< IH Mandaattoken

Datum: 7 oktober 2020
Publicatie: V8.2.0.0

Inhoudsopgave

1 Inleiding

1.1 Doel en scope

Dit document betreft een specificatie van het mandaattoken. Het betreft hier een mandaattoken voor gebruik bij communicatie tussen het goed beheerde Zorgsystemen (GBZ) en het landelijk schakelpunt (LSP).

1.2 Doelgroep voor dit document

Dit document is bedoeld voor softwareontwikkelaars van goed beheerde zorgsystemen en het LSP, die op grond van de HL7v3 communicatiestandaard en op grond van dit document berichten willen uitrusten met het SAML mandaattoken. Daarnaast wordt het plaatsen van de digitale handtekening besproken (zie ook [IH tokens generiek]).

1.3 Documenthistorie

Versie	Datum	Omschrijving
8.0.2.0	31-januari-2018	Initieel document.
8.0.3.0	1-juli-2018	INI-8462: Plaatsing Mandaattoken naast het Transactietoken
8.0.3.0	1-jan-2019	INI-8769: Verduidelijken <security>-header
8.0.3.0	1-jan-2019	INI-8771: Aanpassen controle geldigheid Mandaattoken
8.0.3.0	1-jan-2019	INI-8754: Uitbreiden voorbeeld m.b.t. verwijzing naar certificaatgegevens en verwijzing naar het juiste certificaat met keyUsage non-repudiation (0x40)
8.2.0.0	7-okt-2020	Controle op overseer in hoofstuk 5.1 aangepast.

2 Het SAML mandaattoken

In dit hoofdstuk wordt de inhoud van het SAML mandaattoken besproken die bij mandatering en de berichtauthenticatie met behulp van de UZI-pas wordt gebruikt. Het SAML mandaattoken bevat informatie over de mandaatgever in relatie tot de gemandateerde zorgmedewerker. Het SAML mandaattoken is een op XML gebaseerd SAML assertion en heeft tot doel de *assertions* (bewijs van een bewering) over te brengen tussen partijen.

Alle XML voorbeelden in het document dienen door de betrokken partijen tijdens het bouwen van de uitwisseling getest, en waar nodig, in samenspraak met VZVZ aangepast te worden voor een juiste optimale werking.

Voor het verkrijgen van het SAML mandaattoken en het aanbieden van dit token aan het LSP worden de volgende profielen gebruikt:

- Het gebruik van het SAML mandaattoken (security token) in het kader van het WSS SOAP berichten profiel voor het veilig stellen en uitwisseling van authentieke SOAP berichten.

Dit profiel raakt het koppelvlak:

- goed beheerd zorgsysteem (GBZ) – het landelijk schakelpunt (LSP)

Dit profiel wordt in de volgende paragrafen verder uitgewerkt.

2.1 Structuur

Het SAML mandaattoken is een afgegeven SAML assertion die gebruikt wordt bij mandatering en berichtauthenticatie met behulp van de UZI-pas voor het landelijk EPD. Er wordt gebruik gemaakt van SAML v2.0 [SAML Core].

2.1.1 Assertion

De assertion heeft de volgende structuur (de waarden die in het token gebruikt worden zijn fictief):

Element/@Attribute	0..1	Omschrijving
@ID	1	Unieke identificatie van de Assertion
@Version	1	Versie van het SAML Protocol. Vaste waarde moet zijn 2.0
@IssueInstant	1	Tijdstip van registratie van het mandaat.
Issuer	1	De zorgverlener die het mandaat afgeeft.
@NameQualifier	0	Niet gebruiken
@SPNameQualifier	0	Niet gebruiken
@Format	1	Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"
@SPProviderID	0	Niet gebruiken
Signature	1	Bevat de handtekening over de assertion zoals gezet met behulp van de UZI pas van de zorgverlener die het mandaat verleent (de mandaterende). De handtekening dient geplaatst te zijn met behulp van het handtekening-certificaat op de pas.
Subject	1	Bevat de Organisatie (URA) waarbinnen het mandaat geldig is.

Element/@Attribute	0..1	Omschrijving
BaseID	0	Niet gebruiken
NameID	1	Bevat de URA
EncryptedID	0	Niet gebruiken
SubjectConfirmation	1	Moet aanwezig zijn
@Method	1	'urn:oasis:names:tc:SAML:2.0:cm:sender-vouches'
SubjectConfirmationData	0	Niet gebruiken
@Recipient	0	Niet gebruiken
@NotOnOrAfter	0	Niet gebruiken
@InResponseTo	0	Niet gebruiken
@NotBefore	0	Niet gebruiken
@Address	0	Niet gebruiken
KeyInfo	0	Niet gebruiken
Conditions	1	Moet aanwezig zijn
@NotBefore	1	Moet aanwezig zijn.
@NotOnOrAfter	1	Moet aanwezig zijn.
Condition	0	Niet gebruiken
AudienceRestriction	1	Moet aanwezig zijn
Audience	1	urn:IIroot:2.16.840.1.113883.2.4.6.6:IIext:1 (is de ZIM)
AudienceRestriction	1	Moet aanwezig zijn
Audience	1	urn:IIroot:2.16.840.1.113883.2.4.6.6:IIext:<AppId> (is de verzendende GBZ-applicatie)
ProxyRestriction	0	Niet gebruiken
Advice	0	Niet gebruiken
AuthnStatement	0	Niet gebruiken
AttributeStatement	1	Moet aanwezig zijn
Attribute	1	Moet aanwezig zijn
@Name	1	Vaste waarde: "autorisatieregel/context"
AttributeValue	1	URI waar de autorisatieregel/context gevonden kan worden waarbinnen het mandaat gegeven wordt.

N.B.: bovenstaande tabel bevat de meest gebruikte elementen van SAML assertions en is derhalve niet volledig. Voor niet genoemde elementen geldt: Niet gebruiken.

2.2 Namespaces

Het SAML mandaattoken maakt gebruik van de volgende namespaces. De prefixen zijn niet normatief maar worden in dit document als voorbeelden gebruikt.

Tabel AORTA.STK.t3300 – Namespaces

Prefix	Namespace URI

ds	http://www.w3.org/2000/09/xmldsig#
saml	urn:oasis:names:tc:SAML:2.0:assertion
wss	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd

Bij het gebruik van de namespace-prefixes is het van belang deze na het ondertekenen niet meer te veranderen, dit maakt de digitale handtekening ongeldig.

2.3 Inhoud

De volgende paragrafen beschrijven de verschillende kenmerken en beveiligingsgerelateerde gegevens die het SAML mandaattoken onderscheiden, zoals in [IH tokens generiek] beschreven is.

```
<saml:Assertion ... xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
```

Het SAML mandaattoken begint met het Assertion element en een verwijzing naar de XML SAML namespace voor SAML 2.0 assertions. De attributen behorende bij het Assertion element wordt in paragraaf 2.3.1 Uniekheid beschreven.

2.3.1 Uniekheid

```
ID="token_2.16.528.1.1007.3.3.1234567.1_0123456789"
IssueInstant="2009-06-24T11:47:34Z"
Version="2.0">
```

De volgende attributen van het SAML assertion element maken van de SAML assertion een uniek gegeven, uitgegeven door de verzender van het bericht. Het attribuut ID identificeert op een unieke wijze de assertion. De assertion mag meerdere malen als token gebruikt worden. De waarde moet *mondiaal uniek* zijn voor AORTA berichten, zodat bij samenvoegen van meerdere XML bestanden (in een HL7v3 batch of anderszins) de waarde uniek blijft.

Het wordt aanbevolen een UUID (Universally Unique Identifier)[1] te gebruiken. Bij het gebruik van andere vormen is er een kans, hoe klein ook, dat een ID samenvalt met een ID gemaakt volgens een andere methode van een andere leverancier).

Een ID in XML mag niet met een cijfer beginnen. Bij het gebruik van een UUID is het dus aan te raden een prefix te gebruiken, welke met een letter of underscore ('_') begint.

Het attribuut IssueInstant is een tijdsmoment van uitgifte van de SAML assertion, in andere woorden: het tijdstip van ondertekening. De tijdswaarde is gecodeerd in UTC. Het attribuut Version is de gebruikte SAML versie van de SAML assertion. De aanduiding voor de versie van SAML gedefinieerd in deze specificatie is "2.0".

[1] Zie het RfC4122 opgesteld door het IETF: A Universally Unique Identifier (UUID) URN Namespace

2.3.2 Afzender

```
<saml:Issuer>
  123456789:01.015
</saml:Issuer>
```

De `Issuer` verwijst naar de UZI van de zorgverlener/medewerker die het mandaat registreert (de mandaatgever) in combinatie met de rolcode van diezelfde zorgverlener/medewerker gescheiden door een dubbele punt (:).

2.3.3 Onderwerp

```
<saml:Subject>
  <saml:NameID>
     urn:IIroot:2.16.528.1.1007.3.3:IIext:12345678
  </saml:NameID>
  <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:sender-vouches">
  </saml:SubjectConfirmation>
</saml:Subject>
```

De `Subject` verwijst naar de organisatie waarbinnen het mandaat geldig is.

De URA wordt uitgedrukt met behulp van een URN (Uniform Resource Name). De URN is opgebouwd uit:

```
"urn:IIroot:"<OID voor UZI organisatieIds>":IIext:"<URA>
```

De URN string is opgebouwd uit een IIroot en een IIext. "II" staat voor het HL7v3 datatype Instance Indentifier. Om de namespace in URN uniek te krijgen is II als prefix voor de root en ext geplaatst.

URA's worden uitgedrukt als een id onder het identificatiesysteem "2.16.528.1.1007.3.3". De URA wordt toegekend door het UZI-register. Stel dat de URA de waarde "12345678" heeft, dan ziet de URN er als volgt uit:

`urn:IIroot:`2.16.528.1.1007.3.3`:IIext:`12345678

Vervolgens moet de SubjectConfirmation nog toegevoegd worden:

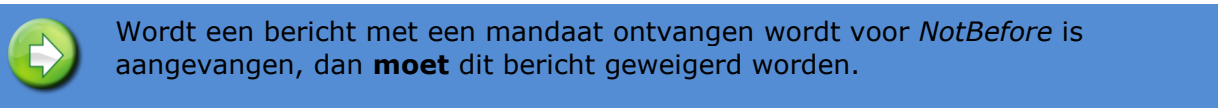
```
  <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:sender-vouches">
  </saml:SubjectConfirmation>
```

2.3.4 Geldigheid

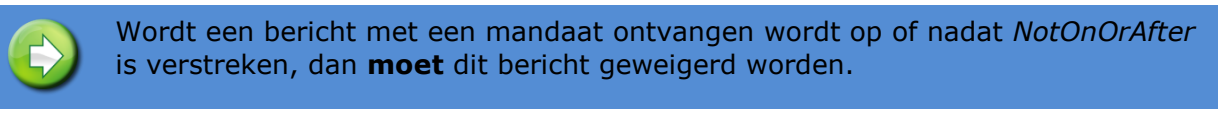
```
<saml:Conditions
 NotBefore="2009-06-24T11:47:34Z"
 NotOnOrAfter="2009-09-24T11:47:34Z">
```

Het attribuut *NotBefore* is de tijd waarop de SAML assertion geldig wordt. Dit hoeft niet de tijd te zijn waarop het mandaat is aangemaakt. Het is mogelijk *NotBefore* in de

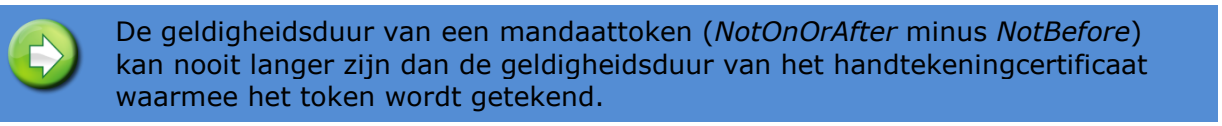
toekomst te zetten. NotBefore moet altijd op of na de aanvang van de geldigheidsdatum van het certificaat (waarmee het mandaat is getekend) liggen.



Het attribuut *NotOnOrAfter* is de tijd waarop de SAML assertion vervalt. *NotOnOrAfter* moet altijd voor het verstrijken van de geldigheid van het certifcaat (waarmee het mandaat is getekend) liggen.

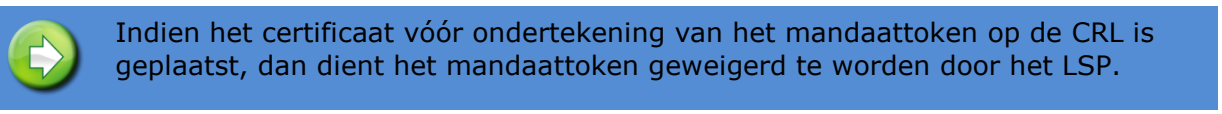


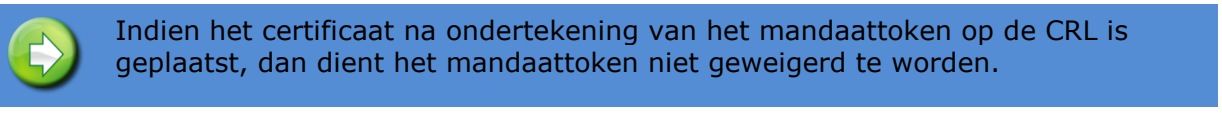
Deze tijd is als bovenstaande tijd geformatteerd. Richtlijn voor het verschil tussen *NotBefore* en *NotOnOrAfter* is niet vastgesteld.



Indien het certificaat waarmee het mandaat is getekend op de CRL is geplaatst, dan dient het mandaattoken niet geweigerd te worden door het LSP. Het is op de CRL niet inzichtelijk om welke reden een certificaat op de CRL is geplaatst. Dit kunnen uiteenlopende redenen zijn zoals een verloren pas of een intrekking van een BIG-registratie. Om het zorgproces niet te frustreren wordt deze controle procesmatig opgepakt door Security Management.

Echter, bij het ondertekenen van het mandaattoken moet er een geldig certificaat gebruikt worden. Indien bij ondertekening van het mandaattoken het certificaat al op de CRL is geplaatst, dan dient het mandaattoken wel geweigerd te worden.





Het inperken van bepaalde partijen (`AudienceRestriction`) waarvoor de assertion bedoeld is wordt beschreven in paragraaf 2.3.5 Ontvanger.

De subelementen `OneTimeUse` en `ProxyRestriction` worden niet gebruikt binnen het `<Conditions>` element bij het mandaattoken.

2.3.5 Ontvanger

In de `AudienceRestriction` wordt beschreven aan wie de SAML assertion is gericht. Aangezien het mandaattoken bedoeld is voor gebruik door een verzendende applicatie en bedoeld is om door de ZIM begrepen te worden, worden er binnen de `AudienceRestriction` twee `Audience` elementen opgenomen, één voor de ZIM en één voor de verzendende GBZ-applicatie.

Het applicatie-id binnen de `AudienceRestriction` wordt uitgedrukt met behulp van een URN (Uniform Resource Name). De URN is opgebouwd uit:

```
"urn:IIroot:"<OID voor AORTA Applicatie-id's>":IIext:"<applicatie-id GBZ>
```

De URN string is opgebouwd uit een IIroot en een IIext. "II" staat voor het HL7v3 datatype Instance Indentifier. Om de namespace in URN uniek te krijgen is II als prefix voor de root en ext geplaatst.

AORTA Applicatie-id's worden uitgedrukt als een id onder het identificatiesysteem "2.16.840.1.113883.2.4.6.6". Het correcte applicatie-id voor het GBZ wordt toegekend bij aansluiting op de AORTA. Stel dat dit "300" zou zijn, dan ziet de URN er als volgt uit:

`urn:IIroot:`2.16.840.1.113883.2.4.6.6`:IIext:`300

De volledige `AudienceRestriction` wordt dan:

```
<saml:AudienceRestriction>
  <!-- Root en extensie van de ZIM -->
  <saml:Audience>urn:IIroot:2.16.840.1.113883.2.4.6.6:IIext:1</saml:Audience>
  <!-- Root en extensie van de Applicatie -->
  <saml:Audience>urn:IIroot: 2.16.840.1.113883.2.4.6.6:IIext:300</saml:Audience>
</saml:AudienceRestriction>
```

2.3.6 Attributen

```
<saml:AttributeStatement>
```

Het volgende attribuut betreft aanvullende gegevens met betrekking tot het mandaat. Er mogen geen andere attributen opgenomen worden in het AttributeStatement dan hier beschreven is.

```
<saml:Attribute Name="autorisatieregel/context">

<saml:AttributeValue>https://goedbeheerdziekenhuis/autorisatieregels/medicatieconte
xt/v2</saml:AttributeValue>
</saml:Attribute>
```

Via de URI dient de lokale autorisatieregel en/of de context opgehaald te kunnen worden waarbinnen het mandaat is uitgegeven. In het voorbeeld is voor een URL gekozen.

Tenslotte wordt het attributen statement blok afgesloten met

```
</saml:AttributeStatement>
```

2.4 Algoritmes

Om de integriteit en onweerlegbaarheid van het SAML mandaattoken te waarborgen wordt een XML Signature geplaatst, zoals beschreven in [IH tokens generiek]. Na plaatsen van de XML Signature kan de ontvanger, met gebruikmaking van de publieke sleutel van het UZI handtekening-certificaat van de verzender onomstotelijk vaststellen dat de getekende SAML assertion ondertekend is met de privé sleutel behorend bij het gebruikte UZI handtekening-certificaat van de UZI-pas van de zorgverlener.

De publieke sleutel van het UZI handtekening-certificaat bevindt zich in de LDAP van het het UZI- register.

De XML Signature van het SAML mandaattoken die gebruikt wordt bij berichtauthenticatie met behulp van de UZI-pas maakt gebruik van de volgende algoritmes, zoals beschreven in [IH tokens generiek]:

- Voor het berekenen van de hashwaarde wordt SHA-256 gebruikt.
- Voor de digitale handtekening in AORTA wordt gebruik gemaakt van een RSA handtekening over een SHA-256 digest.

Omdat de XML Signature onderdeel is van het SAML mandaattoken en in het SAML mandaattoken geplaatst wordt, moet er een "enveloped-signature" transformatie uitgevoerd worden die de Signature tags uit het SAML authenticatietoken verwijderd gevolgd door een “exc-c14n transformatie” (zie ook [SAML Core] §5.4.3 en §5.4.4).

2.5 Opbouw

2.5.1 De headers

Eerst wordt het SAML mandaattoken – het `<saml:Assertion ...>` element aangemaakt en gevuld met die elementen, zoals beschreven in paragraaf 2.3 Inhoud.

```
<saml:Assertion
   ID="token_2.16.528.1.1007.3.3.1234567.1_0123456789"
   IssueInstant="2009-06-24T11:47:34Z"
   Version="2.0"
   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
 ... Zie paragraaf 2.3 Inhoud ...
</saml:Assertion>
```

Het XML Signature blok is onderdeel van het SAML mandaattoken. Het XML Signature blok komt na het `<saml:Issuer>` element.

```
<saml:Assertion
   ID="token_2.16.528.1.1007.3.3.1234567.1_0123456789"
   IssueInstant="2009-06-24T11:47:34Z"
   Version="2.0"
```

```
   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
  <saml:Issuer>
   123456789:01.015
  </saml:Issuer>
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
    ...
    </ds:SignedInfo>
    <ds:SignatureValue>Wuwn...5e4=</ds:SignatureValue>
    <ds:KeyInfo>
      <ds:X509Data>
        <X509IssuerSerial>
          <X509IssuerName>CN=De Auteur CA,O=Nictiz,C=NL</X509IssuerName>
          <X509SerialNumber>359724...41160195</X509SerialNumber>
        </X509IssuerSerial>
      </ds:X509Data>
    </ds:KeyInfo>
  </ds:Signature>  ...
  ... Zie paragraaf 2.3 Inhoud ...
</saml:Assertion>
```

Indien de Signature aangemaakt wordt mogen de strings (saml:Assertion en SignedInfo) inhoudelijk niet meer gewijzigd worden. Ze moeten octet-voor-octet overgenomen worden in het bericht. Strikt genomen is het toegestaan wijzigingen aan te brengen die door canonicalisatie bij de ontvanger weer opgeheven worden, maar wanneer de digitale handtekening door middel van strings wordt opgebouwd, is het een foutgevoelige handeling.

Lange Base 64 waarden zijn afgekort. Wederom kunnen dit als strings worden behandeld, waarbij drie waarden vervangen moeten worden.

Deze drie waarden worden ingevuld:

- Neem het SignedInfo blok op.
- Neem de SignatureValue op.
- Neem certificaatgegevens in het KeyInfo blok op.

Wanneer een bericht een SAML assertion bevat, moet dat bericht precies één bijbehorende digitale handtekening bevatten.

Voor mandaattokens mag er niet meer dan één SAML assertion voorkomen met de gegevens van een daarbij behorende X.509 certificaat als KeyInfo.

Het maken van de XML Signature uit strings levert de SAML assertion op met daarin de Signature.

2.5.2 Plaats van het SAML token en de digitale handtekening

Het SAML authenticatietoken met daarin de digitale handtekening wordt in het WS-Security SOAP Header gezet. Deze dient altijd te bestaan als aparte SAML-assertion naast het Transactietoken [IH Transactietoken].

Het mandaattoken dient tezamen met het transactietoken ([IH transactietoken]) in het zelfde security-element opgenomen te zijn conform de [IH tokens generiek] hoofdstuk 5.1.

3 Compliancy

Bij het opstellen van dit document is onder andere gekeken naar de volgende specificaties:

IHE XUA

Binnen het Integrating the Healtcare Enterprise (IHE) Cross Enterprise User Authentication (XUA) profiel wordt in transactie ITI-40 Provide X-user Assertion de SAML-assertion beschreven.

Idensys

In het Nederlandse Afsprakenstelsel Elektronische Toegangsdiensten wordt binnen de interface specificatie tussen HerkenningsMakelaar en de Dienstverlener de Assertion van de Herkenningsmakelaar beschreven. Idensys maakt gebruik van vergelijkbare SAML elementen met uitzondering van het SubjectID welke, binnen Idensys, wordt weergegeven door een encryptedID.

4 Certificaten

4.1 Te gebruiken certificaat en attributen

Voor het tekenen van het Mandaattoken wordt het **handtekening**certificaat van de persoonlijke UZI-pas gebruikt. Dit certificaat bevat een RSA publieke sleutel. Met de privé sleutel wordt de digitale handtekening gegenereerd. Voor de technische context en het feitelijk genereren van de digitale handtekening met een UZI-pas wordt verwezen naar respectievelijk Bijlage B en Bijlage C uit het document IH Berichtauthenticatie met UZI-Pas [UZI berichttoken] met dien verstande dat in het mandaattoken dus het **handtekening**certificaat[2] wordt gebruikt in plaats van het in de bijlagen vermelde authenticatiecertificaat.

Om de digitale handtekening bij de ZIM te verifiëren, moet de ontvanger over de bijbehorende publieke sleutel beschikken, zie [IH tokens generiek]. Voor verificatie is gekozen door een verwijzing naar het handtekeningcertificaat in het SAML mandaattoken als KeyInfo mee te zenden; de ontvanger moet deze dan met bijvoorbeeld het LDAP protocol ophalen, zie ook [IH tokens generiek].

[2] Technisch dus het certificaat met keyUsage non-repudiation (0x40).

5 Token afhandeling

5.1 Verificatie van het mandaattoken

Het is belangrijk vast te stellen dat de velden in het SAML mandaattoken overeenstemmen met die in het transactietoken en geldig ondertekend zijn. Wanneer dit niet zou gebeuren, kan een kwaadwillende met een gestolen mandaattoken nog steeds gegevens opvragen.

Het SAML mandaattoken wordt door de ontvanger uit het transactietoken gehaald indien aanwezig. Bij gebruik van het SAML mandaattoken moet de ontvanger controleren of:

- De aanduiding voor de versie van SAML gedefinieerd is op "2.0", zie paragaaf 2.3.1 Uniekheid;
- De URA, weergegeven door de NameID van het Subject, moet overeenkomen met de URA binnen het transactietoken en de URA uit het servercertificaat waarmee de TLS-verbinding is opgezet, zie paragraaf 2.3.3 Onderwerp;
- Het bericht ontvangen is binnen de geldigheidsperiode van het token, zie paragraaf 2.3.4 Geldigheid;
- De Assertion correct is ondertekend door de Signature te valideren met het gerefereerde handtekening certificaat.
- Het certificaat waarmee de ondertekening heeft plaatsgevonden geldig was ten tijde van de ondertekening.
- De juiste afzender (issuer) is vastgelegd die deze assertion heeft gecreëerd en ondertekend, zie paragraaf 2.3.2 Afzender. De UZI en rolcode dienen overeen te komen met de bijbehorende waarden uit het UZI-certificaat van de mandaatgever. Die waarden dienen tevens overeen te komen met de Overseer in het HL7v3 bericht;
- De afnemers van het SAML mandaattoken (audience) de ZIM en de verzendende applicatie zijn, zie paragraaf 2.3.5 Ontvanger;
- De als audience opgenomen applicatie moet geregistreerd zijn bij de URA uit het Subject.
- Alleen die attributen zijn gedefinieerd, die zijn beschreven in paragraaf 2.3.6 Attributen;
- Indien Conditionele Query: de overseer in het HL7-bericht moet gelijk zijn aan het eerste gedeelte van de issuer (UZI) in het mandaattoken. Tevens dient het tweede gedeelte van de issuer (de rolcode) in het mandaattoken vergeleken te worden met de rolcode van de overseer in het HL7 bericht;

Het mandaattoken mag meerdere malen gebruikt worden. Het attribuut ‘autorisatieregel/context’ kan niet door de ZIM gecontroleerd worden maar dient wel in de log van de ZIM opgenomen te worden.

Als aan één van de bovenstaande condities niet is voldaan, moet het bericht door de ontvanger geweigerd worden en een SOAP foutmelding aan het verzendende systeem afgegeven worden, zie foutafhandeling in [IH tokens generiek].

Als wel aan alle condities is voldaan, wordt het HL7v3 bericht verder verwerkt.

Bijlage A Referenties

Referentie	Document	Versie
[IH tokens generiek]	Implementatiehandleiding security tokens generiek	8.2.0.0
[IH transactietoken]	AORTA_Auth_IH_Berichtauthenticatie_Transactietoken	8.2.0.0
[SAMLAuthnContext]	Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0 http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf	2.0 15-mrt-2005
[SAML Core]	SAML v2.0 Core Specification https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf	2.0 15-mrt-2005
[SAML Profiles]	Profiles for the OASIS Security Assertion Markup Language (SAML) v2.0 http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf	2.0 15-mrt-2005
[SAML Token]	SAML Token Profile http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SAMLTokenProfile.pdf	1.1 01-feb-2006
[UZI pas]	CA model, Pasmodel, Certificaat- en CRL-profielen, Agentschap CIBG www.uziregister.nl	4.1 september 2010