Ontwerp Authenticatie

Datum: 15 oktober 2024

Publicatie: V8.4.0.0

Inhoudsopgave

1 Inleiding

1.1 Doel en scope

Dit document heeft tot doel de beschrijving en het ontwerp van de authenticatiecomponent binnen de AORTA-architectuur. Het ontwerp beschrijft de werking van de component aan de hand van een context diagram. De interfaces met andere componenten of systemen zijn hierin af te lezen en worden later in detail beschreven.

Het document beperkt zich uitsluitend tot een architectuurontwerp van één enkele component van de ZIM, te weten de authenticatiecomponent. Het geeft het kader en de werking weer waaraan de component moet voldoen. Het is niet een detail beschrijving c.q. instructie voor de daadwerkelijke ontwikkeling, implementatie en beheer ervan.

1.2 Doelgroep voor dit document

Dit document is bedoeld voor die partijen die het Landelijk Schakelpunt en daarbinnen de ZIM willen ontwikkelen en uitvoeren. Het geeft die partijen een conceptueel overzicht over de voorgeschreven wijze van authenticatie die binnen de AORTA-infrastructuur gehanteerd wordt.

Uiteraard is het voor partijen die willen aansluiten aan het landelijk schakelpunt een naslagwerk over de werking van authenticatie. Het kan inzichten geven om in de ontwikkeling van de eigen XIS applicaties beter met authenticatie zaken om te gaan.

Tevens is dit document een basisdocument van de AORTA documentatie set en dient het Nictiz om onderhoud aan de AORTA-architectuur te vereenvoudigen.

1.3 Documenthistorie

Versie	Datum	Omschrijving
6.10.0.0	12-okt-2011	Initiële versie na herstructurering AORTA-documentatie. RfC 34123: BSN in Payload en Transmission wrapper moeten gelijk zijn. RfC 35179: Wijzigingen tbv Authenticatie patiënt voor zorgaanbiederportaal. RfC 35570: Wijzigingen tbv Authenticatie patiënt voor zorgaanbiederportaal. RfC 44797: Controle op subject in SSL-certificaat van GBK/GBP toegevoegd.
6.10.0.0	24-feb-2012	RfC 51819: Controle applicatie-id en FQDN op niveau laag.
6.10.0.0	2-apr-2012	RfC 34123: BSN in Payload of Transmission wrapper.
6.12.1.0	5-dec-2012	RfC 46182: Verscherpen controle ZIM-certifcaat door GBx RfC 50926: Aansluiten GBO
8.0.1.0	15-mei-2017	RfC 52477: Uitwisseling op basis van bouwstenen.
8.0.1.0	15-mei-2017	RfC 76206: SSL verwijderen
8.0.1.0	15-mei-2017	RfC 68025: Controle met betrekking tot URA aangepast
8.0.2.0	31-januari-2018	RfC 77539: Aanpassing ontwerp o.b.v. SAML tokens
8.0.3.0	15-nov-2018	Opgenomen in publicatie 8.0.3.0
8.1.0.0	1-aug-2019	INI-8877: Conditionele query
8.1.0.0	1-aug-2019	INI-8975: Koppeling GBC
8.1.0.0	1-aug-2019	INI-8894: Koppeling DVZA

8.4.0.0	17-okt-2024	INI-9777: Systeemauthenticatie o.b.v. servercertificaat reagerend system Aanpassing paragraaf 5.1.1., 5.2.2 en paragraaf 5.1.3 toegevoegd

2 Kaders en uitgangspunten

2.1 Externe normen en kaders

De authenticatiecomponent is sterk afhankelijk van digitale certificaten. Deze certificaten worden afgegeven door een Certification Service Provider (CSP). De dienstverlening en werkwijze van digitale certificaten is beschreven in een Certificate Policy (CP) afgegeven door de CSP. De Certificate Policy is hiermee een normenkader dat van belang is voor dit authenticatiecomponent. Binnen de AORTA-infrastructuur wordt gebruik gemaakt van de Public Key Infrastructure Overheid (PKIoverheid) als CSP. De CP van de PKIoverheid vormt dit normenkader.

Het agentschap CIBG, de CSP waartoe het UZI-register (Unieke Zorgverlener Identificatie Register) behoort, volgt de CP van de PKIoverheid. De Certificate Policy van de PKIoverheid staat beschreven in [CP PKIO] dat via de website van de PKIoverheid is te raadplegen.

De Wet gebruik burgerservicenummer (BSN) in de zorg (Wbsn-z) vormt het kader voor het identificeren van burgers/patiënten. De Wet regelt dat ook binnen de zorgsector gebruik gemaakt kan worden van het BSN. Zorgaanbieders zijn verplicht het BSN van hun patiënten vast te leggen in hun administratie en te gebruiken bij de onderlinge gegevensuitwisseling (zowel elektronisch als niet-elektronisch) over patiënten.

2.2 Relatie met AORTA-principes en –beslissingen

Deze paragraaf bevat de architectuurbeslissingen waaraan het ontwerp van de authenticatiecomponent moet kunnen voldoen.

Architectuurbeslissingen:

AORTA.ALG.p1020: voor toegang tot patiëntgegevens via AORTA moeten zorgverleners individueel worden geïdentificeerd en geauthenticeerd.

AORTA.ZIM.IeA.p2010 Een zorgverlener wordt geïdentificeerd door het UZI-nummer. Het UZI-nummer is het zorgverlener-id.

AORTA.ZIM.IeA.p2020 Een zorgaanbieder wordt geïdentificeerd door het UZI-Register Abonneenummer (URA). De URA is het zorgaanbieder-id.

AORTA.ZIM.IeA.p2030 Een zorgverlener/medewerker en zorgaanbiederapplicatie(s) maken gebruik van respectievelijk UZI-pas(sen) en UZI-servercertificaten.

AORTA.ZIM.IeA.p2040 De AORTA-infrastructuur zal meerdere generaties van UZI-middelen (passen en servercertificaten) moeten kunnen ondersteunen.

AORTA.ZIM.IeA.p2050 Een klantenloketmedewerker en klantenloketapplicatie(s) maken gebruik van respectievelijk een PKIO-pas en een PKIO-servercertificaat.

AORTA.ZIM.IeA.p2060 Een klantenloketmedewerker wordt geïdentificeerd door een kenmerk dat in zijn persoonsgebonden vertrouwensmiddel is opgenomen. Het kenmerk is onweerlegbaar door de CA (certificate authority) terug te voeren naar één natuurlijk persoon.

AORTA.ZIM.IeA.p2070 Een klantenloketapplicatie (Goed Beheerd Klantenloket applicatie) wordt geïdentificeerd door een fully qualified domain name (FQDN) die in het systeemgebonden vertrouwensmiddel is opgenomen.

AORTA.ZIM.IeA.p2080 Een GBP-applicatie (Goed Beheerd Portaal applicatie) wordt geïdentificeerd door een fully qualified domain name (FQDN) die in het systeemgebonden vertrouwensmiddel is opgenomen.

AORTA.ZIM.IeA.p2090 Een patiënt wordt geïdentificeerd door het BSN-nummer. Het BSN-nummer is het patiënt-id.

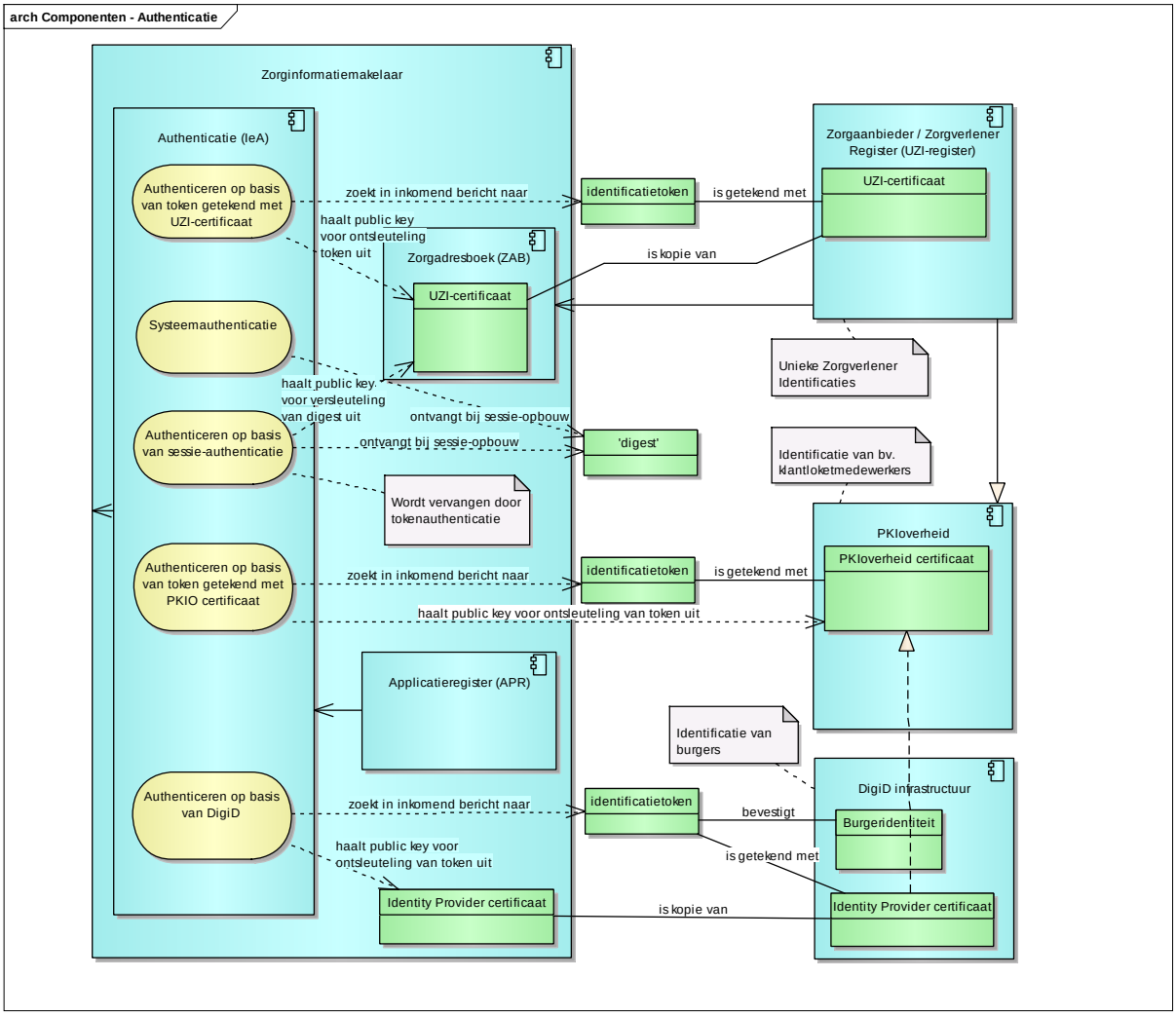
AORTA.ZIM.IeA.p2100 Een patiënt wordt geauthenticeerd door het DigiD-register. De mate waarin op de authenticiteit van een patiënt kan worden vertrouwd wordt bepaald en afgegeven door het DigiD-register.

AORTA.ZIM.IeA.p2110 Een GBO-applicatie wordt geïdentificeerd door een fully qualified domain name (FQDN) die in het systeemgebonden vertrouwensmiddel is opgenomen.

AORTA.ZIM.IeA.p2120 Een GBO-applicatie maakt gebruik van een PKIO-servercertificaat (anders dan het UZI-certificaat).

AORTA.ZIM.IeA.p2130 Een GBZ-applicatie wordt geïdentificeerd door een fully qualified domain name (FQDN) die in het systeemgebonden vertrouwensmiddel is opgenomen.

3 Context van authenticatiecomponent



Figuur ZIM.IeA.d2010.1 Context diagram van de authenticatiecomponent.

De authenticatiecomponent (IeA) is onderdeel van de ZIM component. Deze dient om actoren en systemen die gegevens uitwisselen met of via de ZIM te authenticeren.

3.1 Authenticatie

Authenticatie heeft tot doel, met zekere waarschijnlijkheid, de identiteit van een gebruiker/systeem vast te stellen. De authenticatiecomponent controleert of een opgegeven bewijs van identiteit (attributen) overeenkomt met echtheidskenmerken en of deze valide is.

Deze component is betrokken bij de afhandeling van elk bericht dat bij de ZIM binnenkomt vanuit een aangesloten systeem, zoals bij het opvragen en versturen van patiëntgegevens. De component authenticeert hierbij de auteur (meta-informatie element van HL7-v3 berichten) van een bericht (gebruiker of systeem), aan de hand van attributen die worden meegegeven.

De wijze van het meegeven van deze attributen gebeurt op basis van één van de volgende methoden:

- In het bericht zelf (door middel van een SAML-token);
- Bij het tot stand komen van een TLS sessie.

De Authenticatiecomponent heeft services die ieder een andere wijze van authenticeren uitvoeren:

- Authenticeren op basis van een SAMLtoken;
- Systeemauthenticatie op basis van een servercertificaat.

De Authenticatiecomponent vervult ook nog de functie:

- Identificeren van de ZIM.

Afhankelijk van de te authenticeren berichten die de ZIM ontvangt wordt één van de services aangesproken. De attributen vanuit een bericht worden doorgegeven aan de service.

De betreffende service voert een bewerking uit van controle, validatie en vergelijking op echtheidskenmerken.

Het resultaat van een service is een bewering van authenticatie. Dit kan zijn:

- *Geauthenticeerd*, de activiteiten van deze identiteit kunnen vervolgen.
- *Niet-geauthenticeerd*, verdere verwerking van activiteiten van deze identiteit worden niet toegestaan.
- *Onbepaald*, er zijn onvoldoende gegevens om te authenticeren, en daarmee effectief niet-geauthenticeerd.

Tevens geeft een service het authenticatieniveau af waarmee geauthenticeerd is. Dit komt overeen met het vertrouwensniveau waarmee de inhoud van een bericht verder verwerkt kan worden. Dit kan zijn:

- laag;
- midden;
- substantieel;
- hoog.

Om deze services van authenticeren mogelijk te maken zullen er interfaces zijn met partijen die de identiteiten voorzien (Identity Providers) en om de echtheidskenmerken van de identificaties te verifiëren.

Deze partijen zijn:

- Het UZI-register (CIBG) voor identiteiten met UZI-passen en UZI-(server)certificaten.
- De PKIoverheid voor identiteiten van persoonsgebonden passen met certificaten en systeemcertificaten.

De identiteiten die kunnen worden geauthenticeerd zijn:

- de GBZ'en (dmv UZI-servercertificaat);
- het GBK (dmv PKIO-servercertificaat);
- het GBP (dmv PKIO-servercertificaat);
- het GBO (dmv PKIO-servercertificaat);
- de DVZA (d.m.v. PKIO-servercertificaat);
- de GBC (d.m.v. PKIO-servercertificaat).
- zorgverleners en medewerkers (door middel van UZI-certificaat);
- GBK medewerkers (door middel van PKIO certificaat);

- patiënten/burgers aan de hand van een door DigiD afgegeven bewering (assertion) van identiteit dat is getekend door DigiD;

Het controleren van de validiteit en geldigheid van de certificaten afgegeven voor bovengenoemde partijen wordt afgehandeld volgens de Certificate Policy Statement (CPS) van betreffende Certificate Service Provider (CSP). Voor bovengenoemde certificaten is de CPS van de PKIoverheid [CPS PKIO] leidend. Bij iedere authenticatie op basis van certificaten beschreven in dit document, zal het CPS gevolgd worden om de certificaten te controleren.

3.2 ZIM identificatie

Deze component voorziet tevens in de zelf-identificatie van de ZIM aan andere systemen. Het voorziet in identificerende attributen voor het tot stand komen van communicatieverbindingen (TLS-sessies).

NB: Deze component heeft geen menselijke actor. Om die reden is er geen gebruikersrol gedefinieerd. De component interacteert alleen maar met andere systemen.

4 Interfaces (koppelvlakken)

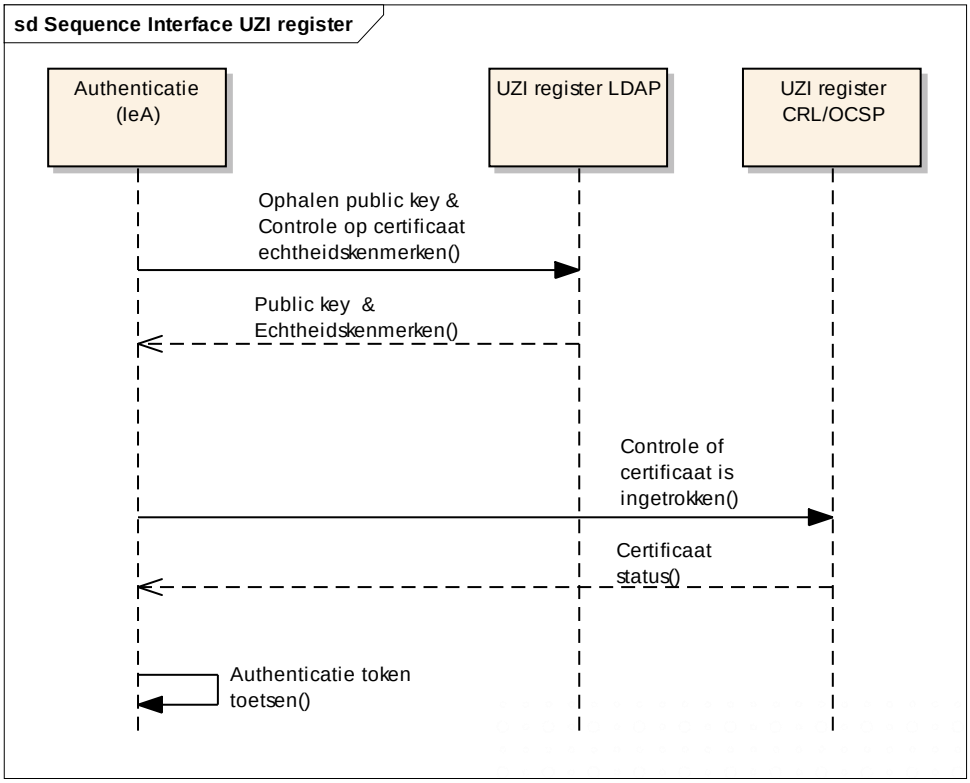
4.1 Systeeminterfaces

De authenticatiecomponent heeft systeeminterfaces met de volgende externe systemen:

- het UZI-register (CIBG);
- de PKIoverheid.

Deze interfaces hebben een ander karakter dan interfaces voor andere ZIM componenten. Ze zijn niet op HL7 berichten gebaseerd. Hoewel de implementatie van de interfaces niet wordt voorgeschreven, zijn sommigen triviaal en vanuit de techniek gestandaardiseerd. Ze kunnen in de interface worden benoemd.

4.1.1 Interface – UZI register



Figuur ZIM.IeA.d2020 Interface met UZI-register

De interface met het UZI-register wordt gebruikt als de authenticatiecomponent een bericht ontvangt met daarin een authenticatietoken dat is ondertekend met een UZI-certificaat. De authenticatiecomponent zal vervolgens het certificaat gaan valideren door de LDAP van het UZI-register te bevragen (welke via een eenmalig beheeractie ge-'trust' moet worden in een certificate store in de ZIM om te voorkomen dat met een vervalst certificaat ook dynamisch een vervalste CA mee geleverd wordt aan de ZIM).

Het unieke serienummer van het UZI-certificaat wordt opgestuurd ter validatie. Het UZI-certificaat is zelf niet voorhanden en wordt opgehaald uit de LDAP van de betreffende CA1 van het UZI-register. Tevens zal

[1] Het UZI-register hanteert een aantal verschillende CA's, afhankelijk van welk type UZI-pas dat is afgegeven.

de Authenticatiecomponent vragen naar de publieke sleutel van de UZI CA die het certificaat heeft afgegeven.

Het UZI-register levert het UZI-certificaat met daarin de publieke sleutel, en het certificaat van de UZI CA die het certificaat heeft afgegeven, met daarin ook een publieke sleutel. Met behulp van de publieke sleutel in het UZI-certificaat wordt het token op integriteit en authenticiteit getoetst.

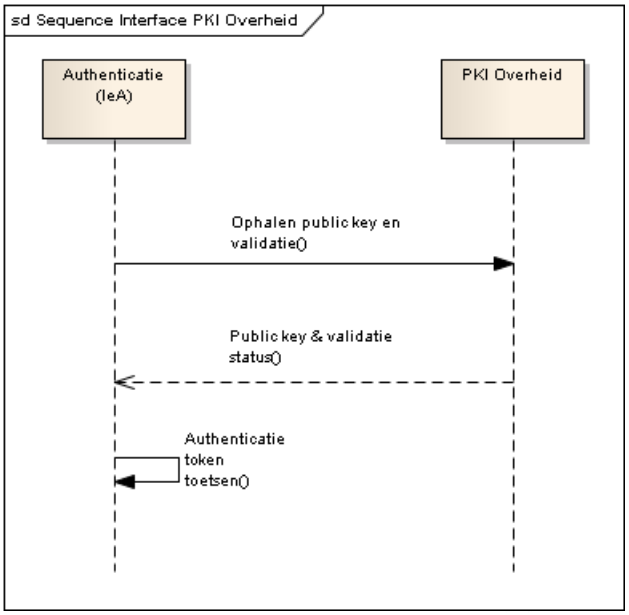
Tabel ZIM.IeA.t2010 Interface UZI register uitgaande bericht

Interface UZI register – uitgaand bericht			
Attribuut	Definitie	Herkomst	Additionele informatie
Certificaat serienummer (1)	Het unieke certificaat nummer afgegeven door UZI register.	Certificaat verwijzing in het bericht	Ter referentie in de • LDAP • CRL • OCSP interface.

Tabel ZIM.IeA.t2020 Interface UZI register antwoordbericht

UZI register – antwoordbericht			
Attribuut	Definitie	Herkomst	Additionele informatie
UZI Certificaat (1)	Het X.509 standaard certificaat, met daarin publieke sleutel.	UZI-register CA	Volgens LDAP en CRL/OCSP protocol.
Certificaat van UZI CA (1)	Het X.509 standaard certificaat van UZI CA met daarin publieke sleutel.	UZI-register CA	Volgens PKI standaarden.

4.1.2 Interface – PKIoverheid



Figuur ZIM.IeA.d2030 Interface met PKIoverheid

De interface met PKIoverheid wordt gebruikt als de authenticatiecomponent een bericht ontvangt met daarin een token dat is ondertekend met een PKIoverheid certificaat.

Authenticatiecomponent zal vervolgens het certificaat gaan valideren door de PKIoverheid te raadplegen. Het unieke serienummer van het certificaat wordt opgestuurd ter validatie. Indien het PKIoverheid certificaat zelf niet voorhanden is wordt deze opgehaald bij de PKIoverheid CA die deze heeft afgegeven (er van uitgaande dat PKIO CSP een publieke LDAP dienst heeft). Tevens zal Authenticatiecomponent vragen naar de publieke sleutel van de PKIoverheid CA die het certificaat heeft afgegeven.

PKIoverheid levert het PKIoverheid certificaat met daarin de publieke sleutel, en het certificaat van de PKIoverheid CA die het certificaat heeft afgegeven, met daarin ook een publieke sleutel.

Met behulp van de publieke sleutel in het PKIoverheid certificaat wordt het token op integriteit en authenticiteit getoetst.

Tabel ZIM.IeA.t2030 Interface PKIoverheid uitgaande bericht

PKIoverheid – uitgaand bericht			
Attribuut	Definitie	Herkomst	Additionele informatie
Certificaat serienummer (1)	Het unieke certificaat nummer afgegeven door PKIoverheid.		Het certificaat serienummer wordt als referentie meegegeven bij een authenticatietoken.

Tabel ZIM.IeA.t2040 Interface PKIoverheid antwoordbericht

Systeeminterface 2 – antwoordbericht		
Attribuut	Definitie	Herkomst
Certificaat (1)	De X.509 standaard certificaat, met daarin publieke sleutel.	PKIoverheid CA
Certificaat van PKIoverheid CA (1)	De X.509 standaard certificaat van PKIO CA met daarin publieke sleutel.	PKIoverheid CA

4.2 Eindgebruikersinterfaces

De authenticatiecomponent heeft geen specifieke eindgebruikersinterface.

5 Services en functies

5.1 Primaire services

De IeA component biedt de volgende authenticatiemogelijkheden:
- authenticeren op basis van SAML-token;
- systeemauthenticatie op basis van een servercertificaat.

Systeemauthenticatie gebeurt t.b.v. verschillende soorten systemen:
- Systeemauthenticatie o.b.v. servercertificaat t.b.v. initiërende systemen;
- Systeemauthenticatie o.b.v. servercertificaat t.b.v. reagerende systemen.

Het ontvangen van berichten als gevolg van het versturen van gegevens door een initiërend systeem (specifiek een versturend systeem), volgt dezelfde afhandeling als systeemauthenticatie o.b.v. servercertificaat t.b.v. reagerende systemen.

Er wordt geen onderscheid gemaakt tussen zorgtoepassings- en infrastructurele berichten. Systeemauthenticatie is in alle gevallen vereist.

5.1.1 Authenticeren op basis van SAML-token

Binnen de AORTA infrastructuur worden er diverse SAML-tokens gebruikt. Voor de opbouw en de inhoudelijke controles van de verschillende SAML-tokens zijn op zich zelf staande documenten geschreven (zie IH BA <toepassing>).

In Figuur 1 wordt de authenticatieafhandeling m.b.t. de tokens beschreven. Dit is een generieke afhandeling met betrekking tot SAML-tokens. Mocht een specifiek token afwijken van de hier beschreven afhandeling, dan zal dat expliciet beschreven worden in de begeleidende tekst.

Er worden alleen tokens geaccepteerd van systemen waarmee een systeemauthenticatie (hoofdstuk **Fout! Verwijzingsbron niet gevonden.**) op basis van TLS succesvol is afgerond.

De IeA stelt vast of de auteur van het bericht en/of de mandaterende zorgverlener een UZI-pas op naam heeft (door controle van het gebruikte certificaat). De IeA raadpleegt de LDAP voor het ophalen van het certificaat waarmee het token is getekend. Vervolgens wordt gecontroleerd en gevalideerd op de juistheid en geldigheid van het certificaat en de certificaat autoriteiten (CA's). In het geval gegevens met betrekking tot een certificaat ontbreken, dan zal het token worden afgewezen en zal er geen authenticatie plaatsvinden. Hetzelfde zal gebeuren als blijkt dat de geldigheid van het certificaat is verlopen of als het certificaat op de CRL is geplaatst.

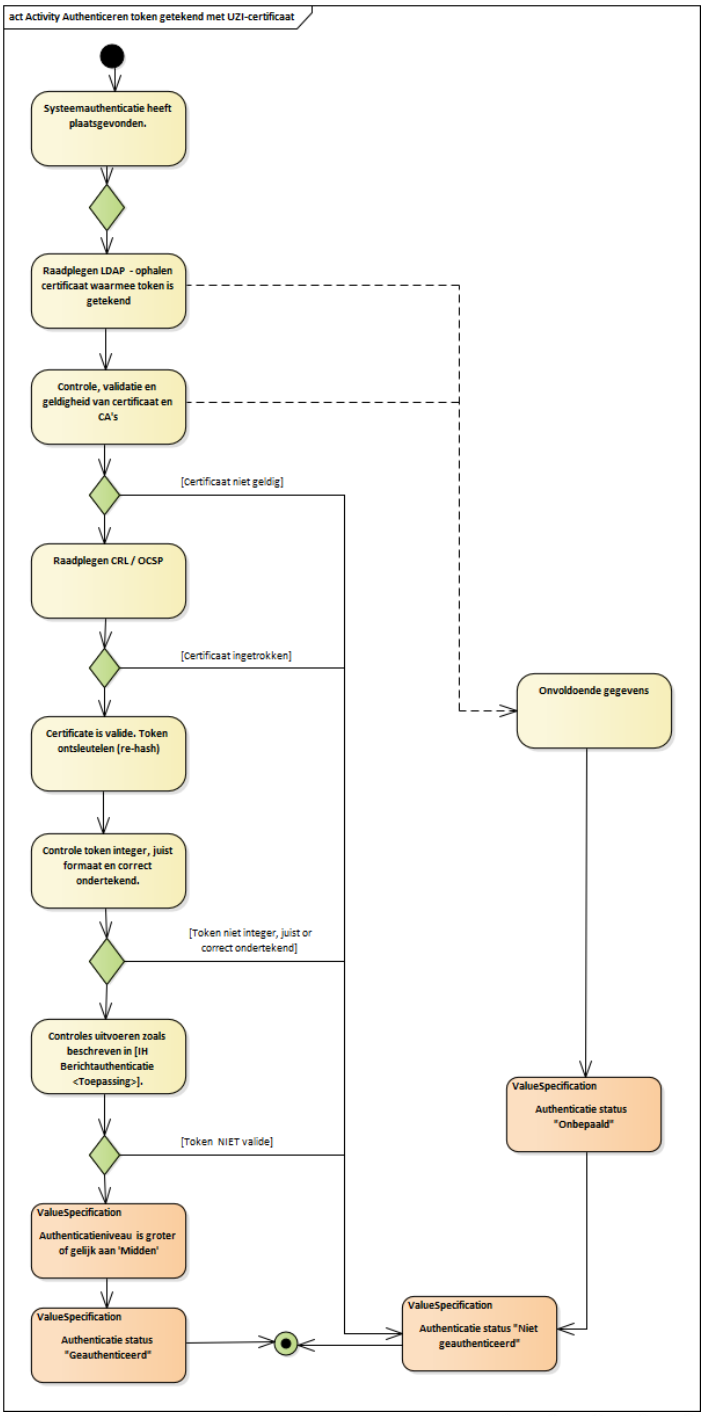
De IeA ontsleutelt het token en controleert het volgende:

a) Het token is correct ondertekend, zoals beschreven in [IH BA <toepassing>];
b) Het token is integer;
c) Het token heeft het juiste formaat, zoals beschreven in [IH BA <toepassing>];

Als laatste stap worden de controles uitgevoerd zoals beschreven in de [IH BA <toepassing>].

Indien alle controles succesvol zijn verlopen wordt het authenticatieniveau bereikt passende bij het niveau van authenticeren (dit is afhankelijk van het element auhtnContextClassRef). De ZIM moet alle authenticatieniveau's kunnen ondersteunen.

Het is mogelijk dat er meerdere tokens zijn opgenomen in het bericht. Al deze tokens dienen afgehandeld te worden zoals in Figuur 1 is opgenomen en is beschreven in de [IH BA <toepassing>]



Figuur 1: Authenticeren o.b.v. SAML-token

5.1.2 Systeemauthenticatie o.b.v. servercertificaat t.b.v. initiërende systemen

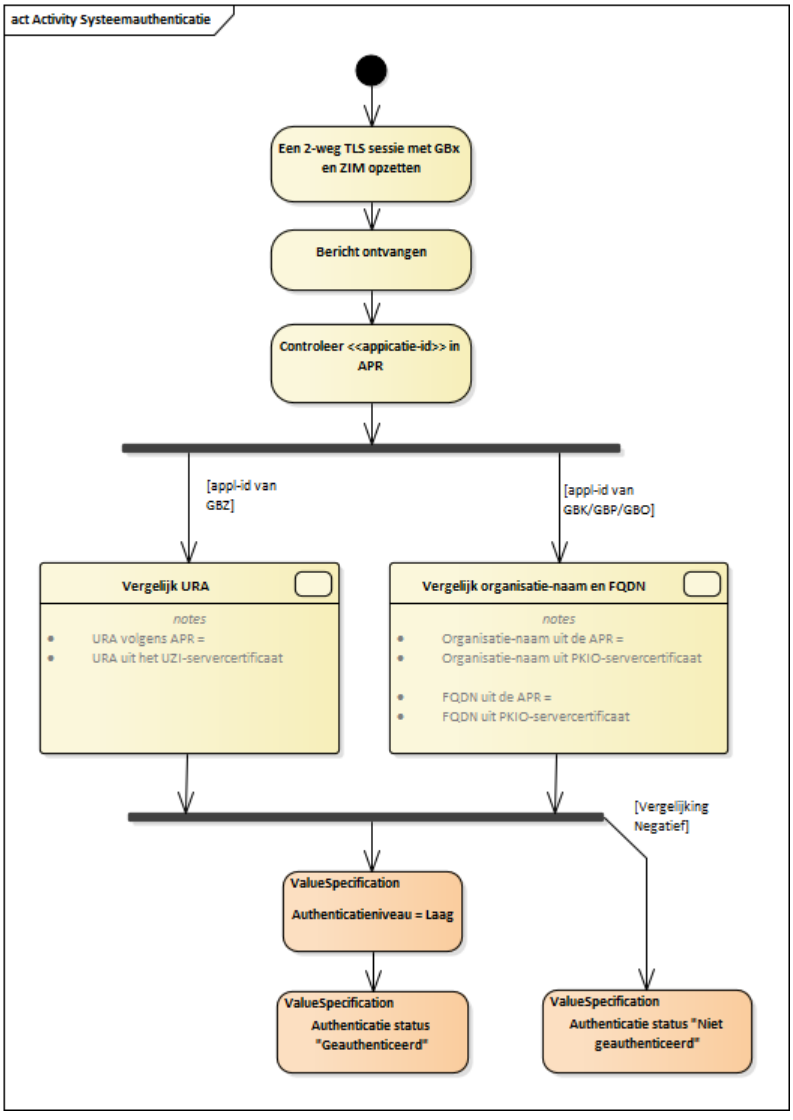
Initiërende systemen beslaan zowel de opvragende als de versturende systemen."

De IeA component authenticeert het servercertificaat met de controles zoals afgebeeld in Figuur 2: Systeemauthenticatie. Hierbij worden de volgende stappen doorlopen:

- Er wordt een 2-weg TLS sessie opgezet tussen GBX en ZIM op basis van hun eigen certificaten (UZI en/of PKIO);

- Er wordt via deze TLS-sessie een bericht ontvangen;
- De IeA component controleert dat de applicatie-id, genoemd als initiërend systeem in het bericht, bekend is binnen het applicatieregister (APR). In het APR worden de bijbehorende URA of Organisatie-naam en FQDN opgezocht.
- In het geval van een GBZ bericht wordt de uit het APR verkregen URA vergeleken met de URA van het UZI client servercertificaat van de TLS-sessie. Additioneel wordt bij een GBZ bericht de fully qualified domain name (FQDN) gecontroleerd en vergeleken met de in het APR aanwezige informatie.
- In het geval van een GBK/GBP/GBO/GBC/DVZA bericht wordt de uit het APR verkregen organisatienaam en FQDN vergeleken met respectievelijk de O (organisationName) en de FQDN uit het PKIoverheid servercertificaat van de TLS-sessie. Additioneel voor het GBK wordt gecontroleerd of het OU (organizationalUnitName) attribuut uit het PKIoverheid servercertificaat de juiste waarde bevat. Additioneel voor het GBP wordt het commonName (CN) attribuut gecontroleerd.

Indien authenticatie succesvol verloopt wordt authenticatieniveau "*Laag*" bereikt.



Figuur 2: Systeemauthenticatie

5.1.3 Systeemauthenticatie o.b.v. servercertificaat t.b.v. reagerende systemen

Ten behoeve van het adresseren van een bericht aan een systeem wordt er een beveiligde verbinding opgezet. Hierbij worden per systeem de volgende stappen doorlopen:

- Er wordt een 2-weg TLS sessie opgezet tussen ZIM en GBX op basis van hun eigen certificaten (UZI en/of PKIO);
- Er wordt via deze TLS-sessie een bevraging doorgestuurd naar het GBX;
- Via dezelfde TLS-sessie (synchrone communicatie) worden de gevraagde gegevens opgestuurd naar de ZIM;
- De IeA component controleert bij een reagerend bericht of de applicatie-id, genoemd als reagerend systeem in het bericht, bekend is binnen het applicatieregister (APR). In het APR worden de bijbehorende URA of Organisatie-naam en FQDN opgezocht;
- In het geval van een bericht afkomstig van een GBZ wordt de uit het APR verkregen URA vergeleken met de URA van het UZI client servercertificaat van de TLS-sessie. Additioneel wordt bij een GBZ bericht de fully qualified domain name (FQDN) gecontroleerd en vergeleken met de in het APR aanwezige informatie;
- In het geval van een bericht afkomstig van een GBO wordt de uit het APR verkregen organisatienaam en FQDN vergeleken met respectievelijk de O (organisationName) en de FQDN uit het PKIoverheid servercertificaat van de TLS-sessie. Additioneel voor het GBP wordt het commonName (CN) attribuut gecontroleerd.

Bovenstaande verwerking geldt ook voor ontvangende systemen. In plaats van het terugsturen van de gevraagde gegevens wordt er een ontvangstbevestiging of een inhoudelijk antwoord teruggestuurd.

5.2 Ondersteunende functies

5.2.1 ZIM identificeren

De Authenticatiecomponent levert de benodigde attributen om de ZIM te identificeren aan andere systemen waarmee (elektronische) verbindingen worden opgezet. Dit is met name van toepassing als een GBX een communicatieverbinding opzet met de ZIM en hierbij wordt in de tweeweg TLS handshake een certificaat gevraagd van de ZIM waarbij de fully qualified domain name (FQDN) gecontroleerd wordt. Of als de ZIM zelf een communicatieverbinding initieert en in de tweeweg TLS handshake zijn eigen certificaat voorziet.

De Authenticatiecomponent component is uitgerust om beheer te voeren over certificaten.

5.3 Beheerfuncties

Er zijn geen specifieke beheerfuncties.

6 Gegevensmodel

6.1 (Logisch) model van entiteiten en relaties

Deze component heeft een koppelvlak met de UZI-register LDAP.

Om performance redenen kan een lokale gegevensopslag van deze LDAP gehanteerd worden (zoals bijvoorbeeld de ZAB). Deze moet regelmatig ververst worden.

Een uitwerking van de datastructuur van deze LDAP is te raadplegen bij het UZI-register

[UZI LDAP datastructuur].

Tabel ZIM.IeA.t2070 Gegevensmodel

Attribuut	Definitie	Herkomst	Additionele informatie
UZI-register LDAP		UZI register	

6.2 Gegevensauthorisatiemodel

Er is geen gegevensauthorisatiemodel gedefinieerd voor dit component.

7 Configuratieaspecten

Voor het authenticatieproces van deze component zijn de volgende configuratie parameters van belang.

Tabel ZIM.IeA.t2080 Configuratieparameters

Configuratieparameter	Betekenis van parameter	Datatype
Max-geldigheidsduur-token[2]	De maximale tijdsduur dat een token geldig is. In het geval van de GBP stelt het GBP niet de geldigheidduur vast maar doet DigiD dat.	Tijd (min.)
ZIM-max-GBZ- gracetijd	tijd in seconden die van de ontvangen waarde *aanvang geldigheid* of *totdat geldigheid* in het token afgetrokken mag worden	Tijd (sec.)
ZIM-max-GBK-gracetijd	tijd in seconden die van de ontvangen waarde *aanvang geldigheid* of *totdat geldigheid* in het token afgetrokken mag worden	Tijd (sec.)
ZIM-max-BSN-gracetijd	tijd in seconden die van de ontvangen waarde *aanvang geldigheid* of *totdat geldigheid* in het token afgetrokken mag worden	Tijd (sec.)
ZIM-max-GBO-gracetijd	tijd in seconden die van de ontvangen waarde *aanvang geldigheid* of *totdat geldigheid* in het token afgetrokken mag worden	Tijd (sec.)

Deze parameters dienen centraal voor de authenticatiecomponent beschikbaar te zijn en zijn bepalend voor de geldigheid van een token. Een GBX geeft bij het produceren van een token, daaraan een geldigheidsperiode mee, met begintijd en eindtijd. Het GBX dient zich te houden aan de maximale tijd dat een token geldig mag zijn. Uiteraard mag een GBX een kortere geldigheidsduur vastleggen. Het is voor de authenticatiecomponent van belang om bij het authenticeren de geldigheidsduur van een token te controleren dat deze niet de maximale geldigheidsduur overschrijdt. Indien dit wel het geval is, is het token niet valide en dient de identiteit niet geauthenticeerd te worden.

Omdat er kleine tijdsverschillen kunnen ontstaan in verband met mogelijk onjuist gesynchroniseerde systeemklokken, of door de transporttijd van een bericht met token, is er een zeker gedoog periode ('Grace'-periode) waarbinnen de begin- en de eindtijd van het token mag fluctueren. Deze 'grace'-periode is voor GBZ, GBK en GBP afzonderlijk in te stellen.

NB: In het kader van de TLS-verbindingen, die feitelijk niet met deze component te maken hebben, zijn er meerdere configuratie parameters vastgesteld. Deze worden voor de compleetheid in Bijlage B: Bijlage B TLS-Sessie configuratieparameters benoemd.

[2] Hoewel een GBX zelf de geldigheidsduur van een token afgeeft, is het wel zaak dat er een uniform maximum gesteld wordt aan de geldigheid. Deze maximum waarde zal de authenticatiecomponent moeten kennen en zal overal gelijk ingesteld moeten worden.

8 Ontwerpaspecten ten behoeve van niet-functionele eisen

Uit oogpunt van *schaalbaarheid* kunnen er meerdere ZIM's zijn die ieder een eigen authenticatiecomponent hebben.

Uit oogpunt van *actualiteit* is het noodzakelijk dat de component met een regelmatige frequentie[3] de lijst met ingetrokken vertrouwensmiddelen (CRL) ophaalt van de uitgevende Certificate Authority (CA).

[3] De regelmatige frequentie is afhankelijk van de ververssnelheid van de lijst. Voor de UZI CRL is dit 3 uur.

9 Interne componentenstructuur en werking

9.1 Interne werking van technische onderdelen.

Voor de authenticatie zijn uit het gehele proces een aantal attributen benodigd. Van deze attributen wordt een vergelijking, een validatie en controle gedaan. Het is noodzaak dat de integriteit van deze attributen gewaarborgd is, alvorens de authenticatie goed kan plaatsvinden.

Een aantal attributen wordt verkregen op netwerkniveau aan de hand van de opgebouwde TLS-sessies (hierin worden certificaten gebruikt om te authenticeren en te versleutelen). En een aantal attributen wordt op applicatieniveau bepaald door de verwerking van het (HL7) bericht en meegestuurde tokens. Deze attributen moeten met elkaar vergeleken worden.

Het Patiënt-id dient voor berichten, waarbij de AttentionLine verplicht is, uit de transmissionwrapper (Attentionline) van het bericht gehaald te worden. Voor berichten waarbij de AttentionLine niet verplicht is dient het Patiënt-id uit de payload van het bericht gehaald te worden.

Bij implementatie zullen de technische onderdelen waaruit deze componenten intern worden opgebouwd, niet direct gekoppeld zijn in de verwerkingsketen. Hoogstwaarschijnlijk zullen ze niet naast elkaar staan en zijn ze verschillend geplaatst in de service centra.

Bij transport en opslag van identificerende gegevens is het van belang dat deze gegevens hun integriteit behouden. Dit kan hoge eisen stellen aan de beveiliging van transport en opslag van deze gegevens. Deze eisen worden voorgeschreven in de PvE's.

Voorbeeld:

De tijdelijke opslag van een URA nummer afkomstig van een TLS-sessie. Dit URA nummer wordt later in het authenticatieproces vergeleken met het URA nummer uit het HL7 bericht.

Dit URA nummer mag tussentijds niet gewijzigd kunnen worden.

Interne versleuteling tijdens transport en opslag zijn dan mogelijke oplossingen.

10 Procedurele beheersaspecten

Geen specifieke aspecten.

Bijlage A Referenties

Tabel ZIM.IeA.t2090 Referenties

Referentie	Document	Versie
[CP PKIO]	Programma van Eisen PKIO, deel 3: Certificate Policies; Logius, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties; http://www.logius.nl/producten/toegang/pkioverheid/aansluiten/programma-van-eisen/	3.0
[CPS PKIO]	CPS Policy Authority PKIoverheid; Logius, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties; http://www.logius.nl/producten/toegang/pkioverheid/documentatie/cps/	3.3
[CPS UZI]	Certification Practice Statement (CPS); CIBG, agentschap van het Ministerie van Volksgezondheid, Welzijn en Sport; https://www.uzi-register.nl/cps/cps.html	4.2
[IH BA PKIO-pas]	Implementatiehandleiding berichtauthenticatie met PKIO-pas	8.4.0.0
[IH BA DigiD]	Implementatiehandleiding berichtauthenticatie met DigiD	8.4.0.0
[IH BA TRANS]	Implementatiehandleiding berichtauthenticatie met Transactietoken	8.4.0.0
[IH BA MAN]	Implementatiehandleiding berichtauthenticatie met Mandaattoken	8.4.0.0
[IH INSCHRIJF]	Implementatiehandleiding inschrijftoken	8.4.0.0
[UZI LDAP datastructuur]	*Toelichting release 2.1 LDAP datastructuur*; CIBG, agentschap van het Ministerie van Volksgezondheid, Welzijn en Sport; Den Haag, 2008	1.2

Bijlage B TLS-Sessie configuratieparameters

Ten behoeve van het opzetten en configureren van de TLS-sessie die de ZIM hanteert zijn de volgende configuratie paramaters gesteld.

Tabel ZIM.IeA.t2100 Configuratieparameters TLS-sessies

Configuratieparameter	Betekenis van parameter	Datatype	Domein (mogelijke waarden)
gebruiker-max- sleutel-duur*	Maximum duur dat tijdelijke TLS-sleutel gebruikt mag worden, waarna deze ververst moet worden.		5 minuten
gebruiker-max-sessie-duur*	Maximum duur van TLS-sessie tussen gebruiker en ZIM, voordat sessie wordt beëindigd.		8 uur
gebruiker-max-sessie-onbruik*	Maximum duur dat een TLS-sessie tussen gebruiker en ZIM niet gebruikt wordt, voordat sessie wordt beëindigd.		30 minuten
systeem-max-sleutel-duur*/**	Maximum duur dat een tijdelijke TLS-sleutel gebruikt mag worden, waarna deze ververst moet worden.		5 minuten
systeem-max-sessie-duur*/**	Maximum duur van een TLS-sessie tussen dossier/postbus en ZIM, voordat de sessie wordt beëindigd.		8 uur
systeem-max-sessie-onbruik*/**	Maximum duur dat een TLS-sessie tussen dossier/postbus en ZIM niet gebruikt wordt, voordat de sessie wordt beëindigd.		15 minuten
gebruiker-max-sessie-duur ***	maximum duur van sessie tussen gebruiker en GBK/GBP, voordat sessie wordt beëindigd.		1 uur
gebruiker-max-sessie-onbruik ***	maximum duur dat een sessie tussen gebruiker en GBK niet gebruikt wordt, voordat sessie wordt beëindigd.		15 minuten
systeem-max-sleutel-duur ***	maximum duur dat een tijdelijke TLS-sleutel gebruikt mag worden, waarna deze ververst moet worden.		5 minuten
systeem-max-sessie-onbruik ***	maximum duur dat een TLS-sessie tussen GBK/GBP en ZIM niet gebruikt wordt, voordat de sessie wordt beëindigd.		15 minuten

* parameters in te stellen door het GBZ

** parameters in te stellen door de ZIM

*** parameter in te stellen door GBP of GBK