Ontwerp Autorisatieprotocol

Datum: 1 mei 2022

Publicatie: V8.3.0.0

Inhoudsopgave

1 Inleiding

1.1 Doel en scope

Dit document beschrijft de werking van het autorisatieprotocol (APT) als component van de ZIM.

De autorisatieprotocolcomponent heeft tot doel om een uitspraak te doen over de bevoegdheid van een zorgpartij, met een bepaalde rol, om een bepaalde interactie uit te voeren. Met interactie wordt verstaan: een elektronische uitwisseling/raadpleging van (patiënt)gegevens van een bepaalde klasse en soort, via het LSP.

1.2 Doelgroep voor dit document

De doelgroep van dit document is primair de leveranciers van de ZIM componenten.

Daarnaast is het een naslagwerk voor de leveranciers van GBX componenten en software.

1.3 Documenthistorie

Versie	Datum	Omschrijving
6.10.0.0	12-okt-2011	Initiële versie
6.12.1.0	12-okt-2012	Ongewijzigde versie als onderdeel van AORTA_Infrastructuur v6·11
8.0.1.0	15-mei-2017	RfC 52477: Uitwisseling op basis van bouwstenen.
8.0.1.0	15-mei-2017	RfC 76144: Autorisatieprofiel verwijderen
8.1.0.0	1-juli-2018	Opgenomen in publicatie 8.1.0.0
8.2.0.0	6-aug-2020	INI-7445: Controle conformance geen onderdeel APT
8.3.0.0	1-mei-2022	Opgenomen in publicatie 8.3.0.0

2 Kaders en uitgangspunten

2.1 Externe normen en kaders

De wet Geneeskundige Behandel Overeenkomst (WGBO) schrijft voor dat een zorgverlener verantwoordelijk is voor patiëntgegevens. Wanneer een andere zorgverlener patiëntgegevens wil opvragen, zal de zorgverlener strikt genomen voor individuele gevallen persoonlijk moeten bepalen:

- heeft de andere zorgverlener een behandelrelatie?
- is de andere zorgverlener rechtstreeks betrokken?
- is er toestemming of bezwaar van de patiënt/cliënt?
- is het noodzakelijk de patiëntgegevens in te zien?
- is de privacy van een derde in het geding?

Het is voor de zorgverlener ondoenlijk om al deze aspecten bij iedere individuele elektronische uitwisseling van gegevens te controleren. Dit heeft geleid tot overkoepelende afspraken, een protocol, waarin zorgverleners elkaar vertrouwen voor gegevensuitwisseling.

Het autorisatieprotocol dient als kader voor het ontwerp van deze autorisatieprotocolcomponent (APT). In dit protocol staat welke soorten patiëntgegevens een zorgverlener, op grond van zijn functie, nodig kan hebben of aan anderen mag verstrekken voor een adequate behandeling. Het autorisatieprotocol is geformuleerd in overleg met beroepsverenigingen van zorgverleners en met belangenverenigingen van patiënten/cliënten. Samenwerkende zorgverleners die willen aansluiten op het landelijk schakelpunt moeten akkoord gaan met het autorisatieprotocol.

Het kan enige tijd duren voordat de koepelverenigingen volledige overeenstemming bereiken over de invulling van het autorisatieprotocol. Het protocol wordt daarom incrementeel ingevuld naar de behoefte van de landelijke toepassingen, te beginnen met Medicatiegegevens (Mg) en Huisartswaarneemgegevens (Hwg).

2.2 Relatie met AORTA-principes en –beslissingen

De volgende architectuurbeslissing ligt ten grondslag aan het ontwerp van het autorisatieprotocol.

- ZIM.APT.p2000 Er komt één centraal beheerd autorisatieprotocol voor landelijke uitwisseling van patiëntgegevens via het landelijk schakelpunt.

3 Context van Autorisatieprotocol component

Het volgende contextdiagram ZIM.APT.d2000 toont de autorisatieprotocolcomponent.

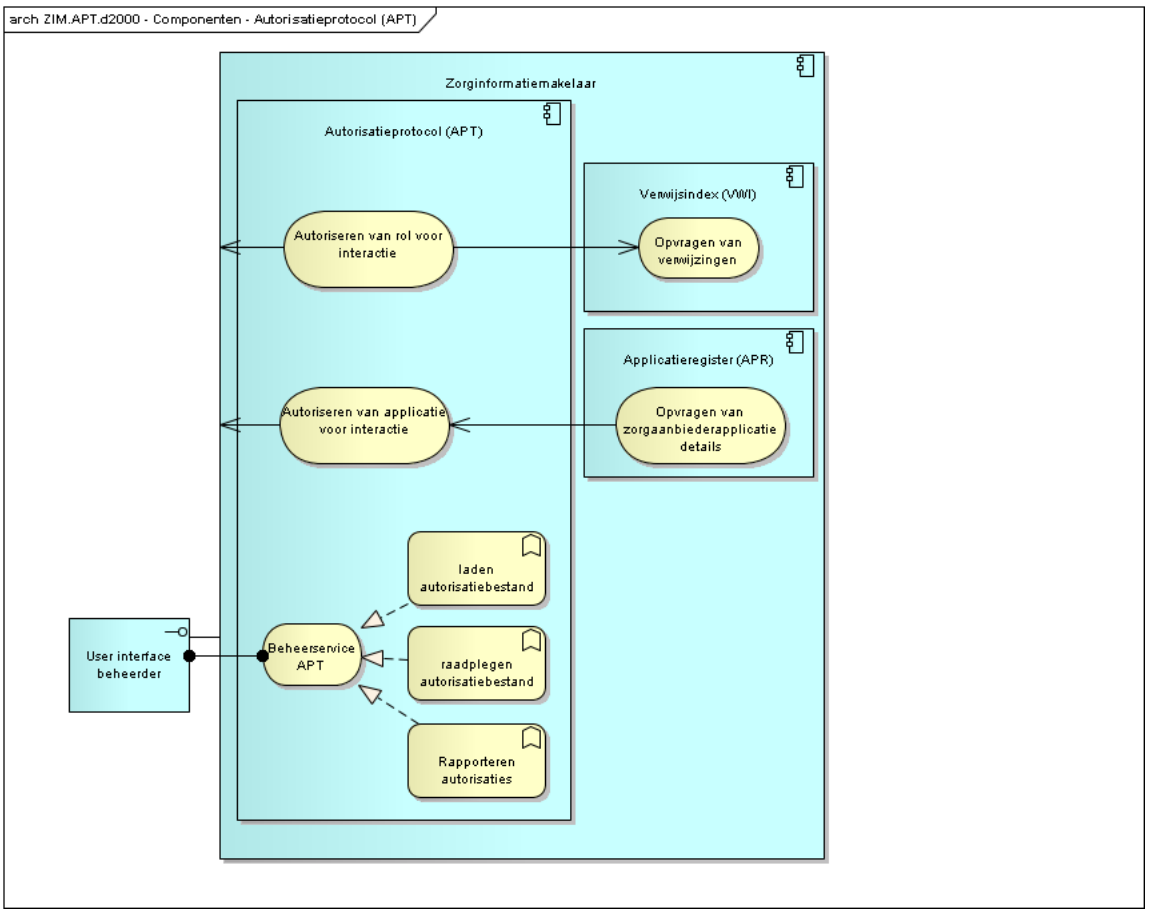

Diagram ZIM.APT.d2000 Context van het autorisatieprotocol

De autorisatieprotocolcomponent (APT) is onderdeel van de ZIM component.

De APT is betrokken bij de afhandeling van elk bericht dat bij de ZIM binnenkomt vanuit een aangesloten systeem. De ZIM spreekt de APT aan als onderdeel van de standaard berichtenafhandeling zoals beschreven in de AORTA Architectuur [Arch AORTA].

Alvorens een ontvangen bericht door de ZIM wordt geautoriseerd, bepaalt APT of de applicatie, die het bericht heeft verzonden, geoorloofd is om de betreffende interactie te versturen. Dit gebeurt middels de dienst '*Autoriseren van de applicatie voor interactie*'. Deze dienst spreekt de *applicatieregister* component aan via '*Opvragen van zorgaanbiederapplicatie details*' om te controleren of de HL7 interactie, door betreffende applicatie verzonden had mogen worden [zie de conformancetabel in het [Ontw APR]].[1]

[1] In de praktijk is dit niet als zodanig geïmplementeerd. De APR zal rechtstreeks benaderd worden om te bepalen of een applicatie geautoriseerd is voor een bepaalde interactie. De conformances van een applicatie worden rechtstreeks uit het

De ZIM spreekt de dienst 'Autoriseren van rol voor interactie' aan om de autorisatiestatus van een bericht te bepalen.

Dit gebeurt alleen in de gevallen waarbij een GBx de interactie met de ZIM initieert.Verzending door de ZIM en berichten van een reagerende GBX worden niet tegen de APT gehouden.

Een oordeel over autorisatie geeft de autorisatie component af aan de ZIM met een autorisatieresultaat.

Daarnaast wordt de dienst *'Autoriseren rol voor interactie'* ook benut door de VWI-component om na een opvraag van de verwijsindex te kunnen bepalen welke indexregels moeten worden gefilterd. Dit geschiedt door voor iedere gegevenssoort die voorkomt in de op te leveren indexregels te controleren of de opvrager op basis van zijn rol geautoriseerd is tot inzage.

Indien de interactie wordt aangegaan binnen een *context* dan wordt de context eerst ontleedt in onderliggende bouwsteentypen en om vervolgens bijbehorende gegevenssoorten te bepalen Dit proces wordt uitgevoerd door de Determinatie en Selectie (DeS) component, zie [Ontw DeS].

De APT biedt een autorisatiebeheerder applicatiediensten voor het raadplegen en aanpassen van het autorisatieprotocol. Deze component biedt een user interface voor de autorisatiebeheerder.

Systeemactoren:

De enige 'gebruiker' van de APT is de ZIM zelf. De ZIM kan gezien worden als de systeemactor voor dit component. Binnen de ZIM zijn er twee componenten die gebruik maken van APT:

- De Orchestratieservice maakt gebruik van de autorisatieprotocolcomponent door na binnenkomst van elk bericht, de autorisatie te raadplegen.
- De Verwijsindexcomponent maakt gebruik van de autorisatieprotocol component wanneer iemand de inhoud van de verwijsindex opvraagt.

Gebruikersactoren:

De autorisatiebeheerder is de enige gebruikersactor op de APT. Door middel van een gebruikersinterface wordt de *'Beheerservice'* van de APT aangesproken.

APR gehaald en gaat niet via de APT. In de toekomst zal dit mogelijk wel via de APT moeten lopen. Vooralsnog blijft deze uitwerking ongewijzigd in het Ontwerp APT staan.

4 Interfaces (koppelvlakken)

4.1 Systeeminterfaces

De APT hanteert geen externe interface voor applicatiediensten buiten de ZIM.

In dit hoofdstuk worden alleen de interne interfaces van de APT besproken:

Tussen ZIM en APT

- Autoriseren van rol voor interactie met eventuele gegevenssoort of context.

Tussen VWI en APT

- Autoriseren van rol voor interactie 'opvragenindex' met gegevenssoort.

Tussen APT en APR

- Autoriseren van applicatie voor interactie.

4.1.1 Interne interface Autoriseren rol voor interactie

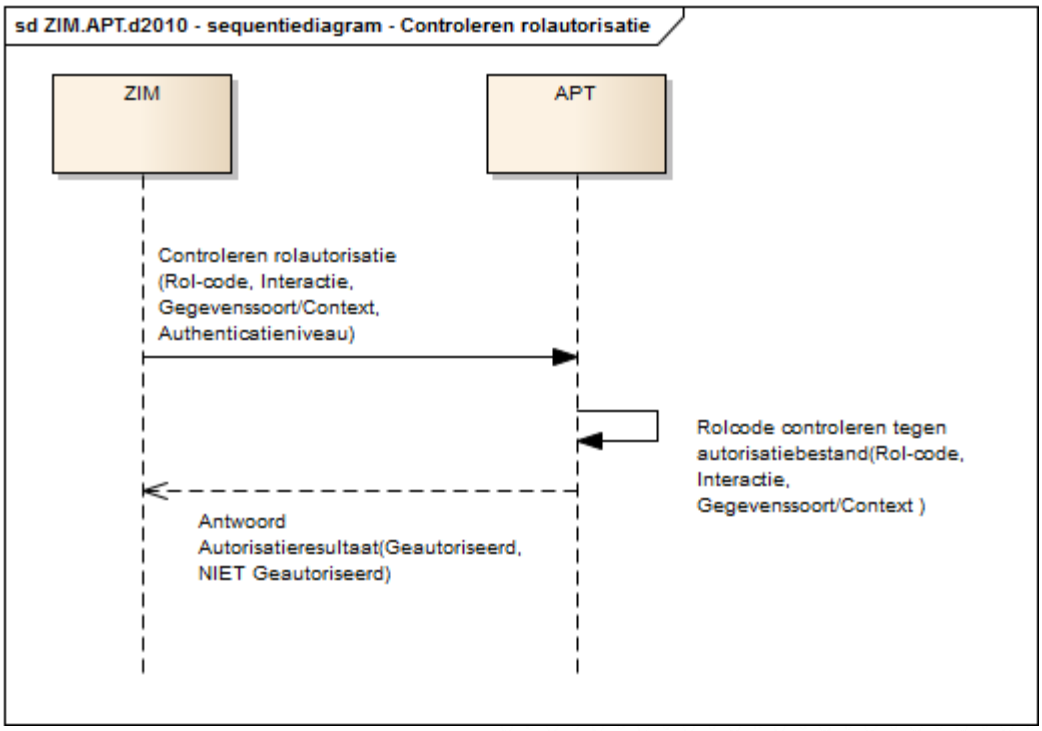

Diagram ZIM.APT.d2010 Sequence diagram van autoriseren rol voor interactie

(Noot: deze interface wordt ook gebruikt door de VWI-component bij de autorisatie van rol voor interactie 'opvragenindex' met gegevenssoort)

Parameters voor de autorisatiebepaling

Tabel ZIM.APT.t2000 Autoriseren rol voor interactie attributen

Attribuut	Definitie	Herkomst	Additionele informatie

Rolcode (1)	De rol van de bedrijfsactor die verantwoordelijk is voor de interactie	Bericht	Deze rol kan zijn:
			• zorgverlener, met:
			  ○ beroepstitel
			  ○ specialisme
			• burger
			• wettelijke vertegenwoordigers van burgers

Interactie (1)	De identificatie van de interactie die men wil uitvoeren	Bericht	
Gegevenssoort (0..1)	De gegevenssoort waarop de interactie van toepassing is.	Bericht	Slechts enkele berichttypes bevatten een gegevenssoort
Context (0..1)	De context waarbinnen de interactie is aangegaan.	Bericht	Slechts enkele berichttypes bevatten een context
Vertrouwensniveau (1)	Het vertrouwensniveau waarmee de afzender van het bericht geauthentiseerd is	Authenticatie (IeA) component	

4.1.2 Interne interface Autoriseren van applicatie voor interactie

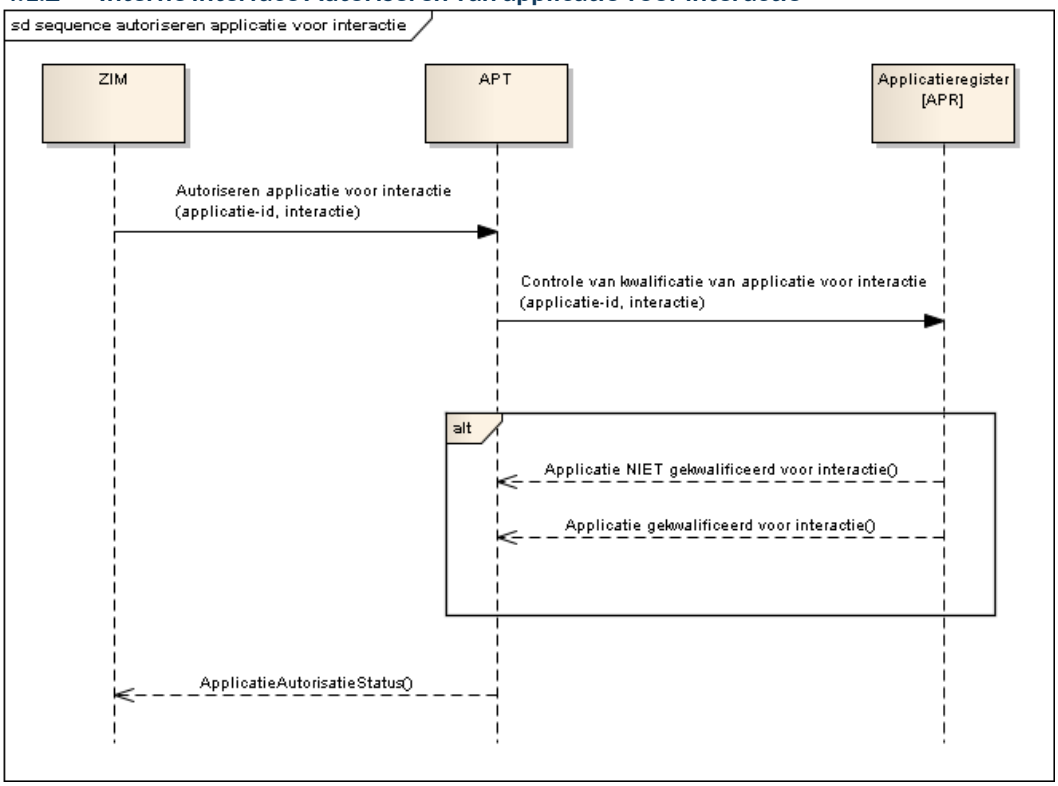

Diagram ZIM.APT.d2020 Sequentiediagram voor het autoriseren van de applicatie voor een interactie.

Parameters voor het autoriseren van de applicatie:

Tabel ZIM.APT.t2010 Autoriseren van applicatie voor interactie attributen

Attribuut	Definitie	Herkomst	Additionele informatie
Interactie-id (1)	De interactie-identificatie	Bericht	
Applicatie-id (1)	De identificatie van de applicatie.	Bericht	
Authenticatieniveau (1)	Het vertrouwensniveau waarmee het bericht geauthentiseerd is.	Authenticatie (IeA) component	

5 Services en functies

5.1 Primaire services

De APT ondersteunt de volgende autorisatieservices:

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

5.1.1 Primaire service 1 - Autoriseren rol voor interactie

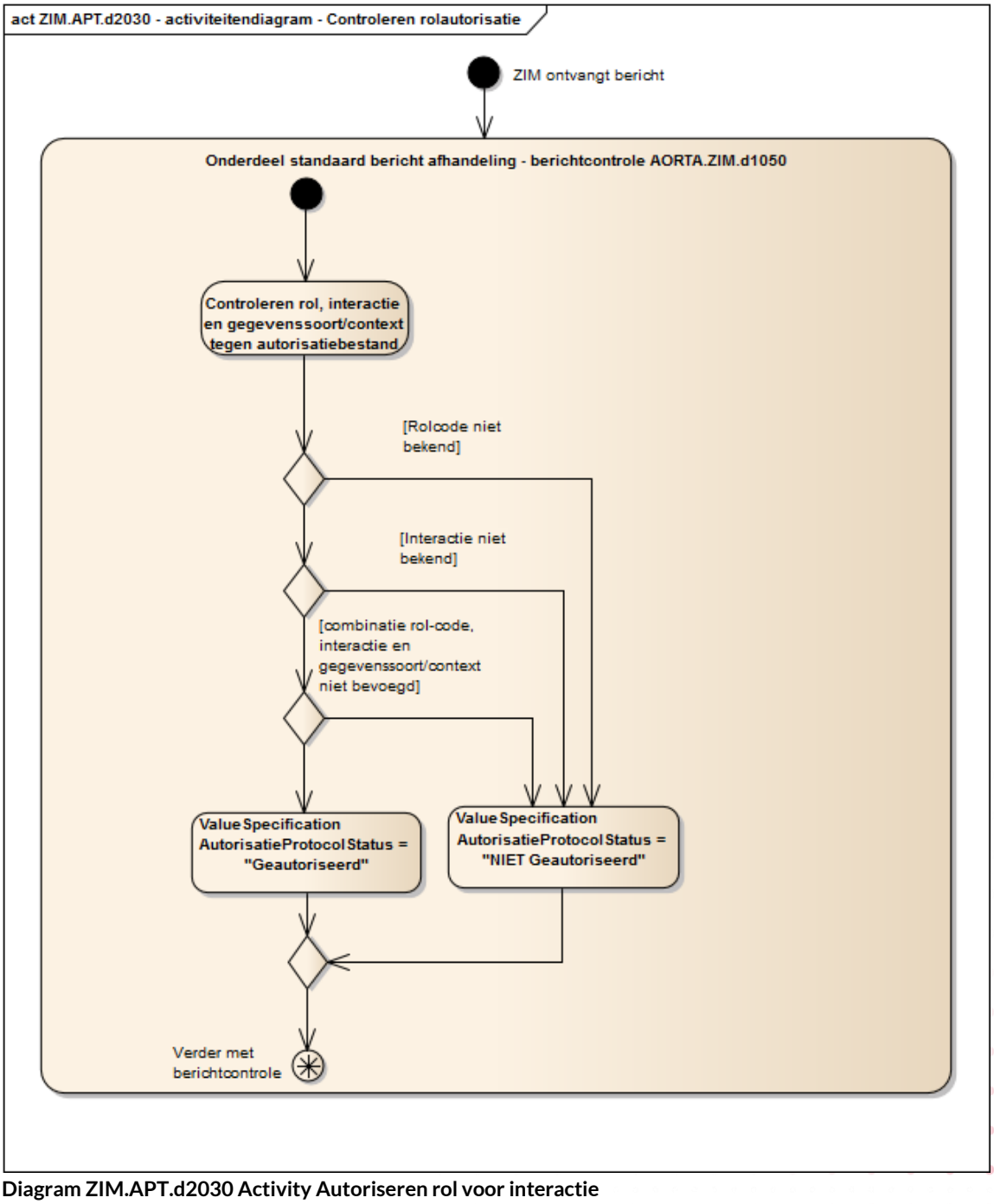

Diagram ZIM.APT.d2030 Activity Autoriseren rol voor interactie

De volgende zaken worden gecontroleerd:

- Is het opgegeven vertrouwensniveau voldoende voor de opgegeven interactie? Dit wordt bepaald aan de hand van het Autorisatiebestand (behandeld in 6.1.4 op pagina 15), dat voor iedere interactie het minimale vertrouwensniveau specificeert.
- Is de opgegeven bedrijfsrol bevoegd voor de opgegeven interactie en eventuele gegevenssoort? Dit wordt bepaald aan de hand van het Autorisatiebestand, dat voor iedere interactie en interactie/gegevenssoort-combinatie of interactie/context-combinatie specificeert welke rollen bevoegd zijn. Mocht de bedrijfsrol of de interactie niet worden gevonden in het autorisatiebestand, dan is er geen bevoegdheid.

De uiteindelijke 'output' parameter *AutorisatieResultaat* van de APT kan één van beide waarden bevatten:

-Geautoriseerd,

óf

-Niet-geautoriseerd

5.1.2 Primaire service 2 - Autoriseren van de applicatie voor interactie

De autorisatiecomponent (APT) gaat na of applicatie die vermeld staat als afzender in een bericht, gekwalificeerd is voor het verzenden van het betreffende interactie-id van datzelfde bericht.

Dit gebeurt door de conformancetabel van het applicatieregister te raadplegen.

Indien dit klopt dan is de applicatie geautoriseerd.

Indien er geen overeenkomst is dan is er *geen* autorisatie voor de applicatie en zal de ZIM voor de verdere foutafhandeling zorgen.

De uiteindelijke 'output' parameter ApplicatieAutorisatieStatus

van de APT kan één van beide waarden bevatten:

-Geautoriseerd;

óf

-Niet-geautoriseerd.

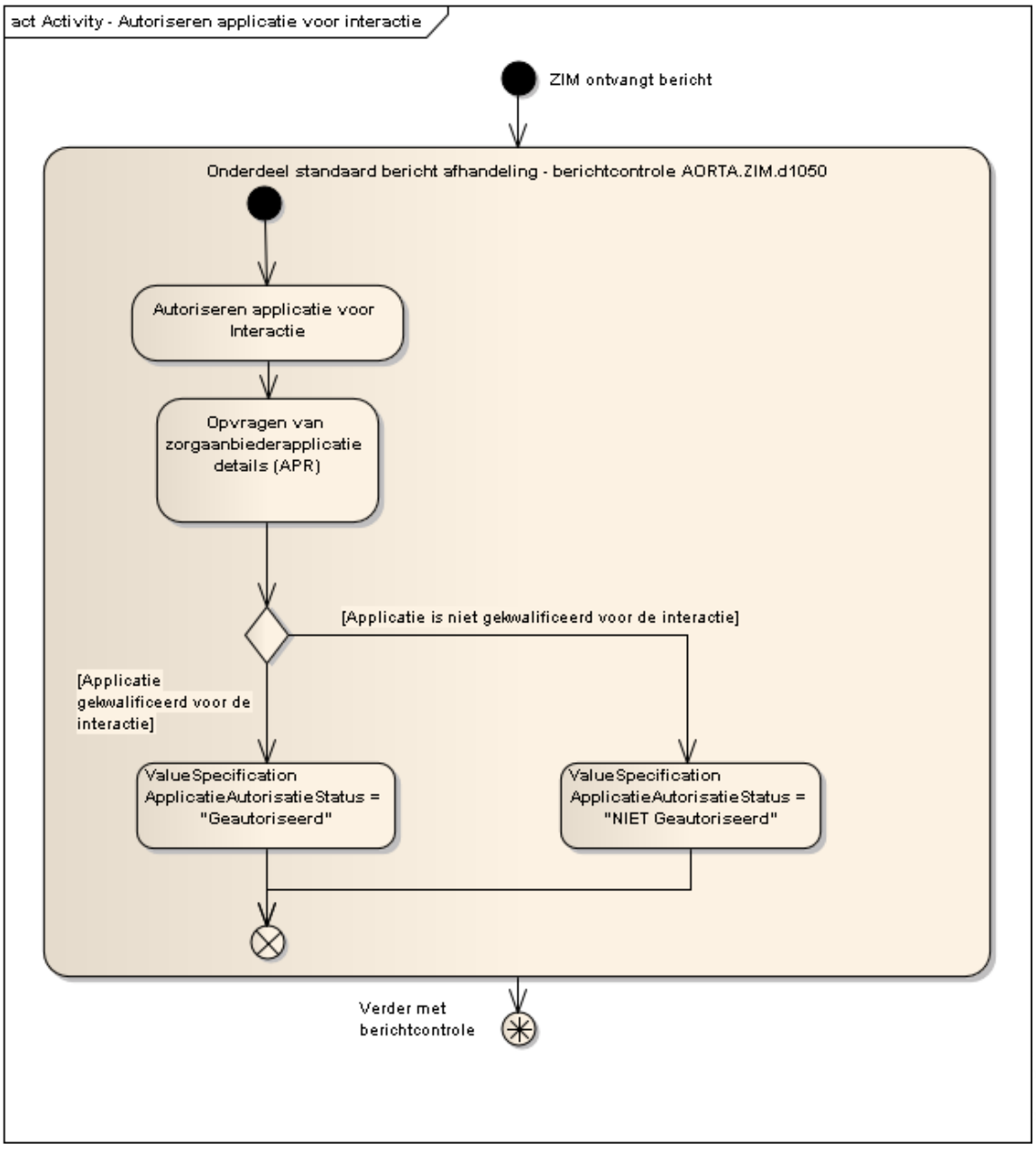

Diagram ZIM.APT.d2040 Activity Autoriseren applicatie voor interactie.

5.2 Beheerfuncties

Autorisatiebeheer functies

Hier zijn de volgende beheerfuncties te onderkennen:

Tabel ZIM.APT.t2020 Beheersfuncties

Beheersfunctie	Type gebruikersinterface	Beschrijving
Laden autorisatiebestand	Naar keuze van de LSP-opdrachtnemer: Bestandsinterface en/of Toetsenbordinterface	Wanneer de autorisatiemanager van het VZVZ Servicecentrum aan de autorisatiebeheerder van het LSP een nieuw autorisatiebestand aanbiedt, moet de autorisatiebeheerder dit bestand in zijn geheel kunnen laden.
Raadplegen autorisatiebestand	Scherminterface	De autorisatiebeheerder moet een geldende autorisatie kunnen inzien, bijv. na een klacht dat een leden van een bepaalde beroepsgroep geen toegang krijgen.
Rapporteren autorisaties	Printerinterface	De autorisatiebeheerder moet alle geldende autorisaties kunnen rapporteren aan Nictiz.

Toelichting: de autorisatiemanager van VZVZ zal het autorisatiebestand aanleveren aan de LSP-opdrachtnemer. De autorisatiebeheerder van het LSP kan dit bestand op verschillende manieren invoeren in (de APT-component van) de ZIM:

- Handmatig door de tabel te laten intoetsen door een autorisatiebeheerder in een gebruikersinterface van de ZIM.
- Geautomatiseerd door de tabel te exporteren naar een geschikt formaat dat kan worden ingelezen door een bestandsinterface van de ZIM.

De keuze voor één van, of beide opties wordt overgelaten aan de LSP-opdrachtnemer.

Alle wijzigingen worden gelogd in de beheerlog, met daarin:

- Identiteit van de autorisatiebeheerder (beheerder ID) (1)
- Datum en Tijd dat de wijziging is doorgevoerd (1)
- Referentie naar de wijziging (een RFC nummer) (1)

6 Gegevensmodel

6.1 (Logisch) model van entiteiten en relaties

Autorisatie valt uiteen in twee verschillende onderdelen:

Algemene Bedrijfsautorisatieregels	Medisch Autorisatie Protocol
gaat over toegang tot alle soorten gegevens: toegangslog, applicatieregister, etc. uit centrale en decentrale bronnen.	gaat uitsluitend over toegang tot medische patiëntgegevens, zoals verspreid over decentrale bronnen van zorgaanbieders.
niet bestemd voor de autorisatiecommissie, de inhoud wordt grotendeels bepaald door wetgeving, zoals Wbp, Wgbo en Wepd	bestemd voor de autorisatiecommissie, die de inhoud per zorgtoepassing zal bepalen op basis van onderhandelingen tussen betrokken beroepsverenigingen
niet instelbaar, anders dan door een nieuwe LSP-release	moet run-time in het LSP kunnen worden ingesteld, want ook een nieuwe zorgtoepassing of context moet kunnen worden geïmplementeerd zonder een nieuwe LSP-release

Beide worden buiten de ZIM vertaald naar een (Technisch) Autorisatiebestand, dat wordt geladen in de ZIM.

6.1.1 (Algemene) Bedrijfsautorisatieregels

De belangrijkste autorisaties zijn wettelijk bepaald door de Wbp, Wgbo. Deze zijn enigszins gestructureerd weergegeven in de (Algemene) Bedrijfsautorisatieregels.

Omdat de Bedrijfsautorisatieregels nogal verschillen per gegevensverzameling, is er nauwelijks een uniform gegevensmodel voor te geven. Dat is ook niet nodig, want ze zullen voor een groot deel in de desbetreffende componenten worden ondergebracht. Alleen de rolgebaseerde delen van die regels kunnen worden ondergebracht in de APT-component.

6.1.2 (Medisch) Autorisatieprotocol

Het (Medische) Autorisatieprotocol is een tabel waarin de autorisatiecommissie per zorgtoepassing vaststelt, welke beroepstitels/specialismen bevoegd zijn om toegang te krijgen tot welke (medische) gegevenssoorten.

Het Autorisatieprotocol is in essentie een reeks van medische autorisatieregels, waarbij iedere autorisatieregel een bevoegdheid definieert tussen:

- Bedrijfsrol;
- gegevenssoort (of filter op gegevensoort);
- context;
- operatie.

Waarbij de bedrijfsrol kan zijn:

- zorgverlener, met als attributen:
  - beroepstitel;
  - eventueel specialisme;
- burger;
- wettelijke vertegenwoordigers van burgers

En waarbij de operatie kan zijn:

R = raadplegen (opvragen, abonneren)

V = verstrekken (vastleggen, aanmelden, versturen, signaleren, overdragen)

Op deze wijze blijft de keuzevrijheid van invullen beperkt tot de essentie:

- mag iemand de gegevenssoort raadplegen of bouwstenen uit de gegevenssoort binnen een bepaalde context (privacy-belang);
- mag iemand de gegevenssoort verstrekken (integriteits-belang).

Dit ongeacht de wijze (sturen of opvragen) waarop. Bij raadplegen is het immers niet relevant of je iets *opvraagt* dan wel *ontvangt* (=toegestuurd krijgt).

Merk op dat de gegevenssoort een ruim begrip is: niet alleen de gegevenssoorten zoals ze worden aangemeld in de verwijsindex, maar ook de gegevensverzamelingen zoals ze worden verstuurd of opgeleverd. Bijvoorbeeld bij WDH/Hwg beschouwen we het *eerstelijnsdossier*, de *professionele samenvatting* en het *waarneemverslag* als één gegevenssoort.

6.1.3 Vertaaltabel

De zogenaamde Vertaaltabel wordt door VZVZ bijgehouden en gebruikt om het (Medische) Autorisatieprotocol en de (Algemene) Bedrijfsautorisatieregels te vertalen naar een (Technische) Autorisatiebestand dat kan worden geladen in de ZIM.

6.1.4 (Technisch) Autorisatiebestand

Binnen de ZIM wordt alleen het (Technische) Autorisatiebestand bijgehouden als gegevensobject.

Het Autorisatiebestand is in essentie een reeks van technische autorisatieregels, waarbij iedere autorisatieregel een bevoegdheid definieert tussen:

- bedrijfsrol;
- functionele interactie.

De bedrijfsrol kan zijn:

- zie paragraaf 6.1.2

En waarbij de functionele interactie bestaat uit:

- functionele naam;
- technische interactie-id;
- technische gegevenssoort-id of technische context-id;
- minimaal vereist vertrouwensniveau;
- gegevensdomein.

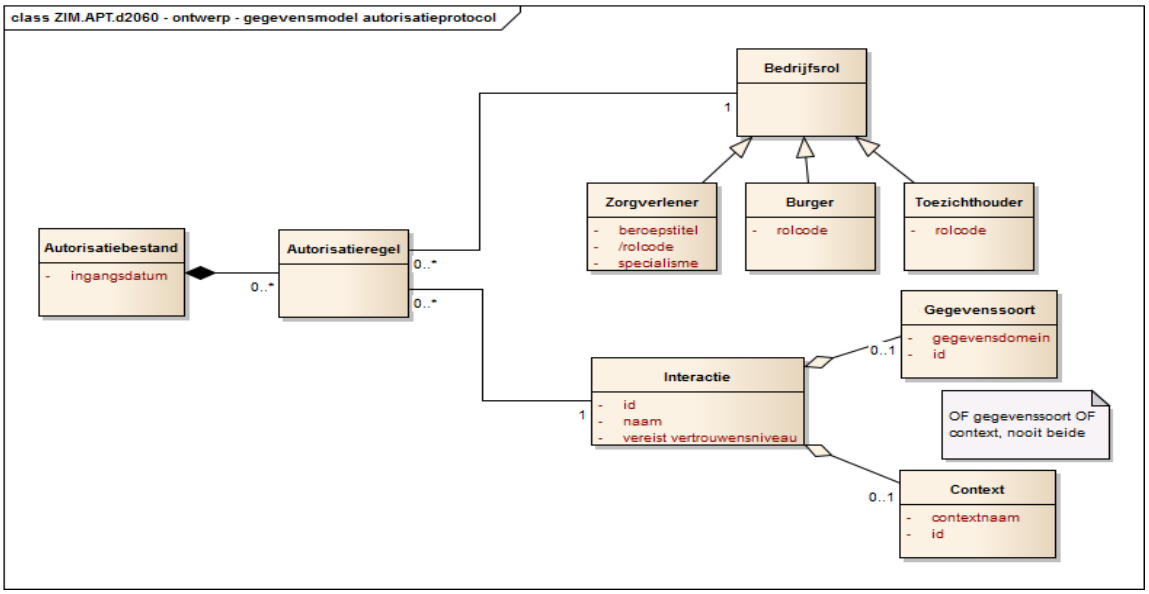

Diagram ZIM.APT.d2050 Gegevensmodel (Technisch) Autorisatiebestand

Tabel ZIM.APT.t2030 Attributen van (Technisch) Autorisatiebestand

Attribuut	Definitie	Additionele informatie
Bedrijfsrol (1)	De rol van een persoon in het zorgproces	
Beroepstitel (1)	Beroepstitel van een zorgverlener, zoals vastgelegd in UZI-register en op UZI-pas	
Specialisme (0..1)	Eventueel specialisme van een zorgverlener, zoals vastgelegd in UZI-register en op UZI-pas	
Functionele interactie-naam		
Technische interactie-id	De in HL7v3 gebruikte identificatie van interacties	
Technische gegevenssoort-id	De in HL7v3-berichten gebruikte code voor gegevenssoorten	Sluit context-id uit
Technische context-id	De in HL7v3-berichten gebruikte code voor context	Sluit gegevenssoort-id uit
Minimaal vereist vertrouwensniveau		
Gegevensdomein	De verzameling gegevenssoorten die centraal staat binnen een zorgtoepassing of servicecomponent	Voorbeelden: Zorgadresboek, Verwijsindex, Medicatiegegevens,

6.2 Gegevensautorisatiemodel

Autorisatie tot het gegevensmodel van het autorisatieprotocol is beperkt tot de rol van autorisatiebeheerder. Deze rol kan procesmatig binnen de organisatie gedekt zijn.

Een autorisatiebeheerder heeft update rechten tot het autorisatieprotocol.

Tabel ZIM.APT.t2070 Gegevensautorisatiemodel

Gegevensautorisatiemodel (aanduiding CRUD-rechten per rol)		
Entiteit	Autorisatiebeheeder	
Autorisatieregel	Update	alleen voor medische interacties

7 Configuratieaspecten

Niet van toepassing.

8 Ontwerpaspecten ten behoeve van niet-functionele eisen

Er zijn voor de autorisatieprotocolcomponent geen specifieke niet-functionele eisen gesteld en daarom zijn er geen ontwerp aspecten mee gemoeid.

Niet-functionele eisen als beschikbaarheid, capaciteit, schaalbaarheid en performance komen overeen met de eisen die aan de ZIM-component gesteld worden.

Uit oogpunt van *vertrouwelijkheid* zijn er geen beperkingen.

Uit oogpunt van *integriteit* is het belangrijk te kunnen achterhalen wie het autorisatieprotocol heeft aangepast, bijvoorbeeld door middel van een beheerlog (merk op dat dit overeenkomt met architectuurprincipe AORTA.ALG.p1060 dat gegevens traceerbaar zijn).

Uit oogpunt van *beheerbaarheid* is het wenselijk het autorisatieprotocol centraal te onderhouden.

9 Interne componentenstructuur en werking

Voor dit component is geen interne componentstructuur of werking beschreven.

10 Procedurele beheersaspecten

Voor elke zorgtoepassing wordt een autorisatiecommissie samengesteld uit de medische beroepsverenigingen en patiëntenverenigingen. Deze autorisatiecommissie heeft als taak om een (Medisch) Autorisatieprotocol vast te stellen voor die zorgtoepassing. Dat gebeurt initieel bij de invoering van die zorgtoepassing, maar later kan het Autorisatieprotocol worden gewijzigd of uitgebreid, wanneer dat nodig is.

De autorisatiemanager van VZVZ zal op onregelmatige tijdstippen een Autorisatieprotocol voor een bepaalde zorgtoepassing in ontvangst nemen. Daarbij zal worden afgesproken wanneer het nieuwe protocol van kracht moet worden. De autorisatiemanager zal op basis van het nieuwe Autorisatieprotocol-deel en alle eerder ontvangen Autorisatieprotocol-delen een technisch Autorisatiebestand laten genereren met behulp van een Vertaaltabel. Het Autorisatiebestand, in Excel-formaat, zal vervolgens worden aangeboden aan de LSP-opdrachtnemer.

De autorisatiebeheerder van de LSP-opdrachtnemer zal het Autorisatiebestand ontvangen en run-time laden in de ZIM. Dat kan op verschillende manieren:

- Handmatig door de Excel-tabel te laten intoetsen door een autorisatiebeheerder in een gebruikersinterface van de ZIM.
- Geautomatiseerd door de Excel-tabel te exporteren naar een geschikt XML-formaat dat kan worden ingelezen door een bestandsinterface van de ZIM.

De keuze voor één van, of beide opties wordt overgelaten aan de LSP-opdrachtnemer.

Het Autorisatiebestand bevat niet alleen autorisaties met betrekking tot zorgtoepassingen en patiëntgegevens, maar ook autorisaties met betrekking tot infrastructurele gegevensbronnen, zoals de toegangslog, het zorgadresboek, etcetera. Die autorisaties zijn vertaald vanuit de (Algemene) Bedrijfsautorisatieregels.

Deze (Algemene) Bedrijfsautorisatieregels zijn in tegenstelling tot het (Medisch) Autorisatieprotocol niet vrij instelbaar, ze zijn door de architect van AORTA grotendeels afgeleid van wetgeving en het vertrouwensmodel. Eventuele wijziging van deze Bedrijfsautorisatieregels vergt in principe een nieuwe AORTA-release, omdat het ontwerp van de diverse services/componenten in sterke mate wordt bepaald door die Bedrijfsautorisatieregels.

De onderstaande tabel geeft een samenvatting:

Bedrijfsactor	Bedrijfsproces	Bedrijfsobject (input)	Bedrijfsobject (output)
Architect	Opstellen (algemene) autorisatieregels	Wbp, Wgbo, Wepd + Vertrouwensmodel	(Algemene) Bedrijfs-autorisatieregels
Ontwerpers	Ontwerpen <service/ component>	(Algemene) Bedrijfs-autorisatieregels	Ontwerpdocumenten <service/component> + Vertaaltabel
Autorisatie-commissies	Vaststellen autorisatie voor <zorgtoepassing>	Gegevens-richtlijn voor <zorgtoepassing>	(Medisch) Autorisatieprotocol voor <zorgtoepassing>
Autorisatie manager	Genereren (technisch) autorisatiebestand	(Medisch) Autorisatieprotocol voor alle zorgtoep. + Vertaaltabel	(Technisch) Autorisatiebestand
Autorisatie beheerder	Laden autorisatie-bestand in ZIM	(Technisch) Autorisatiebestand	Werkende APT-service/component

De autorisatiebeheerder werkt op verzoek van de autorisatiemanager het landelijke autorisatieprotocol bij. Alleen na opdracht van de autorisatiemanager zal de autorisatiebeheerder aanpassingen doen aan het autorisatieprotocol. Een opdracht zal altijd gebaseerd zijn op een geregistreerd wijzigingsverzoek (RFC).

De autorisatiebeheerder rapporteert over al zijn handelen terug naar de autorisatiemanager en maakt hiervan een verslag als onderdeel van het wijzigingsverzoek (RFC).

Bijlage A Referenties

Referentie	Document	Versie
[Ontw Authenticatie]	Ontwerp authenticatie	8.1.0.0
[Ontw APR]	Ontwerp applicatieregister	8.1.0.0
[Ontw SDS]	Ontwerp Selectie en Determinatie Service	8.1.0.0
[Arch AORTA]	Architectuur AORTA	8.1.0.0