# < IH inschrijftoken

Datum: 1 oktober 2019
Publicatie: V8.1.0.0

# Inhoudsopgave

# 1 Inleiding

## 1.1 Doel en scope

Dit document heeft tot doel een handleiding te geven voor de implementatie van het koppelvlak tussen het goed beheerde Zorgsystemen (GBZ) en het landelijk schakelpunt (LSP) voor wat betreft de toe te passen technieken voor de authenticatie van zorgverleners en medewerkers.

## 1.2 Doelgroep voor dit document

Dit document is bedoeld voor softwareontwikkelaars van goed beheerde zorgsystemen en het LSP, die op grond van de HL7v3 communicatiestandaard en op grond van dit document berichten willen uitrusten met het SAML inschrijftoken. Het SAML inschrijftoken is met name vereist bij gebruik van een conditionele query.

Daarnaast wordt in dit document het plaatsen van de digitale handtekening besproken (zie ook [IH tokens generiek]).

## 1.3 Documenthistorie

| Versie | Datum | Omschrijving |
|---|---|---|
| v8.1.0.0 | 21-juli-2019 | Initieel document. |
| | | |
| | | |

# 2 Het SAML inschrijftoken

In dit hoofdstuk wordt de inhoud van het SAML inschrijftoken besproken. Het SAML inschrijftoken bevat de, binnnen een zorgorganisatie, gevalideerde BSN en is ondertekend door een zorgverlener/medewerker. Het SAML inschrijftoken is een op XML gebaseerde SAML assertion en heeft tot doel de *assertions* (bewijs van een bewering) over te brengen tussen partijen.

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

## 2.1 Structuur

Het SAML inschrijftoken is een afgegeven SAML assertion met betrekking tot de gevalideerde BSN die gebruikt wordt bij berichtauthenticatie voor het landelijk EPD. Het SAML inschrijftoken is ondertekend met behulp van een UZI-pas van een zorgverlener/medewerker. Er wordt gebruik gemaakt van SAML v2.0 [SAML Core].

## 2.2 Assertion

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

| Element/@Attribute | 0..1 | Omschrijving |
|---|---|---|
| @ID | 1 | Unieke identificatie van de Assertion |
| @Version | 1 | Versie van het SAML Protocol. Vaste waarde moet zijn 2.0 |
| @IssueInstant | 1 | Tijdstip van uitgifte van de Assertion. |
| Issuer | 1 | De URA van de zorgaanbieder organisatie waarbinnen de face to face controle heeft plaatsgevonden |
| @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 (Z) of de UZI medewerkerpas van de medewerker (N). De handtekening dient geplaatst te zijn met behulp van het authenticatie certificaat op de pas. |
| Subject | 1 | BSN van de patient waarvan de BSN gevalideerd is. |
| BaseID | 0 | Niet gebruiken |
| NameID | 1 | Bevat de gevalideerde BSN. |
| EncryptedID | 0 | Niet gebruiken |
| 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 |

| Element/@Attribute | 0..1 | Omschrijving |
|---|---|---|
| @NotOnOrAfter | 0 | Niet gebruiken |
| @InResponseTo | 0 | Niet gebruiken |
| @NotBefore | 0 | Niet gebruiken |
| @Address | 0 | Niet gebruiken |
| KeyInfo | 1 | Bevat de X509 Issuer.serial van de medewerkerspas of zorgverlenerpas. |
| Conditions | 1 | Moet aanwezig zijn. |
| @NotBefore | 1 | Moet aanwezig zijn. |
| @NotOnOrAfter | 1 | Moet aanwezig zijn. Mag maximaal 1,5 jaar na @NotBefore liggen. |
| Condition | 0 | Niet gebruiken |
| AudienceRestriction | 1 | Moet aanwezig zijn |
| Audience | 1..* | Minimaal 1 element: urn:IIroot:2.16.840.1.113883.2.4.6.6:IIext:1 (is de ZIM). Meerdere audiences zijn toegestaan. |
| ProxyRestriction | 0 | Niet gebruiken |
| Advice | 0 | Niet gebruiken |
| AuthnStatement | 1 | Moet aanwezig zijn |
| @AuthnInstant | 1 | Tijdstip van BSN validatie. |
| @SessionIndex | 0 | Niet gebruiken |
| AuthnContext | 1 | Moet aanwezig zijn |
| AuthnContextClassRef | 1 | urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI |
| AttributeStatement | 1 | Moet aanwezig zijn |
| Attribute | 1 | Moet aanwezig zijn. |
| @Name | 1 | Vaste waarde: “WID Controle Root” |
| AttributeValue | 1 | Root van de MessageID van de WID controle |
| Attribute | 1 | Moet aanwezig zijn. |
| @Name | 1 | Vaste waarde: “WID Controle Extensie” |
| AttributeValue | 1 | Extensie van de MessageID van de WID controle |
| Attribute | 1 | Moet aanwezig zijn. |
| @Name | 1 | Vaste waarde: “SBV-Z Controle Root” |
| AttributeValue | 1 | Root van de MessageID van de SBV-Z controle |
| Attribute | 1 | Moet aanwezig zijn. |
| @Name | 1 | Vaste waarde: “SBV-Z Controle Extensie” |
| AttributeValue | 1 | Extensie van de MessageID van de SBV-Z controle |
| Attribute | 1 | Moet aanwezig zijn. |
| @Name | 1 | Vaste waarde: “Uitvoerder” |
| AttributeValue | 1 | De UZI van de zorgverlener of medewerker die het token heeft ondertekend. |

| Element/@Attribute | 0..1 | Omschrijving |
|---|---|---|
| | | |

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

## 2.3 Namespaces

Het SAML inschrijftoken die gebruikt wordt bij berichtauthenticatie maakt gebruik van de volgende namespaces. De prefixen zijn niet normatief maar worden in dit document als voorbeelden gebruikt.

**Tabel AORTA.STK.t3300 – Namespaces**

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

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

## 2.4 Inhoud

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

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

Het SAML inschrijftoken begint met het Assertion element en een verwijzing naar de XML SAML namespace voor SAML 2.0 assertions. De attributen behorende bij het Assertion element wordt in paragraaf 2.4.1 Uniekheid beschreven.

### 2.4.1 Uniekheid

```
ID="token_dd1c1f96-f0b0-4026-a978-4d724c0a0a4f"
IssueInstant="2009-06-24T11:47:34Z"
Version="2.0">
```

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

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

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

Het attribuut IssueInstant is een tijdsmoment van uitgifte van de SAML assertion. De tijdswaarde is gecodeerd in UTC. Het attribuut Version is de gebruikte SAML versie van de SAML assertion. De aanduiding voor de versie van SAML gedefinieerd in deze specificatie is "2.0".

### 2.4.2 Afzender

```
<saml:Issuer>
 <!-- De Issuer verwijst naar de organisatie waarbinnen de BSN validatie heeft
plaats gevonden.-->
     urn:IIroot:2.16.528.1.1007.3.3:IIext:12345678
</saml:Issuer>
```

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

```
"urn:IIroot:"<OID voor UZI 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

### 2.4.3 Onderwerp

```
<saml:Subject>
  <saml:NameID>
   950052413
  </saml:NameID>
  <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:sender-vouches
">
  </saml:SubjectConfirmation>
</saml:Subject>
```

De `Subject` verwijst naar de door de zorgverlener/medewerker gevalideerde BSN. De BSN validatie dient plaatsgevonden te hebben aan de balie door:

- Een face to face controle van de patient en diens Wettelijk Identiteits Document (WID)
- Een, door het systeem uitgevoerde, controle van de geldigheid van het WID bij SBV-Z
- Een, door het systeem uitgevoerde, controle van de correctheid van het BSN bij SBV-Z

Vervolgens moet de SubjectConfirmation nog toegevoegd worden:

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

### 2.4.4 Geldigheid

```
<saml:Conditions
 NotBefore="2009-06-24T11:47:34Z"
 NotOnOrAfter="2010-12-24T11:47:34Z">
```

Het attribuut *NotBefore* is de tijd waarop de SAML assertion geldig wordt. NotBefore moet altijd op of na de aanvang van de geldigheidsdatum van het certificaat (waarmee het inschrijftoken is getekend) liggen.

Wordt een bericht met een inschrijftoken ontvangen voor *NotBefore* is aangevangen, dan **moet** dit bericht geweigerd worden.

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 inschrijftoken is getekend) liggen.

Wordt een bericht met een inschrijftoken ontvangen op of nadat *NotOnOrAfter* is verstreken, dan **moet** dit bericht geweigerd worden.

Deze tijd is als bovenstaande tijd geformatteerd. Het maximaal toegestane verschil tussen *NotBefore* en *NotOnOrAfter* is anderhalf jaar.

De geldigheidsduur van een inschrijftoken (*NotOnOrAfter* minus *NotBefore*) kan nooit langer zijn dan de geldigheidsduur van het authenticatiecertificaat waarmee het token wordt getekend.

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

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

Indien het certificaat vóór ondertekening van het inschrijftoken op de CRL is geplaatst, dan dient het inschrijftoken geweigerd te worden door het LSP.

Indien het certificaat na ondertekening van het inschrijftoken op de CRL is geplaatst, dan dient het inschrijftoken niet geweigerd te worden.

Het inperken van bepaalde partijen (`AudienceRestriction`) waarvoor de assertion bedoeld is wordt beschreven in paragraaf 2.4.5 Ontvanger.

### 2.4.5 Ontvanger

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

In de `AudienceRestriction` wordt beschreven aan wie de SAML assertion is gericht. In ieder geval dient de ZIM als audience voor te komen (`IIext:1`). Meerdere Audience elementen is toegestaan.

Voor de `<Audience>` parameter is gekozen voor URN. De URN string is opgebouwd uit een IIroot en een IIext. "II" staat voor het HL7v3 datatype Instance 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 de GBZ-applicatie wordt toegekend bij aansluiting op de AORTA. Stel dat dit "300" zou zijn, dan ziet de URN er als volgt uit:

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

### 2.4.6 Authenticatie

```
<saml:AuthnStatement
 AuthnInstant="2009-06-24T11:47:34"
 SessionIndex="token_2.16.528.1.1007.3.3.1234567.1_0123456789">
```

Het subject, de gevalideerde BSN, in de SAML assertion is geauthenticeerd door middel van een authenticatiemiddel van de uitvoerende zorgverlener/medewerker.

```
<saml:AuthnContext>
  <saml:AuthnContextClassRef
>urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI</saml:AuthnContextClassRef>
</saml:AuthnContext>
```

Binnen de gebruikte applicatie beveiligingsstandaarden is er sprake van verschillende vertrouwensniveaus.

Binnen de SAML-specificatie geeft men een authenticatie-context (*AuthnContext*) mee die de context van het gebruikte authenticatiemiddel aangeeft. Hiervoor zijn een aantal contexten gespecificeerd, zie [SAMLAuthnContext], die gebruikt worden als referentiekader voor de communicatie tussen de ZIM en andere componenten zoals GBZ applicaties.

Uitgaande van de beveiligingsniveaus van GBZ, zorgverlener/medewerker en UZI-pas wordt het "*urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI*" beveiligingsniveau gehanteerd om het AORTA vertrouwensniveau midden voor zorgverleners weer te geven.

```
</saml:AuthnStatement>
```

Afsluiting authentication statement.

### 2.4.7 Attributen

```
<saml:AttributeStatement>
```

De volgende attributen zijn gegevens die relevant zijn met betrekking tot de uitgevoerde BSN validatie. De volgorde van de attributen in het AttributeStatement is niet relevant. Er mogen geen andere attributen opgenomen worden in het AttributeStatement dan hier beschreven is.

**WID Controle**

```
<saml:Attribute Name="WID Controle Root">
  <saml:AttributeValue>2.16.528.1.1007.3.3.1234567.1</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="WID Controle Extensie">
  <saml:AttributeValue>0123456789</saml:AttributeValue>
</saml:Attribute>
```

De Attributen WID Controle Root en WID Controle Extensie vormen een uniek gegeven, uitgegeven door de verzender van het bericht naar de SBV-Z waarmee de controle op de geldigheid van het WID is uitgevoerd.

**SBV-Z Controle**

```
<saml:Attribute Name="SBV-Z Controle Root">
  <saml:AttributeValue>2.16.528.1.1007.3.3.1234567.1</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="SBV-Z Controle Extensie">
  <saml:AttributeValue>0123456789</saml:AttributeValue>
</saml:Attribute>
```

De Attributen SBV-Z Controle Root en SBV-Z Controle Extensie vormen een uniek gegeven, uitgegeven door de verzender van het bericht naar de SBV-Z waarmee de controle op de geldigheid van het BSN is uitgevoerd.

**Uitvoerder**

```
<saml:Attribute Name="Uitvoerder">
  <saml:AttributeValue>123456789</saml:AttributeValue>
</saml:Attribute>
```

Het attribuut Uitvoerder bevat het UZI van de zorgverlener/medewerker die de BSN validatie heeft uitgevoerd en het token heeft ondertekend.

**attributeStatement blok**

Het attributen statement blok ziet er dan bijvoorbeeld zo uit (de volgorde van de attributen is niet relevant):

```
<saml:AttributeStatement>
  <saml:Attribute Name="WID Controle Root">
    <saml:AttributeValue>2.16.528.1.1007.3.3.1234567.1</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute Name="WID Controle Extensie">
    <saml:AttributeValue>0123456789</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute Name="SBV-Z Controle Root">
    <saml:AttributeValue>2.16.528.1.1007.3.3.1234567.1</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute Name="SBV-Z Controle Extensie">
    <saml:AttributeValue>0123456789</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute Name="Uitvoerder">
    <saml:AttributeValue>123456789</saml:AttributeValue>
  </saml:Attribute>
</saml:AttributeStatement>
```

Tenslotte wordt het attributen statement blok afgesloten met

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

## 2.5 Algoritmes

Om de integriteit en onweerlegbaarheid van het SAML inschrijftoken te waarborgen wordt een XML Signature geplaatst, zoals beschreven in [IH tokens generiek]. Na plaatsen van de XML Signature kan de ontvanger, met gebruikmaking van het persoonsgebonden UZI-certificaat van de verzender en de CA certificaten zoals verstrekt door het UZI-register, onomstotelijk vaststellen dat het SAML inschrijftoken ondertekend is met de privé sleutel behorend bij het gebruikte certificaat van de zorgmedewerker.

De XML Signature van het SAML inschrijftoken die gebruikt wordt bij berichtauthenticatie met behulp van de 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 inschrijftoken en in het SAML inschrijftoken geplaatst wordt, moet er een "enveloped-signature" transformatie uitgevoerd worden die de Signature tags uit het SAML inschrijftoken verwijderd gevolgd door een "exc-c14n transformatie" (zie ook [SAML Core] §5.4.3 en §5.4.4).

## 2.6 Opbouw

### 2.6.1 De headers

Eerst wordt het SAML inschrijftoken – het `<saml:Assertion ...>` element aangemaakt en gevuld met die elementen, zoals beschreven in paragraaf 2.4 Inhoud.

```
<saml:Assertion
   ID="token_2.16.528.1.1007.3.3.1234567.1_0123456789"
   IssueInstant="2009-06-24T11:47:34Z"
   Version="2.0"
   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
 ... Zie paragraaf 2.4 Inhoud ...
</saml:Assertion>
```

Het XML Signature blok is onderdeel van het SAML inschrijftoken. Het XML Signature blok komt na het `<saml:Issuer>` element. Na de Signature volgt de rest van de inhoud van de assertion.

```
<saml:Assertion
   ID="token_2.16.528.1.1007.3.3.1234567.1_0123456789"
   IssueInstant="2009-06-24T11:47:34Z"
   Version="2.0"
   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
  <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
   urn:IIroot:?:IIext:?
  </saml:Issuer>
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
    ...
    </ds:SignedInfo>
    <ds:SignatureValue>Wuwn...5e4=</ds:SignatureValue>
    <ds:KeyInfo>
      <wss:SecurityTokenReference>
        <ds:X509Data>
        ...
        </ds:X509Data>
      <wss:SecurityTokenReference>
    </ds:KeyInfo>
  </ds:Signature>  ...
  ... Zie paragraaf 2.3 Inhoud ...
</saml:Assertion>
```

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

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

Deze drie waarden worden ingevuld:

- Neem het SignedInfo blok op.
- Neem de SignatureValue op.
- Neem certificaatgegevens in het KeyInfo blok op, in de vorm van een verwijzing (X509IssuerSerial).

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

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

### 2.6.2 Plaats van het SAML token en de digitale handtekening

Het SAML inschrijftoken met daarin de digitale handtekening wordt in het WS-Security SOAP Header gezet. Op het `<wss:Security>` element **moet** een `soap:mustUnderstand="1"` vlag opgenomen worden, die aangeeft dat de ontvanger dit security element **moet** verwerken en een `soap:actor="http://www.aortarelease.nl/actor/zim"` die aangeeft dat de ZIM dit security element verwerkt.

```
<soap:Header xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  ...
  <wss:Security xmlns:wss=
    "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
    soap:actor="http://www.aortarelease.nl/actor/zim" soap:mustUnderstand="1">
       <saml:Assertion ... >
       <saml:Issuer>...</saml:Issuer>
       <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
        ...
        </ds:SignedInfo>
        <ds:SignatureValue>Wuwn...5e4=</ds:SignatureValue>
        <ds:KeyInfo>
          <ds:X509Data>
          ...
          </ds:X509Data>
        </ds:KeyInfo>
       </ds:Signature>
    ... Zie paragraaf 2.3 Inhoud ...
       </saml:Assertion ... >
  </wss:Security>
</soap:Header>
```

# 3 Certificaten

## 3.1 Te gebruiken certificaat en attributen

De UZI-pas kent een aantal modellen:

**Tabel AORTA.STK.t3210 – UZI pastype**

| Naam UZI-pastype | Codering Pastype |
|---|---|
| **Zorgverlenerpas** | Z |
| **Medewerkerpas op naam** | N |
| **Medewerkerpas niet op naam** | M |
| **Servercertificaat** | S |

De pas die gebruikt wordt voor het ondertekenen van een inschrijftoken moet een zorgverlenerpas of een medewerkerpas op naam zijn. Hoewel het pastype gecodeerd is opgenomen in het authenticiteitcertificaat (in het `subjectAltName` attribuut), dient een applicatie op basis van de uitgevende CA vast te stellen wat het pastype van de UZI-pas is.

De signature wordt gezet met de sleutel voor authenticiteit (keyUsage=digitalSignature, hexadecimaal 0x80).

De attributen in het authenticiteitcertificaat worden gegeven in de vorm van een Distinguished Name (DN), zie [IH tokens generiek].

De waarden van deze attributen voor de relevante UZI-passen zijn:

**Tabel AORTA.STK.t3220 – DN attributen van zorgverlenerspas**

| Attribuut | Omschrijving | Waarde |
|---|---|---|
| **CN** | Issuer.commonName | *Derde generatie:*<br>UZI-register Zorgverlener CA G3<br>Voor mogelijke volgende generaties wordt verwezen naar het UZI-register:<br>https://www.uziregister.nl/ |
| **O** | Issuer.organisationName | agentschap Centraal Informatiepunt Beroepen Gezondheidszorg |
| **C** | Issuer.countryName | NL |

De issuer.commonName verschilt per 'generatie' UZI-passen. Het is mogelijk dat verschillende 'generatie' UZI-passen door elkaar worden gebruikt. Daarom dient de Issuer DN dynamisch afgeleid te worden uit het gebruikte authenticatiecertificaat.

**Tabel AORTA.STK.t3230 – DN attributen van medewerkerpas op naam**

| Attribuut | Omschrijving | Waarde |
|---|---|---|
| **CN** | Issuer.commonName | *Derde generatie:*<br>UZI-register Medewerker op naam CA G3<br>Voor mogelijke volgende generaties wordt verwezen naar het UZI-register:<br>https://www.uziregister.nl/ |
| **O** | Issuer.organisationName | agentschap Centraal Informatiepunt Beroepen Gezondheidszorg |
| **C** | Issuer.countryName | NL |

Om de digitale handtekening bij het LSP te verifiëren, moet de ontvanger over de bijbehorende publieke sleutel beschikken, zie [IH tokens generiek].

Voor verificatie is gekozen een verwijzing naar het certificaat mee te zenden; de ontvanger moet deze dan met bijvoorbeeld het LDAP protocol ophalen in de directory van het UZI-register.

Zie voor de verdere beschrijving van de passen [UZI pas].

Noot: uiteraard mogen in het testtraject alleen UZI-testpassen gebruikt worden. Het gebruik hiervan wordt verder niet uitgewerkt in deze handleiding. De werking is identiek.

# 4 Token afhandeling

## 4.1 Verificatie van het bericht

Het is belangrijk vast te stellen dat de velden in het SAML inschrijftoken een correcte waarde hebben en geldig ondertekend zijn. Wanneer dit niet zou gebeuren, kan een kwaadwillende met een gestolen token nog steeds gegevens opvragen van bv. ieder willekeurig burgerservicenummer.

De ontvanger controleert of de WS-Security SOAP Header voor hem bestemd is, zie soap attribuut actor.

Het SAML inschrijftoken wordt door de ontvanger uit de WS-Security SOAP Header gehaald indien de WS-Security SOAP Header voor de ontvanger bestemd is en dat de ontvanger deze moet verwerken. Bij gebruik van het SAML inschrijftoken moet de ontvanger controleren of:

- De aanduiding voor de versie van SAML gedefinieerd is op "2.0", zie paragaaf 2.4.1 Uniekheid;
- De juiste organisatieID is opgenomen die deze assertion heeft gecreëerd en de gebruiker heeft geauthenticeerd, zie paragraaf 2.4.2 Afzender. Het zorgaanbiederID in het token dient overeen te komen met de zorgaanbiederID in het bericht. Tevens dient de zorgaanbiederID overeen te komen met:
    - De URA van het transactietoken
    - De URA uit het mandaattoken
- Het BSN uit het Subject zie paragraaf 2.4.3 Onderwerp overeenkomt met het BSN uit het transactietoken en het BSN uit het HL7-bericht;
- De Assertion correct is ondertekend door de Signature te valideren met het gerefereerde certificaat.
- Het gebruikte certificaat waarmee de ondertekening heeft plaatsgevonden geldig was ten tijde van de ondertekening.
- Indien het certificaat op de CRL is geplaatst, dan dient dit plaats te hebben gevonden nadat het token gegenereerd en ondertekend is.
- De relevante certificaatketen te valideren op geldigheid.
- De geldigheidsperiode van het token, zie paragraaf 2.4.4 Geldigheid, niet langer is dan 1,5 jaar;
- Het bericht ontvangen is binnen de geldigheidsperiode van het token, zie paragraaf 2.4.4 Geldigheid;
- De afnemer van het SAML inschrijftoken (audience) minimaal de ZIM is, zie paragraaf 2.4.5 Ontvanger;
- De zorgverlener/zorgmedewerker is geauthenticeerd via het voorgedefinieerde authenticatiemiddel, de SmartCardPKI, zoals beschreven in paragraaf 2.4.6 Authenticatie;
- Alleen die attributen zijn gedefinieerd, die zijn beschreven in paragraaf 2.4.7 Attributen;
- De attribuutwaarde van Uitvoerder overeenkomt met het UZI-nummer van het gerefereerde certificaat, zie paragraaf 2.4.7 Attributen;
- De attributen WID Controle Root, WID Controle Extensie, SBV-Z Controle Root en SBV-Z Controle Extensie, zie paragraaf 2.4.7 Attributen, aanwezig zijn en een waarde hebben.

Het inschrijftoken mag meerdere malen gebruikt worden. De attributen WID Controle Root, WID Controle Extensie, SBV-Z Controle Root en SBV-Z Controle Extensie kunnen niet door de ZIM gecontroleerd worden.

Het tokenID dient in de log van de ZIM opgenomen te worden.

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

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

# Bijlage A Referenties

| Referentie | Document | Versie |
|---|---|---|
| [IH tokens generiek] | AORTA_Auth_IH_Security_tokens_generiek | 8.1.0.0 |
| [Transactietoken] | AORTA_Auth_IH_Berichtauthenticatie_Transactietoken | 8.1.0.0 |
| [Mandaattoken] | AORTA_Auth_IH_Mandaattoken | 8.1.0.0 |
| [SAMLAuthnContext] | Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0<br>http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf | 2.0<br>15-mrt-2005 |
| [SAML Core] | SAML v2.0 Core Specification<br>https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf | 2.0<br>15-mrt-2005 |
| [SAML Profiles] | Profiles for the OASIS Security Assertion Markup Language (SAML) v2.0<br>http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf | 2.0<br>15-mrt-2005 |
| [SAML Token] | SAML Token Profile<br>http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SAMLTokenProfile.pdf | 1.1<br>01-feb-2006 |
| [UZI pas] | CA model, Pasmodel, Certificaat- en CRL-profielen, Agentschap CIBG<br>www.uziregister.nl | 9.6<br>26 april 2019 |