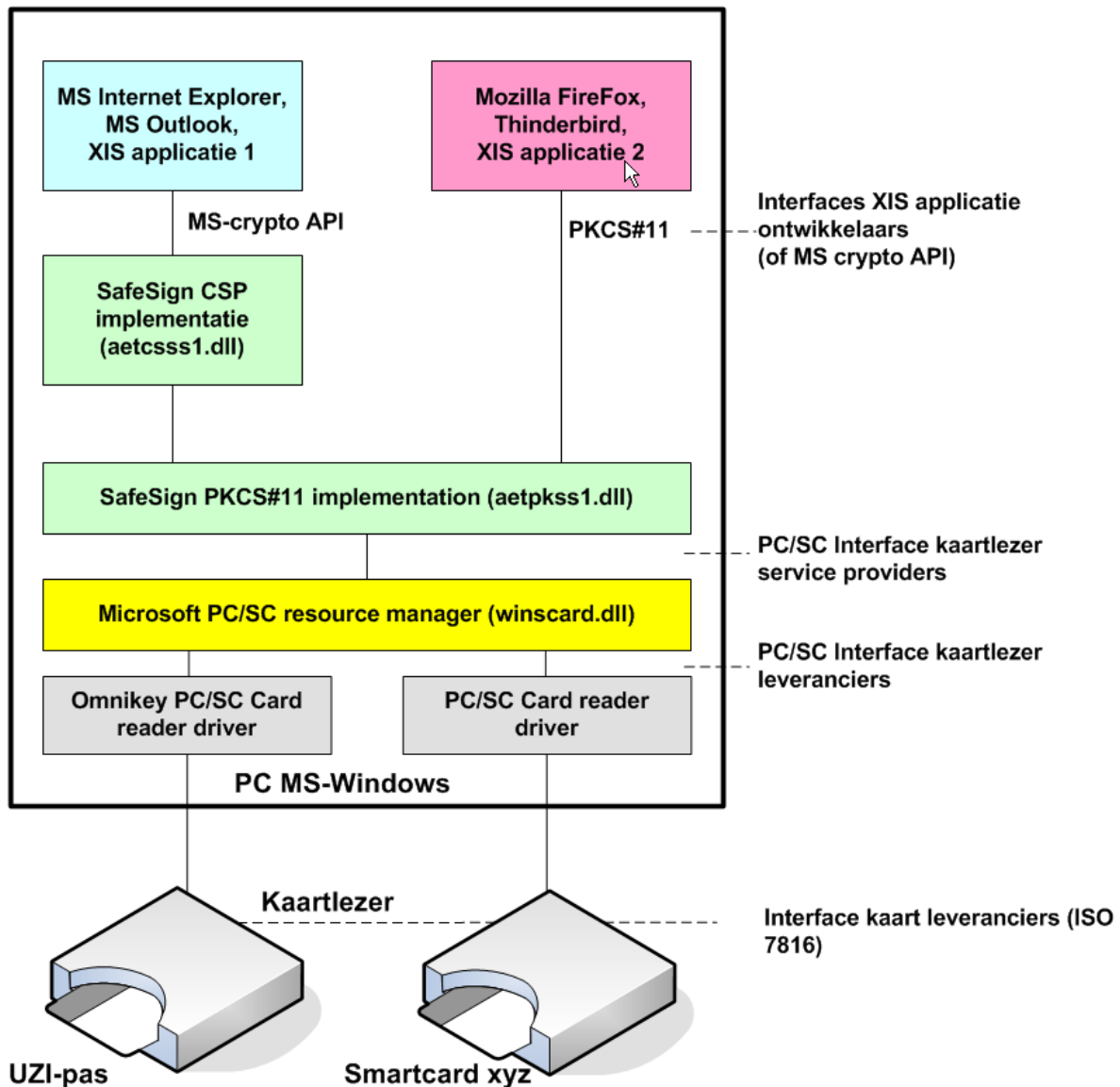
Het gebruik van de PKCS#11 interface heeft de voorkeur vanwege de volgende overwegingen:

- Open standaard die breed gedragen is in de industrie;
- Platform (Operating System) onafhankelijk;
- Performance is beter en beter te optimaliseren;
- Meer controle over het exacte aanroepen van de UZI-pas vanuit de toepassing.

Dit is de reden dat in de voorbeelden alleen PKCS#11 functies zijn genoemd.

10.3.2.12.6.3 Software architectuur voor benadering UZI-pas

Onderstaand figuur geeft schematisch en globaal weer welke software componenten gebruikt worden bij het aanroepen van de UZI-pas vanuit een XIS-applicatie. Beide interfaces zijn hierbij weergegeven.



Figuur 1: Software architectuur bij gebruik UZI-pas op MS-Windows PC

Toelichting standaard interfaces

Rechts in de figuur zijn de belangrijkste standaard interfaces aangegeven. Deze interfaces realiseren de volgende zaken:

- Generieke interfaces voor XIS-applicatie ontwikkelaars: PKCS#11 en MS Crypto API (Cryptographic Service Provider). Deze standaarden screenen de technische complexiteit van de UZI-pas af en maakt de XIS-applicatie onafhankelijk van de kaartlezer, hardware van de UZI-pas en het operating system op de UZI-pas;
- De PC/SC interface voor middleware en kaartlezer software. Deze standaard maakt het gebruik van de UZI-pas mogelijk met kaartlezers van diverse leveranciers (Omnikey, Gemplus, etc.) en

van verschillende fysieke interfaces met de PC (USB, PCMCIA, Serieel). De PC/SC resource managers (wincard.dll) zijn componenten van het operating system en zorgt dat meerdere applicaties logisch gezien tegelijkertijd met 1 UZI-pas kunnen communiceren. Dit is hieronder apart toegelicht;

- De ISO 7816 standaard. Deze maakt het mogelijk om in de toekomst smartcards te gebruiken van andere leveranciers (hardware chip en card operating system) onafhankelijk van de in gebruik zijnde kaartlezers en applicaties.

Toelichting PC/SC resource management

Met de SafeSign middleware is het mogelijk dat meerdere client-applicaties logisch gezien 'tegelijkertijd' gebruik maken van de UZI-pas, bijvoorbeeld Outlook, IE, FireFox en één of meer lokale XIS-clients.

Op het laagste niveau kan de UZI-pas slechts communiceren met één applicatie omdat het (zoals de meeste smartcards) een 'single-threaded device' is dat sequentieel alle communicatie afhandelt. Dit hoeft geen probleem te zijn want bij printers of database records kan er uiteindelijk ook maar één applicatie tegelijk gebruik maken van de resource. De PC/SC resource manager van MS-Windows dwingt af dat iedere applicatie afzonderlijk de UZI-pas 'claimt' en de communicatie afhandelt. Op dat moment blokkeren de andere toepassingen totdat de communicerende toepassing klaar is. Vervolgens kan een andere toepassing communiceren met de UZI-pas. De SafeSign middleware communiceert dus altijd via de PC/SC resource manager met de UZI-pas.

Ondanks het resource management vanuit het OS en de middleware zijn er wel een aantal richtlijnen vanuit de PC/SC standaard voor de applicaties[2]. Ook als er op hoog abstractieniveau ontwikkeld wordt –door gebruik te maken van third party libraries- is het van groot belang om de onderliggende PC/SC architectuur goed te begrijpen. Tevens dient men te verifiëren dat de applicatierichtlijnen uit de PC/SC standaard ingevuld zijn, samengevat:

- Communiceer alleen met de pas als het nodig is;
- Geef geen reset naar de smartcard;
- Claim geen exclusieve toegang tot de smartcard behalve als dat noodzakelijk is;
- Beëindig connecties bij afsluiten van de applicatie[3].

10.3.2.12.6.4 Gebruik van UZI-pas voor authenticatie

Op de website van het UZI-register is een [AETSDK] beschikbaar die toelichting geeft bij de stappen die nodig zijn voor het ondertekenen van een authenticatie challenge met behulp van PKCS#11 functies.

Deze stappen zijn bij tokenauthenticatie identiek aan de huidige authenticatie met TLS voor zover het gaat om het aanroepen van de UZI-pas. Het verschil zit in de "challenge/data/digestvalue/hashwaarde" die ondertekend wordt. Bij tokenauthenticatie is dat de hash-waarde van het security

token en bij implementatie van een TLS client is dat de hash-waarde die conform de TLS specificaties wordt berekend tijdens de TLS handshake fase.

De stappen voor het gebruik van de UZI-pas zijn:

- Laad de PKCS #11 library
- Initialiseer de PKCS #11 library (C_Initialize)
- Zoek een token^[4] (C_GetSlotList, C_WaitForSlotEvent)
- Open een session met het token (C_OpenSession)
- Zoek het authenticatiecertificaat op het token (C_FindObjects...)
- Log in met PIN (C_Login)
- Zoek de bijbehorende sleutel (C_FindObjects...)
- Teken de challenge/digestvalue (C_Sign...)
- Log uit (C_Logout)
- Beëindig sessie (C_CloseSession)
- Sluit PKCS #11 af (C_Finalize)

Voor een verdere toelichting wordt verwezen naar de [AETSDK] die een presentatie bevat waarin iedere PKCS#11 functie aanroep is toegelicht. Daarnaast bevat de SDK ook voorbeeldcode.

[1] AET Europe B.V. –de leverancier van SafeSign- ondersteunt meer operating systemen dan het UZI-register.

[2] Deel 7 bevat de *Application Domain and Developer Design Considerations*. Paragraaf 3.3 gaat over *Device Sharing and Control*. Zie www.pcscworkgroup.com¹⁶⁶.

[3] De middleware zorgt ervoor dat PKCS#11 of Crypto API aanroepen niet onnodig gecombineerd worden, maar dat kleine atomaire transacties uitgevoerd worden met de smartcard.

[4] In de PKCS#11 context is een 'token' een hardware token: een smartcard.

10.3.2.12.7 Bijlage C Token implementatie

Deze bijlage met een voorbeeld van het tekenen gaat uit van het gebruik van een door NCSC als "goed" beoordeelde SHA algoritme.

10.3.2.12.7.1 Maak een signedData blok

Het token moet aangemaakt worden en voorzien van de gegevens uit het bericht.

¹⁶⁶ <http://www.pcscworkgroup.com>

Het volgende is een voorbeeld van een token:

```
<signedData xmlns="http://www.aortarelease.nl/805/"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
utility-1.0.xsd"
wsu:Id="_2.16.528.1.1007.3.3.1234567.1_0123456789">
  <authenticationData>
    <messageId>
      <root>2.16.528.1.1007.3.3.1234567.1</root>
      <extension>0123456789</extension>
    </messageId>
    <notBefore>20070128173600</notBefore>
    <notAfter>20070128174059</notAfter>
    <addressedParty>
      <root>2.16.840.1.113883.2.4.6.6</root>
      <extension>1</extension>
    </addressedParty>
  </authenticationData>
  <coSignedData>
    <triggerEventId>QURX_TE990011NL</triggerEventId>
    <patientId>
      <root>2.16.840.1.113883.2.4.6.3</root>
      <extension>012345672</extension>
    </patientId>
  </coSignedData>
</signedData>
```

De tekstwaarden (Id, root, notBefore, notAfter, triggerEventId en extension) worden vervangen door de waarden voor het betreffende bericht. De overige teksten zijn 'vaste' teksten (voor communicatie met de ZIM). De tekst kan aangemaakt worden in ASCII of UTF-8. Gebruik wederom bij voorkeur een lange string zonder regeleinden.

10.3.2.12.7.2 Maak het signedData blok canoniek

Het signedData blok moet canoniek gemaakt worden volgens [EXCC14N]. Bovenstaand voorbeeld is canoniek (m.u.v. regeleinden voor de leesbaarheid). Voor de canonieke vorm zijn de volgende zaken van belang:

- Het Id attribuut moet double quoted zijn.
- De namespaces moeten voor het wsu:Id attribuut staan. Deze specificatie vermijdt het gebruik van attributen zoveel mogelijk om de canonicalisatie makkelijker te maken: in dit ene geval is dit niet mogelijk. Let op dat namespaces en wsu:Id gescheiden zijn met een enkele spatie: dit is in het voorbeeld hierboven niet meer zichtbaar.
- De namespaces moeten alfabetisch gerangschikt zijn.
- Alle regeleinden moeten met linefeed worden gedaan. Door de standaardtools voor bewerking van platte tekst zal op Unix-systemen een linefeed gebruikt worden, op Macintosh een carriage return en op Windows carriage return + linefeed. Eenvoudiger is alle whitespace (regeleinden, tabs, spaties) weg te laten uit de signedData. In de voorbeeldbestanden is dat ook gedaan. Voor de leesbaarheid worden hier wel nieuwe regels gebruikt. (maar: alle berekeningen zijn gedaan zonder whitespace, dus voor het narekenen van bijvoorbeeld een door NCSC als "goed" beoordeelde SHA algoritme digest moeten de regeleinden wel verwijderd worden.)
In het algemeen geldt dat whitespace tussen de verschillende <tag>s significant is: XML is immers een documentformaat, waar whitespace een belangrijk deel van de opmaak is. Whitespace tussen de tags is dus toegestaan: een conformant XML processor zal deze ook nooit "zomaar" wijzigen. Veel XML-toepassingen als de DOM en XSLT maken het mogelijk expliciet aan te geven hoe met whitespace omgegaan moet worden. Bij verwerking van digitale handtekeningen is het altijd nodig "preserveWhitespace" of vergelijkbare attributen op "True" te zetten. Exclusive Canonicalization zal niets met de whitespace tussen tags doen (wél met whitespace binnenin tags).
- Het door NCSC als "goed" beoordeelde SHA algoritme wordt berekend over het signedData element, dus er mag ook geen whitespace of newline voor of na het element meegetekend worden.
- Gebruik geen whitespace binnenin de tags, met uitzondering van een enkele spatie voor de attributen.
- Sla signedData op als ASCII of UTF-8. Dat is mogelijk omdat alle gegevens getallen of codes zijn (en niet bijv. namen van patiënten). Eigenlijk moeten bestanden die getekend worden in UTF-8 encoding zijn. De eerste 128 karakters (0 t/m 127) van UTF-8 hebben echter dezelfde hexadecimale waarden als ASCII. Er mogen beslist geen karakters in voorkomen uit de range 128-256 van b.v. ISO-Latin of Windows-1292: deze zijn niet hetzelfde in UTF-8. Voor het authenticatietoken zijn ook geen andere waarden nodig dan de eerste 128 ASCII karakters.

- Geen Byte Order Mark (BOM) toevoegen. UTF-8 staat het gebruik van een BOM toe. Applicaties kunnen deze gebruiken om te bepalen of de byte-ordering Little Endian of Big Endian is. Canonieke XML staat echter geen BOM toe – dat is ook geen probleem, aangezien UTF-8 verplicht is. Bij het gebruik van UTF-8 strings is het bij het wegschrijven dus van belang geen BOM te schrijven. Het gebruik van een BOM kan gedetecteerd worden door het bestand waarin de signedData is weggeschreven te openen: als de eerste drie octets EF BB BF zijn, is dit de BOM, en is het bestand niet correct. Als de eerste octets anders zijn, is er geen BOM gebruikt.

Of (in plaats van het bovenstaande)

- Maak het signedData blok canoniek volgens Exclusive XML Canonicalization met een geschikte library.

10.3.2.12.7.3 Bereken de SHA digest van het signedData blok

Van de signedData moet een door NCSC als “goed” beoordeelde SHA algoritme digest berekend worden. Deze digest – een verzameling octets – wordt gecodeerd met Base 64.

10.3.2.12.7.4 Maak het SignedInfo blok

XML Signature maakt gebruik van een SignedInfo blok voor de digitale handtekening. Dit ziet er als volgt uit:

```
<SignedInfo xmlns="http://www.w3.org/2000/09/xmldsig#">

  <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">

  </CanonicalizationMethod>

  <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha512">

  </SignatureMethod>

  <Reference URI="#_2.16.528.1.1007.3.3.1234567.1_0123456789">

    <Transforms>

    <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></Transform>

    </Transforms>

    <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha512"></DigestMethod>

    <DigestValue>xx5...Gus2g=</DigestValue>

  </Reference>
```

```
</SignedInfo>
```

Wederom is in de voorbeeldbestanden een string gebruikt zonder linefeeds, maar zijn deze hier voor de leesbaarheid toegevoegd.

Dit hele blok tekst kan als ASCII of UTF-8 string in de code gebruikt worden. Er zijn twee delen die vervangen moeten worden.

In de Reference ("#_2.16.528.1.1007.3.3.1234567.1_0123456789") moet de juiste Id worden toegevoegd: dit is de waarde van het Id-attribuut uit het signedData element.

In DigestValue (xx5...Gus2g=) wordt de in de vorige paragraaf berekende door NCSC als "goed" beoordeelde SHA algoritme digest, in Base 64 vorm, geplaatst.

De SignedInfo strings moeten een SignedInfo blok opleveren in canonieke vorm. Het bovenstaande blok is in canonieke vorm, wanneer tenminste alle geregleinden verwijderd worden. Verder zijn nog twee zaken van belang:

- Lege tags: <tag att="1"/> moeten voorzien worden van een expliciete eind-tag: <tag att="1"></tag>
- De namespace van XML Signature moet opgenomen zijn in het SignedInfo element. Bij genereren van een XML Signature uit een toolkit zal deze namespace vaak in het omliggende <Signature> element opgenomen zijn. Bij gebruik van [EXCC14N] wordt deze bij het canoniek maken van <SignedInfo> hier toegevoegd.

10.3.2.12.7.5 Selecteer het authenticatiecertificaat en de bijbehorende private key

De volgende cryptografische objecten op de UZI-pas zijn noodzakelijk bij berichtauthenticatie:

1. Het authenticatiecertificaat.
2. De private key behorende bij het authenticatiecertificaat. Deze key wordt gebruikt om de DigestValue te ondertekenen. Deze bewerking wordt op de UZI-pas zelf uitgevoerd.

Globaal zijn de volgende stappen nodig.

1. Zoek het authenticatiecertificaat:
 - Normaalgesproken met de PKCS#11 functie C_FindObjects;

- Certificaten zijn uit elkaar te houden op basis van de X.509 keyUsage;

Er zijn ook hulpfuncties beschikbaar in de [AETSDK] waarmee eenvoudig het juiste certificaat is te selecteren, waaronder C_FindAuthenticationCertificate.

1. Zoek de bij het authenticatiecertificaat behorende private key:

- Deze sleutel kan bij het certificaat worden gezocht op basis van het CKA_ID attribuut
- Normaalgesproken met C_FindObjects...

Er zijn ook hulpfuncties beschikbaar in de [AETSDK] die eenvoudige selectie van de juiste private key bij een bepaald certificaat mogelijk maken: C_FindCertificatePrivateKey.

In de [AETSDK] is een nadere toelichten te vinden van bovenstaande (hulp)functies.

10.3.2.12.7.6 Bereken de "RSA with SHA" waarde over SignedInfo

Bereken de "RSA with SHA" SignatureValue over het SignedInfo blok met het certificaat en plaats deze in een <Signature> element. Zorg ervoor dat de signature in Big Endian vorm wordt gemaakt. Bij netwerkcommunicatie wordt altijd Big Endian gebruikt. O.a. Windows gebruikt normaal Little Endian. Bewerk de resulterende octets volgens Base 64:

```
<SignatureValue>DpB...GW7A==</SignatureValue>
```

Base 64 staat wel whitespace zoals spaties en regeleinden toe, dus ook met regeleinden is de waarde geldig.

Base64 moet gebruikt worden zoals gespecificeerd in [MIME].

Wanneer SHA-256 wordt gebruikt, wordt "RSA with SHA-256" als type voor de SignatureValue gekozen.

10.3.2.12.7.7 Neem het juiste certificaat op

De volgende string wordt aangemaakt voor de certificaatverwijzing. Uiteraard wordt de juiste referentie naar het gebruikte certificaat ingevoegd in het voorbeeld.

```

<KeyInfo>

  <wss:SecurityTokenReference>

    <ds:X509Data xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

      <ds:X509IssuerSerial>

        <ds:X509IssuerName>CN=TEST UZI-register Zorgverlener CA G21, O=agentschap Centraal
        Informatiepunt Beroepen Gezondheidszorg, C=NL</ds:X509IssuerName>

        <ds:X509SerialNumber>359...195</ds:X509SerialNumber>

      </ds:X509IssuerSerial>

    </ds:X509Data>

  </wss:SecurityTokenReference>

</KeyInfo>

```

Uitgangspunt is dat de WSS namespace gedeclareerd is zoals hierboven opgenomen. Afhankelijk van de gebruikte pas moet de eerste string "TEST UZI-register Zorgverlener CA G21" vervangen worden door de betreffende CA (zie AORTA.STK.t3220 en AORTA.STK.t3230). De tweede string "359...195" wordt vervangen door het serial number van de pas (decimaal).

11 Bestandenlijst

File	Modified
AORTA_Arch_Configuratieinstellingen.xls ¹⁶⁷	Oct 14, 2025 by Ilias Abarkan ¹⁶⁸
AORTA_Auth_Ontw_Authenticatie.pdf ¹⁶⁹	Oct 14, 2025 by Ilias Abarkan ¹⁷⁰
AORTA_ApBh_Ontw_Applicatieregister.pdf ¹⁷¹	Oct 14, 2025 by Ilias Abarkan ¹⁷²
AORTA_Proces_VWI_Synchronisatie.pdf ¹⁷³	Oct 14, 2025 by Ilias Abarkan ¹⁷⁴
AORTA_Wrp_IH_Berichtwrappers_HL7.pdf ¹⁷⁵	Oct 14, 2025 by Ilias Abarkan ¹⁷⁶
AORTA_GZN_PvE_Goedbeheerd ZorgNetwerk.pdf ¹⁷⁷	Oct 14, 2025 by Ilias Abarkan ¹⁷⁸
AORTA_SDS_Ontw_DeterminatieService.pdf ¹⁷⁹	Oct 14, 2025 by Ilias Abarkan ¹⁸⁰
AORTA_Sgl_Ontw_Gebeurtenisverwerking.pdf ¹⁸¹	Oct 14, 2025 by Ilias Abarkan ¹⁸²
AORTA_Sgl_Ontw_Abonnementenregister.pdf ¹⁸³	Oct 14, 2025 by Ilias Abarkan ¹⁸⁴

167. https://vzvz.atlassian.net/wiki/download/attachments/1890812421/AORTA_Arch_Configuratieinstellingen.xls?api=v2

168. <https://vzvz.atlassian.net/wiki/people/712020:ee8dd293-ac84-471e-8494-7ad7b1cf319e>

169. https://vzvz.atlassian.net/wiki/download/attachments/1890812421/AORTA_Auth_Ontw_Authenticatie.pdf?api=v2

170. <https://vzvz.atlassian.net/wiki/people/712020:ee8dd293-ac84-471e-8494-7ad7b1cf319e>

171. https://vzvz.atlassian.net/wiki/download/attachments/1890812421/AORTA_ApBh_Ontw_Applicatieregister.pdf?api=v2

172. <https://vzvz.atlassian.net/wiki/people/712020:ee8dd293-ac84-471e-8494-7ad7b1cf319e>

173. https://vzvz.atlassian.net/wiki/download/attachments/1890812421/AORTA_Proces_VWI_Synchronisatie.pdf?api=v2

174. <https://vzvz.atlassian.net/wiki/people/712020:ee8dd293-ac84-471e-8494-7ad7b1cf319e>

175. https://vzvz.atlassian.net/wiki/download/attachments/1890812421/AORTA_Wrp_IH_Berichtwrappers_HL7.pdf?api=v2

176. <https://vzvz.atlassian.net/wiki/people/712020:ee8dd293-ac84-471e-8494-7ad7b1cf319e>

177. https://vzvz.atlassian.net/wiki/download/attachments/1890812421/AORTA_GZN_PvE_Goedbeheerd%20ZorgNetwerk.pdf?api=v2

178. <https://vzvz.atlassian.net/wiki/people/712020:ee8dd293-ac84-471e-8494-7ad7b1cf319e>

179. https://vzvz.atlassian.net/wiki/download/attachments/1890812421/AORTA_SDS_Ontw_DeterminatieService.pdf?api=v2

180. <https://vzvz.atlassian.net/wiki/people/712020:ee8dd293-ac84-471e-8494-7ad7b1cf319e>

181. https://vzvz.atlassian.net/wiki/download/attachments/1890812421/AORTA_Sgl_Ontw_Gebeurtenisverwerking.pdf?api=v2

182. <https://vzvz.atlassian.net/wiki/people/712020:ee8dd293-ac84-471e-8494-7ad7b1cf319e>

183. https://vzvz.atlassian.net/wiki/download/attachments/1890812421/AORTA_Sgl_Ontw_Abonnementenregister.pdf?api=v2

184. <https://vzvz.atlassian.net/wiki/people/712020:ee8dd293-ac84-471e-8494-7ad7b1cf319e>

AORTA_Uitw_Async_Asynchrone_Bestandsuitwisseling.pdf ¹⁸⁵	Oct 14, 2025 by Ilias Abarkan ¹⁸⁶
AORTA_TLG_Ontw_Toegangslog.pdf ¹⁸⁷	Oct 14, 2025 by Ilias Abarkan ¹⁸⁸
AORTA_Uitw_Opv_Ontw_Opvragen_patientgegevens.pdf ¹⁸⁹	Oct 14, 2025 by Ilias Abarkan ¹⁹⁰
AORTA_Uitw_Stu_Ontw_Versturen_patientgegevens.pdf ¹⁹¹	Oct 14, 2025 by Ilias Abarkan ¹⁹²
AORTA_VWI_IH_Verwijsindex_HL7.pdf ¹⁹³	Oct 14, 2025 by Ilias Abarkan ¹⁹⁴
AORTA_VWI_Best_practices_VWI_synchronisatie.pdf ¹⁹⁵	Oct 14, 2025 by Ilias Abarkan ¹⁹⁶
AORTA_VWI_Ontw_Verwijsindex.pdf ¹⁹⁷	Oct 14, 2025 by Ilias Abarkan ¹⁹⁸
AORTA_Ontw_Foutentabel.xlsx ¹⁹⁹	Oct 14, 2025 by Ilias Abarkan ²⁰⁰
AORTA_Aut_Ontw_Autorisatieprotocol.pdf ²⁰¹	Oct 14, 2025 by Ilias Abarkan ²⁰²
AORTA_Ontw_Foutentabel_Bijlage.pdf ²⁰³	Oct 14, 2025 by Ilias Abarkan ²⁰⁴

185. https://vzvz.atlassian.net/wiki/download/attachments/1890812421/AORTA_Uitw_Async_Asynchrone_Bestandsuitwisseling.pdf

186. <https://vzvz.atlassian.net/wiki/people/712020:ee8dd293-ac84-471e-8494-7ad7b1cf319e>

187. https://vzvz.atlassian.net/wiki/download/attachments/1890812421/AORTA_TLG_Ontw_Toegangslog.pdf?api=v2

188. <https://vzvz.atlassian.net/wiki/people/712020:ee8dd293-ac84-471e-8494-7ad7b1cf319e>

189. https://vzvz.atlassian.net/wiki/download/attachments/1890812421/AORTA_Uitw_Opv_Ontw_Opvragen_patientgegevens.pdf?api=v2

190. <https://vzvz.atlassian.net/wiki/people/712020:ee8dd293-ac84-471e-8494-7ad7b1cf319e>

191. https://vzvz.atlassian.net/wiki/download/attachments/1890812421/AORTA_Uitw_Stu_Ontw_Versturen_patientgegevens.pdf?api=v2

192. <https://vzvz.atlassian.net/wiki/people/712020:ee8dd293-ac84-471e-8494-7ad7b1cf319e>

193. https://vzvz.atlassian.net/wiki/download/attachments/1890812421/AORTA_VWI_IH_Verwijsindex_HL7.pdf?api=v2

194. <https://vzvz.atlassian.net/wiki/people/712020:ee8dd293-ac84-471e-8494-7ad7b1cf319e>

195. https://vzvz.atlassian.net/wiki/download/attachments/1890812421/AORTA_VWI_Best_practices_VWI_synchronisatie.pdf?api=v2

196. <https://vzvz.atlassian.net/wiki/people/712020:ee8dd293-ac84-471e-8494-7ad7b1cf319e>

197. https://vzvz.atlassian.net/wiki/download/attachments/1890812421/AORTA_VWI_Ontw_Verwijsindex.pdf?api=v2

198. <https://vzvz.atlassian.net/wiki/people/712020:ee8dd293-ac84-471e-8494-7ad7b1cf319e>

199. https://vzvz.atlassian.net/wiki/download/attachments/1890812421/AORTA_Ontw_Foutentabel.xlsx?api=v2

200. <https://vzvz.atlassian.net/wiki/people/712020:ee8dd293-ac84-471e-8494-7ad7b1cf319e>

201. https://vzvz.atlassian.net/wiki/download/attachments/1890812421/AORTA_Aut_Ontw_Autorisatieprotocol.pdf?api=v2

202. <https://vzvz.atlassian.net/wiki/people/712020:ee8dd293-ac84-471e-8494-7ad7b1cf319e>

203. https://vzvz.atlassian.net/wiki/download/attachments/1890812421/AORTA_Ontw_Foutentabel_Bijlage.pdf?api=v2

204. <https://vzvz.atlassian.net/wiki/people/712020:ee8dd293-ac84-471e-8494-7ad7b1cf319e>

[IH Toestemming - v.1.2 - VJZ.pdf](#)²⁰⁵Oct 14, 2025 by
[Ilias Abarkan](#)²⁰⁶

[uitw_versiebeheer.pdf](#)²⁰⁷Oct 14, 2025 by
[Ilias Abarkan](#)²⁰⁸

205. <https://vzvz.atlassian.net/wiki/download/attachments/1890812421/IH%20Toestemming%20-%20v.1.2%20-%20VJZ.pdf?api=v2>

206. <https://vzvz.atlassian.net/wiki/people/712020:ee8dd293-ac84-471e-8494-7ad7b1cf319e>

207. https://vzvz.atlassian.net/wiki/download/attachments/1890812421/uitw_versiebeheer.pdf?api=v2

208. <https://vzvz.atlassian.net/wiki/people/712020:ee8dd293-ac84-471e-8494-7ad7b1cf319e>

12 VZVZ Registratie van OID en codesystemen

Zorgstandaarden maken gebruik van Object IDentifiers (OID's), zodat bijvoorbeeld codestelsels, subsets binnen codestelsels en valuesets uniek te identificeren zijn. HL7 Nederland heeft OID '2.16.840.1.113883.2.4.3.111' toegekend aan VZVZ Servicecentrum.

In het onderstaande overzicht vindt u alle OID's die onder '2.16.840.1.113883.2.4.3.111' zijn geregistreerd. Hierin zijn ook OID's opgenomen die momenteel niet in gebruik zijn:

OID	Omschrijving
2.16.840.1.113883.2.4.3.111	VZVZ servicecentrum
2.16.840.1.113883.2.4.3.111.2.1	OID voor Mitz
2.16.840.1.113883.2.4.3.111.5.2	Type Grote bestanden
2.16.840.1.113883.2.4.3.111.5.2.1	VWI: XIS registratie van verwijzingen
2.16.840.1.113883.2.4.3.111.5.2.2	VWI: LSP vergelijking van verwijzingen
2.16.840.1.113883.2.4.3.111.5.3	Alle OID's mbt XDS
2.16.840.1.113883.2.4.3.111.5.3.1	Alle XDS affinity domains
2.16.840.1.113883.2.4.3.111.5.3.1.1	Viewer Helmond
2.16.840.1.113883.2.4.3.111.5.3.1.x.1	Hieronder worden alle applicaties gedefinieerd binnen XDS affinity domains, dus in de vorm van 2.16.840.1.113883.2.4.3.111.5.3.1.x.1.ID
2.16.840.1.113883.2.4.3.111.5.3.1.1.1	Productieomgeving Helmond
2.16.840.1.113883.2.4.3.111.5.3.1.1.2	Testomgeving Helmond

2.16.840.1.113883.2.4.3.111.5.4	Workflow Statuscode
2.16.840.1.113883.2.4.3.111.5.5	Workflow ProcesID
2.16.840.1.113883.2.4.3.111.5.6	Workflow TaakID
2.16.840.1.113883.2.4.3.111.5.7	Workflow Volgnummer
2.16.840.1.113883.2.4.3.111.5.8	Workflow
2.16.840.1.113883.2.4.3.111.5.9	Toestemming Statuscodes
2.16.840.1.113883.2.4.3.111.5.10	Alle OID's mbt Mitz
2.16.840.1.113883.2.4.3.111.5.10.1	Gegevenscategorieën voor landelijke toestemmingen
2.16.840.1.113883.2.4.3.111.5.10.2	Toestemmings Migratie Code
2.16.840.1.113883.2.4.3.111.5.11	Statuscodes van aanmeldingen in VWI (voor oa COVID-19)
2.16.840.1.113883.2.4.3.111.3	VZVZ projecten
2.16.840.1.113883.2.4.3.111.3.1	HL7v3 wrappers AORTA 8 project
2.16.840.1.113883.2.4.3.111.3.2	Applicatieregister (APR)
2.16.840.1.113883.2.4.3.111.3.3	Generiek opvragen

2.16.840.1.113883.2.4.3.111.3.4	HL7v3 Basis Componenten
2.16.840.1.113883.2.4.3.111.3.7	Abonnementenregister (ABR)
2.16.840.1.113883.2.4.3.111.3.8	Toegangslog (TLG)
2.16.840.1.113883.2.4.3.111.3.9	Verwijsindex (VWI)
2.16.840.1.113883.2.4.3.111.3.10	AORTA (in zijn geheel)
2.16.840.1.113883.2.4.3.11.60.102 (Bestond al voordat er VZVZ projecten werden aangemaakt)	Berichtwrappers (WRP)
2.16.840.1.113883.2.4.3.111.3.12	Medicatieproces op het LSP
2.16.840.1.113883.2.4.3.111.3.13	Asynchrone bestandsuitwisseling (ABU)
2.16.840.1.113883.2.4.3.111.3.14	Ketenzorg op het LSP
2.16.840.1.113883.2.4.3.111.3.15	Generieke Patientuitwisseling
2.16.840.1.113883.2.4.3.111.3.16	GBP
2.16.840.1.113883.2.4.3.111.3.17	PROVES
2.16.840.1.113883.2.4.3.111.3.18	Dossieroverdracht
2.16.840.1.113883.2.4.3.111.3.19	Generieke workflow

2.16.840.1.113883.2.4.3.111.3.20	Patiënttoestemming
2.16.840.1.113883.2.4.3.111.3.21	Acute Zorg op het LSP
2.16.840.1.113883.2.4.3.111.3.22	Dienstverlener Zorgaanbieder
2.16.840.1.113883.2.4.3.111.3.23	Verwijzen
2.16.840.1.113883.2.4.3.111.3.24	Dossieroverdracht Huisartsen
2.16.840.1.113883.2.4.3.111.3.25	Labuitslagen op het LSP
2.16.840.1.113883.2.4.3.111.3.26	Bronstelsel t.b.v. MedMij
2.16.840.1.113883.2.4.3.111.3.27	PPMT
2.16.840.1.113883.2.4.3.111.3.28	HIS t.b.v. OPEN
2.16.840.1.113883.2.4.3.111.3.29	Vaccinaties
2.16.840.1.113883.2.4.3.111.1.5.1	AORTA Contextcodes
2.16.840.1.113883.2.4.3.111.1.5.2	AORTA Parametertypes
2.16.840.1.113883.2.4.3.111.1.5.3	AORTA Bouwsteentypes
2.16.840.1.113883.2.4.3.111.1.5.4	AORTA RequestID

2.16.840.1.113883.2.4.3.111.1 5.5	AORTA TransformationID
2.16.840.1.113883.2.4.3.111.1 9.1	Message-id's voor voorbeeldberichten
2.16.840.1.113883.2.4.3.111.1 9.2	Message-id's voor getransformeerde berichten
2.16.840.1.113883.2.4.3.111.2 0	OID voor ZORG-ID
2.16.840.1.113883.2.4.3.111.2 0.2	Taakcode
2.16.840.1.113883.2.4.3.111.2 0.5	Proof of ownership
2.16.840.1.113883.2.4.3.111.2 0.7	Certification Practice Statement
2.16.840.1.113883.2.4.3.111.4	Hash over PatiëntID
2.16.840.1.113883.2.4.3.111.6	COA nummer
2.16.840.1.113883.2.4.3.111.7	Geboortedatum patiënt

12.1 Registratie van URI's

Hieronder een lijst van URI's die VZVZ in gebruik heeft genomen bij het gebruik van HL7 FHIR

URI	Omschrijving
http://www.vz vz.nl/fhir/StructureDefinition/gegevensdienst-id	Voor gegevensdienst-id's van Medmij binnen het ZAB
http://www.vz vz.nl/fhir/StructureDefinition/organizationName-type	Organisatienaam type binnen het ZAB
http://www.vz vz.nl/fhir/StructureDefinition/organizationName-active	Of de organisatienaam nog actief is binnen het ZAB
http://www.vz vz.nl/fhir/StructureDefinition/telecom-name	Naam van het telefoonnummer binnen het ZAB
http://www.vz vz.nl/fhir/NamingSystem/organization-type	Organisatietype voor het ZAB. Hierin staan de code zoals ze in AllSolution bestaan
http://vz vz.nl/fhir/NamingSystem/fqdn (alias voor urn:iETF:rfc:2068 en urn:iETF:rfc:2616)	Aanduiding van FQDN in ZAB

13 AORTA Verklarende woordenlijst

13.1 Afkortingen

Deze sectie bevat de lijst met AORTA-specifieke afkortingen en hun betekenis.

Afkorting	Beschrijving
2FA	Twee Factor Authenticatie. Eenduidige identificatie van de gebruiker door combinatie van twee componenten (iets dat de gebruiker weet, iets wat de gebruiker bezit of iets dat onlosmakelijk verbonden met de gebruiker).
AGB	Algemene gegevensbeheercode, een code voor de identificatie van zorgaanbieders ten behoeve van hun declaraties bij zorgverzekeraars.
AIS	Apotheekinformatiesysteem.
AMvB	Algemene maatregel van bestuur.
AWBZ	Algemene wet bijzondere ziektekosten.
Bbsn-z	Besluit gebruik burgerservicenummer in de zorg.
BIG	Wet op de beroepen in de individuele gezondheidszorg.
BSN	Uniek identificerend nummer voor iedereen die een relatie heeft met de Nederlandse overheid; cijfermatig gelijk aan het sofi-nummer. Dit nummer mag alleen worden verwerkt of uitgewisseld als dit uit een betrouwbare bron komt of is verkregen van een partij die het nummer al uit een betrouwbare bron heeft verkregen.
BVBSN	Beheervoorziening BSN.
CA	Certification authority, een TTP die PKI-sleutels certificeert en deze certificaten uitgeeft.
CBP	College bescherming persoonsgegevens.
CDR	Clinical data repository, operationele database die gegevens vanuit diverse systemen samenvoegt en zo een uniform beeld van een patiënt creëert.
CIBG	Centraal Informatiepunt Beroepen Gezondheidszorg, agentschap van het ministerie van VWS.

CPI	Centrale patiëntindex.
CRL	Certificate Revocation List, in een PKI gebruikte (digitale) lijst met ingetrokken certificaten die niet meer geaccepteerd mogen worden.
DAP	Dossier Afspraken en Procedures.
DBC	Diagnose-behandelingcombinatie.
DCN	Datacommunicatienetwerk.
DNS	Domain name system, mechanisme voor het toekennen van hostnamen aan systemen op het internet of een ander IP-netwerk en het vertalen van die hostnamen naar IP-adressen.
DICOM	Digital imaging and communications in medicine.
DigiD	Digitale Identiteit, is de naam van een systeem waarmee Nederlandse overheden op internet iemands ²⁰⁹ ide ²¹⁰ n ²¹¹ titeit kunnen verifiëren.
EHR	Electronic health record, een engelse vertaling voor EPD.
EMD	Elektronisch medicatiedossier, een zorgtoepassing in AORTA. Per oktober 2008 hernoemd naar medicatiegegevens.
e-NIK	Elektronische nationale identiteitskaart, digitaal equivalent van het paspoort.
EPD	Elektronisch patiëntendossier.
EVS	Elektronisch voorschrijfsysteem, systeem dat gebruikt wordt ter ondersteuning van het voorschrijven van medicatie.
F2F	Face to face. Een visuele controle van een persoon en diens WID-document ter vaststelling van de identiteit van de persoon.
FQDN	Fully qualified domain name, domeinnaam die in een DNS een domein eenduidig en volledig specificeert.
GBA	Gemeentelijke basisadministratie. Een onderdeel van de Basisregistratie Personen waarin voor de overheid relevante <i>persoonsgegevens</i> van Nederlandse ingezetenen worden vastgelegd.

209. [http://nl.wikipedia.org/wiki/Identificatie_\(informatica\)](http://nl.wikipedia.org/wiki/Identificatie_(informatica))

210. [http://nl.wikipedia.org/wiki/Identificatie_\(informatica\)](http://nl.wikipedia.org/wiki/Identificatie_(informatica))

211. [http://nl.wikipedia.org/wiki/Identificatie_\(informatica\)](http://nl.wikipedia.org/wiki/Identificatie_(informatica))

GBK	Goed beheerd klantenloket. De organisatie die namens de patiënt of diens wettelijke vertegenwoordiger informatieverzoeken naar het landelijk schakelpunt doorzet en onder de strikte privacyregels de opgeleverde informatie doorzet naar de patiënt of diens wettelijke vertegenwoordiger.
GBO	Goedbeheerd systeem dat geen UZI-servercertificaat kan krijgen. Alle hardware, software, processen en organisatieonderdelen die gebruikt worden om onderzoek te verrichten op grote verzamelingen gegevens die via het LSP ontsloten worden. Hierbij valt bijvoorbeeld te denken aan onderzoek naar het effect van een bepaalde batch inenting bij zuigelingen.
GBP	Goed Beheerd Patiëntenportaal. Alle hardware, software, processen en organisatieonderdelen die nodig zijn om een patiëntenportaal aan te bieden zodat de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie die via het portaal wordt verstrekt kunnen worden gegarandeerd. Dit omvat dus ook eventuele hardware, software, processen en organisatieonderdelen van leveranciers die door de GBP-organisatie wordt ingezet voor het realiseren van een GBP.
GBx	Goed beheerd systeem. Een verzamelnaam voor systemen die zijn gekwalificeerd voor aansluiting op het LSP, zoals GBZ, GBP of GBK.
GBZ	Goed Beheerd Zorgsysteem. Alle hardware, software, processen en organisatieonderdelen die nodig zijn om een <i>zorgsysteem</i> aan te bieden zodat de <i>vertrouwelijkheid</i> , <i>integriteit</i> en <i>beschikbaarheid</i> van de informatie die met het <i>zorgsysteem</i> wordt verstrekt kunnen worden gegarandeerd.
GGZ	Geestelijke gezondheidszorg.
GZN	Goedbeheerd Zorgnetwerk, voorheen ZSP. Alle hardware, software, processen en organisatieonderdelen die nodig zijn voor realisatie van een netwerkverbinding tussen het LSP en een GBx conform de eisen van de VZVZ op gebied van vertrouwelijkheid, integriteit en beschikbaarheid.
HAGRO	Huisartsengroep.
HAP	Huisartsenpost.
HOED	Huisartsen onder één dak.
HIS	Huisartsinformatiesysteem.
HL7	Health Level 7, internationale organisatie voor standaardisatie van de informatie-uitwisseling in de zorg. In de documentatie die betrekking heeft op de techniek wordt soms de term HL7 gebruikt als verwijzing naar HL7v3.
HL7v3	Health Level 7 version 3, op XML gebaseerde standaard voor informatie-uitwisseling in de zorg.

ICA	Intoleranties, Contra-indicaties en Allergieën.
ICD	International classification of diseases.
ICPC	International classification of primary care.
ICTU	ICT Uitvoeringsorganisatie (voor overheden) .
ID, id	Identiteit of identificatie.
IGZ	Inspectie voor de Gezondheidszorg.
IHE	Integrating the healthcare enterprise.
IJZ	Inspectie Jeugdzorg.
KNMG	Koninklijke Nederlandsche Maatschappij tot bevordering der Geneeskunst.
LIS	Laboratoriuminformatiesysteem.
LSP	Landelijk Schakelpunt. Het geheel van hardware, software, processen en organisatieonderdelen die nodig zijn voor de realisatie van de ZIM-diensten voor het opvragen en aanmelden van zorggegevens.
MAP	(zie) Medisch autorisatieprotocol
MPI	Master Patient Index, een systeem dat patiëntnummers uit verschillende zorginformatiesystemen kan vertalen.
Nictiz	Nationaal ICT instituut in de Zorg.
NHG	Nederlands Huisartsen Genootschap
NIK	Nederlandse Identiteitskaart. Een identiteitskaart met een geldigheid van vijf (minderjarigen) of tien jaar (18 jaar en ouder) waarop geen vingerafdrukken zijn vastgelegd.
Nonce	Is een afkorting en staat voor number used once. Hiermee wordt een waarde bedoeld die maar één keer in het berichtenverkeer voorkomt.
NTP	Network time protocol, protocol voor het synchroniseren van tijd klokken tussen verschillende ICT-voorzieningen.

OID	Object identifier, een standaard wijze voor de identificatie van objecten, zie http://www.alvestrand.no/objectid/ □
OZIS	Open Zorg InformatieSysteem, systeem van de stichting OZIS, dat tot doel heeft informatie-uitwisseling in de eerstelijnsgezondheidszorg te bevorderen.
PACS	Picture archiving and communication system.
PGD	Persoonlijk Gezondheidsdossier. Een door de <i>patiënt</i> of zijn wettelijke <i>vertegenwoordiger</i> beheerd levenslang dossier met een gestandaardiseerde gegevensverzameling van relevante gezondheidsinformatie dat wordt gebruikt voor het nemen van regie over gezondheid en zorg.
PKI	Public key infrastructure, een methode voor beveiliging gebaseerd op het gebruik van publieke en private sleutels.
PKIO	PKIoverheid, uitvoerende instantie en beheerder van de verzameling richtlijnen voor de beveiliging van overheidsgegevens met PKI.
PS	(zie) Professionele Samenvatting
RA	Registratie-autoriteit, een TTP die aanvragen voor certificering namens de CA afhandelt.
RIAGG	Regionale instelling voor ambulante geestelijke gezondheidszorg.
RIBW	Regionale instelling voor beschermd wonen.
RIM	Reference information model, informatiemodel dat de basis vormt voor de ontwikkeling van digitale berichten, zie [HL7v3] en CEN tc251.
RIS	Radiologie-informatiesysteem.
RNI	Register niet-ingezetenen. Een onderdeel van de Basisregistratie Personen waarin voor de overheid relevante <i>persoonsgegevens</i> van emigranten en vreemdelingen die geen ingezetene van Nederland zijn maar wel diensten van de Nederlandse Overheid afnemen worden geregistreerd.
RSA	Cryptografisch algoritme dat gebruik maakt van sleutelparen (publieke en private sleutels), zie PKI.
SAML	Security Assertion Markup Language, definieert een op XML gebaseerde OASIS standaard voor de uitwisseling van beveiligingsgerelateerde informatie tussen vertrouwde partijen.
SBV	Sectorale berichtenvoorziening van het BSN-stelsel.

SBV-Z	SBV voor de zorgsector.
SEH	Spoedeisende hulp.
SHA-2	Verzamelnaam voor een reeks hash-algoritmen (SHA-224, SHA-256, SHA-384 en SHA-512) gepubliceerd in 2002 door NIST (SHA-224 in 2004). Opvolgers van SHA-1, die een langere hashwaarde en meer zekerheid bieden.
SLA	Service level agreement, Engels voor SNO.
SNO	Serviceniveauovereenkomst, een overeenkomst tussen dienstaanbieder en dienstafnemer waarin het niveau van de afgesproken dienstverlening beschreven staat.
TTP	Trusted third party, rol van een vertrouwde derde binnen een PKI-kader.
URA	UZI-register abonneenummer, identificatienummer van de zorgaanbieder die UZI-passen heeft aangevraagd.
URI	Universal resource identifier, wijze van identificeren van informatiebronnen op het internet.
URL	Uniform resource locator, verwijst naar de locatie van een informatiebron, bijvoorbeeld een webpagina of een ander bestand.
URN	Uniform resource name, is een Uniforme Resource Identifier (URI) dat gebruik maakt van de urn systematiek, en identificeert niet de informatiebron. De urn is als volgt opgebouwd: "urn:"<contextnaam>":"<specifieke stringnaam>"
UZI	Unieke zorgverleneridentificatie, landelijk identificatienummer voor zorgverleners, zorginstellingen en zorgsystemen.
UZОВI	Unieke zorgverzekeraaridentificatie, landelijk identificatienummer voor zorgverzekeraars.
VIV	Vertrouwde Identiteitsverstrekker. Een door de VZVZ vertrouwde organisatie die een dienst levert voor het verifiëren van identiteit van de <i>gebruiker</i> .
VGU	Vereenvoudigd gebruik UZI-pas.
VWI	Verwijsindex, onderdeel van de ZIM, het LSP.
WBP	Wet bescherming persoonsgegevens.

Wbsn-z	Wet gebruik burgerservicenummer in de zorg.
WDH	Waarneemdossier voor huisartsen, een zorgtoepassing in AORTA. Per oktober 2008 hernoemd naar huisartswaarneemgegevens.
WEH	Wet elektronische handtekeningen.
WGBO	Wet op de geneeskundige behandelingsovereenkomst.
WID	Wet op de identificatieplicht.
WOG	Wet op de geneesmiddelenverstrekking.
XIS	Generieke term voor HIS, AIS, ZIS, etc. (zorginformatiesysteem).
ZAIS	Ziekenhuisapotheekeinformatiesysteem.
ZAB	Zorgadresboek.
ZIM	Zorginformatiemakelaar, onderdeel van de basisinfrastructuur in de zorg waarlangs alle aangesloten GBZ'en veilig patiëntgegevens kunnen uitwisselen.
ZIS	Ziekenhuisinformatiesysteem.

13.2 Begrippen

Deze sectie bevat de lijst met AORTA-specifieke begrippen en hun betekenis.

Begrip	Beschrijving
Aanmelden	Zie publiceren
ACA	Advies Commissie Autorisatie
AORTA-versie	Een versie van de AORTA-documentatie is een bepaalde geïdentificeerde samenhangende verzameling documentatie van AORTA.

Abonnee	<i>Zorgaanbieder</i> die met het <i>UZI-register</i> een overeenkomst sluit om <i>UZI-passen</i> te kunnen afnemen.
Abonneenummer	Identificerend nummer aan een abonnee of een beheerorganisatie, in geval van de zorgaanbieder als abonnee wordt ook gesproken over URA
Afgeleide contra-indicatie	Een afgeleide contra-indicatie is een conditie die niet direct vastgesteld is (door diagnostiek of inzage in een dossier), maar wordt afgeleid uit het gebruik van bepaalde medicijnen. Zo zal het gebruik van insuline kunnen leiden tot de afgeleide contra-indicatie 'diabetes', zelfs als deze conditie zelf niet is vastgesteld en niet bekend is uit het dossier van de patiënt.
Allergie	Een allergie is een vorm van overgevoeligheid, met als verbijzondering dat de ongewenste reactie wordt veroorzaakt door het immuunsysteem van het lichaam. Een allergie is dus per definitie een overgevoeligheid, maar een overgevoeligheid is niet automatisch een allergie. In het bijzonder wordt hier alleen de intolerantie ten aanzien van het gebruik van een geneesmiddel verstaan, maar bijvoorbeeld niet een noten allergie of bijensteken.
AORTA	AORTA is de landelijk beschikbare infrastructuur voor berichtuitwisseling in de zorg in Nederland. Officieus staat AORTA voor Architectuur, Ontwerp, Realisatie, Test en Acceptatie. 1) Het concept van gegevensuitwisseling in de zorgsector, beschreven in de door de VZVZ ontwikkelde architectuur; 2) De door de VZVZ ontwikkelde architectuur voor gegevensuitwisseling in de zorgsector; 3) De <i>basisinfrastructuur</i> die gegevensuitwisseling in de zorgsector zoals beschreven in de door de VZVZ ontwikkelde architectuur mogelijk maakt.
Applicatie	programmatuur die bepaalde functies kan leveren aan <i>gebruikers</i> of andere <i>ICT-voorzieningen</i> .
Applicatie-(XIS-)versie	Een versie van een XIS is een XIS dat gekwalificeerd is voor een bepaalde AORTA-versie.
Authenticatie	Het proces waarbij iets (iemand) nagaat of iets(iemand) daadwerkelijk is wat(wie) het(hij) beweert te zijn.
Authenticatiemiddel	Een technisch middel waaraan de identiteit van een gebruiker kan worden gekoppeld met een bepaalde mate van betrouwbaarheid (bijvoorbeeld gebruikersnaam/wachtwoord, chipkaart, PKI certificaat, mobiele telefoon of combinatie)
Authenticatie sterkte	Een maat hoe sterk de koppeling is tussen een authenticatiemiddel en de identiteit van de gebruiker

Authenticatietoken	Een bestemde bewering omtrent de authenticiteit van de afzender van (delen van) een bericht.
Authenticeren	verifiëren van de identiteit van een persoon of organisatie.
Authenticiteit	zekerheid dat de identiteit waarvoor een persoon of organisatie zich uitgeeft juist is.
Autoriseren	toekennen van bevoegdheden aan een persoon of organisatie.
Autorisatieprofiel	door <i>patiënt/cliënt</i> bepaalde autorisatietabel die bepaalt welke categorieën van zijn <i>patiëntgegevens</i> voor welke <i>zorgaanbieders</i> toegankelijk zijn onder welke voorwaarden.
Autorisatieprotocol	door <i>zorgaanbieders</i> gedefinieerde autorisatietabel die bepaalt welke categorieën <i>patiëntgegevens</i> voor welke categorieën <i>zorgaanbieders</i> toegankelijk zijn onder welke voorwaarden.
Basisinfrastructuur	geheel aan <i>ICT-voorzieningen</i> en bijbehorende organisatorische voorzieningen, dat dient als gemeenschappelijke basis voor de diverse <i>zorgtoepassingen</i> .
Behandelrelatie	een behandelrelatie is de relatie tussen een patiënt/cliënt en de personen die rechtstreeks betrokken zijn bij de uitvoering van de behandelingsovereenkomst. De wettelijke kaders voor een behandelingsovereenkomst zijn beschreven in de WGBB. Een behandelrelatie is in algemene zin moeilijk te definiëren omdat het in de praktijk een complex en dynamisch begrip is. Zodra een patiënt bijvoorbeeld wordt doorverwezen naar een andere zorgaanbieder ontstaat een nieuwe behandelrelatie. Als de zorgverlener al dan niet tijdelijk wordt vervangen, wat in de praktijk vaak gebeurt (vakantie, deeltijd, verloof, arts-assistenten, co-assistenten etc.) ontstaat eveneens een nieuwe behandelrelatie. Het is bovendien niet altijd op voorhand duidelijk hoe lang de behandelrelatie gaat duren en wanneer die dus als beëindigd beschouwd moet worden. Wat wel voor alle zorgverleners en medewerkers duidelijk moet zijn is of men gegevens verwerkt in het kader van een behandelrelatie. Dat kan in individuele gevallen steeds worden bepaald. Voor toegang tot het landelijk EPD is het hebben van een behandelrelatie een voorwaarde.
Beheerdersnummer	een 9-cijferig nummer dat de pashouder van een <i>beheerderpas</i> identificeert.
Beheerderpas	persoonsgebonden vertrouwensmiddel voor <i>beheerders</i> , uitgegeven door het CIBG.
Beheerderregister	<i>Register voor beheerders en hun organisatie</i> vastgelegd bij het CIBG.
Beheerorganisatie	<i>XIS-leverancier</i> die diensten levert aan zorgaanbieders of de <i>interne beheer organisatie</i> van een zorgaanbieder die met het <i>beheerderregister</i> een overeenkomst sluit om (<i>GBZ</i>) <i>beheerderpassen</i> te kunnen afnemen.

Beheerverantwoordelijke	<i>zorgverlener</i> of <i>zorgaanbieder</i> die verantwoordelijk is voor het bewaren van bepaalde <i>patiëntgegevens</i> en het zonodig ter beschikking stellen daarvan aan anderen.
Bereikbaarheidsgegevens	informatie die nodig is om een persoon of organisatie te kunnen bereiken, zoals telefoon, e-mail of adres.
Beschikbaarheid	kans dat een systeem in staat is de gespecificeerde <i>diensten</i> of <i>functies</i> te bieden.
Betrokkenheid	verantwoordelijkheid van een <i>zorgverlener</i> ten opzichte van een <i>patiënt/cliënt</i> met betrekking tot de overeengekomen <i>zorgdienst</i> .
Betrouwbaarheid	kans dat een systeem de gespecificeerde <i>diensten</i> of <i>functies</i> uitvoert conform de specificatie (IEC 61508).
Betrouwbaarheidsniveau	Zie Authenticatie sterkte.
Betrouwbare bron	Systeem dat gegevens aanlevert waarvan de juistheid gegarandeerd is.
(Beveiligings-) Token	Een verzameling, na verificatie betrouwbare, beweringen met betrekking tot een beveiligingsaspect. Bijvoorbeeld de bewering dat de afzender van een bericht authentiek is.
Bijwerking	Een bijwerking is een neveneffect van een geneesmiddel (dus een effect buiten de bedoelde therapeutische werking). Er zijn zowel bekende als onvoorziene bijwerkingen. Bekende bijwerkingen horen bij de aard van de medicatie en zijn in principe beschreven in de productinformatie. Onvoorziene bijwerkingen zijn kenmerkend voor een zogenaamd 'Adverse Drug Event', waarbij in een specifiek geval iets mis gaat na toediening van de medicatie. Een 'Adverse Drug Event' kan ook een bekende bijwerking betreffen, die met onverwachte intensiteit optreedt. Een bijwerking kan het gevolg zijn van een overgevoeligheid of allergie, maar ook van bijvoorbeeld interacties met andere medicatie.
Certificaat	in een <i>PKI</i> gebruikt digitaal document, uitgegeven door een <i>TTP</i> , dat dient ter identificatie van een server of gebruiker.
Cliënt	persoon die verpleging of verzorging geniet of mogelijk zal genieten.
Canonieke XML	standaardvorm van <i>XML</i> zonder lexicale vrijheden, opdat bitsgewijs kan worden gecontroleerd of twee <i>XML</i> -documenten semantisch identiek zijn.
Comorbiditeit	Comorbiditeit is het tegelijkertijd aanwezig zijn van twee of meer stoornissen of aandoeningen bij een patiënt. Dit is in het algemeen het geval bij het gelijktijdig aanwezig zijn van lichamelijke, geestelijke en vaak de daaropvolgende sociale problemen bij een persoon.

Conditie	Condities zijn patiëntkenmerken die van invloed kunnen zijn op medicatieveiligheid. Daaronder worden op dit moment verstaan: Overgevoeligheid (intolerantie) en allergieën voor geneesmiddelen en contra-indicaties.
Contra-indicatie	Een conditie waarbij het gebruik van bepaalde geneesmiddelen en/of hulpstoffen niet is toegestaan dan wel slechts met bepaalde voorzorgen kan plaatsvinden. Voorbeelden van conditie: zwanger, aandoening, leeftijd, ... Relatieve of absolute contra-indicaties zijn de redenen (intoleranties en co-morbiditeiten) waardoor geneesmiddelen aangepast of niet moet worden voorgeschreven cq gebruikt.
Convergeren	<i>Doorschakelen</i> van berichten van meerdere afzenders naar één bestemming.
Definitief gekoppeld	koppeling van <i>patiëntgegevens</i> aan een <i>BSN</i> waarbij er geen onzekerheden (meer) zijn omtrent de juistheid van de koppeling.
DigiD-register	Het DigiD-register is een gemeenschappelijke ICT-voorziening waarin burgers kunnen worden geregistreerd, die door het DigiD-register zijn voorzien van vertrouwensmiddelen en waarmee burgers kunnen worden geauthenticeerd.
Divergeren	<i>Doorschakelen</i> van berichten van één afzender naar meerdere bestemmingen.
Documentatieset	een verzameling van specifieke versies van documenten die op enig moment gezamenlijk een complete beschrijving geven van een logisch afgebakend onderwerp, zoals de <i>AORTA-basisinfrastructuur</i> of een <i>zorgtoepassing</i> .
Doorschakelen	actie van een schakelpunt inzake het ontvangen en vervolgens <i>doorsturen</i> , <i>divergeren</i> of <i>convergeren</i> van een bericht.
Doorsturen	<i>Doorschakelen</i> van berichten van één afzender naar één bestemming.
Duplicaatbericht	bericht dat identiek is aan een eerder bericht.
Eigen GBZ-verklaring	een door een <i>zorgaanbieder</i> of in opdracht van een <i>zorgaanbieder</i> door een derde ondertekende verklaring, welke inhoudt dat de bij die <i>zorgaanbieder</i> aanwezige processen, procedures en ict-configuratie(s) geschikt zijn voor het verkrijgen van toegang tot en gebruik van <i>AORTA</i> .
Elektronisch patiëntendossier	<i>ICT-voorziening</i> die toegang geeft tot de verschillende <i>patiëntdossiers</i> binnen een <i>zorginstelling</i> .

Elektronisch Voorschrijf Systeem	Een elektronisch voorschrijfsysteem is een geautomatiseerd systeem waarmee langs elektronische en gestructureerde weg voorschriften kunnen worden vastgelegd en waarmee tegelijkertijd onveilige situaties kunnen worden gesignaleerd tijdens het voorschrijven van geneesmiddelen. Door een elektronisch voorschrijfsysteem te gebruiken kunnen fouten worden voorkomen bij het lezen van recepten en kunnen onveilige situaties worden voorkomen, zoals dubbelmedicaties, contra-indicaties, interacties met andere geneesmiddelen en overgevoeligheidsreacties.
Episode	reeks van opeenvolgende <i>zorgcontacten</i> die een <i>patiënt/cliënt</i> heeft met een of meer <i>zorgaanbieders</i> in het kader van een bepaalde <i>zorgvraag</i> .
Fictief BSN	Een BSN dat is uitgegeven door het SBV-z dat voldoet aan de numeriek kenmerken van een BSN, maar niet te traceren is naar een natuurlijk persoon.
Fictief dossier	Een patiëntdossier van een niet bestaand natuurlijk persoon.
Fictieve (patiënt)gegevens	Patiëntgegevens van een niet bestaand natuurlijk persoon
Gastgebruik	<i>Gastgebruik</i> van een <i>UZI-pas</i> . Het gebruik van een <i>UZI-pas</i> in een <i>GBZ</i> van een andere <i>zorgaanbieder</i> dan de <i>zorgaanbieder</i> die de desbetreffende <i>UZI-pas</i> heeft aangevraagd bij het <i>UZI-register</i> .
Gastheerzorgaanbieder	Een <i>zorgaanbieder</i> waar een <i>zorgverlener</i> een <i>UZI-pas</i> gebruikt die niet door die <i>zorgaanbieder</i> bij het <i>UZI-register</i> is aangevraagd.
Gastzorgverlener/medewerker	Een <i>zorgverlener/medewerker</i> die bij een <i>GBZ</i> een <i>UZI-pas</i> gebruikt die niet door de <i>zorgaanbieder</i> van dat <i>GBZ</i> bij het <i>UZI-register</i> is aangevraagd.
GBP-organisatie	De organisatie die eigenaar is van een patiëntenportaal en daartoe software aanschaft, processen inricht en organisatieonderdelen bemant of laat bemannen door externe dienstenleveranciers (die daardoor volgens deze definitie onderdeel van de GBP-organisatie uitmaken).
GBZ-applicatie	<i>Zorgapplicatie</i> die als onderdeel van een <i>GBZ</i> is aangesloten op de <i>ZIM</i> .
GBZ-beheerderpas	<i>Zie Beheerderpas</i> , specifiek voor een beheerder van een <i>GBZ</i>
Gebruiker	<i>Zorgaanbieder, zorgverlener, medewerker, beheerder</i> of <i>patiënt/cliënt</i> die een <i>applicatie</i> gebruikt.
Gebruikersessie	Tijdsduur dat een <i>gebruiker</i> via een <i>GBZ-applicatie</i> gebruik maakt van zijn bevoegdheden tot landelijke uitwisseling van patiëntgegevens.

Gebruikersinteractie	actie van een <i>gebruiker</i> met betrekking tot het landelijk uitwisselen van <i>patiëntgegevens</i> .
Gegevenssoort	typering van een soort van <i>patiëntgegevens</i> .
Hash	Een cryptografische bewerking van een data-blok dat leidt tot een specifieke waarde van een vaste lengte. Deze waarde is een unieke voor het betreffende data-blok.
Heraanmelden	bijwerken van een eerder gedane aanmelding bij de verwijzindex. Zie ook publiceren.
Herroepen	ongeldig maken, bijvoorbeeld van een <i>patiëntstuk</i> .
HL7-bericht	Digitaal <i>patiëntbericht</i> , conformerend aan de <i>HL7-standaard</i> , dat dient als middel om <i>patiëntgegevens</i> te versturen tussen systemen.
Hoofdbehandelaar	<i>Zorgaanbieder</i> waarmee een <i>patiënt/cliënt</i> een behandelovereenkomst heeft.
Huisartswaarneem gegevens	een zorgtoepassing in AORTA. Per oktober 2008 is waarneemdossier voor huisartsen (WDH) hiernaar hernoemd.
Idempotent	eigenschap van een bewerking dat het resultaat daarvan bij herhaling gelijk is aan dat bij eenmalige uitvoering. Is van belang bij het correct afhandelen van duplicaatberichten.
Identificeren	bepalen van de identiteit van een persoon of organisatie.
Identity Provider	een dienstverlener die diensten verleent om de identiteit vast te stellen van een gebruiker en informatie hierover uitgeeft.
Inhoudsverantwoorde lijke	<i>zorgverlener</i> of <i>zorgaanbieder</i> die verantwoordelijk is voor de juistheid van de medische inhoud van bepaalde <i>patiëntgegevens</i> .
Integriteit	zekerheid dat bepaalde gegevens niet (ongemerkt) zijn of worden gewijzigd.
Interactiemechanisme	wijze waarop een GBZ een <i>HL7-bericht</i> moet uitwisselen met de <i>ZIM</i> , afhankelijk van het type <i>HL7-bericht</i> .
Intolerantie	Zie Overgevoeligheid (de koepelorganisaties hebben voorkeur voor de term Overgevoeligheid).

Kennisgeving	Een bericht (set gegevens) die een zorgpartij ter informatie aan één of meer andere zorgpartijen stuurt. Dit als gevolg van een bepaalde gebeurtenis die door een zorgpartij is waargenomen of tot stand gebracht. Van de ontvanger wordt geen antwoordbericht verwacht. (Zie ook: Kennisgeving, Signalering).
Klantenloket	Onder het Klantenloket wordt de organisatie verstaan die verantwoordelijk is voor het GBP en het GBK.
Klantenloketmedewerker	Een medewerker van het Klantenloket.
Kwalificatie	de uitkomst van het proces van <i>kwalificeren</i> , een verklaring van de kwalificerende instelling waar in staat of en in hoeverre het onderwerp voldoet aan de kwalificatiecriteria.
Kwalificeren	proces waarbij geverifieerd wordt in hoeverre het onderwerp (in deze context een <i>ZSP</i> , <i>XIS</i> of <i>GBZ</i>) voldoet aan de geldende kwalificatiecriteria.
Landelijk schakelpunt	de centrale ICT-omgeving waar landelijk alle goed beheerde informatiesystemen via gekwalificeerde ZSP's gegevens mee uitwisselen. Het LSP draagt zorg voor de authenticatie van gebruikers en goed beheerde informatiesystemen, het autoriseren van gebruikers conform de met koepelorganisaties gemaakte afspraken, de verwijzing naar aangemelde medische gegevens, het routeren van landelijk gestandaardiseerde berichten en het registreren van patiëntgegevensaanmeldingen en -raadplegingen. Binnen de wettelijke kaders maakt het LSP inzage mogelijk voor patiënt en toezichthouder.
Mandateren	overdragen van bevoegdheden bij het delegeren van taken.
Mandaatbeheerder	de door een zorgverlener aangewezen persoon om binnen een GBZ voor de zorgverlener mandaten te mogen beheren. Deze persoon kan zijn de zorgmanager of een security manager.
Medebehandelaar	<i>Zorgaanbieder</i> die in opdracht van een <i>hoofdbehandelaar</i> handelt.
Medewerker	persoon in dienst van een <i>zorginstelling</i> of in dienst bij een <i>zorgverlener</i> die in opdracht daarvan ondersteunende diensten verleent.

Medicatiebewakingsig naal	Medicatiebewakingsignalen zijn waarschuwingen die door een medicatiebewakingsysteem worden gegenereerd. Voorbeelden van medicatie bewaking zijn: • Bewaken op interacties met andere geneesmiddelen die de patiënt gebruikt; • Bewaken op individuele gevoeligheden, ongevoeligheden of overgevoeligheden van de patiënt voor het desbetreffende geneesmiddel; • Bewaken op onjuiste dosering; • Bewaken op (pseudo) dubbelmedicatie; • Bewaken op contra-indicaties en andere patiëntkenmerken.
Medicatieproces	een zorgtoepassing in AORTA waarmee medicatievoorschriften, -verstrekkingen en ICA-gegevens kunnen worden uitgewisseld.
Medicatieverstrekking	Een medicatie verstrekking is de registratie van de, door een apotheek of apotheekhoudende huisarts, geleverde medicatie. Bij de verstrekking worden vastgelegd: het middel, de toedieningsvorm, de sterkte en de dosering en de periode dat het middel gebruikt moet worden. Daarnaast wordt de verstrekte hoeveelheid opgenomen.
Medicatievoorschrift	Een medicatie voorschrift is de elektronische vastlegging van afspraak tussen voorschrijver en patiënt waarin minimaal wordt vastgelegd : het middel, de toedieningsvorm, de sterkte en de dosering. Wanneer er een opdracht volgt tot levering door een apotheek wordt de te verstrekken hoeveelheid gespecificeerd. Een voorschrift kan leiden tot een verstrekkingverzoek, maar dat hoeft niet (bijvoorbeeld wanneer de patient nog voldoende medicatie op voorraad heeft).
Medisch Autorisatieprotocol	In het medisch autorisatie protocol (MAP) staat welke soorten patiëntgegevens een zorgverlener, op grond van zijn functie, nodig kan hebben of aan anderen mag verstrekken voor een adequate behandeling. Het MAP is geformuleerd in overleg met beroepsverenigingen van zorgverleners en met belangenverenigingen van patiënten/cliënten. Berichtuitwisseling via het LSP wordt getoetst aan de hand van het MAP.
Metagegevens	gegevens die karakteristieken van bepaalde gegevens beschrijven.
Non-conformiteit	het niet voldoen aan een gespecificeerde eis.
Observatie	Onder observatie wordt elke activiteit verstaan waarbij door het beschouwen van een situatie een bepaald onderzoeksresultaat wordt verkregen. Dit kan variëren van een laboratoriumonderzoek tot een röntgenfoto, maar ook een lengtemeting of een diagnosestelling zijn (medische) observaties (met een 'auteur' als de bron ervan).
Onbetrouwbare bron	Systeem dat gegevens aanlevert die mogelijk onjuist zijn en dus niet voor waar aangenomen kunnen worden.

Onweerlegbaarheid	zekerheid dat een handeling niet kan worden ontkend door degene die hem heeft uitgevoerd.
Opdrachtbericht	bericht waarmee de afzender de ontvanger verzoekt een bepaalde handeling uit te voeren. een bericht (set gegevens) die een zorgpartij als verzoek aan één andere zorgpartij stuurt. Van de ontvanger wordt verwacht dat deze een antwoordbericht terugstuurt waarin staat of het verzoek wordt aanvaard dan wel afgewezen. In geval van aanvaarding wordt bovendien verwacht dat het resultaat van de opdracht als kennisgeving wordt teruggestuurd. (Zie ook: Kennisgeving, Signalering)
Opvraagbericht	bericht waarmee de afzender de ontvanger om bepaalde informatie vraagt.
Overgevoeligheid	Een overgevoeligheid is een (patiëntgebonden) lichamelijk kenmerk (conditie), die kan leiden tot een ongewenste reactie op blootstelling aan bepaalde stoffen. Een overgevoeligheid zal dus een contra-indicatie vormen voor medicijnen die deze stoffen bevatten. Een overgevoeligheid is de potentie tot het ontstaan van een (patiëntgebonden) onvoorziene bijwerking. Voorbeelden zijn: Intolerantie voor penicilines (de groep) of amoxiciline (een specifieke peniciline), maar ook voor bijvoorbeeld bepaalde hulpstoffen in een geneesmiddel.
Patiënt	persoon die geneeskundig onderzoek of behandeling geniet of mogelijk zal genieten.
Patiëntbericht	bericht met <i>patiëntgegevens</i> , dat in het kader van samenwerking wordt verstuurd aan een <i>zorgaanbieder</i> .
Patiëntcontact	gelegenheid waarbij een <i>zorgverlener</i> beroepsmatig in contact is met een <i>patiënt</i> , bijvoorbeeld een consult, en die normaliter leidt tot bijwerking van het <i>patiëntdossier</i> .
Patiëntdocument	persistente verzameling van samenhangende <i>patiëntgegevens</i> , die als één geheel wordt vastgelegd, opgevraagd en verstuurd.
Patiëntgegevens	(persoonlijke, logistieke, medische en/of financiële) gegevens over een bepaalde <i>patiënt/cliënt</i> die zijn vastgelegd in het kader van een <i>zorgdienst</i> .
Patiëntkluis	verzameling van <i>patiëntgegevens</i> van één <i>patiënt/cliënt</i> onder beheer van die <i>patiënt/cliënt</i> zelf.
Patiëntdossier	verzameling van <i>patiëntgegevens</i> van één <i>patiënt/cliënt</i> onder beheer van de verantwoordelijke <i>zorgaanbieder</i> .
Patiëntenindex	Lijst met <i>identificerende</i> gegevens van <i>patiënten</i> bij een <i>zorgaanbieder</i> .

Patiëntstuk	deel van, of uittreksel uit, een <i>patiëntdossier</i> .
Persoonsgegevens	Gegevens conform art. 29 van de Data Protection Working Party van de Europese Commissie (01248/07/EN WP 136), kort samengevat 'alle informatie gerelateerd aan geïdentificeerde of identificeerbare natuurlijke personen'.
PKIO-pas	persoonsgebonden vertrouwensmiddel uitgegeven door een door PKIO gecertificeerde CA.
PKIO-servercertificaat	systeemgebonden vertrouwensmiddel uitgegeven door een door PKIO gecertificeerde CA
Publiceren (van het patiëntendossier)	Ook wel aanmelden genoemd. Het voor andere zorgaanbieders beschikbaar maken van het patiëntendossier door een verwijzing aan te brengen in de centrale verwijzindex (VWI) van het LSP
Professionele Samenvatting	De set gegevens die geldt als samenvatting van het medisch dossier van een patiënt bij een huisarts, als vastgesteld door de beroepsgroep van huisartsen, vertegenwoordigd door de NHG.
Query	zie <i>opvraagbericht</i> .
Reconstructiehorizon	tijdshorizon in het verleden tot wanneer een <i>gebruikersinteractie</i> moet kunnen worden gereconstrueerd.
Rol	een veelgebruikte term met verschillende interpretaties, zie verder onder <i>betrokkenheid</i> , <i>werkverband</i> , <i>toepassingsrol</i> en <i>zorgverlenerfunctie</i> .
Security token	Beveiligingsinformatie die in de header onder het security element van een SOAP bericht geplaatst wordt. Voor deze informatie zijn verschillende authenticatie schema's beschikbaar, zoals gebruikersnaam/wachtwoord, X.509 certificaat, SAML Assertion, etc.
Semantische compatibiliteit	twee applicaties zijn semantisch compatibel wanneer ze op berichten van elkaar reageren zoals de andere partij dat verwacht.
Signalering	een bericht (set gegevens) die een systeem ter informatie stuurt aan een zorgpartij. Dit als gevolg van een bepaalde gebeurtenis die door een systeem werd gedetecteerd of veroorzaakt. Van de ontvanger wordt geen antwoordbericht verwacht. (Zie ook: Opdracht, Kennisgeving)
Smoketest	De situatie waarbij er een nieuwe of geüpdate versie van een XIS-applicatie in de productie omgeving wordt ingevoerd (geïmplementeerd). Hierbij worden enkele initiële configuraties en basisfuncties nagelopen om de juiste werking van de applicatie te verifiëren. De fasen van testen, acceptatie en kwalificeren zijn hierbij reeds gepasseerd.

Syntactische compatibiliteit	twee applicaties zijn syntactisch compatibel wanneer ze de berichten van elkaar accepteren zonder onverwachte foutmeldingen.
Tekortkoming	onvolkomenheid of zwakte in het voldoen aan een gespecificeerde eis.
Terugwaartse compatibiliteit	een oudere applicatie X en een nieuwere X+1 zijn syntactisch terugwaarts compatibel wanneer X+1 berichten van X kan accepteren zonder onverwachte foutmeldingen.
Technisch GBZ	wanneer er bij een zorgaanbieder (URA) meerdere GBZ-delen gedefinieerd zijn met ieder een apart GBZ-id.
Time-out	het verlopen van een tijdsinterval waarbinnen een systeem het resultaat van een actie afwacht alvorens een fout wordt verondersteld.
Toepassingsrol	rol van een <i>applicatie</i> in het kader van een bepaalde landelijke <i>zorgtoepassing</i> .
Toestandsbericht	bericht waarmee de afzender de ontvanger op de hoogte stelt van de toestand waarin de afzender zich bevindt.
Toezichthouder	een door de overheid aangesteld, onafhankelijk en onpartijdig instituut dat toeziet op naleving van wet- en regelgeving door organisaties zoals CBP, IGZ en IJZ
Token authenticatie	authenticatie waarbij gebruik gemaakt wordt van een authenticatietoken.
Transactie	reeks van twee of meer <i>interacties</i> die als één geheel moeten worden uitgevoerd.
UZI-nummer	een 9-cijferig nummer dat de pashouder of service uniek identificeert.
UZI-pas	persoonsgebonden vertrouwensmiddel voor <i>zorgverleners</i> en hun <i>medewerkers</i> , uitgegeven door het <i>UZI-register</i> . UZI-passen van het type 'medewerker niet op naam' bevatten geen persoonsgebonden informatie.
UZI-register	<i>Register voor zorgverleners.</i>
UZI-servercertificaat	systeemgebonden vertrouwensmiddel voor <i>ICT-voorzieningen</i> van <i>zorgaanbieders</i> , uitgegeven door het <i>UZI-register</i> .
Vertegenwoordiger (van een patiënt)	Is een wettelijke vertegenwoordiger danwel een gemachtigde. Onder wettelijk vertegenwoordiger wordt verstaan ouders, voogd, curator en mentor van de patiënt. In voorkomende gevallen kan de rol van curator, mentor, voogd worden uitgeoefend door familieleden in een bepaalde graad tot de patiënt dan wel door ongerelateerde, door de rechterlijke macht aangewezen, derde natuurlijke en niet-natuurlijke rechtspersonen.

Vertrouwelijkheid	zekerheid dat bepaalde gegevens uitsluitend door bevoegden kunnen worden ingezien.
Vertrouwensmiddel	middel waarmee iemand elektronisch geïdentificeerd kan worden, zich kan <i>authenticeren</i> en eventueel een elektronische handtekening kan zetten.
Vertrouwensniveau	de mate waarin op enig moment de communicatie tussen partijen <i>vertrouwelijk</i> , <i>integer</i> en <i>onweerlegbaar</i> is, uitgedrukt in een voorgedefinieerd niveau.
Virtueel Patiëntdossier	verzameling van organisatorisch en geografisch verspreide <i>patiëntdossiers</i> die zodanig toegankelijk zijn, als waren zij één groot <i>patiëntdossier</i> .
Virtueel Postkantoor	verzameling van organisatorisch en geografisch verspreide postbussen die alle <i>zorgaanbieders</i> zodanig bereikbaar maken, als vormden zij één <i>zorgaanbieder</i> .
Voorlopig gekoppeld	koppeling van <i>patiëntgegevens</i> aan een BSN waarbij er (nog)onzekerheden zijn omtrent de juistheid van die koppeling.
Voorwaartse compatibiliteit	een oudere applicatie X en een nieuwere X+1 zijn syntactisch voorwaarts compatibel wanneer X berichten van X+1 kan accepteren zonder onverwachte foutmeldingen.
Werkverband	de verantwoordelijkheid van een <i>zorgpartij</i> ten opzichte van zijn eventuele <i>zorginstelling</i> met betrekking tot het verlenen van <i>zorgdiensten</i> .
Werkcontext	de relatie waarin de patiënt en de zorgverlener in professionele zin zich tot elkaar bevinden. De werkcontext bepaalt onder andere of er gegevens opgevraagd moeten worden ten behoeve van de behandeling en/of consult etc.
WID-document	Wet op de Identificatieplicht-document. Een document dat als wettelijk identificatiemiddel gebruikt kan worden: paspoort, NIK of rijbewijs.
XIS-acceptatie	Een door VZVZ ondertekende verklaring dat een XIS-applicatie voldoet aan de door VZVZ gestelde eisen voor het mogen aansluiten op AORTA. Het hebben van een XIS-typekwalificatie van Nictiz is een randvoorwaarde om het acceptatieproces in te gaan.
XIS-applicatie	onderdeel van een XIS dat als <i>GBZ-applicatie</i> zou kunnen functioneren.
XIS-typekwalificatie	een door Nictiz ondertekende verklaring dat een <i>XIS-applicatie</i> voldoet aan de door Nictiz gestelde eisen. Een overzicht van de verleende XIS-typekwalificaties en van de daarbij behorende software van ICT-leveranciers in de geldende versies en releases is opgenomen onder http://www.nictiz.nl .

Zorgaanbieder	door de minister van Volksgezondheid, Welzijn en Sport aangewezen categorieën van <i>zorgverleners</i> en <i>zorginstellingen</i> . (omvat <i>zorgverlenerpraktijk</i>)
Zorgapplicatie	<i>Applicatie</i> die ter beschikking van een <i>zorgpartij</i> , nader onder te verdelen in <i>zorgaanbiederapplicatie</i> , patiëntapplicatie, etc.
<i>Zorgadresboek</i>	gids waarin <i>zorginstellingen</i> en <i>zorgverleners</i> de door hun geboden <i>zorgdiensten</i> en bereikbaarheidsgegevens kunnen vermelden.
Zorgaanbiedernummer	identificatienummer van een <i>zorgverlener</i> of <i>medewerker</i> , zonodig in combinatie met het identificatienummer van de <i>zorginstelling</i> .
Zorgaanbiederpostbus	verzameling door <i>zorgaanbieder</i> af te handelen <i>patiëntberichten</i> .
Zorgaanbiederregister	<i>Register</i> met <i>zorgaanbieders</i> die <i>zorgpartijen</i> in staat stelt <i>zorgaanbieders</i> te identificeren.
Zorgconsument	<i>Patiënt</i> of <i>cliënt</i> .
Zorgcontact	sessie waarin een <i>zorgaanbieder</i> aandacht besteedt aan één of meer <i>zorgvragen</i> van een <i>patiënt/cliënt</i> .
Zorgdienst	dienst gericht op het onderzoeken, verbeteren, behouden of ondersteunen van de lichamelijke of geestelijke gezondheidstoestand van een <i>patiënt/cliënt</i> .
ZORG-ID Smartcard	Authenticatiemiddel voor de ondertekening van inschrijftokens en transactietokens.
Zorginformatiesysteem	<i>ICT-voorziening</i> die rechtstreeks ter beschikking staat van een <i>zorgaanbieder</i> .
Zorginstelling	organisatorisch verband van <i>zorgverleners</i> en ondersteunende <i>medewerkers</i> dat <i>zorgdiensten</i> verleent aan een <i>patiënt/cliënt</i> .
Zorgpartij	persoon of organisatie die een primaire rol speelt bij de verlening van <i>zorgdiensten</i> .
Zorgproduct	product benodigd bij het onderzoeken of gericht op het verbeteren, behouden of ondersteunen van de lichamelijke of geestelijke gezondheidstoestand van een <i>patiënt/cliënt</i> .
Zorgnetwerk	regionaal samenwerkingsverband van <i>zorgaanbieders</i> en <i>zorgverzekeraars</i> .
Zorgsysteem	zie <i>zorginformatiesysteem</i> .

Zorgtoepassing	1) toepassing van landelijke uitwisseling van <i>patiëntgegevens</i> tussen samenwerkende <i>zorgaanbieders</i> , ten behoeve van een bepaalde <i>zorgdienst</i> 2) functionele aanvulling op de <i>basisinfrastructuur</i> ter ondersteuning van de uitwisseling van <i>patiëntgegevens</i> in het kader van specifieke zorgprocessen.
Zorgverlener	Beroepsbeoefenaar als bedoeld in de artikelen 3, 34 en 36a van de Wet op de beroepen in de individuele gezondheidszorg (Wet BIG). Persoon die beroepsmatig <i>zorgdiensten</i> verleent aan een <i>patiënt/cliënt</i> .
Zorgverlenerfunctie	de beroepstitel (en eventueel het specialisme) van een <i>zorgverlener</i> die bepaalt welke <i>zorgdiensten</i> hij of zijn <i>zorginstelling</i> kan verlenen.
Zorgverlenerpraktijk	praktijk van een zelfstandig werkende <i>zorgverlener</i> .
Zorgverzekeraar	ziekenfonds, ziektekostenverzekeraar of zorgkantoor.
Zorgvraag	behoefte van een <i>patiënt/cliënt</i> aan een <i>zorgdienst</i> .
ZSP-kwalificatie	een door Nictiz afgegeven verklaring dat het door de zorgserviceprovider (ZSP) ter beschikking gestelde ICT-systeem voldoet aan de door Nictiz op enig moment gestelde eisen.

14 Referenties

Referentie	Document	Versie
[AORTA DAP]	AORTA dossier afspraken en procedures ("AORTA DAP")	27 januari 2014 Versie 2.3
[ArchiMate]	http://www.opengroup.org/archimate/doc/ts_archimate/	-
[AV23]	G.W. van Blarkom en drs. J.J. Borking; <i>Beveiliging van persoonsgegevens - Achtergrondstudie en verkenning nr. 23</i> ; Registratiekamer, April 2001	April 2001
[DigiD]	http://www.logius.nl/producten/toegang/digid	-
[Foutentabel]	Foutentabel	8.4.0.0
[Decor]	http://decor.nictiz.nl/pub/vzvz/	
[HL7 FHIR Security and Privacy]	Secpriv-module - FHIR v3.0.2 (hl7.org) ²¹²	FHIR v3.0.2
[HL7 FHIR Exchange]	Exchange-module - FHIR v4.0.1 (hl7.org) ²¹³	
[IH Transport]	Implementatiehandleiding berichttransport	8.4.0.0
[KWZi]	Ministerie van VWS, directie voorlichting en communicatie - Kwaliteitswet zorginstellingen	-
[NEN 7510]	NEN 7510 – Medische informatica – Informatiebeveiliging in de zorg – Algemeen, NNI, april 2004	2017
[Ontw APR]	Ontwerp applicatieregister	8.4.0.0
[Ontw APT]	Ontwerp autorisatieprotocol	8.4.0.0
[Ontw Authenticatie]	Ontwerp authenticatie	8.4.0.0

212. <http://hl7.org/fhir/STU3/secpriv-module.html>

213. <http://hl7.org/fhir/exchange-module.html>

[Ontw OPV]	Ontwerp opvragen patiëntgegevens	8.4.0.0
[Ontw Sgl ABR]	Ontwerp abonnementenregister	8.4.0.0
[Ontw Sgl GBV]	Ontwerp gebeurtenisverwerking	8.4.0.0
[Ontw STU]	Ontwerp versturen patiëntgegevens	8.4.0.0
[Ontw TLG]	Ontwerp toegangslog	8.4.0.0
[Ontw VWI]	Ontwerp verwijzindex	8.4.0.0
[PvE GBx Rollen]	Programma van eisen infrastructurele systeemrollen. Deze staan in het PvE van de bijbehorende zorgtoepassing	8.4.0.0
[IH TRANS]	Implementatiehandleiding Berichtauthenticatie Transactietoken	8.4.0.0
[IH MAN]	Implementatiehandleiding Berichtauthenticatie Mandaattoken	8.4.0.0
[IH INSCHRIJF]	Implementatiehandleiding Berichtauthenticatie Inschrijftoken	8.4.0.0
[IH PKIO]	Implementatiehandleiding Berichtauthenticatie PKIO	8.4.0.0
[PKIO]	http://www.logius.nl/producten/toegang/pkioverheid	-
[SBV-Z]	http://www.sbv-z.nl/diensten	-
[UML]	http://www.uml.org/	-
[UZI]	http://www.uziregister.nl	-
[Vertrouwensmodel]	A.Ekker; <i>Vertrouwensmodel landelijke infrastructuur voor gegevensuitwisseling</i> ; Nictiz publicatie 10041, november 2010	Nov. 2010
[WBIG]	Wet op de beroepen in de gezondheidszorg	-
[AVG]	Algemene Verordening Gegevensbescherming	-
[Wbsn-z]	Wet gebruik burgerservicenummer in de zorg	-

[WGBO]	Wet op de geneeskundige behandelingsovereenkomst	-
[WS-I basic profile]	Web Services Interoperability basic profile	1.0
[WS-I basic security profile]	Web Services Interoperability basic security profile	1.0
[Zienswijze CBP]	College Bescherming Persoonsgegevens; <i>Zienswijze CBP over doorstartmodel voor landelijke uitwisseling medische gegevens</i> ; 9 augustus 2011	9-aug-2011
[MITZ-IHOG]	VZVZ_Mitz_Implementatiehandleiding_OpenGesloten	3.6.0.0
[MITZ-IHMAN]	VZVZ_Mitz_Implementatiehandleiding_Migreren-Abonneren-Notificeren	3.6.0.0

15 Errata

Op deze pagina worden correcties (errata) gepubliceerd op reeds vastgestelde versies van het AORTA afsprakenstelsel.

Een erratum beschrijft inhoudelijke of redactionele fouten die na publicatie zijn geconstateerd in de officiële documentatie, en die invloed kunnen hebben op de juiste interpretatie of toepassing van het stelsel.

Elk erratum vermeldt:

- de referentie naar het betreffende document en versienummer;
- de oorspronkelijke tekst;
- de gecorrigeerde tekst;
- de aard van de correctie (redactioneel, technisch, inhoudelijk);
- en de datum van publicatie van het erratum.

Zodra een nieuwe versie van het afsprakenstelsel wordt uitgebracht waarin de correctie is verwerkt, vervalt het erratum automatisch.

Op dit moment zijn er geen errata.

16 Addenda

Op deze pagina worden aanvullingen (addenda) gepubliceerd op het AORTA afsprakenstelsel.

Een addendum bevat aanvullende of verduidelijkende afspraken die nog niet zijn opgenomen in de meest recente formeel vastgestelde versie van het stelsel, maar die reeds als richtinggevend of van kracht worden beschouwd.

Elk addendum vermeldt:

- de aanleiding voor de aanvulling;
- de relatie met bestaande onderdelen van het stelsel;
- de inhoud van de toevoeging of verduidelijking;
- de datum van inwerkingtreding.

Addenda worden bij de eerstvolgende release beoordeeld voor integratie in de formele documentatie.

Op dit moment is er geen addendum.