

Architectuur AORTA

Datum: 1 oktober 2019

Publicatie: V8.1.0.0

Inhoudsopgave

1 Inleiding 8

1.1	Doel en scope	8
1.2	Doelgroep voor dit document	8
1.3	Leeswijzer	8
1.4	Toelichting op de gebruikte notatie	9
1.5	Documenthistorie	9

2 Samenvatting 11

2.1	Primaire interacties	11
2.2	Ondersteunende interacties	11
2.3	Authenticatie en autorisatie	11
2.4	Betrokken informatiesystemen	12
2.5	Berichtuitwisseling	13
2.6	Non-functionele aspecten en beveiliging	13

3 Inleiding en context 14

3.1	Achtergrond	14
3.2	Wettelijk kader	15
3.2.1	Wet op de geneeskundige behandelingsovereenkomst [WGBO]	15
3.2.2	Wet beroepen in de individuele gezondheidszorg [WBIG]	15
3.2.3	Kwaliteitswet zorginstellingen [KWZi]	15
3.2.4	Algemene verordening gegevensbescherming [AVG]	15
3.2.5	Wet gebruik burgerservicenummer in de zorg Wbsn-z	16
3.3	Architectuurprincipes	16

4 Primaire interacties: het opvragen en sturen van patiëntgegevens 19

4.1	Interacties	19
4.2	Actoren	19
4.2.1	Zorgverlener	20
4.2.2	Zorgaanbieder	20
4.2.3	Medewerker van een zorgaanbieder	20
4.2.4	Patiënt	20
4.2.5	Goed Beheerde Organisatie	21
4.3	Toekenning van rollen aan actoren	21
4.3.1	Opvragen van patiëntgegevens	21
4.3.2	Sturen van patiëntgegevens	22
4.3.3	Toegangsbeperkingen	23
4.4	Toegangsmodeel	24
4.4.1	Opt-in van de patiënt	24
4.4.2	Behandelrelatie	24
4.4.3	Bevoegdheid op basis van BIG-titel	25
4.4.4	Mandatering	25
4.4.5	Vertegenwoordiging	25

4.4.6	Samenwerkingsverband.....	26
4.5	Identificatie en authenticatie.....	26
4.6	Patiëntgegevens.....	27
4.7	Het zoeken van gegevenshouders en gegevensontvangers	27
5	Ondersteunende interacties	29
5.1	Ondersteunende interacties	29
5.2	Actoren en rollen	31
5.2.1	SBV-Z	31
5.2.2	Landelijk schakelpunt.....	31
5.2.3	Klantenloket en Medewerker klantenloket	31
5.2.4	Autorisatiecommissie.....	32
5.2.5	Toezichthouder.....	32
5.2.6	Rollen.....	32
5.2.7	Mandatering.....	32
5.3	Opvragen/verifiëren BSN en controleren omloopstatus WID	32
5.4	Aan- en afmelden van patiëntgegevens	33
5.5	Raadplegen verwijsindex	33
5.6	Bijhouden van abonnementen en signaleren van gebeurtenissen	33
5.7	Selecteren van zorgaanbieders, zorgverleners en zorgaanbiederapplicaties	34
5.8	Raadplegen toegangslog.....	34
5.9	Vastleggen autorisatieprotocollen	34
5.10	Vastleggen determinatietabellen	34
6	Informatiesystemen	36
6.1	Inleiding	36
6.2	Zorginformatiemakelaar	37
6.2.1	Opvraag patiëntgegevens	39
6.2.2	Sturen patiëntgegevens.....	39
6.2.3	Verwijsindex	39
6.2.4	Zorgadresboek	39
6.2.5	Applicatieregister	39
6.2.6	Abonnementenregister	40
6.2.7	Authenticatie.....	40
6.2.8	Autorisatieprotocol.....	40
6.2.9	Toegangslog.....	40
6.2.10	Gebeurtenisverdeler en gebeurtenisafhandelaars	40
6.2.11	Selectie Determinatie Service.....	40
6.3	Goed beheerd informatiesysteem (GBx)	40
6.4	zorginformatiesystemen (XIS) en het Goed beheerd zorgsysteem (GBZ)	41
6.5	Goed beheerd patiëntportaal (GBP).....	42
6.6	Goed beheerd klantenloketsysteem (GBK)	42
6.7	Goed beheerde organisatie (GBO).....	43
6.8	Dienstverlener Zorgaanbieder (DVZA)	43
6.9	Goed beheerde connector (GBC).....	43

6.10	Basisregistraties en vertrouwensmiddelen	43
6.10.1	UZI-register	43
6.10.2	PKIO	44
6.10.3	DigiD.....	44
6.10.4	SBV-Z	44
7	Beheerinteracties	45
7.1	Actoren en rollen	45
7.1.1	GBx-beheerder en GBZ-beheerder	45
7.1.2	Beheerder ZIM	45
7.2	Toegang van GBZ-beheerders tot primaire en ondersteunende interacties	45
7.3	Beheer van aansluitingen	46
7.4	Beheer van de verwijzindex	46
7.5	Beheer van het zorgadresboek	47
7.6	Beheer van zorgtoepassingen.....	47
7.7	Beheer van selectie en determinatieserver.....	47
8	Interacties tussen informatiesystemen	48
8.1	Algemene beschrijving van interacties.....	48
8.2	Systeemrollen	49
8.3	Zorgtoepassingen	50
9	Primaire informatiesysteeminteracties – opvragen en sturen van gegevens	51
9.1	Opvragen van patiëntgegevens	51
9.1.1	Interface LSP.OPV.i1010: opvragen van patiëntgegevens	52
9.1.2	Interface LSP.OPV.i1020: opvragen van patiëntgegevens binnen context....	53
9.2	Versturen van patiëntgegevens	53
9.2.1	Interface LSP.STU.i1010: sturen van patiëntgegevens.....	53
10	Ondersteunende informatiesysteeminteracties	55
10.1	Aan- en afmelden van patiëntgegevens	55
10.1.1	Interface LSP.VWI.i1025: Publiceren gegevens	56
10.1.2	Interface LSP.VWI.i2035: Afmelden verwijzing laag	56
10.1.3	Interface LSP.VWI.i1090: Synchroniseren indexgegevens met vergelijking	56
10.1.4	Controle op opt-in bij het aanmelden van patiëntgegevens	56
10.2	Raadplegen van de verwijzindex	57
10.2.1	Interface LSP.VWI.i1060: Actualiteitscontrole	58
10.2.2	Interface LSP.VWI.i1080: opvragen index midden.....	58
10.3	Bijhouden van abonnementen en signaleren van gebeurtenissen	58
10.3.1	Interface LSP.ABR.i1010: Registreren abonnement	59
10.3.2	Interface LSP.ABR.i1020: Beëindigen abonnement.....	59
10.3.3	Interface LSP.ABR.i1030: Opvragen abonnementen	59
10.3.4	Interface GBX.SGL.i1050: Verwerken abonnementsignaal.....	59
10.4	Selecteren van zorgaanbieders, zorgverleners en zorgaanbiederapplicaties	61
10.5	Raadplegen van de toegangsllog.....	62
10.5.1	Interface LSP.TLG.i1010: raadplegen toegangsllog	62

10.5.2	ZIM-interne service: registreren toegangsgebeurtenis	62
10.6	Vastleggen autorisatieprotocollen.....	63
10.6.1	ZIM-interne service: autoriseren van rol voor interactie	64
10.6.2	ZIM-interne service: autoriseren van applicatie voor interactie	64
10.6.3	Beheerfunctie 'raadplegen autorisatiebestand'	65
10.6.4	Beheerfunctie 'laden autorisatiebestand'	65
10.6.5	Beheerfunctie 'rapporteren autorisaties'	65
10.7	Vastleggen determinatietabellen	65
10.7.1	ZIM-interne service: Bepalen bouwsteentypen en selectieparameters.....	66
10.7.2	ZIM-interne service: Bepalen gegevenssoorten	67
10.7.3	Beheerfunctie 'raadplegen determinatietabel'	67
10.7.4	Beheerfunctie 'laden determinatietabel'	67
10.7.5	Beheerfunctie 'rapporteren SDS configuratie'	67
10.8	Opvragen/verifiëren BSN en controleren omloopstatus WID	67
11	Applicatie-interacties voor beheer	68
11.1	Raadplegen en bewerken van het applicatieregister	68
11.1.1	Interface LSP.APR.i1010: verifiëren communicatiekoppeling (tick-tock)	69
11.1.2	Interface LSP.APR.i1020: verifiëren applicatiekoppeling (ping-pong)	69
11.1.3	Interface LSP.APR.i1075: Beheren TKID	69
11.1.4	Rol van het APR bij beperking van het opleveren van gegevens tot een beperkte groep van zorgverleners (regionale beperking)	69
11.2	Beheer van de verwijzindex	70
11.2.1	Beheer van het zorgadresboek	70
11.2.2	Beheer van overige aspecten van de ZIM	71
12	Overzicht van systeemrollen	73
13	Berichtafhandeling	74
13.1	Protocollen.....	74
13.2	Berichtafhandeling door de ZIM	76
13.2.1	Validatie van de berichtsyntax	77
13.2.2	Authenticatie en autorisatie van de zorgverlenerapplicatie	77
13.2.3	Authenticatie van de gebruiker / pashouder	77
13.2.4	Autorisatie op basis van het autorisatieprotocol	80
13.2.5	Inhoudelijke verwerking van het bericht	80
13.2.6	Loggen van het bericht	83
13.3	Foutafhandeling	83
13.4	Afhandelen van berichtversies	84
14	Infrastructurele aspecten	85
14.1	Conceptueel overzicht infrastructuur	85
14.1.1	Initiërende systemen.....	85
14.1.2	Communicatienetwerken.....	85
14.1.2.1	Goedbeheerd ZorgNetwerk (GZN)	85
14.1.2.2	Domain Name Service.....	85
14.1.2.3	Domein aorta-zorg.nl.....	85

14.1.2.4	IP-adresreeksen	87
14.1.2.5	Internet-koppeling	87
14.1.2.6	Protocollen	87
14.1.3	Centrale infrastructuur	88
14.1.4	Externe systemen/infrastructuren	88
14.1.5	Reagerende systemen	88
14.1.6	Basisregistraties en certificatiediensten	88
14.2	Operationele aspecten	89
14.2.1	Beschikbaarheid	89
14.2.2	Capaciteit en schaalbaarheid	90
14.2.3	Responstijden.....	90
15	Beveiliging	91
Bijlage A	Referenties	93

1 Inleiding

1.1 Doel en scope

Dit document behandelt de architectuur van AORTA.

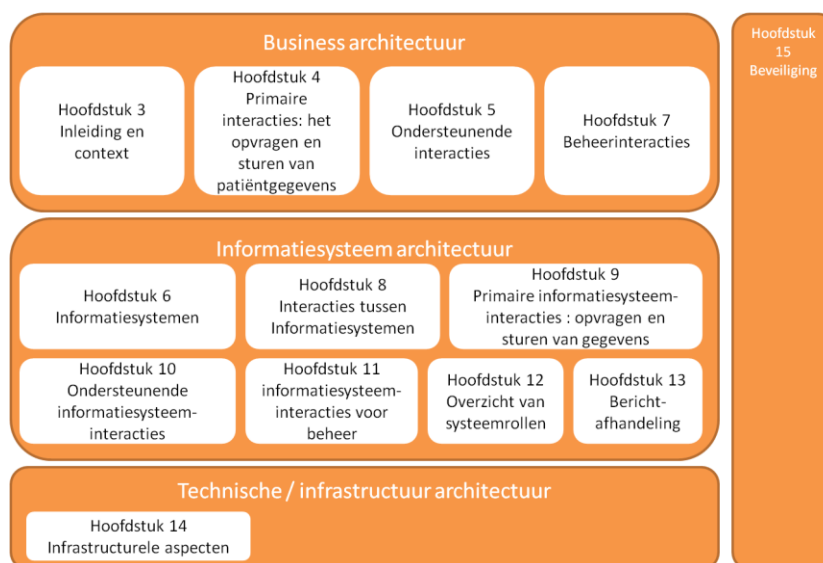
AORTA is de landelijk beschikbare infrastructuur voor berichtuitwisseling in de zorg in Nederland.

1.2 Doelgroep voor dit document

Dit document is gericht op zorgaanbieders, leveranciers van zorginformatiesystemen en de leverancier van het landelijk schakelpunt en geeft deze partijen een overzicht van de belangrijkste aspecten van de generieke functionaliteit van AORTA.

1.3 Leeswijzer

De architectuurbeschrijving in dit document is niet zozeer gericht op specifieke zorgprocessen, maar in meer algemene zin op het op generieke wijze faciliteren van informatieuitwisseling in de zorg. De architectuurbeschrijving in dit document is globaal onder te verdelen in vier secties, namelijk de 'business' architectuur, de informatiesysteemarchitectuur, de technische of infrastructuurarchitectuur en een aparte bespreking van de beveiligingsaspecten.



De 'business' architectuur behandelt op een abstract niveau enkele belangrijke architectuurprincipes, de actoren en rollen die betrokken zijn bij informatieuitwisseling in de zorg, de interacties tussen deze actoren en de randvoorwaarden die een rol spelen bij de uitwisseling van informatie. De business architectuur is opgenomen in hoofdstukken 3, 4, 5 en 7, en wordt zoveel mogelijk behandeld zonder in te gaan op de informatiesystemen die bij het uitwisselen van informatie een rol spelen.

De informatiesysteemarchitectuur is opgenomen in 6 tot en met 13 (met uitzondering van hoofdstuk 7) en gaat in op de informatiesystemen waarmee binnen de AORTA-architectuur de uitwisseling van informatie tussen zorgverleners wordt gefaciliteerd. Daarbij geeft hoofdstuk 6 een overzicht van de betrokken informatiesystemen en worden in hoofdstuk 8 tot en met 11 de relevante interacties tussen deze informatiesystemen

beschreven. Hoofdstuk 12 geeft een samenvattend overzicht van de diverse rollen die de betrokken informatiesystemen hebben in de systeeminteracties binnen AORTA. Hoofdstuk 13 gaat meer in detail in op enkele bijzonderheden van de berichtuitwisseling binnen de AORTA-architectuur.

De technische of infrastructuurarchitectuur wordt in dit document alleen op conceptueel niveau behandeld in hoofdstuk 14. Hierbij wordt echter niet in detail ingegaan op implementatiekeuzes zoals specifieke productkeuzes, toewijzing van functionaliteit aan gespecialiseerde technische componenten of uitwerking van de netwerkinfrastructuur. Hiervoor wordt verwezen naar de technische beschrijvingen die zijn gemaakt in het kader van de fysieke implementatie van de infrastructuur, gebaseerd op de architectuur.

In hoofdstuk 15 wordt tenslotte een globaal samenvattend overzicht gegeven van beveiligingsaspecten, waarvan de meeste aspecten ook al in eerdere hoofdstukken zijn behandeld.

1.4 Toelichting op de gebruikte notatie

Tekst tussen vierkante haken [] verwijst naar referenties in bijlage A.

Architectuurprincipes en een beperkte groep van belangrijke centrale definities zijn voorzien van een kader.

Om te komen tot standaardisatie in notatie van architectuurdiagrammen wordt in dit document gebruik gemaakt van een beperkt aantal notatietechnieken.

Overwegend wordt gebruik gemaakt van de in Nederland ontwikkelde modelleertaal voor architectuur 'ArchiMate', die onder beheer staat van "The Open Group". Behoudens enkele uitzonderingen volgen alle diagrammen de ArchiMate-notatie. Voor een overzicht van de relevante concepten wordt verwezen naar [ArchiMate].

Daarnaast wordt in hoofdstuk 13 gebruik gemaakt van activiteendiagrammen volgens de modelleertaal UML van de "Object Management Group" (zie [UML]).

Voor de nummering van diagrammen, architectuurprincipes, eisen en tabellen is een coderingstelsel gekozen dat tot doel heeft om deze artefacten binnen de gehele AORTA-documentatieset één uniek nummer te geven.

1.5 Documenthistorie

Versie	Datum	Omschrijving
6.10.0.0	12-okt-2011	RFC 34508 – van toepassing verklaren NEN 7510 op LSP
6.10.0.0	12-okt-2011	RFC 35171 - Versiebeheer
6.10.0.0	12-okt-2011	RFC 35179 – Authenticatie patiënt voor ZA portaal
6.10.0.0	12-okt-2011	RFC 35181 – Opnemen "fictieve BSN's"
6.10.0.0	12-okt-2011	RFC 35188 – Signalering / abonneefunctie
6.10.0.0	12-okt-2011	RFC 36012 – Synchronisatie GBZ en VWI
6.10.0.0	12-okt-2011	RFC 42826 – Verwijderen BOV uit AORTA 7
6.10.0.0	12-okt-2011	RFC 42949 – Wijzigen datamodel applicatieregister
6.10.0.0	12-okt-2011	RFC 33574 – Uitgifte hostnamen door LSP ipv ZSP
6.10.0.0	12-okt-2011	RFC 46035 – Opt-in voor beschikbaar maken en opvragen van gegevens via AORTA
6.12.1.0	5-dec-2012	RFC 51921 - ZSP label in GBZ-domeinnaam corrigeren

		RFC 51929 - APR: HL7 wijzigingsberichten opnemen RFC 50926 - Aansluiten zonder UZI-servercertificaat RFC 51962 - Regionalisatie RFC 52769 - SBV-Z lijnen weer beschikbaar in LSP
6.12.0.0	17-juni-2013	RfC 53149: Totaal bezwaar is verwijderd uit de documentatie RfC 52946: Signalering eerste aanmelding is verwijderd uit de documentatie RfC 53063: Notificatie Patiënt toegevoegd RfC 52985: VWI: Unieke entries obv BSN gegevenssoort URA applicatie-id RfC 52542: Verplichting GBZ synchronisatie VWI RfC 52866: VWI aanmelden/afmelden op laag Naamgeving: Zorg Service Provider (ZSP) is Goedbeheerd Zorg Netwerk (GZN) geworden.
6.12.15.0	14-dec-2015	RfC 69525: VWI synchronisatie service toegevoegd.
6.14.0.0	15-mei-2017	RfC 73327: Toevoegen Actualiteitscontrole
8.0.1.0	15-mei-2017	RfC 52477: Uitwisseling op basis van bouwstenen
8.0.1.0	15-mei-2017	RfC 63912: Lijn tussen ZIM en SBV is opgeheven.
8.0.1.0	15-mei-2017	RfC 73281: Zorgaanbiedersadresboek herzien
8.0.1.0	15-mei-2017	RfC 76144: Autorisatieprofiel verwijderd
8.0.1.0	15-mei-2017	RfC 76145: Aanpassen DeS naar SDS
8.0.1.0	15-mei-2017	RfC 76206: SSL verwijderen
8.0.1.0	15-mei-2017	RfC 76215: Oude ZAB verwijderen
8.0.1.0	15-mei-2017	RfC 76227: Opschonen APR-berichten
8.0.1.0	15-mei-2017	RfC 76226: Opschonen VWI-berichten
8.0.2.0	31-jan-2018	RfC 75382: Mandaattokens
8.0.3.0	15-nov-2018	INI-8571: WBP vervangen door AVG
8.0.3.0	15-nov-2018	INI-8760: Uitbreiding met CZT-mechanisme (hoofdstuk 7.6)
8.0.3.0	15-nov-2018	INI-8807: Uitbreiding met externe componenten/infrastructuren (hoofdstuk 14.1.4).
8.1.0.0	1-aug-2019	INI-8936: Verwijderen interface LSP.APR.i1060 en LSP.APR.i1040
8.1.0.0	1-aug-2019	INI-8937: Afhandelen berichtversies door ZIM
8.1.0.0	1-aug-2019	INI-8894: Koppeling DVZA
8.1.0.0	1-aug-2019	INI-8847: Opvragen gegevens zonder raadpleging VWI
8.1.0.0	1-aug-2019	INI-8877: Conditionele query
8.1.0.0	1-aug-2019	INI-8874: Aanpassen VWI m.b.t. bouwstenen

2 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.

2.1 Primaire interacties

AORTA ondersteunt als primaire interacties¹ 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.

2.2 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.

2.3 Authenticatie en autorisatie

AORTA authenticceert zorgverleners en patiënten die via AORTA gegevens uitwisselen. Zorgverleners moeten hiertoe beschikken over een UZI-pas, die hun unieke zorgverleneridentificatie 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 (opt-in), 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.

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

Klantenloketmedewerkers kunnen hierbij enkele gegevens namens de patiënt opvragen. Klantenloketmedewerkers identificeren zich met een PKIO-pas.

2.4 Betrokken informatiesystemen

AORTA.ALG.d1000 geeft een vereenvoudigd overzicht van de informatiesystemen die betrokken zijn bij AORTA.

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

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;²
 - 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;
- goed beheerde connector (GBC), connector die patiëntgegevens ontsluit van externe infrastructuren aan de AORTA-infrastructuur;
- dienstverlener zorgaanbieder (DVZA), connector die patiëntgegevens uit de AORTA-infrastructuur ontsluit aan het MedMij-netwerk.

Voor systeemauthenticatie moeten systemen beschikken over een UZI-servercertificaat (GBZ) of een servercertificaat van PKIoverheid (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.

² 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.

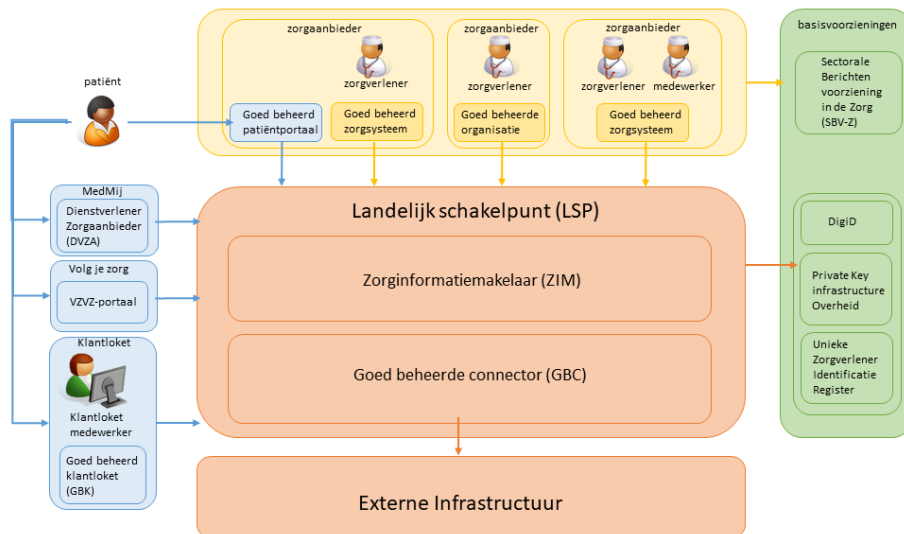


Diagram AORTA.ALG.d1000– overzicht AORTA

2.5 Berichtuitwisseling

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).

2.6 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], dat een geheel vormt van technische, organisatorische en juridische waarborgen. In de architectuur komen vooral de technische waarborgen aan de orde.

3 Inleiding en context

3.1 Achtergrond

Zorgverleners in Nederland zijn op grond van de [WGBO] verplicht tot het inrichten van een dossier waarin alle gegevens omtrent de behandeling en de gezondheid van de patiënt worden opgenomen. 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 toekomstvaste 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 een [Vertrouwensmodel] waarbinnen gebruikers eenduidig worden geïdentificeerd, geauthenticeerd en geautoriseerd voor gegevensuitwisselingen. Alle uitwisselingen vinden plaats over beveiligde verbindingen tussen geïdentificeerde systemen en 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.

Elk van deze aspecten wordt in dit architectuurdocument en de hieraan gerelateerde documenten (zie bijlage A) verder uitgewerkt.

3.2 Wettelijk kader

De zorg in Nederland is in belangrijke mate wettelijk gereguleerd. Ook bij vastlegging en uitwisseling van informatie in de zorg speelt wetgeving een rol. Een uitgebreide behandeling hiervan valt buiten de reikwijdte van architectuurdocumentatie, maar aangezien enkele wetten voor een begrip van de architectuurcontext relevant zijn, worden ze hier kort genoemd.

3.2.1 Wet op de geneeskundige behandelingsovereenkomst [WGBO]

De WGBO regelt de privaatrechtelijke verhouding tussen hulpverlener en patiënt. Voor de hulpverlener geldt een dossierplicht. Inzage in het dossier voor andere hulpverleners dan diegenen die betrokken zijn bij de behandeling is alleen mogelijk met toestemming van de patiënt. Inzage zonder toestemming is mogelijk als wet- of regelgeving daartoe verplicht. De patiënt zelf heeft recht op inzage in diens dossier en recht op een afschrift hiervan. De WGBO stelt tevens bewaartermijnen vast voor dossiergegevens.

3.2.2 Wet beroepen in de individuele gezondheidszorg [WBIG]

De WBIG bevat een systeem van titelbescherming voor een aantal beroepsgroepen in de zorg. Personen die deze titels mogen voeren, worden opgenomen in het BIG-register, een register onder beheer van het CIBG, een uitvoeringsorganisatie van het ministerie van Volksgezondheid, Welzijn en Sport (VWS).

3.2.3 Kwaliteitswet zorginstellingen [KWZi]

De KWZi bevat normen voor het bieden van verantwoorde zorg door zorginstellingen. De wet is van toepassing op alle instellingen waar in georganiseerd verband zorg wordt aangeboden, zoals ziekenhuizen en verpleeghuizen, maar ook bijvoorbeeld groepspraktijken van samenwerkende fysiotherapeuten. Solistisch werkende beroepsbeoefenaren, zoals een huisarts met een assistent, vallen niet onder de KWZi. In de KWZi worden onder meer eisen gesteld ten aanzien van de organisatie en het kwaliteitssysteem. Het gebruik van AORTA kan worden beschouwd als onderdeel van het verlenen van verantwoorde zorg in de zin van de KWZi.

3.2.4 Algemene verordening gegevensbescherming [AVG]

De AVG bevat bepalingen die digitale communicatie voorschrijven in het contact met burgers en medeverwerkers. Een voorbeeld daarvan is dat indien een inzageverzoek elektronisch is gedaan, de informatie op elektronische wijze en in een gebruikelijk format worden verstrekt. Ook voor andere verzoeken geldt indien deze elektronisch zijn gedaan, dat zoveel mogelijk elektronisch beantwoord moet worden.

Nieuwe rechten in de AVG zijn het recht op dataportabiliteit en het recht op vergetelheid. Het recht op dataportabiliteit houdt in dat de betrokkene in bepaalde gevallen (namelijk wanneer er sprake is van elektronische gegevensverwerking) het recht heeft om zijn gegevens in een gestructureerde, gangbaar en machine-leesbare vorm te verkrijgen. En dat hij deze mag overdragen aan een andere verantwoordelijke. Als het technisch

mogelijk is, heeft de betrokkene het recht de gegevens rechtstreeks te laten doorsturen van de ene naar de andere verantwoordelijke.

Een andere toevoeging aan de rechten is het recht op vergetelheid. Indien de betrokkene hierom verzoekt, dient de verantwoordelijke de persoonsgegevens van deze betrokkene te wissen. Dit strekt ver. De verantwoordelijke moet er dan namelijk voor zorgen, dat de gegevens uit alle systemen verwijderd worden, ook als deze systemen zich bij sub-verwerkers bevinden.

Tot slot worden er in de AVG meer verplichtingen en bevoegdheden aan verwerkers en verantwoordelijken opgelegd c.q. toegekend. Om te voorkomen dat de verwerker een lichter regime zou treffen dan de verantwoordelijke bij dezelfde gegevensbescherming, of de verantwoordelijke de regelgeving ontloopt of niet goed kan uitvoeren, legt de AVG de verwerker zwaardere verplichtingen op. De verantwoordelijke moet de op hem rustende verplichtingen inzake gegevensbescherming eveneens opleggen aan de verwerker(s) die hij inschakelt.

De verantwoordelijke heeft een verantwoordingsplicht opgelegd gekregen. Deze verplichting brengt met zich mee, dat de verantwoordelijke aan moet kunnen tonen, hoe hij de beginselen, zoals die zijn opgenomen in artikel 5 AVG, naleeft. Daarvoor is het nodig, dat de verantwoordelijke betrokkenen informatie verstrekt over de verzameling van gegevens, de betrokkenen toegang geeft tot die gegevens, aangeeft hoe met die gegevens omgegaan wordt, etc. De verantwoordelijke dient maatregelen toe te passen die, door ontwerp en standaardinstellingen, ertoe leiden dat de gegevensbeschermingsbeginselen doeltreffend worden uitgevoerd (privacy by design, privacy by default).

De verantwoordelijke dient aan te tonen dat hij aan deze verplichtingen voldoet, door het in stand houden van een Verwerkingsregister en het uitvoeren van gegevens-effectbeoordelingen (Privacy Impact Assessments).

3.2.5 Wet gebruik burgerservicenummer in de zorg Wbsn-z

De Wbsn-z regelt dat in alle berichtgeving tussen zorgaanbieders het burgerservicenummer aanwezig moet zijn om persoonsverwisseling en daardoor (mogelijke) medische fouten te voorkomen. Een burgerservicenummer mag pas door de zorgaanbieder worden gebruikt nadat de patiënt zich heeft gelegitimeerd met een wettelijk identificatiedocument.

3.3 Architectuurprincipes

Aan AORTA liggen enkele belangrijke architectuurprincipes ten grondslag. Deze principes worden hier behandeld, waarbij de achterliggende argumentatie en de implicaties worden aangegeven.

AORTA.ALG.p1000: patiëntgegevens worden steeds bij het bronsysteem opgevraagd.

Het primaire doel van AORTA is het faciliteren van de uitwisseling van patiëntgegevens tussen zorgverleners. Er wordt een *transportfaciliteit* beoogd en niet een vervanging van het bronsysteem. Er wordt dus geen medisch inhoudelijke informatie vastgelegd in een (nieuwe) centrale bron buiten de bronsystemen van de zorgaanbieders.

Voor zover (niet medische) gegevens op een centrale plek worden opgeslagen dient dit uitsluitend om:

- de gegevensbronnen op efficiënte wijze te kunnen ontsluiten;
- vast te kunnen stellen wie welke gegevens mag uitwisselen via AORTA;
- vast te kunnen stellen wie op welk moment gegevens heeft uitgewisseld via AORTA.

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.
- De eigenaar van het bronsysteem houdt de controle over de gegevens.
- Doordat geen centrale database ontstaat is er minder kans op gebruik van de gegevens voor andere doeleinden dan de oorspronkelijke.

AORTA.ALG.p1010: aan aangesloten zorgsystemen worden uitsluitend eisen gesteld die noodzakelijk zijn voor veilige gestandaardiseerde uitwisseling van gegevens.

Zorgverleners werken met diverse zorginformatiesystemen die zij afnemen van verschillende marktpartijen. AORTA is 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 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.

AORTA.ALG.p1020: voor toegang tot patiëntgegevens moeten zorgverleners persoonlijk worden geïdentificeerd en geauthenticeerd³.

Het is uitsluitend voor zorgverleners waarvan de identiteit eenduidig is vastgesteld en bewezen toegestaan om patiëntgegevens te raadplegen.

AORTA.ALG.p1030: de mate van toegang van zorgverleners tot patiëntgegevens wordt bepaald door de rol van de zorgverlener.

Niet alle vastgelegde gegevens zijn noodzakelijkerwijs relevant voor andere zorgverleners. Met het oog op privacy is het niet wenselijk om gegevens uit te wisselen die niet nodig zijn voor de behandeling van de patiënt door een zorgverlener. Daarom wordt de toegang voor zorgverleners beperkt aan de hand van hun rol.

AORTA.ALG.p1040.1: gegevens worden slechts beschikbaar gesteld door zorgaanbieders via AORTA na toestemming van de patiënt; bovendien kunnen patiënten de toegang van (specifieke) zorgverleners tot hun gegevens inperken.

Elektronische uitwisseling van patiëntgegevens tussen zorgverleners is privacygevoelig. Het is op basis van bestaande wetgeving (behoudens enkele uitzonderingen) nodig, maar ook maatschappelijk wenselijk dat de patiënt expliciet instemt met het beschikbaar

³ Identificatie is het vaststellen van de identiteit van een gebruiker. Authenticatie is het geven van een bevestiging dat de persoon in kwestie inderdaad degene is voor wie hij zich uit geeft, op grond van een bewijs van identiteit.

maken van zijn gegevens via AORTA, ook al wordt deze beschikbaarheid van gegevens geacht in het belang te zijn van de patiënt.

Patiënten hebben verder de mogelijkheid om uitwisseling via AORTA desgewenst voor specifieke zorgverleners toe te staan of te blokkeren.

AORTA.ALG.p1050: patiënten hebben via AORTA toegang tot hun eigen gegevens.

Patiënten hebben in de “papieren wereld” op grond van de [WGB0] het recht op inzage in en afschrift van hun dossier dat individuele zorgverleners over hen bijhouden. Het ligt daarom voor de hand dat gegevens die elektronisch beschikbaar worden gesteld voor uitwisseling via AORTA, ook via AORTA beschikbaar worden gesteld aan de patiënt. Hierdoor wordt het eenvoudiger voor de patiënt om gebruik te maken van het recht op inzage in en afschrift van zijn dossier.

AORTA.ALG.p1060: toegang tot patiëntgegevens wordt vastgelegd en is hierdoor traceerbaar.

Patiëntgegevens zijn privacygevoelige gegevens die alleen toegankelijk mogen zijn voor de behandelende zorgverleners en de patiënt zelf. Daarom is het van belang dat precies kan worden vastgesteld wie deze gegevens heeft geraadpleegd of verstuurd.

AORTA.ALG.p1070: De AORTA architectuur ondersteunt informatie-uitwisseling via berichten met informatie opgenomen in voorgedefinieerde, herbruikbare bouwstenen.
--

Gebruik van voorgedefinieerde, herbruikbare bouwstenen als elementaire informatiedelen voor het samenstellen van berichten 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.

4 Primaire interacties: het opvragen en sturen van patiëntgegevens

4.1 Interacties

Het primaire doel van AORTA is het ondersteunen van informatie-uitwisseling tussen zorgverleners. Hiertoe ondersteunt AORTA een tweetal primaire interacties⁴, 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.

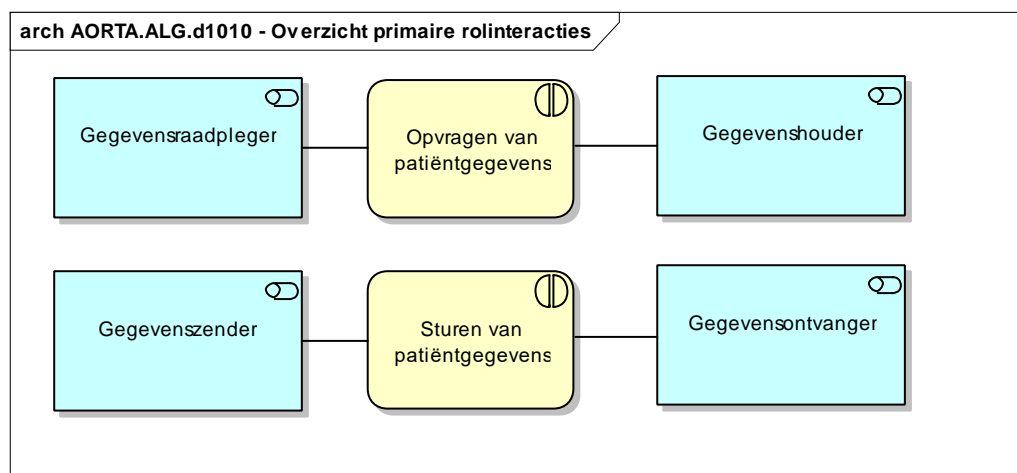


Diagram AORTA.ALG.d1010 - primaire interacties van AORTA

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.

4.2 Actoren

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

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

⁴ Een 'interactie' is een wisselwerking tussen organisaties, personen en/of systemen, waarbij gegevens kunnen worden uitgewisseld.

4.2.1 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.

4.2.2 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.

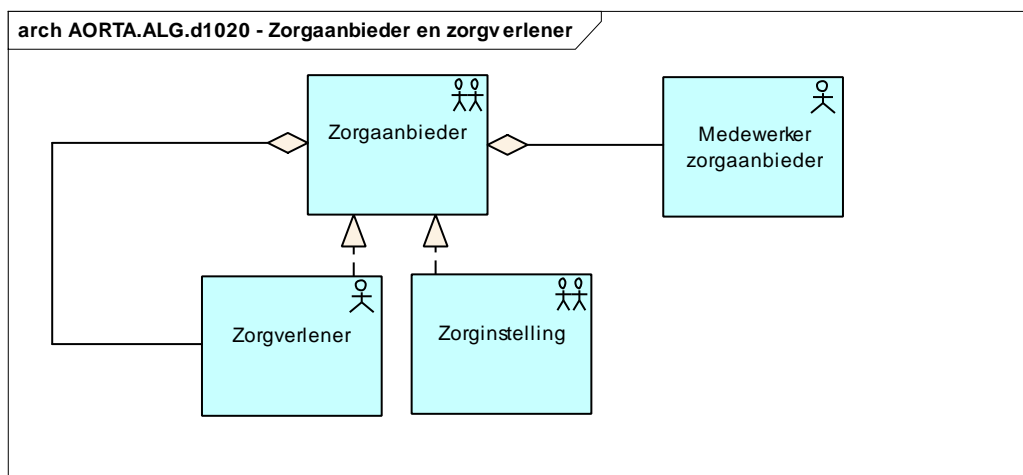


Diagram AORTA.ALG.d1020 - illustratie van het begrip zorgaanbieder

4.2.3 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.

4.2.4 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 burgerservicenummer aanwezig moet zijn, kan de patiënt in de praktijk elke persoon zijn aan wie een burgerservicenummer 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.

4.2.5 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 PKIoverheid servercertificaat. In geval een instelling is voorzien van een PKIoverheid servercertificaat gelden dezelfde uitgangspunten als voor een zorgaanbieder.

Alleen zorgverleners (zoals beschreven in hoofdstuk 4.2.1) kunnen gegevens uitwisselen via de AORTA infrastructuur. Binnen een GBO dienen dus wel zorgverleners werkzaam te zijn om patiëntgegevens op te kunnen vragen.

4.3 Toekenning van rollen 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'.

4.3.1 Opvragen van patiëntgegevens

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

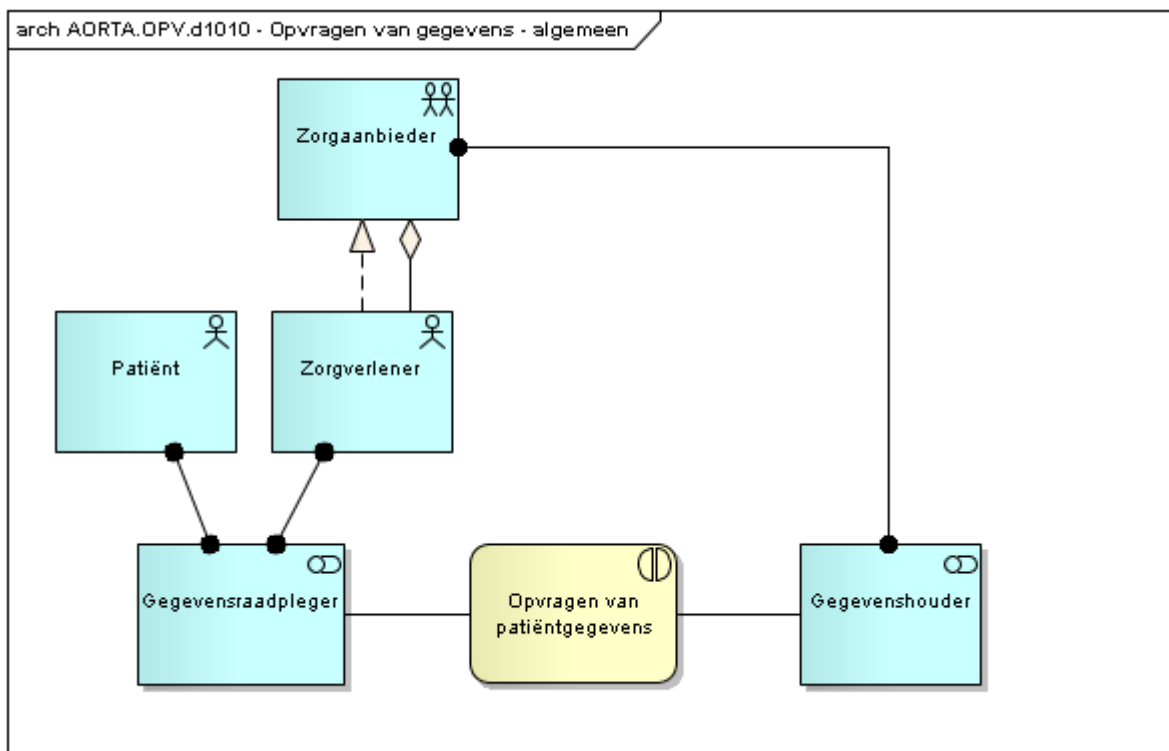


Diagram AORTA.OPV.d1010 - opvragen van patiëntgegevens

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.

4.3.2 Sturen van patiëntgegevens

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

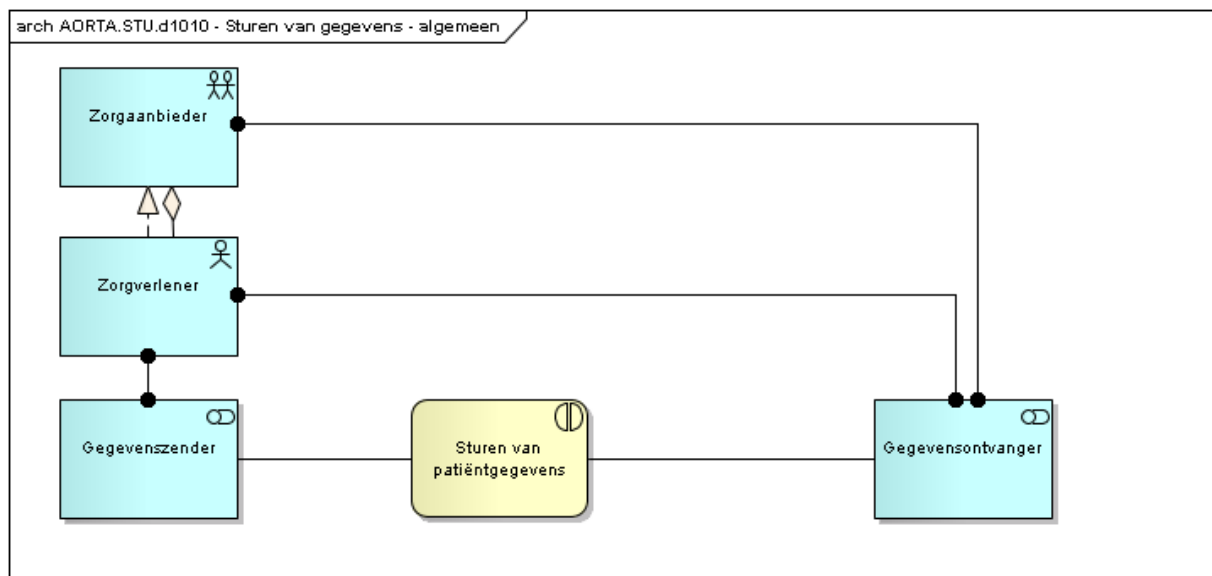


Diagram AORTA.STU.d1010 - Sturen van patiëntgegevens

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.

4.3.3 Toegangsbeperkingen

De modellen in paragraaf 4.3.1 en 4.3.2 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.

4.4 Toegangsmodel

Het model van toegangsregels is het toegangsmodel. Om het toegangsmodel te bespreken is het noodzakelijk om enkele aanvullende begrippen te introduceren, namelijk:

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

4.4.1 Opt-in van de patiënt

De [AVG] en [WGBO] bieden het wettelijk kader voor het uitwisselen van gegevens in de zorg. Op grond van deze wetgeving geldt voor uitwisseling van medische gegevens onder de in dit document beschreven condities⁵, dat expliciete toestemming nodig is van de patiënt voor het beschikbaar stellen van gegevens door een gegevenshouder aan een gegevensraadpleger.

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.

4.4.2 Behandelrelatie

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

De volgende zorgaanbieders⁶ of zorgverleners hebben een behandelrelatie volgens de [WGBO]:

- degene die een behandelingsovereenkomst⁷ 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.

⁵ Zie voor een uitgebreide interpretatie van de wettelijke condities de [Zienswijze CBP].

⁶ De WGBO 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.

⁷ Zie [WGBO] (artikel 7:446 BW)

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.

4.4.3 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 specialisme⁸ van de betrokken zorgverleners. Het resultaat van deze afstemming wordt vastgelegd in een autorisatie*protocol* en in determinatietabellen.

4.4.4 Mandatering

Zoals uitgelegd in subparagraaf 4.3.1 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.

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

4.4.5 Vertegenwoordiging

Zoals beschreven in subparagraaf 4.3.1 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 [WGBO] voor een precieze beschrijving van deze uitzonderingssituaties. Bij de bespreking van de informatiesystemen voor patiënttoegang in paragraaf 6.5 en 6.6 wordt aangegeven in hoeverre deze uitzonderingen in de architectuur een rol spelen.

⁸ 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.

4.4.6 Samenwerkingsverband

Zoals uitgelegd in subparagraaf 4.3.1 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.

4.5 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 patiënt gegevens 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 Wbsn-z 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 subparagraaf 13.2.3).
- 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 medewerkerpas 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 organisatiename die gerelateerd is aan de URA niet noodzakelijk herleidbaar tot één vestigingslocatie of organisatieonderdeel van die zorgaanbieder.

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

4.6 Patiëntgegevens

In dit architectuurdocument wordt onder 'patiëntgegevens' verstaan: medisch inhoudelijke gegevens en administratieve gegevens over een patiënt. 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, een internationaal geaccepteerde open standaard voor uitwisseling van medische informatie. In paragraaf 13.1 wordt nader ingegaan op enkele aspecten van de HL7v3 berichtstructuur.

4.7 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 locatiegegevens 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.

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 het Zorgaanbiedersadresboek een mogelijkheid om identificerende zorgaanbieder- en zorgverlenergegevens op te zoeken met de bijbehorende (technische) adressering.

Het Zorgaanbiedersadresboek (ZAB) is een database waarin diverse zorgaanbiedersgegevens en zorgverlenersgegevens zijn opgeslagen en raadpleegbaar worden gemaakt voor derden.

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

5 Ondersteunende interacties

5.1 Ondersteunende interacties

Naast de primaire interacties van opvragen en sturen van patiëntgegevens, biedt AORTA een aantal ondersteunende ('secundaire') interacties, die behandeld worden in dit hoofdstuk, voornamelijk los van de implicaties op informatiesysteemniveau (deze komen aan de orde in hoofdstuk 6 en 7). Een overzicht van de ondersteunende interacties wordt gegeven in diagram AORTA.ALG.d1030.6.

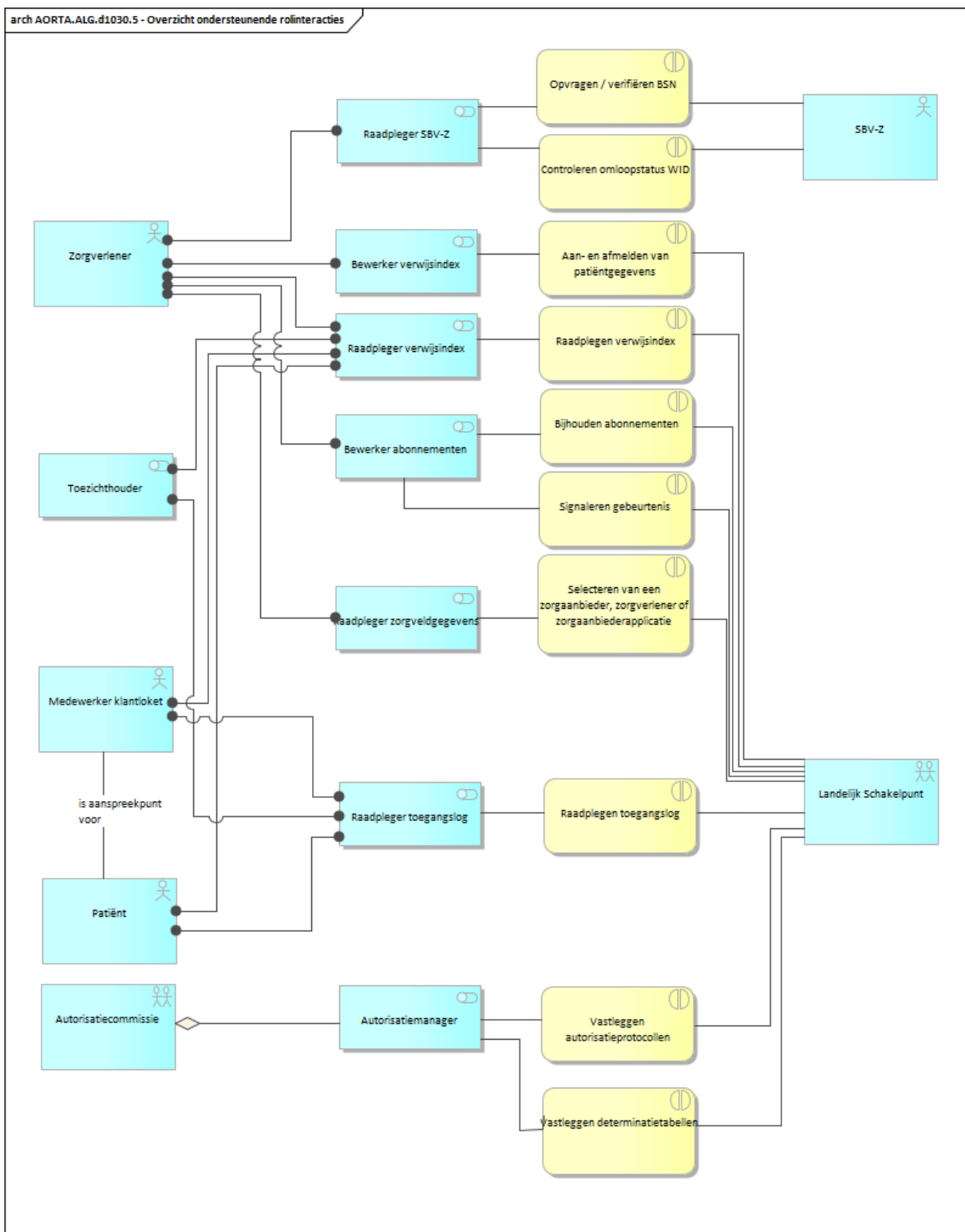


Diagram AORTA.ALG.d1030.6 - overzicht van ondersteunende interacties

Bij de volgende ondersteunende interactie wisselen eindgebruikers gegevens uit met de Sectorale Berichten Voorziening in de Zorg (SBV-Z) (zie 5.2.1):

- 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 toegangslog;
- vastleggen van autorisatieprotocollen;
- vastleggen van determinatietabellen.

De bovenstaande interacties worden vanaf paragraaf 5.3 besproken.

Naast bovenstaande interacties kunnen eindgebruikers door gebruik van een abonnementsfunctie aangeven dat zij in bepaalde situaties een abonnementssignaal willen ontvangen van het LSP.

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. Een abonnementssignaal, is een signaal dat door het LSP wordt verstrekt aan een actor die een abonnement heeft genomen op dergelijke signalen (zie verder paragraaf 5.6). In het geval de actor een patiënt betreft, dan wordt gesproken over een notificatie in plaats van over een abonnementssignaal.

5.2 Actoren en rollen

De actoren 'zorgverlener' en 'patiënt' zijn geïntroduceerd in paragraaf 4.2. Aanvullende actoren worden hier besproken.

5.2.1 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.

5.2.2 Landelijk schakelpunt

Het Landelijk Schakelpunt (LSP) (geïntroduceerd in paragraaf 4.7) 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.

5.2.3 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 verwijfsindexgegevens en toegangsloggegevens, zie 5.5 en 5.8). Klantenloketmedewerkers worden geïdentificeerd aan de hand van een PKIoverheidscertificaat (zie subparagraaf 6.10.2).

5.2.4 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 in subparagraaf 4.4.3. 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.

5.2.5 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).

5.2.6 Rollen

In het overzichtsdiagram AORTA.ALG.d1030.6 worden diverse rollen geïntroduceerd, zoals 'bewerker verwijfsindex' en 'raadpleger verwijfsindex'. 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 verwijfsindex' geldt bijvoorbeeld dat een zorgverlener toegang krijgt tot andere indexgegevens dan een patiënt.

5.2.7 Mandatering

De mogelijkheid van mandatering die is geïntroduceerd in subparagraaf 4.4.4 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.

5.3 Opvragen/verifiëren BSN en controleren omloopstatus WID

De Wbsn-z 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.⁹ Ook kan een zorgverlener de

⁹ 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

omloopstatus van een aan hem aangeboden identificatiedocument bij de SBV-Z controleren.

5.4 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.

5.5 Raadplegen verwijsindex

Het raadplegen van de verwijsindex 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 verwijsindex terug te vinden.

De rol van 'raadpleger verwijsindex' 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 verwijsindex 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 verwijsindexgegevens te raadplegen;
- de toezichthouder op het correct gebruik van AORTA.

5.6 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 abonnementshouder 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.

gelegitimeerd met een geldig wettelijk identificatiedocument, is sprake van 'voorlopig gekoppelde' patiëntgegevens; na legitimatie is sprake van 'definitief gekoppelde' patiëntgegevens.

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.

5.7 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 (ZAB). 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 subparagraaf 4.3.2) zijn zowel zorgaanbieders als zorgverleners opgenomen in dit adresboek.

De gegevenszender moet ook de zorgaanbiederapplicatie (het informatiesysteem¹⁰ van een zorgaanbieder) waarnaar de gegevens daadwerkelijk worden gestuurd kunnen opzoeken. Hiertoe houdt het LSP in aanvulling op een zorgadresboek een applicatieregister (APR) bij.

5.8 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 of verstuurd. Omdat het LSP optreedt als intermediair bij raadplegen en sturen van patiëntgegevens kan het LSP nauwkeurig bijhouden in een log wie bij raadplegen 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 geraadpleegd.
- 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.

5.9 Vastleggen autorisatieprotocollen

Zoals beschreven in subparagraaf 4.4.3 wordt een autorisatieprotocol vastgesteld waarin wordt vastgelegd per zorgverlenerberoep- 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.

5.10 Vastleggen determinatietabellen

Zoals beschreven in subparagraaf 4.4.3 wordt een determinatietabel vastgesteld waarin wordt vastgelegd per zorgverlenerberoep- en specialisatie welke gegevens kunnen

¹⁰ De termen 'informatiesysteem' en 'applicatie' worden in dit document beide gebruikt voor het aanduiden van een systeem voor gegevensverwerking.

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.

6 Informatiesystemen

In dit hoofdstuk worden de verschillende informatiesystemen besproken, die betrokken zijn bij de uitwisseling van gegevens via AORTA.

6.1 Inleiding

AORTA.INF.d1020 geeft in een vereenvoudigd infrastructuurdiagram¹¹ een overzicht van de informatiesystemen die elk afzonderlijk in dit hoofdstuk worden besproken.

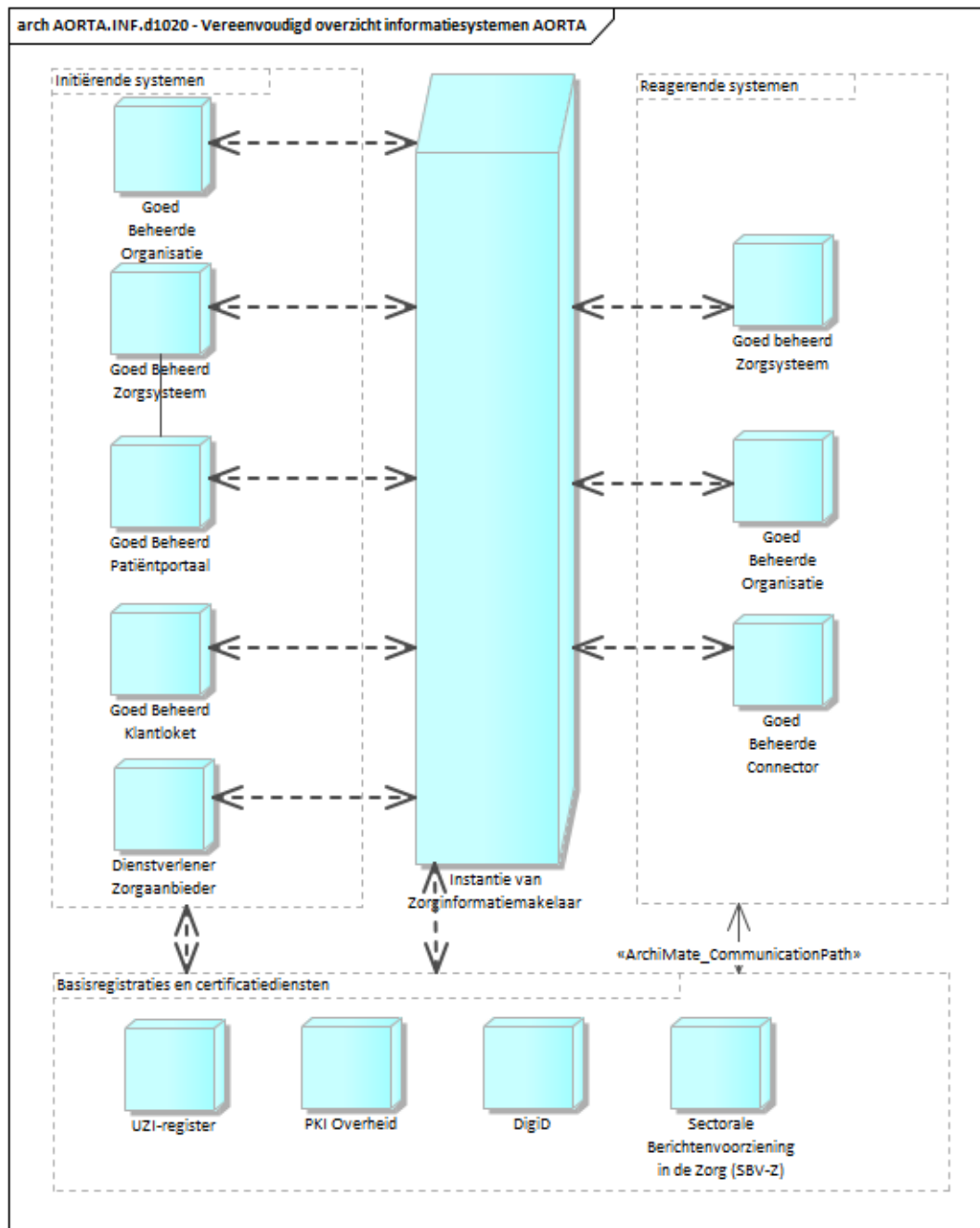


Diagram AORTA.INF.d1020 – overzicht informatiesystemen AORTA

¹¹ Zie voor een meer uitgebreide bespreking van de infrastructuur hoofdstuk 14

Centraal in AORTA staat de Zorginformatiemakelaar (ZIM) (zie paragraaf 6.2), 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 paragraaf 6.3).

Tot de groep van GBx'en behoren:

- een goed beheerd zorgsysteem (GBZ, zie paragraaf 6.4), een informatiesysteem dat door een zorgverlener of een medewerker wordt gebruikt om een patiëntdossier in te richten;
- een goed beheerd patiëntportaal (GBP, zie paragraaf 6.5), een portaal dat patiënten toegang geeft tot hun eigen gegevens;
- het goed beheerd klantenloketsysteem (GBK, zie paragraaf 6.6), het toegangssysteem van de klantenloketorganisatie.
- een goed beheerde organisatie (GBO, zie paragraaf 6.7), een informatiesysteem dat door een zorgverlener of een medewerker wordt gebruikt om een patiëntdossier in te richten.

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

- de Dienstverlener Zorgaanbieder (DVZA, zie paragraaf 6.8), connector die patiëntgegevens uit de AORTA-infrastructuur ontsluit aan informatiesystemen in het MedMij-netwerk.
- de goed beheerde connector (GBC, zie paragraaf 6.9), 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 certificatiediensten, namelijk:

- het UZI-register (zie paragraaf 6.10.1), dat unieke zorgverleneridentificaties van zorgverleners bevat;
- PKIoverheid (zie paragraaf 6.10.2), een infrastructuur voor het uitgeven en beheren van digitale certificaten;
- DigiD (zie paragraaf 6.10.3), een register van persoonsidentiteiten voor burgers.

Het GBx heeft aanvullend nog toegang tot de service van de Sectorale Berichten Voorziening in de Zorg (SBV-Z, reeds geïntroduceerd in subparagraaf 5.2.1; zie paragraaf 6.10.4 voor de systeemdiensten van SBV-Z).

6.2 Zorginformatiemakelaar

De 'Zorginformatiemakelaar' (ZIM) is een centraal berichtuitwisselingsplatform, 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. De term 'informatiemakelaar' is van toepassing omdat het platform in feite optreedt als een 'makelaar'¹² van informatie.

De ZIM heeft binnen AORTA de volgende taken:

¹² Parallel aan de Engelse term 'message broker'

- 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 abonnementsignaal 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 ZAB:

- 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 ZAB is naast de ZIM gepositioneerd, maar voor het overzicht wordt de ZAB-functionaliteit ook meegenomen in de beschrijving binnen dit hoofdstuk (hoofdstuk 6.2.4).

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 in hoofdstuk 7 en in de ontwerpdocumenten van de individuele componenten.

De ZIM beschikt naast de logische componenten over een orchestratieservice¹³. 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 strategie wordt in detail behandeld in paragraaf 13.2.

¹³ Zowel de componenten en orchestratieservice worden op logisch niveau beschreven. Over de fysieke implementatievorm van componenten en orchestratieservice worden geen uitspraken gedaan.

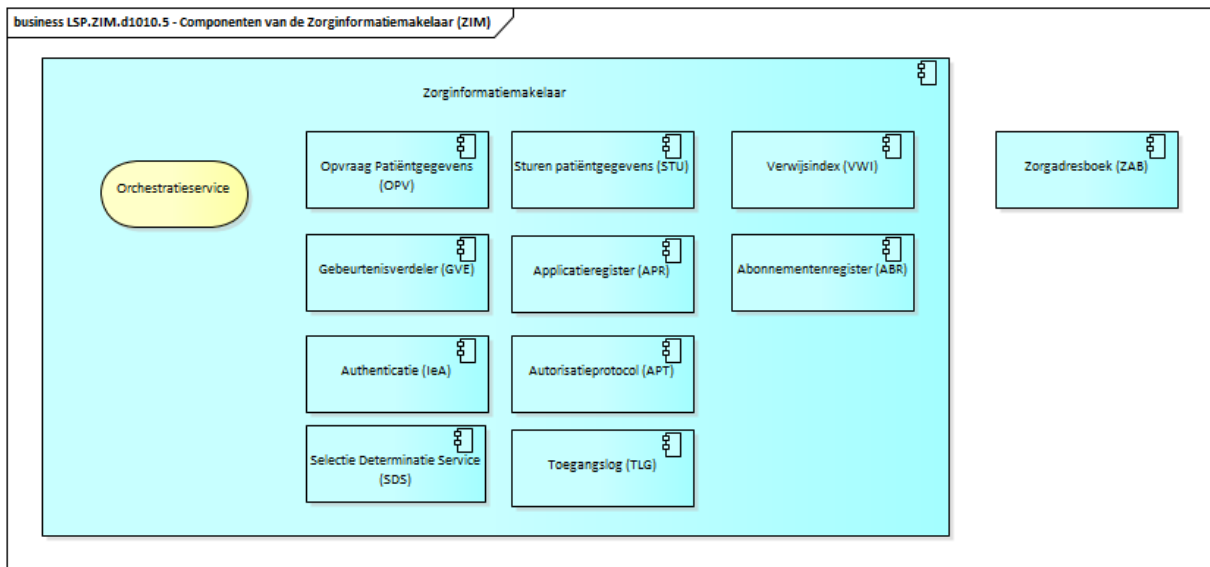


Diagram LSP.ZIM.d1010.5 - systeemcomponenten binnen de Zorginformatiemakelaar

6.2.1 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.

6.2.2 Sturen patiëntgegevens

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

6.2.3 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.

6.2.4 Zorgadresboek

Het ZAB is gepositioneerd naast de ZIM, maar is wel opgenomen in de LSP-omgeving. Het ZAB 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.

Het ZAB is vooral bedoeld als hulpmiddel voor gegevenszenders, om hen bij het versturen van gegevens via AORTA in staat te stellen om het informatiesysteem te vinden waarnaar zij een bericht willen sturen. Om dit te bereiken kan de gegevenszender via het zorgadresboek eerst de zorgaanbieder of zorgverlener zoeken die eigenaar is van het informatiesysteem. Het zorgadresboek is dus niet zozeer opgezet als een algemene zorgaanbiedergids om zorgaanbieders ook buiten AORTA om te kunnen bereiken.

6.2.5 Applicatieregister

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

6.2.6 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.

6.2.7 Authenticatie

Deze 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 authenticceert hierbij de initiator van het bericht, aan de hand van informatie die in het bericht is meegegeven.

Het authenticatiemechanisme wordt in algemene zin besproken in hoofdstuk 13.2.3 en verder uitgewerkt in [Ontw Authenticatie].

6.2.8 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.

6.2.9 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 waardoor elk uitwisseling achteraf controleerbaar is.

6.2.10 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 (zie subparagraaf 6.2.6) om te controleren welke systemen een abonnement hebben voor een bepaalde gebeurtenis.

6.2.11 Selectie Determinatie Service

Deze component is betrokken bij het bepalen van de op te leveren bouwstenen en de specifieke invulling van deze bouwstenen. De op te leveren bouwstenen en de specifieke invulling hiervan worden bepaald aan de hand van de context van de opvraag en de rolcode¹⁴ van de zorgverlener die de opvraag doet.

6.3 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

¹⁴ In het geval er sprake is van een mandaat, zal de rolcode van de mandaterende zorgverlener bepalend zijn.

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.

6.4 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 ZIM¹⁵. 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 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 verantwoordelijkheden¹⁶:

- Het GBZ legt de basis voor authenticatie van de gegevensraadpleger of gegevenszender. Allereerst authenticert het GBZ zelf de eindgebruiker als deze aanloopt 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.

¹⁵ Het voldoen aan de implementatie- en exploitatie-eisen wordt getoetst door een eigen verklaring van de beheerorganisatie en uitvoering van steekproefsgewijze schouwingen.

¹⁶ Deze lijst van verantwoordelijkheden is niet limitatief. Hier worden enkele kernverantwoordelijkheden genoemd die bij het GBZ worden belegd in tegenstelling tot de ZIM.

- 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.

6.5 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 subparagraaf 4.3.1 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:¹⁷

- 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 subparagraaf 4.4.5). Eventuele vertegenwoordigers zijn daarom aangewezen op het klantenloket.

6.6 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 subparagraaf 5.2.3.

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.

¹⁷ Op het moment van publicatie bestaan nog geen concrete GBP-implementaties.

6.7 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.

6.8 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.

6.9 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.

6.10 Basisregistraties en vertrouwensmiddelen

6.10.1 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.

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.

6.10.2 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.

6.10.3 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 hoofdstuk 13.2.3).

6.10.4 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 paragraaf 6.4).

7 Beheerinteracties

In hoofdstuk 5 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 zijn geïntroduceerd in hoofdstuk 6, kunnen ook de beheerinteracties kort worden geïntroduceerd. Deze worden echter alleen behandeld voor zover zij leiden tot eisen aan de functionaliteit van de ZIM. 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].

7.1 Actoren en rollen

Ten behoeve van beheer worden de volgende aanvullende rollen onderscheiden.

7.1.1 GBx-beheerder en GBZ-beheerder¹⁸

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 zonodig 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.

7.1.2 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 subparagraaf 5.2.2).

7.2 Toegang van GBZ-beheerders tot primaire en ondersteunende interacties

In hoofdstuk 4 en in hoofdstuk 5 zijn de primaire en ondersteunende interacties 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 op patiëntgegevens mogen door GBZ-beheerders alleen worden uitgevoerd in relatie tot fictieve BSN's.

¹⁸ In operationele zin wordt de beheerderrol per betrokken organisatie verder uitgewerkt in [AORTA DAP].

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-zorgverlenerpas, 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.

7.3 Beheer van aansluitingen

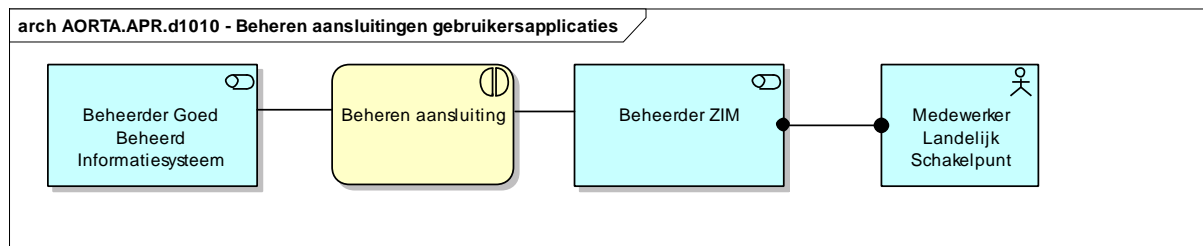


Diagram AORTA.APR.d1010 - interactie voor het beheren van aansluitingen

De ZIM bewaart informatie over aangesloten informatiesystemen in het APR (zie paragraaf 5.7). 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.

7.4 Beheer van de verwijsindex

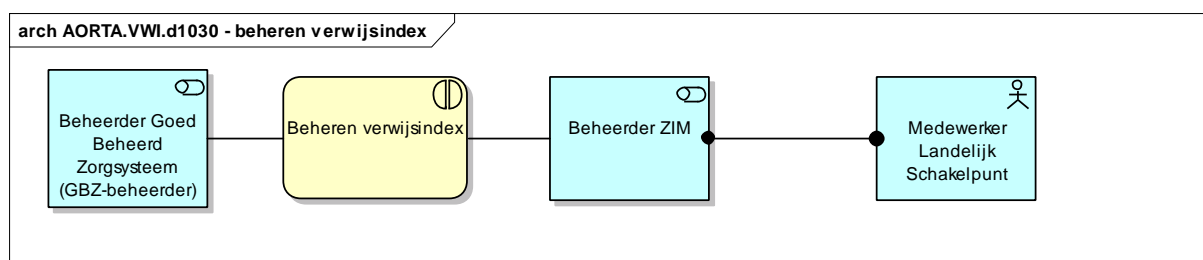


Diagram AORTA.VWI.d1030 – beheren van de verwijsindex

In de VWI van de ZIM staan alle aanmeldingen van alle GBZ'en. 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 aanmeldingen 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.

7.5 Beheer van het zorgadresboek

De gegevens over zorgaanbieders en zorgverleners in het ZAB (zie paragraaf 5.7) worden overgenomen uit een centraal zorgaanbieder/zorgverlenerregister (het UZI-register (zie paragraaf 4.5)) en de VZVZ-administratie.

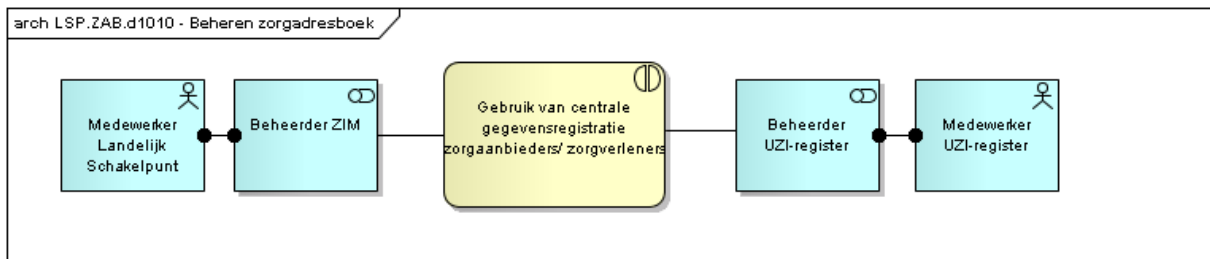


Diagram LSP.ZAB.d1010 - interactie voor het beheer van het adresboek

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

7.6 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 zoals omschreven in hoofdstuk 4: Primaire interacties: het opvragen en sturen van patiëntgegevens.

7.7 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.

8 Interacties tussen informatiesystemen

De volgende hoofdstukken (9 tot en met 11) beschrijven hoe binnen AORTA de interacties uit hoofdstuk 4, 5 en 7 worden gerealiseerd door de informatiesystemen uit hoofdstuk 6. Hierbij ligt de nadruk op de generieke interfaces die de ZIM aanbiedt aan aangesloten informatiesystemen.

8.1 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 initieërend 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 initieërend 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 orchestratieservice van de ZIM. De orchestratieservice 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 in paragraaf 13.2.

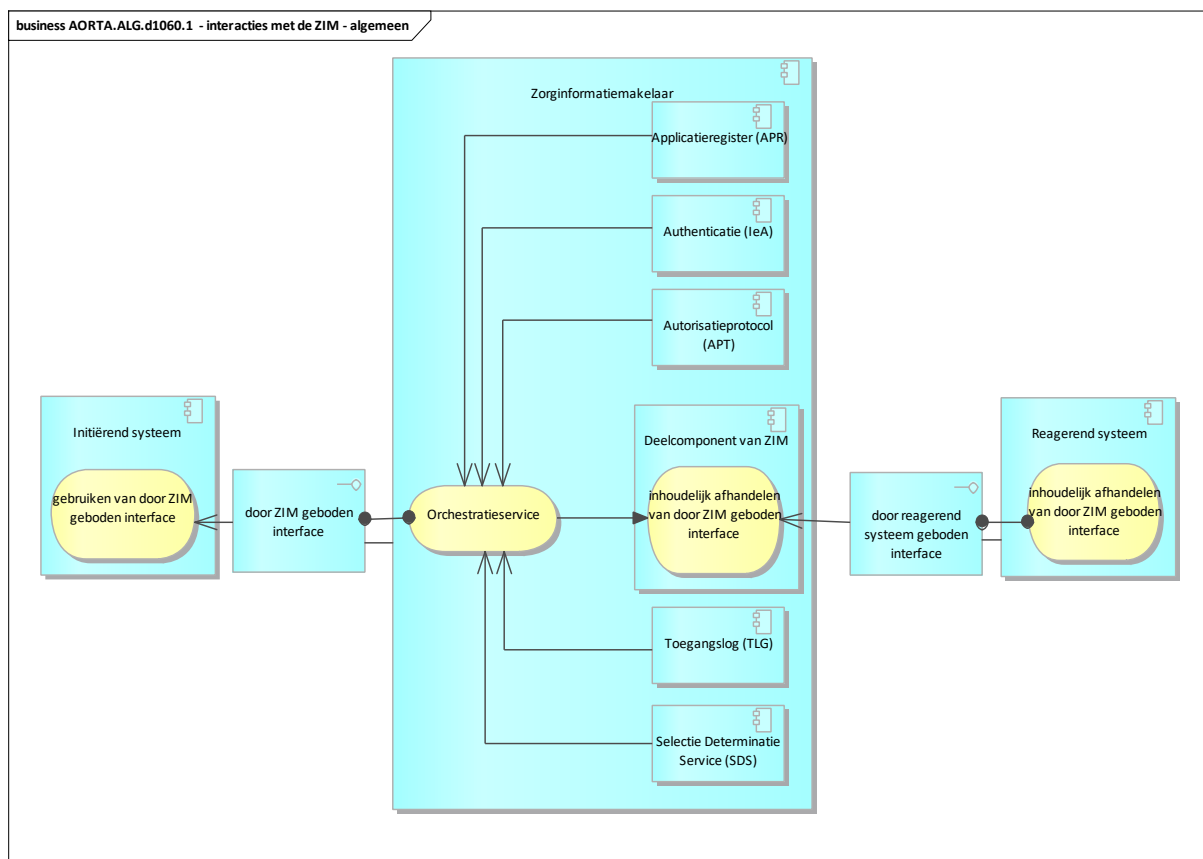


Diagram AORTA.ALG.d1060.1 – algemene beschrijving van interacties met de ZIM

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 hoofdstukken 9 tot en met 11 wordt gevolgd.

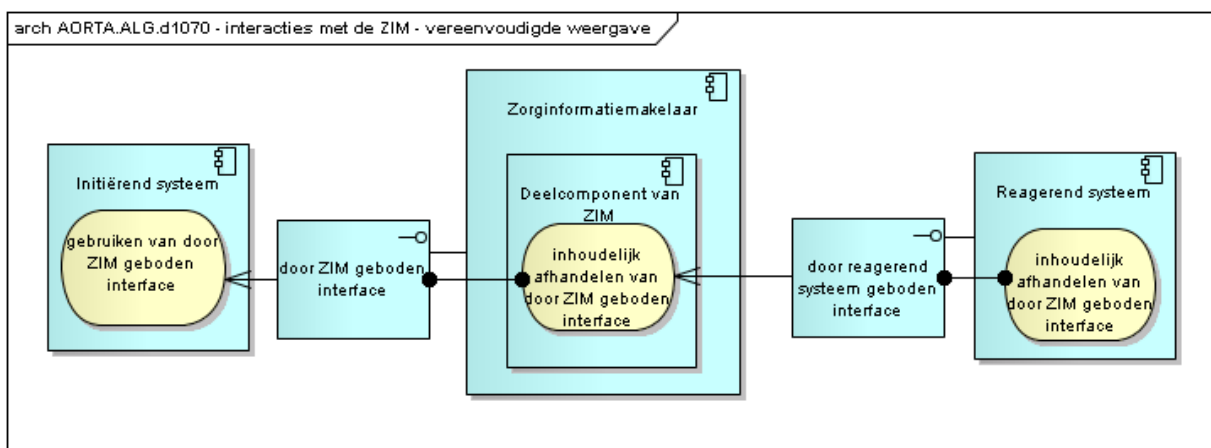


Diagram AORTA.ALG.d1070 – vereenvoudigde weergave van AORTA.ALG.d1060.1

8.2 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 softwareproduct (bv. een XIS) een kwalificatie te behalen voor specifieke combinaties van systeemrollen.

In hoofdstukken 9 tot en met 11 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 12.

8.3 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.

9 Primaire informatiesysteeminteracties – opvragen en sturen van gegevens

In dit hoofdstuk wordt uitgewerkt hoe de primaire interacties, zoals besproken in hoofdstuk 4, worden uitgewerkt op informatiesysteemniveau.

9.1 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 bijgehouden in de Verwijsindex (VWI), die onderdeel is van de ZIM. 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.¹⁹

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.i1010²⁰. Deze situatie is weergegeven in diagram AORTA.OPV.d1050.

¹⁹ Deze functionaliteit wordt alleen geboden via de interface LSP.OPV.i1020.

²⁰ 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.

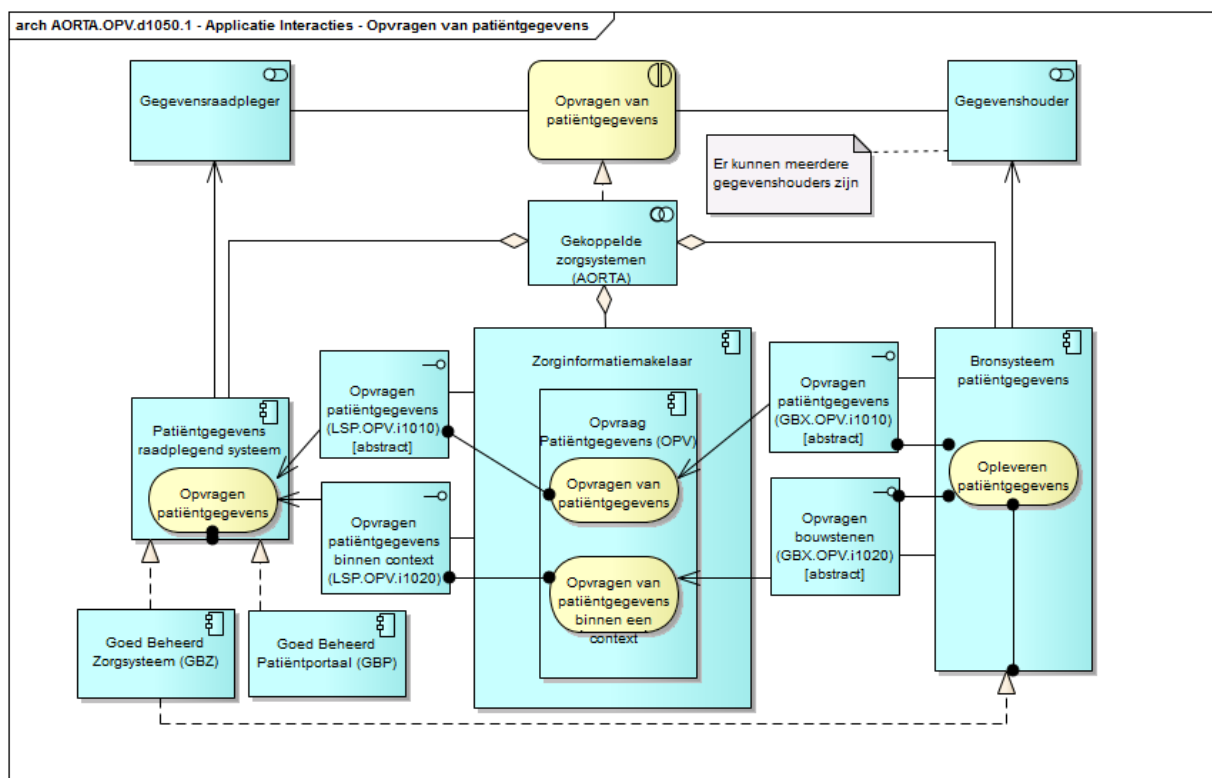


Diagram AORTA.OPV.d1050.1 - informatiesysteeminteracties voor het opvragen van patiëntgegevens

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, huisartswaarneemgegevens) worden concrete implementaties ontworpen van de interface 'opvragen patiëntgegevens' (bijvoorbeeld 'opvragen medicatievoorschriften'). De interface 'opvragen bouwstenen' wordt ingevuld door specifieke bouwsteen bevragingen (bijvoorbeeld 'opvragen medicatieverstrekkingen'). Waar sprake is van abstracte interfaces wordt dit expliciet benoemd.

9.1.1 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.²¹ De OPV component verzamelt vervolgens de resultaten en beantwoordt het oorspronkelijke verzoek.²²

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]).

9.1.2 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.²³

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

9.2 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 subparagraaf 10.3).

De ZIM biedt voor het sturen één interface:

- LSP.STU.i1010: Versturen van patiëntgegevens

Een systeem dat deze interface implementeert heeft de systeemrol 'gegevensversturend systeem'.

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

9.2.1 Interface LSP.STU.i1010: sturen van patiëntgegevens

²¹ Omdat de ZIM hierbij de vraag afkomstig van één applicatie uitzet naar meerdere applicaties wordt gesproken van 'divergeren' van een verzoek.

²² Omdat hierbij de antwoorden afkomstig van meerdere applicaties weer worden gebundeld, wordt gesproken van 'convergeren' van antwoorden.

²³ 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 bevraagd.

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, huisartswaarneemgegevens) worden concrete implementaties ontworpen van deze interface (bijvoorbeeld 'versturen medicatievoorschrift').

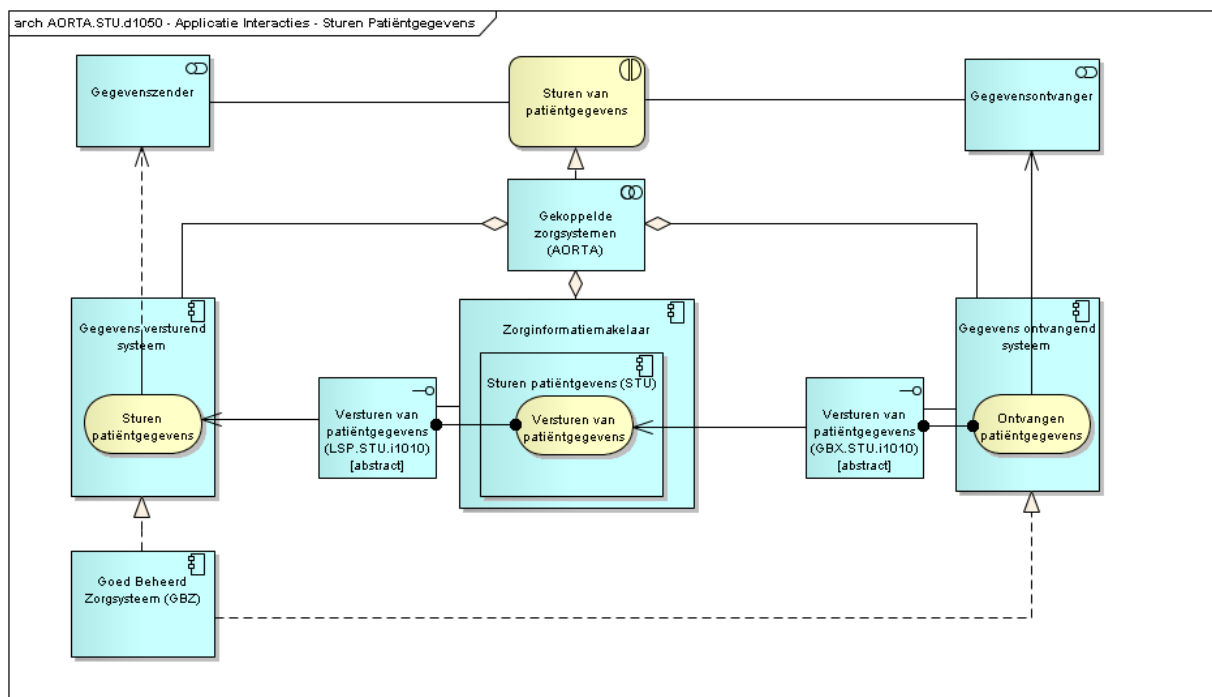


Diagram AORTA.STU.d1050 - informatiesysteeminteracties voor het sturen van patiëntgegevens

10 Ondersteunende informatiesysteeminteracties

In dit hoofdstuk wordt uitgewerkt hoe de ondersteunende interacties, zoals besproken in hoofdstuk 5, worden uitgewerkt op informatiesysteemniveau.

10.1 Aan- en afmelden van patiëntgegevens

Om een ongerichte opvraag van patiëntgegevens via AORTA door andere zorgverleners mogelijk te maken, moet een zorgverlener het bestaan van patiëntgegevens in zijn eigen informatiesysteem aanmelden bij het Landelijk Schakelpunt.

Deze aanmelding leidt tot het opnemen van een nieuwe verwijzing in de Verwijsindex (VWI) die onderdeel is 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 patient (zie verder 10.6).

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.

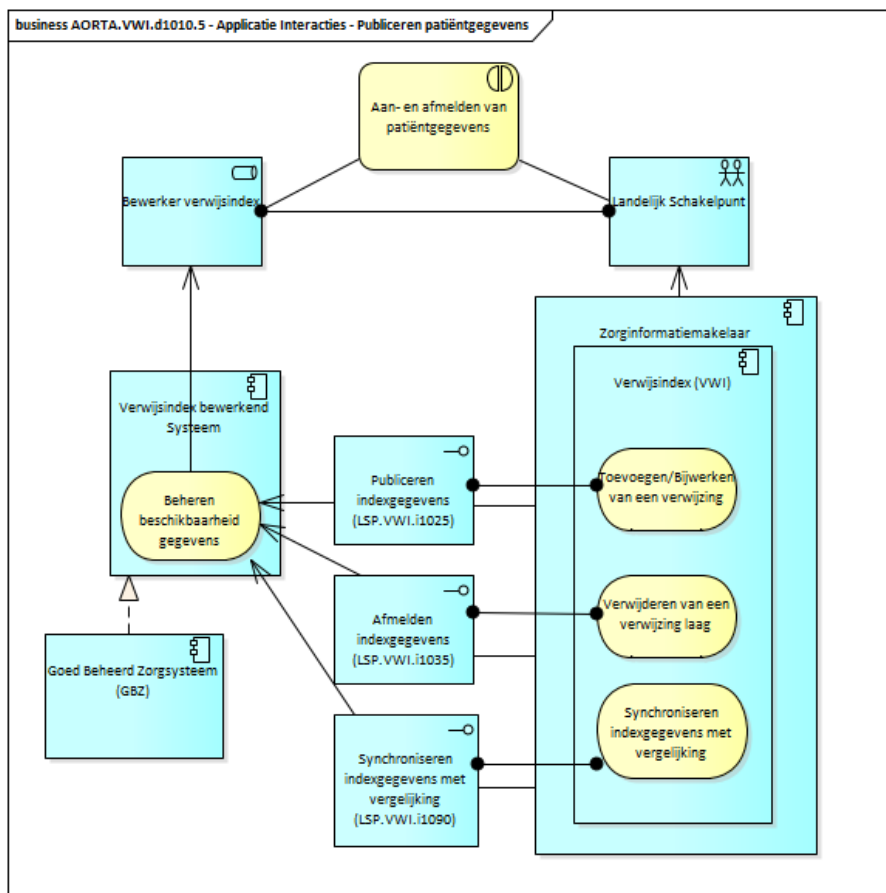


Diagram AORTA.VWI.d1010 - informatiesysteeminteracties voor het beschikbaar maken van patiëntgegevens

10.1.1 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.

10.1.2 Interface LSP.VWI.i2035: Afmelden verwijzing laag

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.

10.1.3 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.

10.1.4 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 beschijft 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].

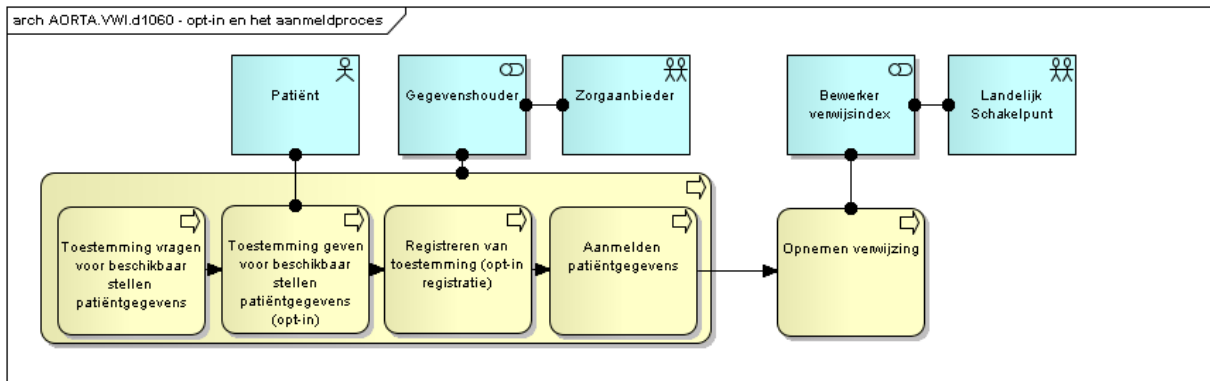


Diagram AORTA.VWI.d1060 - Opt-in en het aanmeldproces

1. Elke zorgverlener die als gegevenshouder verantwoordelijk is voor het beschikbaar stellen van gegevens via het Landelijk Schakelpunt vraagt (eenmalig) 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 verwijzindex.²⁴ 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 verwijzindex neemt de verwijzing op.

10.2 Raadplegen van de verwijzindex

De Verwijzindex (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 verwijzindex:

- LSP.VWI.i1060: Actualiteitscontrole;
- LSP.VWI.i1080: Opvragen indexgegevens midden.

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

²⁴ 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).

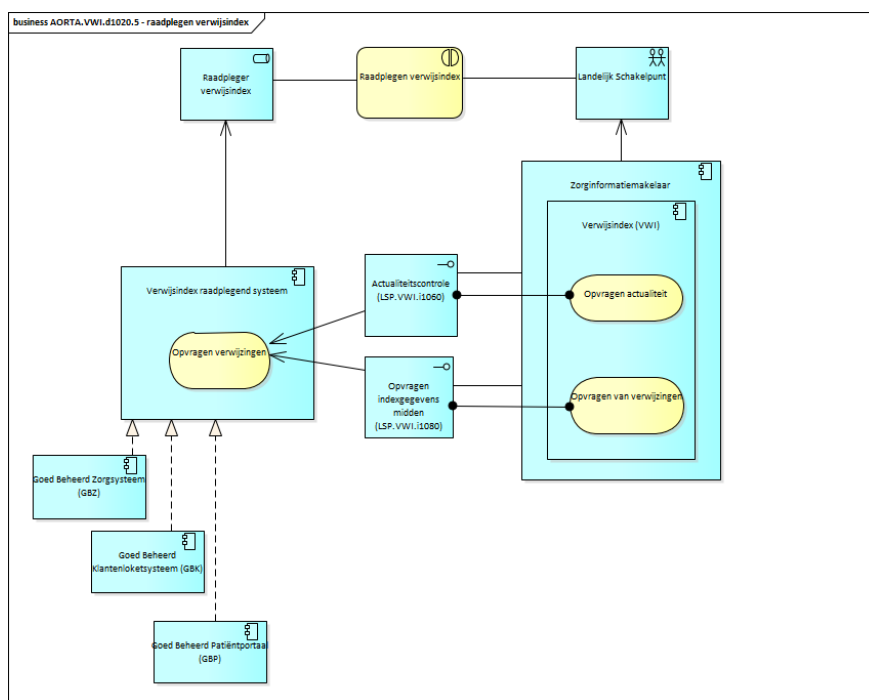


Diagram AORTA.VWI.d1020.3 - informatiesysteeminteracties voor het raadplegen van de verwijzindex

10.2.1 Interface LSP.VWI.i1060: Actualiteitscontrole

Om te bepalen of er nieuwe gegevens beschikbaar zijn gekomen sinds een bepaalde datum kan een GBZ via de service 'Opvragen actualiteit' een actualiteitscontroleverzoek 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 ontkenning terug. Voor het opvragen van de actualiteit wordt het opvragenActualiteit-bericht verstuurd op autorisatie-niveau laag door het Verwijzindex Raadlegendend Systeem.

10.2.2 Interface LSP.VWI.i1080: opvragen index midden

De 'opvragen index' interface biedt de mogelijkheid om een overzicht op te vragen van de verwijzingen 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 verwijzing 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.

10.3 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 verwijzindex 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 verwijzindex. De ZIM stuurt dan automatisch een abonnementsignaal 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 'abonnementssignaal ontvangend systeem'.

De systeemrollen 'abonnerend systeem' en 'abonnementssignaal 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 abonnementssignaleringsafhandelaar 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 abonnementssignaal ontvangend systeem in staat zijn om abonnementssignaal-berichten te verwerken. Hiervoor moet het de volgende interface aanbieden:

- GBX.SGL.i1050: Verwerken abonnementssignaal

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

10.3.1 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.

10.3.2 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.

10.3.3 Interface LSP.ABR.i1030: Opvragen abonnementen

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

10.3.4 Interface GBX.SGL.i1050: Verwerken abonnementssignaal

De interface 'verwerken abonnementssignaal' moet door een abonnementssignaal-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 abonnementssignaal-bericht bevat geen medisch inhoudelijke informatie. Het ontvangen van een abonnementssignaal-bericht kan eventueel aanleiding zijn om vervolgens medisch inhoudelijke informatie via de ZIM op te vragen.

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

10.4 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 applicatieID 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'.

10.5 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 GBP²⁵ 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].

10.5.1 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.

10.5.2 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.

²⁵ 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.

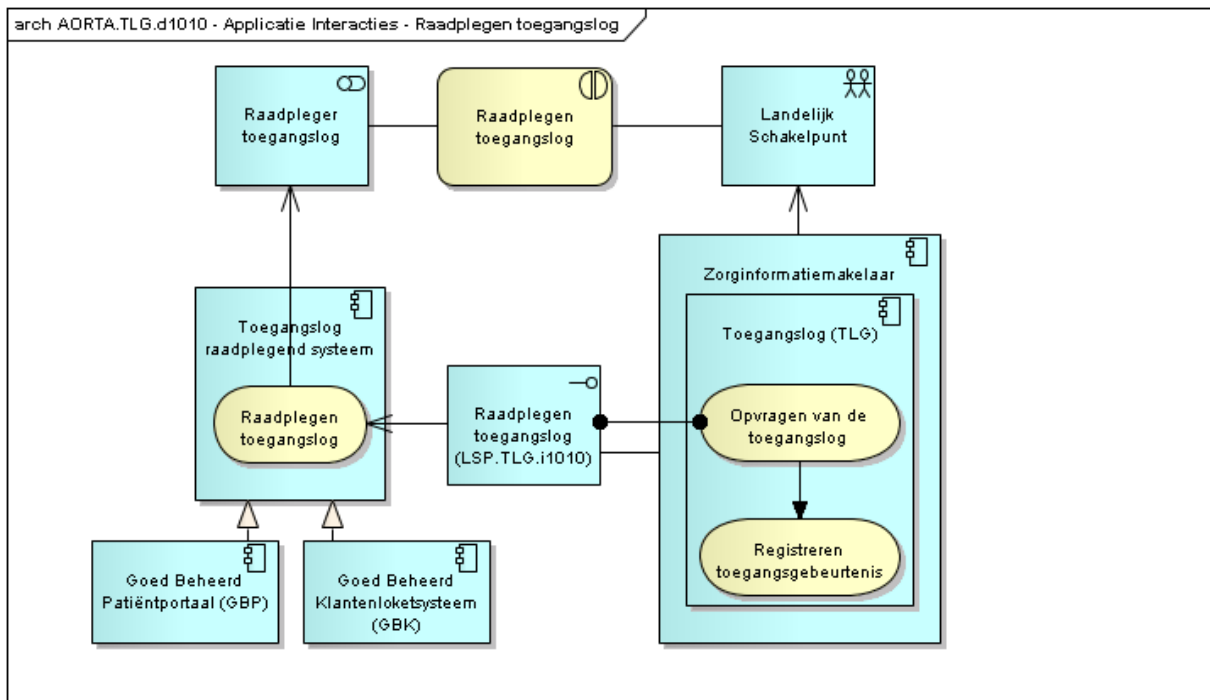


Diagram AORTA.TLG.d1010 - informatiesysteeminteracties voor raadplegen van de toegangslog

10.6 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.

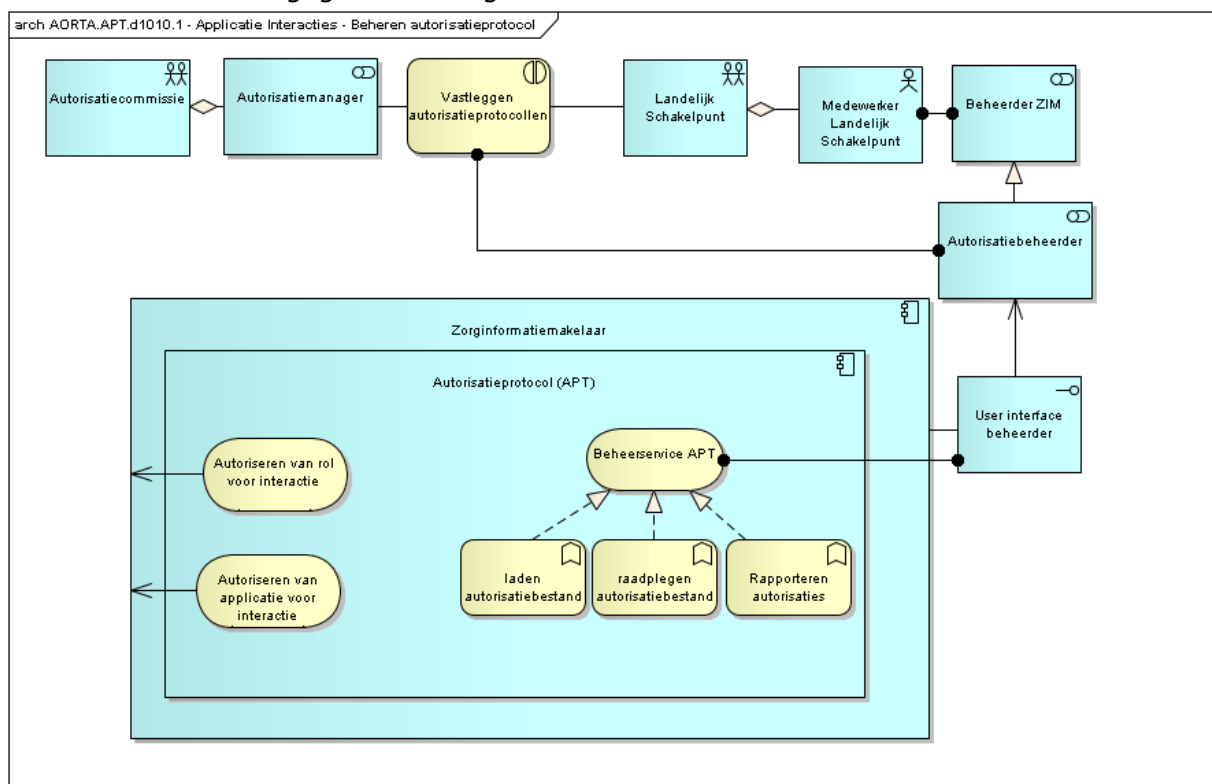


Diagram AORTA.APT.d1010.1 - informatiesysteeminteracties voor het beheer van het autorisatieprotocol

10.6.1 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.

10.6.2 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 gestuurd. 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.

10.6.3 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.

10.6.4 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.

10.6.5 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 subparagraaf 6.2.5).

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

10.7 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 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.

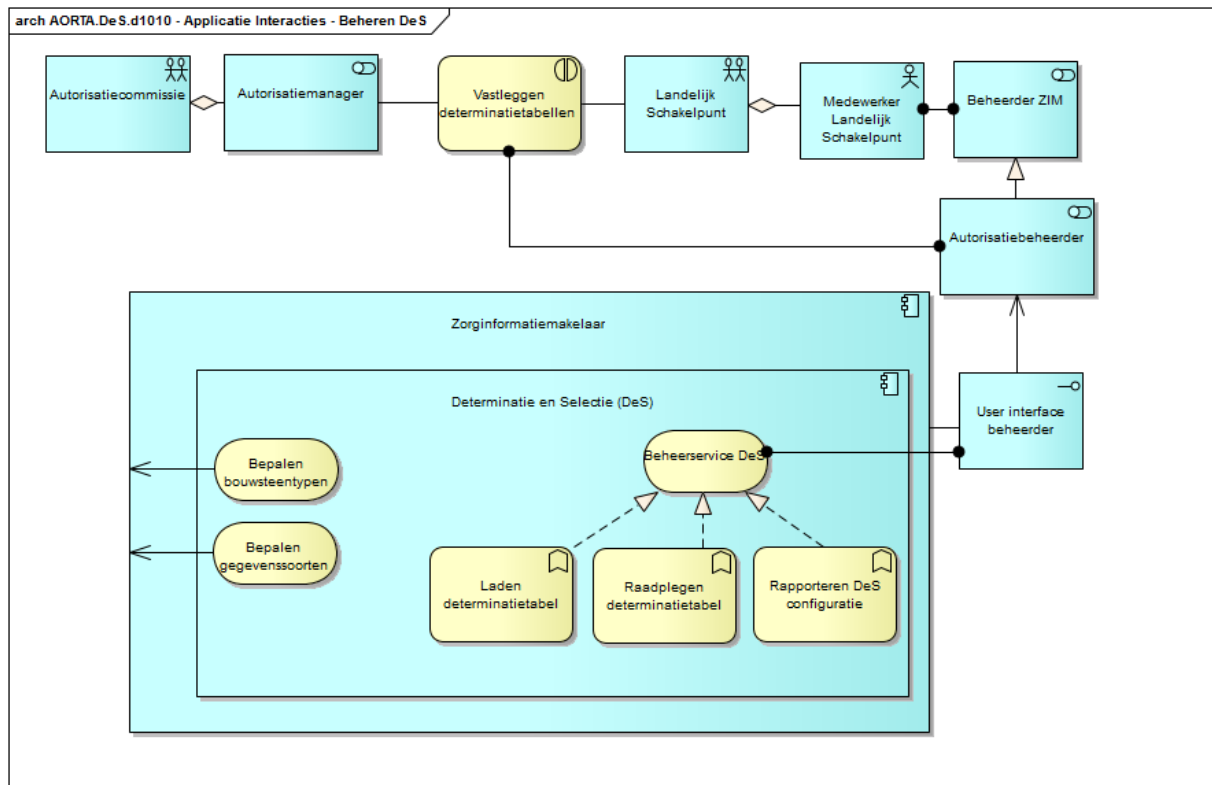


Diagram AORTA.SDS.d1010 - informatiesysteeminteracties voor het beheer van de Selectie en Determinatie Service

10.7.1 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 bouwsteeninstantiaties.

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.

10.7.2 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 verwijsindex.

10.7.3 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 reconstruering van door de ZIM verstuurde opvraagberichten.

10.7.4 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.

10.7.5 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.

10.8 Opvragen/verifiëren BSN en controleren omloopstatus WID

De SBV-Z (zie subparagraaf 6.10.4) 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.

De systeemrol die deze interfaces gebruikt wordt aangeduid als 'patiëntadministrerend systeem'. Omdat binnen AORTA bij communicatie over patiënten een correct BSN nodig is, moet een GBZ beschikken over een 'patiëntadministrerend 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.

11 Applicatie-interacties voor beheer

In dit hoofdstuk wordt uitgewerkt hoe de beheersmatige interacties, zoals besproken in hoofdstuk 7, worden uitgewerkt op informatiesysteemniveau.

11.1 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 URI²⁶ 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)²⁷
- 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 LSP.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.

²⁶ Uniform Resource Identifier, in dit geval het webadres waaronder de applicatie bereikbaar is

²⁷ Deze interface zal langzaam uitgefaseerd worden. Voor XIS-leveranciers zal deze interface geen verplichting meer zijn.

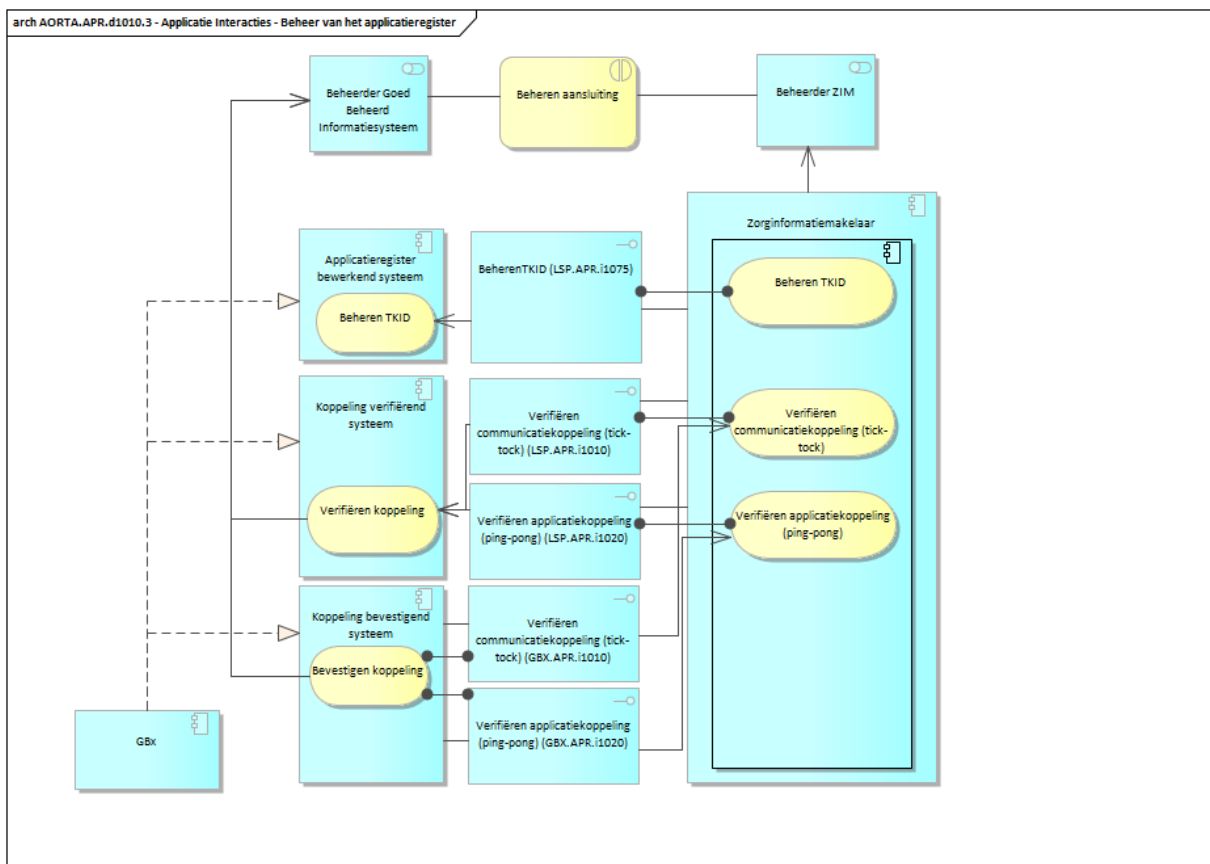


Diagram AORTA.APR.d1010.6 - applicatie-interacties voor het beheer van het applicatieregister

11.1.1 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.

11.1.2 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.

11.1.3 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.

11.1.4 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 beheer 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].

11.2 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 lokale administratie synchroon te houden met de verwijfsindex.

Daarnaast kent de VWI, evenals andere componenten van de ZIM (zie subparagraaf 11.2.2), 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.

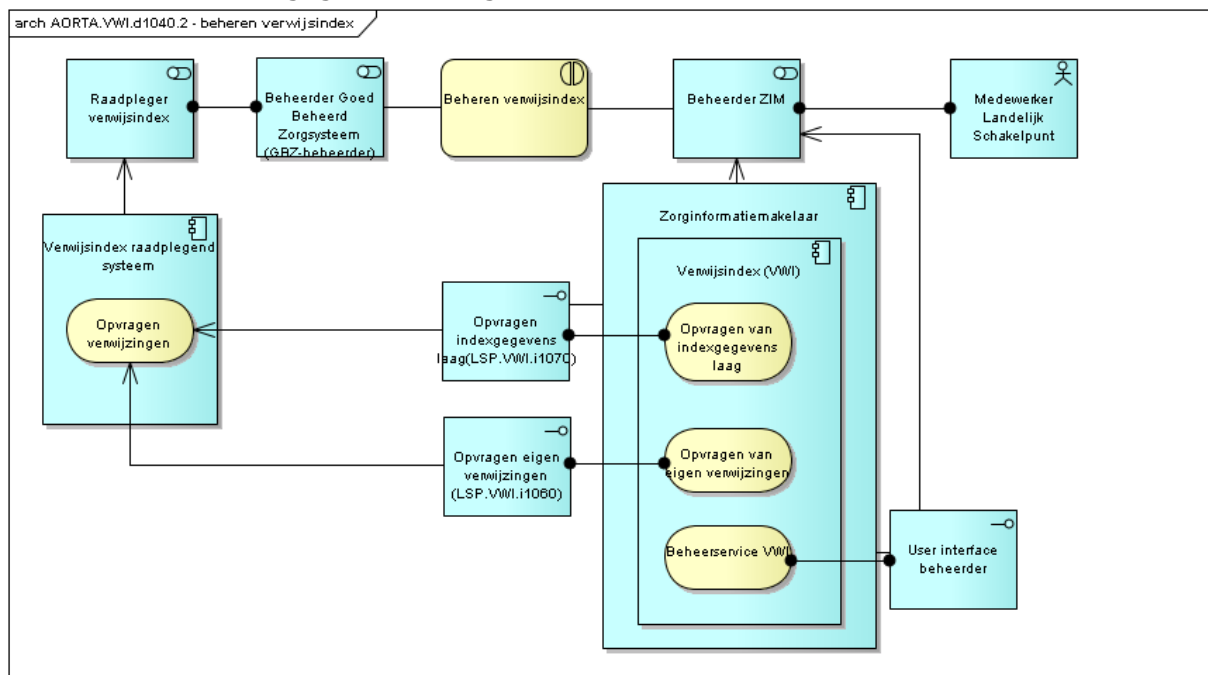


Diagram AORTA.VWI.d1040.2 – beheren verwijfsindex

11.2.1 Beheer van het zorgadresboek

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

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

11.2.2 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 storingsen 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. Foutafhandeling wordt verder besproken in paragraaf 13.3. 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.

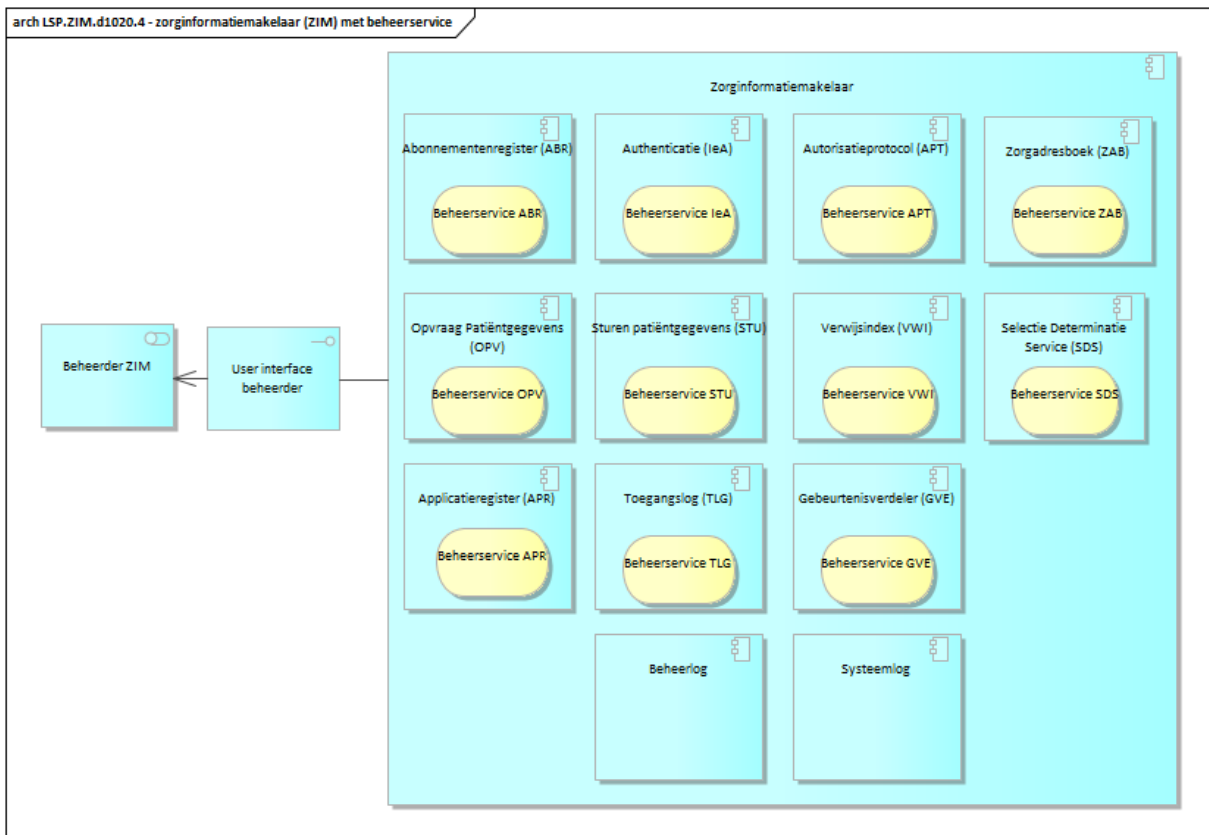


Diagram LSP.ZIM.d1020.4– beheer services, beheerlog en systeemlog

12 Overzicht van systeemrollen

Diagram GBX.ALG.d1010.4 geeft een samenvattend overzicht van de systeemrollen die zijn geïntroduceerd in de hoofdstukken 9, 10 en 11. 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.

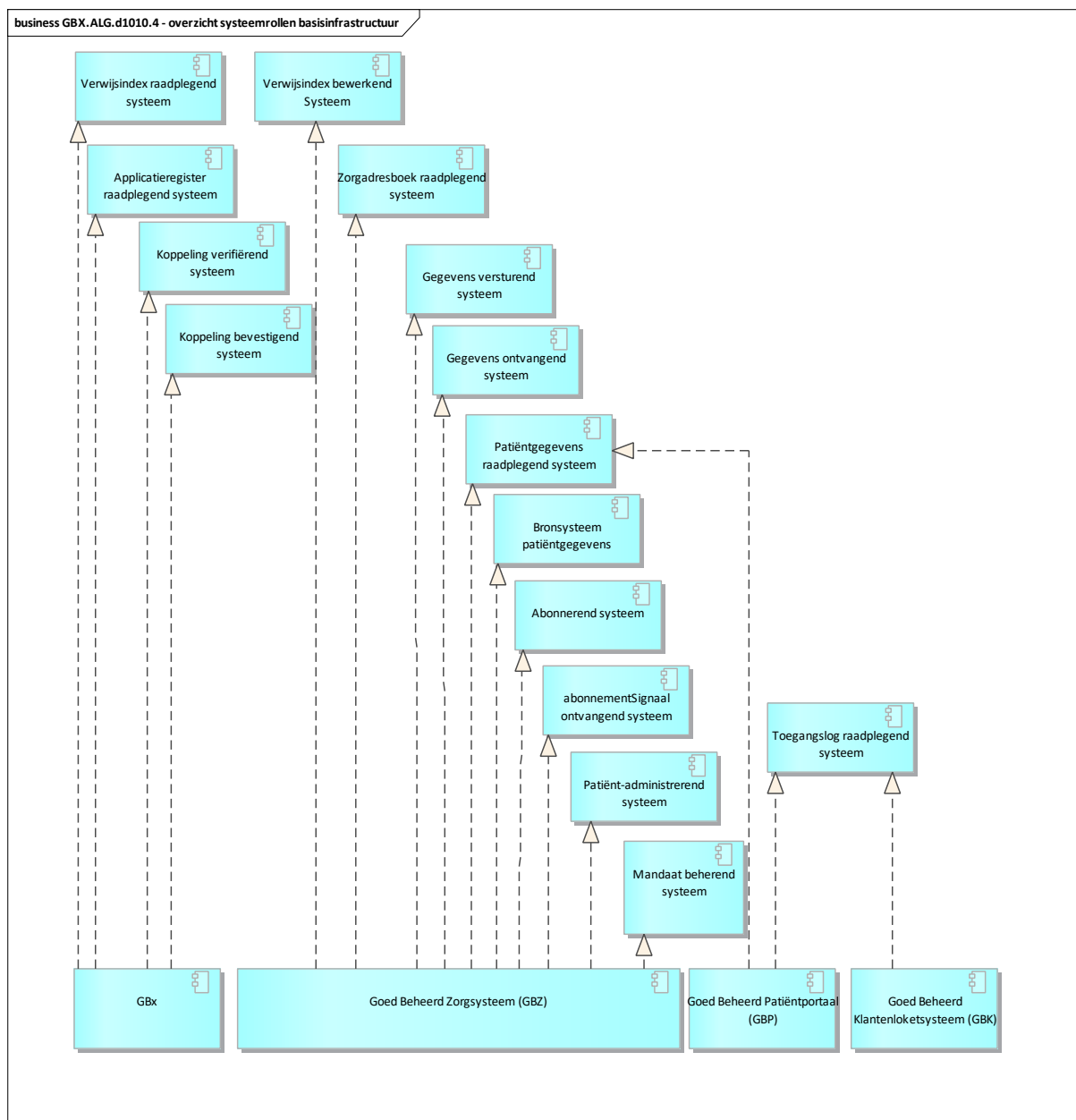


Diagram GBX.ALG.d1010.4 – overzicht systeemrollen basisinfrastructuur AORTA

13 Berichtafhandeling

13.1 Protocollen

De applicatie-interacties die zijn beschreven in hoofdstuk 7 worden gerealiseerd door uitwisseling van berichten tussen de applicaties. Voor uitwisseling van medische gegevens wordt binnen AORTA gebruik gemaakt van de internationale HL7v3 standaard. Voor het transport van HL7v3 berichten/documenten over internetprotocollen zijn aanvullende keuzen nodig ten aanzien van transport- en beveiligingsprotocollen.

Hiertoe 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.

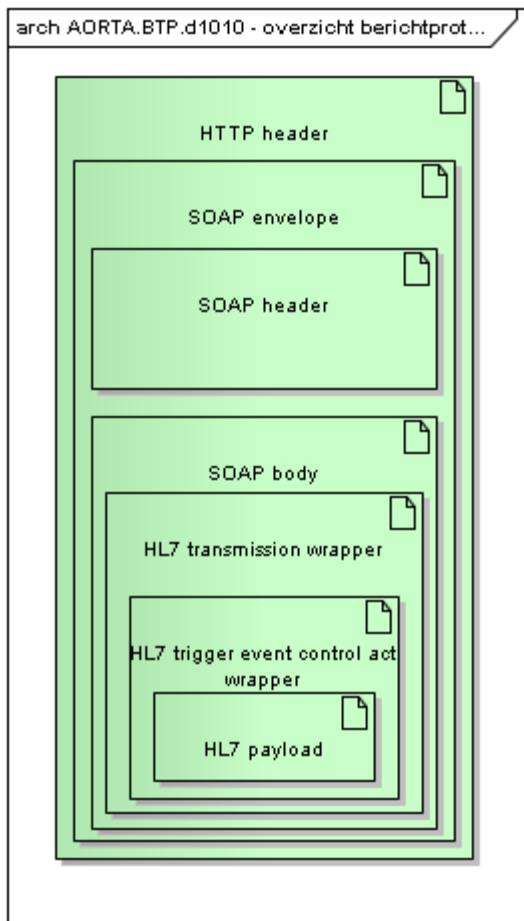


Diagram AORTA.BTP.d1010 - overzicht berichtprotocol-`stack`

Diagram AORTA.BTP.d1010 geeft een overzicht van de protocollen die gebruikt worden voor berichtuitwisseling op de applicatielaag. Tussen applicatielaag en transportlaag (van het TCP/IP model) wordt gebruik gemaakt van Transport Layer Security (TLS).²⁸

²⁸ Het UZI-registerabonneenummer (URA) wordt afgeleid uit het servercertificaat van het initiërend systeem tijdens het tot stand komen van de TLS-handshake en wordt vervolgens op het niveau van de applicatielaag gebruikt (zie verder 13.2.3).

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')²⁹; 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.

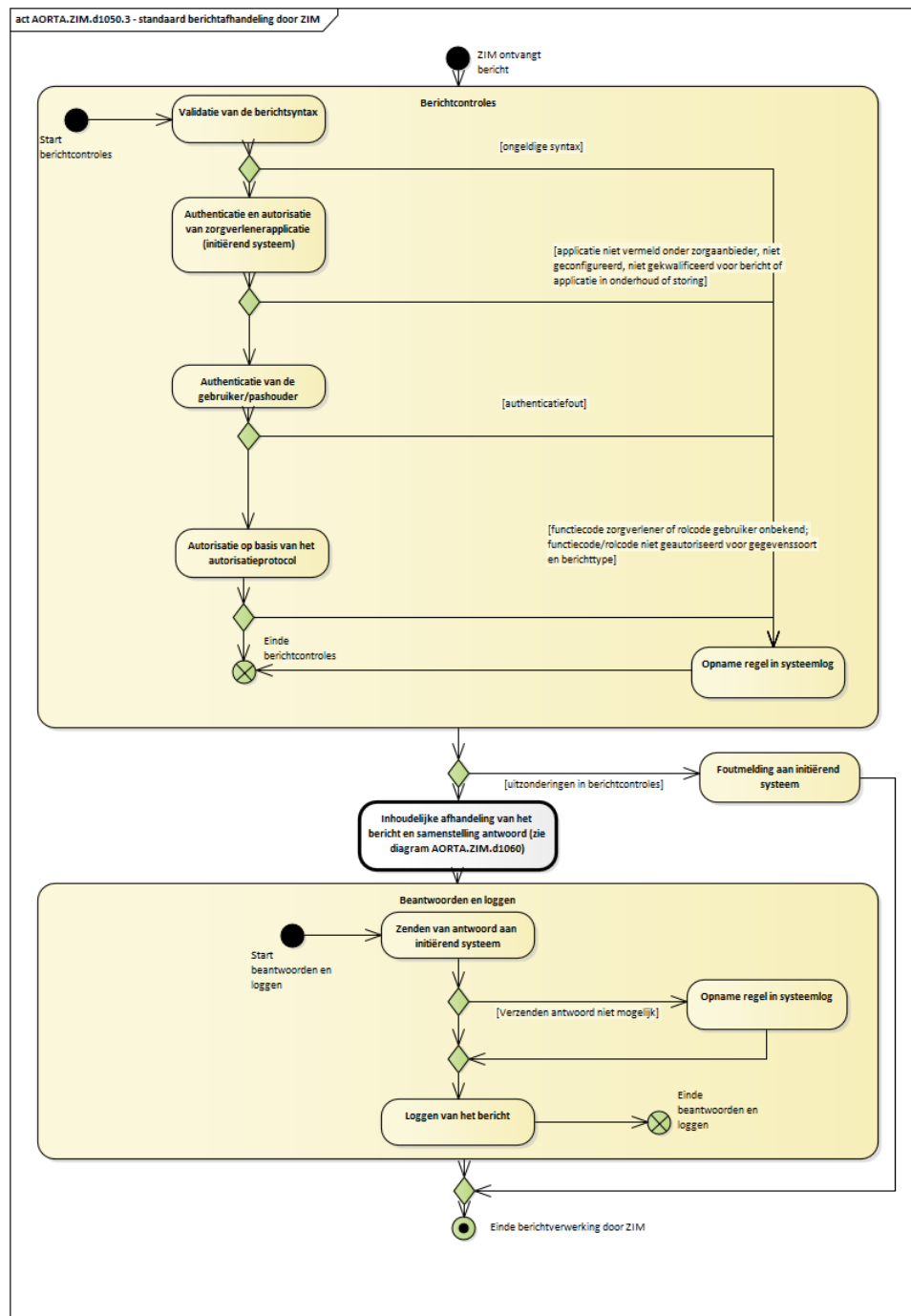
Diagram AORTA.BTP.d1010 gaat niet in op de gebruikte SOAP-headerprotocollen. Hiervoor wordt verwezen naar de implementatiehandleiding [IH Transport].

Meer gedetailleerde informatie over de protocollen en de samenstelling van HL7-berichten is opgenomen in de implementatiehandleidingen [IH Transport] en [Decor]. Voor protocollen onder de applicatielaag wordt verwezen naar subparagraaf 14.1.2.

²⁹ Auteur en eindverantwoordelijke kunnen dezelfde personen zijn.

13.2 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.d1050.2.



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'.

13.2.1 Validatie van de berichtsyntax

De ZIM controleert (een gedeelte van) het bericht op geldigheid ten opzichte van XML schema's³⁰. 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 paragraaf 13.1) van het bericht.

13.2.2 Authenticatie en autorisatie van de zorgverlenerapplicatie

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 servercertificaat³¹. 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.³²

13.2.3 Authenticatie van de gebruiker / pashouder

Bij uitwisseling van gegevens met of via de ZIM moet de authenticiteit van de gebruiker van de applicatie die gegevens uitwisselt met voldoende waarborg worden vastgesteld. Hiertoe heeft de gebruiker een vertrouwensmiddel aan de hand waarvan de gebruiker kan worden geauthenticeerd (zie paragraaf 6.10). Een zorgverlener maakt hiertoe gebruik van een UZI-pas. Een klantenloketmedewerker maakt gebruik van een PKIOverheidpas. De patiënt kan zich authenticeren door middel van DigiD.

³⁰ Deze schema's zijn gebaseerd op normatieve beschrijvingen in implementatiehandleidingen.

³¹ 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.

³² Berichten voor beheer van het applicatieregister (zie hoofdstuk 11.1) zijn hierop een uitzondering, indien hiermee de applicatie weer actief wordt gemeld na een onderhoud of storing.

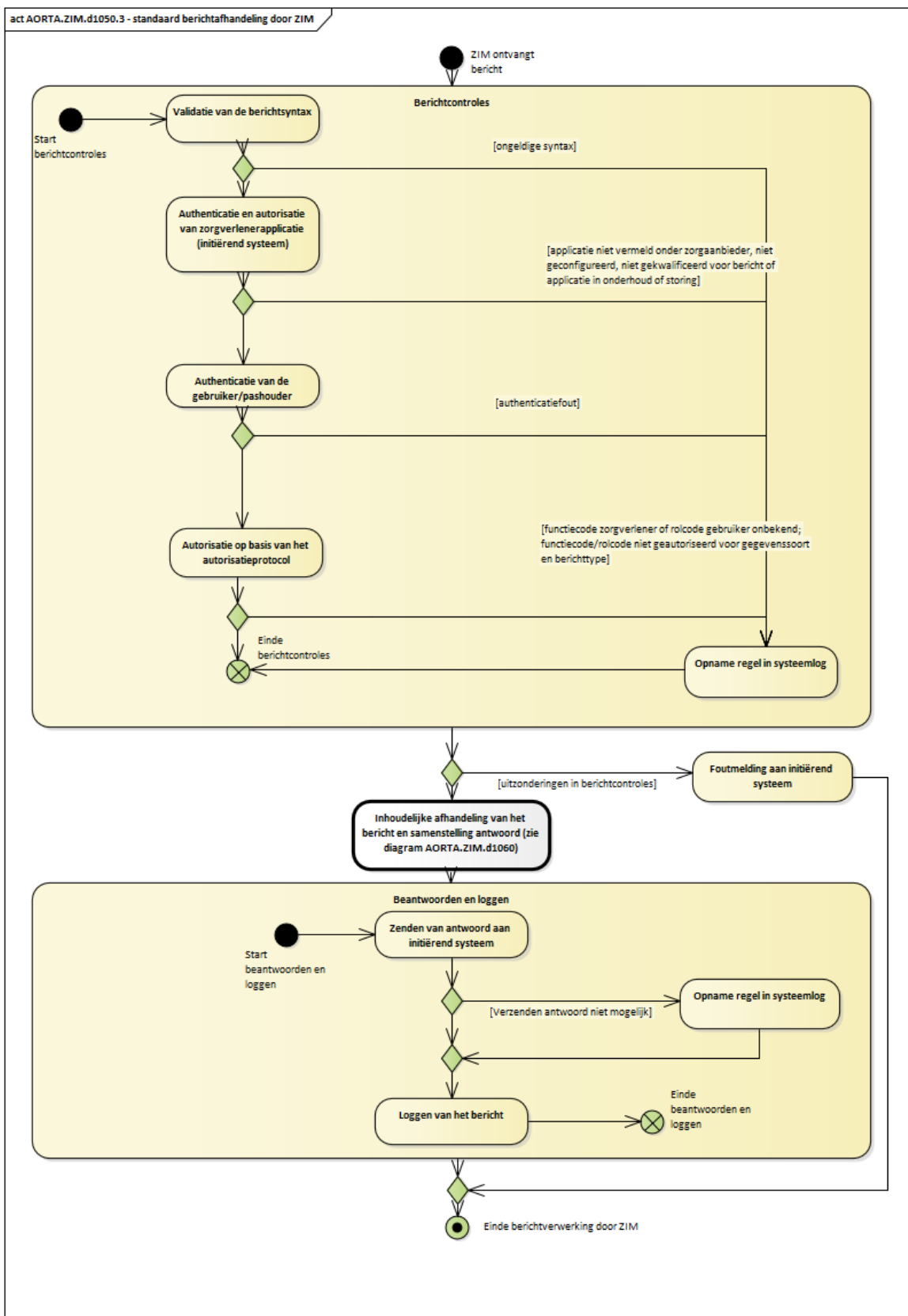


Diagram AORTA.ZIM.d1050.2 - standaard berichtafhandeling door de ZIM

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 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 TRANS] 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 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 MAN] 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 INSCHRIJF] 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 opvraagmechanisme wordt gebruikt. In tabel Tabel 1 zijn de verschillende voorkomens van tokens i.c.m. een specifieke opvraag beschreven.

Bij het uitwisselen van berichten met de ZIM zijn twee vertrouwensniveaus mogelijk, 'laag' en 'midden'³³. Het vereiste vertrouwensniveau wordt per berichttype vastgesteld.

- Niveau 'laag' houdt in dat alleen de organisatie van de afzender wordt vastgesteld en niet de persoonlijke identiteit. De gebruiker heeft voor niveau laag in principe geen pas nodig, omdat de organisatie uit het servercertificaat van het GBx kan worden afgeleid.
- Niveau 'midden'³⁴ vereist authenticatie van de individuele afzender en vereist dus dat een token(s) (afhankelijk van de situatie zoals is opgenomen in Tabel 1) in het bericht aanwezig is. Dit niveau is minimaal vereist voor medisch inhoudelijke gegevens.

Zie voor een verdere discussie van dit aspect het [Ontw Authenticatie].

Tabel 1: Gebruik van de diverse tokens

Opvraag	Vertrouwensniveau	Mandaat	Tokens
---------	-------------------	---------	--------

³³ 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.

³⁴ 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 en het gebruik van twee-factor authenticatie geldt in feite dat bij authenticatie op basis van een UZI-pas de identiteit van de eindgebruiker met hoge betrouwbaarheid wordt vastgesteld.

Generieke opvraag	Midden (of hoger)		T of P
Generieke opvraag	Midden (of hoger)	X	M en T
Conditionele opvraag	n.v.t. ³⁵	X	M, T en I

Voor tokens die zijn getekend met een persoonlijke UZI- of PKIO-pas 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.³⁶

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- pas³⁷ en het servercertificaat van de ZIM) wordt niet ondersteund.

13.2.4 Autorisatie op basis van het autorisatieprotocol

Het autorisatieprotocol controleert of de zorgverlenerfunctie 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 zorgverlenerfunctie geautoriseerd is voor het verzenden van een specifieke interactie.

In het geval van patiënttoegang of toegang van een klantenloketmedewerker wordt de combinatie van berichtuitwisseling en rolcodes gecontroleerd.

Zie voor een verdere discussie van autorisatie op basis van het autorisatieprotocol het [Ontw APT].

13.2.5 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 (zie de bespreking in hoofdstuk 7 voor de mogelijke berichten). 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).

³⁵ 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.

³⁶ 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.

³⁷ 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 werkstation van de gebruiker.

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.

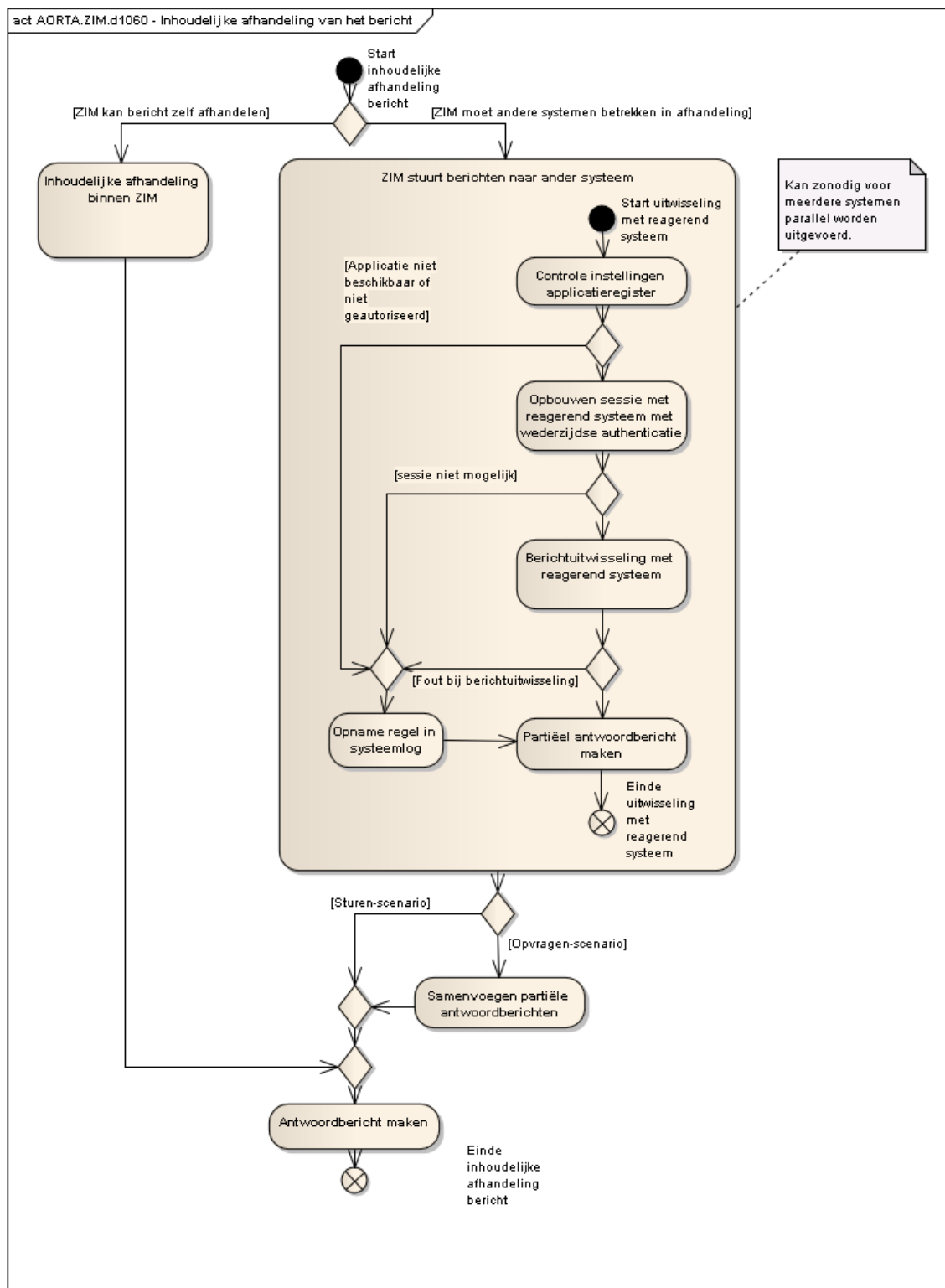


Diagram AORTA.ZIM.d1060 - generieke aspecten van inhoudelijke afhandeling bericht door ZIM

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).

13.2.6 Loggen van het bericht

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.

13.3 Foutafhandeling

In de berichtafhandeling zoals beschreven in paragraaf 13.2 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-niveau³⁸ wordt deze fout opgenomen in het antwoord aan het

³⁸ Er is een lijst van HL7-v3 meldingscodes gedefinieerd die is opgenomen in de foutentabel.

initiërend systeem.³⁹ 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 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.

13.4 Afhandelen van berichtversies

De specificaties van de AORTA-infrastructuur en bijbehorende zorgtoepassingen vallen onder versiebeheerprocedures⁴⁰; 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 paragraaf 6.4), 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].

³⁹ Het initiërend systeem is vrij om de ontvangen meldcode te verrijken met een zelfgekozen tekst voor presentatie aan de eindgebruiker.

⁴⁰ Een beschrijving van deze versiebeheerprocedures valt buiten de reikwijdte van dit architectuurdokument.

14 Infrastructurele aspecten

14.1 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 hoofdstuk 6 logisch worden gekoppeld om berichtenuitwisseling tussen deze systemen te faciliteren.

Voor de duidelijkheid is de figuur opgedeeld in lagen.

14.1.1 Initiërende systemen

De bovenste laag toont de informatiesystemen die een interactie via AORTA kunnen initiëren. Zoals besproken in de systeeminteracties in hoofdstuk 7 zijn dit GBZ'en, GBP'en het GBK en de DVZA samen aangeduid als GBx.

14.1.2 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.

14.1.2.1 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.⁴¹

14.1.2.2 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.

14.1.2.3 Domein aorta-zorg.nl

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

⁴¹ 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.

overigens beperkt tot de door het LSP toegekende reeks, zie hieronder bij 'IP-adresreeksen'.

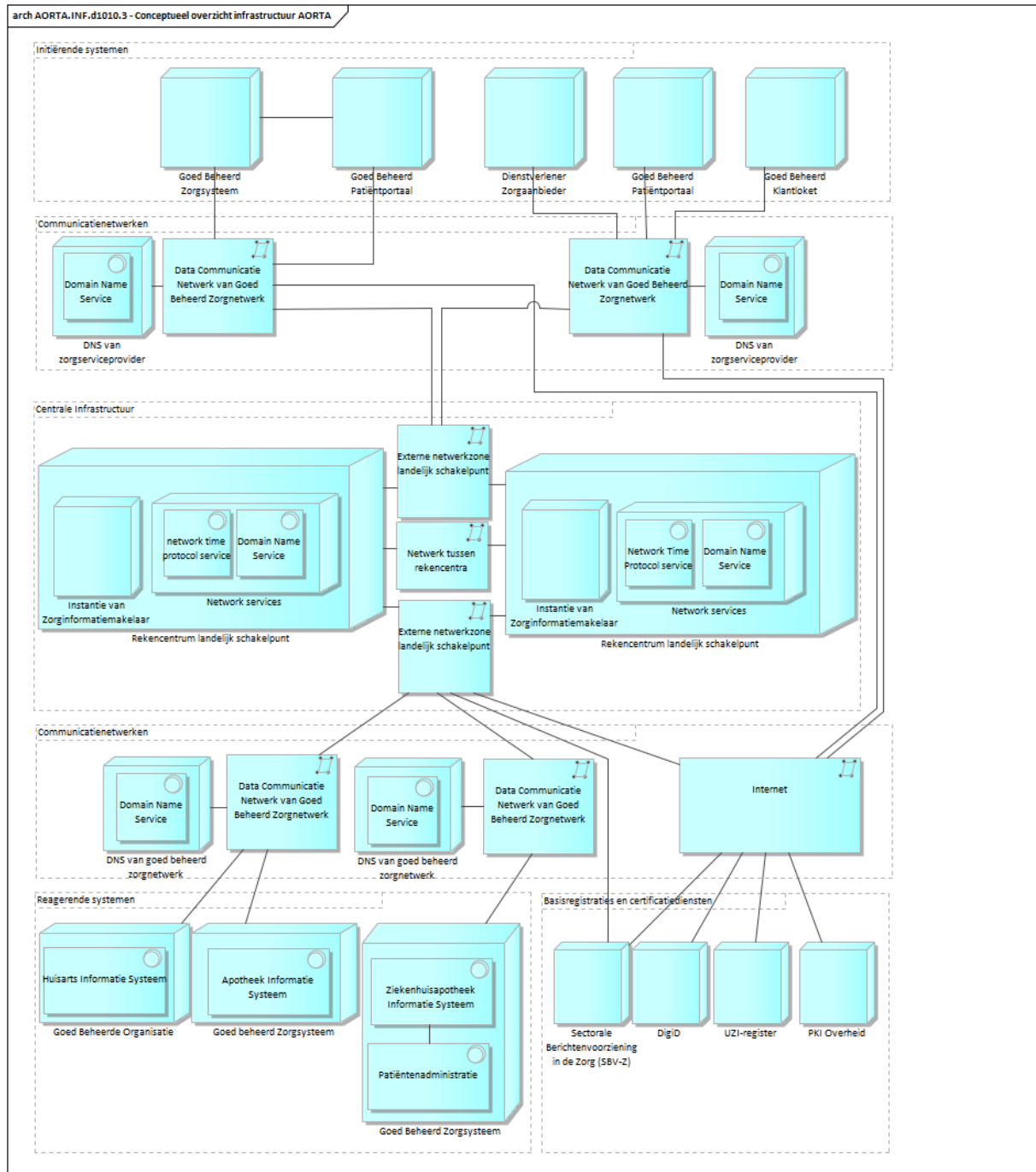


Diagram AORTA.INF.d1010.4: conceptueel overzicht van de AORTA infrastructuur

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'. De FQDN wordt tevens vastgelegd als URI van het GBx in het applicatieregister van de ZIM.

14.1.2.4 IP-adresreeksen

Een GBx dat via het DCN van 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 locale 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).

14.1.2.5 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 6.10.4) worden via het internet geleverd.
- GBZ'en moeten in staat zijn om de digitale certificaten op de UZI-passen 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.⁴²

14.1.2.6 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 paragraaf 13.1). 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.

⁴² 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.

14.1.3 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.⁴³
- 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.

14.1.4 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.

14.1.5 Reagerende systemen

Diverse XIS-systemen (huisartsinformatiesystemen, apotheekinformatiesystemen, ziekenhuisapotheekinformatiesystemen, 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 ziekenhuisapotheekinformatiesysteem en patiëntadministratiesysteem.

Een GBZ kan overigens in de ene interactie het initiërend systeem zijn en in een andere interactie het reagerend systeem.

14.1.6 Basisregistraties en certificatediensten

Onder basisregistraties en certificatediensten vallen de infrastructuren van UZI-register (zie 6.10.1), PKIoverheid (zie 6.10.2), DigiD (zie 6.10.3) en SBV-Z (zie 6.10.4). Deze zijn beschikbaar via het internet voor zowel de ZIM (met uitzondering van het SBV-Z) als voor GBx'en. UZI-register en PKIoverheid zijn voor GBx'en adresseerbaar via het internet óf via de netwerkinfrastructuur van de ZIM.

⁴³ 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.

14.2 Operationele aspecten

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.

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.

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.

15 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 fases 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 (zie paragraaf 6.4). 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 (zie paragraaf 6.4. Ook voor GBP en GBK gelden dergelijke eisen.

Een GBx moet bij aansluiting worden geregistreerd in het applicatieregister van de ZIM (zie subparagraaf 6.2.5). 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, afkomstig van UZI-register of, in het geval van GBP, GBK en niet UZI-abonnee, PKIoverheid (zie paragraaf 6.10). De gebruikers van een GBZ moeten beschikken over UZI-passen (voor inhoudelijke interacties UZI-passen op naam), voor het GBK moeten gebruikers beschikken over PKIO-passen. 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 (zie subparagraaf 13.2.3).

Bij het uitwisselen van patiëntgegevens worden aan het GBZ onder meer eisen gesteld ten aanzien van (zie paragraaf 6.4):

- 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 (zie ook 13.2):

- de geldigheid van de berichtssyntax 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.

Bijlage A 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 Blarckom 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	8.1.0.0
[Decor]	http://decor.nictiz.nl/pub/vzvz/	
[IH Transport]	Implementatiehandleiding berichttransport	8.1.0.0
[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	8.1.0.0
[Ontw APT]	Ontwerp autorisatieprotocol	8.1.0.0
[Ontw Authenticatie]	Ontwerp authenticatie	8.1.0.0
[Ontw OPV]	Ontwerp opvragen patiëntgegevens	8.1.0.0
[Ontw Sgl ABR]	Ontwerp abonnementenregister	8.1.0.0
[Ontw Sgl GBV]	Ontwerp gebeurtenisverwerking	8.1.0.0
[Ontw STU]	Ontwerp versturen patiëntgegevens	8.1.0.0
[Ontw TLG]	Ontwerp toegangslog	8.1.0.0
[Ontw VWI]	Ontwerp verwijsindex	8.1.0.0
[PvE ZIM]	Programma van eisen zorginformatiemakelaar	8.1.0.0
[PvE GBx Rollen]	Programma van eisen infrastructurele systeemrollen	8.1.0.0
[IH TRANS]	Implementatiehandleiding Berichtauthenticatie Transactietoken	8.1.0.0
[IH MAN]	Implementatiehandleiding Berichtauthenticatie Mandaattoken	8.1.0.0
[IH INSCHRIJF]	Implementatiehandleiding Berichtauthenticatie Inschrijftoken	8.1.0.0
[IH PKIO]	Implementatiehandleiding Berichtauthenticatie PKIO	8.1.0.0
[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