< IH Berichtauthenticatie met PKIO

Datum: 1 februari 2019
Publicatie: V8.0.3.0

Inhoudsopgave

1 Inleiding 3
1.1 Doel en scope 3
1.2 Doelgroep voor dit document 3
1.3 Documenthistorie 3
2 Het SAML authenticatietoken 4
2.1 Structuur 4
2.2 Namespaces 5
2.3 Inhoud 5
2.3.1 Uniekheid 5
2.3.2 Onderwerp 6
2.3.3 Geldigheid 6
2.3.4 Afzender 7
2.3.5 Ontvanger 8
2.3.6 Authenticatie 8
2.3.7 Attributen 8
2.4 Algoritmes 10
2.5 Opbouw 10
2.5.1 De headers 10
2.5.2 Plaats van het SAML token en de digitale handtekening 12
3 Certificaten 13
3.1 Te gebruiken certificaat en attributen 13
4 Token afhandeling 14
4.1 Verificatie van het bericht 14
Bijlage A Referenties 15

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 beheerd klantenloket (GBK) en het landelijk schakelpunt (LSP) voor wat betreft de toe te passen technieken voor de authenticatie van klantenloketmedewerkers.

1.2 Doelgroep voor dit document

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

1.3 Documenthistorie

Versie	Datum	Omschrijving
v6.10.0.0	12-okt-2011	RfC 46142: SOAP Headers van tokens worden uitgebreid met soap:actor.
v6.11.0.0	12-okt-2012	Ongewijzigde herpublicatie als onderdeel van AORTA-Infrastructuur v6·11
v6.12.0.0	17-juni-2013	RfC 58592: Subject.organizationName gewijzigd naar Vereniging van Zorgaanbieders voor Zorgcommunicatie.
v8.0.1.0	15-mei-2017	Opgenomen in publicatie 8.0.1.0
v8.0.2.0	31-januari-2018	RfC 76680: Uitbreiding DigiD authenticatieniveaus
V8.0.3.0	15-nov-2018	Opgenomen in publicatie 8.0.3.0

2 Het SAML authenticatietoken

In dit hoofdstuk wordt de inhoud van het SAML authenticatietoken besproken die bij berichtauthenticatie met behulp van de PKIO-pas wordt gebruikt. Het SAML authenticatietoken bevat informatie over de toegepaste authenticatie en identificatie van de klantenloketmedewerker en namens welke patiënt het verzoek wordt afgehandeld. Het SAML authenticatietoken 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 Nictiz aangepast te worden voor een juiste optimale werking.

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

- Het gebruik van het SAML authenticatietoken (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 klantenloket (GBK) – het landelijk schakelpunt (LSP)

Dit profiel wordt in de volgende paragrafen verder uitgewerkt.

2.1 Structuur

Het SAML authenticatietoken is een afgegeven SAML assertion die gebruikt wordt bij berichtauthenticatie met behulp van de PKIO-pas voor het landelijk EPD. Het SAML authenticatietoken heeft de volgende structuur (de waarden die in het token gebruikt worden zijn fictief):

```
<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">
  <!-- De partij (klantenloket applicatie) die deze assertion heeft gecreëerd, -->
  <!-- wordt als een OID gepresenteerd. Moet door de GBK organisatie geregeld worden -->
  <!-- Applicatie-id van de GBK-applicatie, zoals toegekend bij aansluiting. -->
  <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
   urn:IIroot:2.16.840.1.113883.2.4.6.6:IIext:?
  </saml:Issuer>
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
   ...
  </ds:Signature>
  <!-- Het onderwerp -->
  <saml:Subject>
   <!-- Serienummer van persoonlijk certificaat van een medewerker-->
   <saml:NameID>urn:cert:359724154776965087907738313562 41</saml:NameID>
  </saml:Subject>
  <!-- Geldigheidsduur en geldige toehoorder van de assertion -->
  <saml:Conditions
   NotBefore="2009-06-24T11:47:34Z"
   NotOnOrAfter="2009-06-24T11:52:34Z">
   <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>
  </saml:Conditions>
  <saml:AuthnStatement
   AuthnInstant="2009-06-24T11:47:34"
```

```
    SessionIndex="token_2.16.528.1.1007.3.3.1234567.1_0123456789">
    <!-- Authenticatiemiddel -->
    <saml:AuthnContext>
<saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI</saml:AuthnCont
extClassRef>
    </saml:AuthnContext>
  </saml:AuthnStatement>
  <!-- Overige HL7 attributen die ondertekend worden -->
  <saml:AttributeStatement>
    <saml:Attribute Name="triggerEventId">
      <saml:AttributeValue>QURX_TE990011NL</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="messageIdRoot">
      <saml:AttributeValue>2.16.528.1.1007.3.3.1234567.1</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="messageIdExt">
      <saml:AttributeValue>0123456789</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="burgerServiceNummer">
      <saml:AttributeValue>950052413</saml:AttributeValue>
    </saml:Attribute>
  </saml:AttributeStatement>
</saml:Assertion>
```

2.2 Namespaces

Het SAML authenticatietoken die gebruikt wordt bij berichtauthenticatie met behulp van de PKIO-pas 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 authenticatietoken onderscheiden, zoals in [IH tokens generiek] beschreven is.

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

Het SAML authenticatietoken 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 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. De aanbevolen methode is:

- begin met de string "token" en een underscore "_"
- voeg hier de root van het HL7v3 message.id aan toe
- voeg hier een underscore "_" aan toe
- voeg hier de extension van het HL7v3 message.id aan toe
- bijvoorbeeld: token_2.16.528.1.1007.3.3.1234567.1_0123456789

Deze methode garandeert dat iedere waarde uniek is, ook wanneer meerdere HL7v3 berichten in een XML bestand worden samengevoegd. (De methode kan niet verplicht worden, omdat de extension van een message.id niet numeriek hoeft te zijn, en het dus mogelijk is dat deze karakters bevat die in een XML ID niet toegestaan zijn. In dat geval dient een leverancier er zelf voor te zorgen een waarde te genereren die uniek is voor een AORTA bericht. Hierbij dient dan een UUID (Universally Unique Identifier) gebruikt te worden. 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).

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".

2.3.2 Onderwerp

```
<saml:Subject>
  <saml:NameID>
   urn:cert:359724154776965087907738313562 41
  </saml:NameID>
</saml:Subject>
```

Het Subject bevat identificerende gegevens van het systeem dat de transactie heeft geïnitieerd. Het subject bevat het serienummer van het authenticiteitcertificaat. Het Subject wordt als URN (Uniform Resource Name) genoteerd en wordt aan de hand van het PKIoverheid-certificaat gevalideerd. De URN is opgebouwd uit:

```
"urn:cert:"<serienummer authenticiteitcertificaat>
```

Het OID (Object IDentifier) van het serienummer van het certificaat is een uniek identificerend kenmerk, binnen de context van een gegeven CA, en is onweerlegbaar terug te voeren naar de klantenloketmedewerker.

2.3.3 Geldigheid

```
<saml:Conditions
 NotBefore="2009-06-24T11:47:34Z"
 NotOnOrAfter="2009-06-24T11:52:34Z">
```

Het attribuut *NotBefore* is de tijd waarop de SAML assertion geldig wordt. Dit hoeft niet de tijd te zijn waarop het bericht is aangemaakt. Het is mogelijk *NotBefore* in de toekomst te zetten, en het bericht na deze tijd pas te verzenden.

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

Het attibuut *NotOnOrAfter* is de tijd waarop de SAML assertion vervalt.

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

Deze tijd is als bovenstaande tijd geformatteerd. Richtlijn voor het verschil tussen *NotBefore* en *NotOnOrAfter* is 5 minuten. Het wordt sterk aanbevolen de SAML assertion direct (binnen 5 minuten) te gebruiken voor berichten die verzonden worden (dus terwijl de klantenloketmedewerker achter diens computer zit). Het gaat immers om het voorkomen van misbruik van onderschepte tokens, en 5 minuten is meer dan voldoende om de hele keten van vraag tot antwoord te doorlopen.

De geldigheidsduur van een token (*NotOnOrAfter* minus *NotBefore*) mag niet langer dan 5 minuten zijn. Wordt een bericht ontvangen waarin deze geldigheidsduur overschreden is, dan **moet** dat bericht geweigerd worden, ook al is het tijdstip *NotOnOrAfter* nog niet verstreken.

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 berichtauthenticatie met behulp van de PKIO-pas.

2.3.4 Afzender

```
<!-- Applicatie-id van de GBK-applicatie, zoals toegekend bij aansluiting. -->
<!-- Root en extensie van het GBK, Moet GBK org. aanvragen en regelen. -->
  urn:IIroot:2.16.840.1.113883.2.4.6.6:IIext:?
</saml:Issuer>
```

Het applicatie-id van de afzender die deze SAML assertion heeft gecreëerd en de gebruiker authenticeert. De Issuer 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 GBK>
```

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 GBK 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

2.3.5 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. De waarden in de elementen zijn (voorlopig) vaste waarden. Voor de `<Audience>` parameter is (ook) gekozen voor URN, zie voor opbouw paragraaf 2.3.4 Afzender.

2.3.6 Authenticatie

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

Het subject, een klantenloketmedewerker, in de SAML assertion is geauthenticeerd door middel van een authenticatiemiddel op een gegeven moment.

```
<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 GBK applicaties.

Uitgaande van de beveiligingsniveaus van GBK, klantenloketmedewerker en PKIO-pas wordt het "*urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI*" beveiligingsniveau gehanteerd om het AORTA vertrouwensniveau midden voor klantenloketmedewerkers weer te geven.

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

Einde van de gegevens voor de authenticatie conform de SAML specificatie.

2.3.7 Attributen

```
<saml:AttributeStatement>
```

De volgende attributen zijn gegevens uit het HL7v3 bericht die met de authenticatie meegetekend worden. Dit zijn kopieën van gegevens die elders in hetzelfde HL7v3 bericht voorkomen. 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.

```
<saml:Attribute Name="triggerEventId">
  <saml:AttributeValue>QURX_TE990011NL</saml:AttributeValue>
</saml:Attribute>
```

Het attribuut TriggerEventId wordt altijd meegetekend. Het trigger event identificeert *de aanleiding voor het verzenden* van het bericht, en bepaalt dus de intentie van de verzender. Merk op dat het trigger event geen verplicht element in het HL7v3-bericht zelf is. Dit attribuut meesturen verhindert veel soorten aanvallen, bijvoorbeeld het token van een query kapen en proberen deze te hergebruiken voor het afhandelen van verzoeken van patiënten en hun vertegenwoordigers om inzage te verkrijgen in de verwijsindex. Het is ook mogelijk de interactionId te gebruiken: deze wijzigt echter tussen versies van berichten, het triggerEventId meestal niet, zodat een nieuwe versie van het bericht niet noodzakelijk wijzigingen voor het token tot gevolg heeft.

```
<saml:Attribute Name="messageIdRoot">
  <saml:AttributeValue>2.16.528.1.1007.3.3.1234567.1</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="messageIdExt">
  <saml:AttributeValue>0123456789</saml:AttributeValue>
</saml:Attribute>
```

De Attributen messageIdRoot en messageIdExt vormen een uniek gegeven, uitgegeven door de verzender van het HL7v3-bericht. De combinatie van de attribuutwaarden messageIdRoot en messageIdExt moeten gelijk zijn aan het uiteindelijk gebruikte HL7v3 message.Id.

```
<saml:Attribute Name="burgerServiceNummer">
  <saml:AttributeValue>950052413</saml:AttributeValue>
</saml:Attribute>
```

Voor berichten die betrekking hebben op een enkele patiënt, wordt het burgerServiceNummer (BSN) van de patiënt opgenomen. Dit maakt ook weer vele aanvallen onmogelijk, namelijk gegevens van een andere patiënt proberen op te vragen. Dit geldt voor alle berichten die betrekking hebben op één en niet meer dan één patiënt.

Het BSN in het token moet overeenkomen met het BSN in het bericht. In het geval er sprake is van een voorloopnul in het bericht, dan dient deze ook overgenomen te worden in het token.

Voor berichten die geen betrekking hebben op een persoon waarvan het burgerServiceNummer bekend is, wordt het burgerServiceNummer weggelaten.

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

```
<saml:Attribute Name="triggerEventId">
 <saml:AttributeValue>QURX_TE990011NL</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="messageIdRoot">
 <saml:AttributeValue>2.16.528.1.1007.3.3.1234567.1</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="messageIdExt">
 <saml:AttributeValue>0123456789</saml:AttributeValue>
</saml:Attribute>
```

Tenslotte wordt het attributen statement blok afgesloten met

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

2.4 Algoritmes

Om de integriteit en onweerlegbaarheid van het SAML authenticatietoken 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 PKIoverheid-certificaat van de verzender en de CA certificaten zoals verstrekt door PKIoverheid, onomstotelijk vaststellen dat het SAML authenticatietoken ondertekend is met de privé sleutel behorend bij het gebruikte en meegezonden certificaat van de klantloketmedewerker.

De XML Signature van het SAML authenticatietoken die gebruikt wordt bij berichtauthenticatie met behulp van de PKIO-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 authenticatietoken en in het SAML authenticatietoken geplaatst wordt, moet er een "enveloped-signature" transformatie uitgevoerd worden die de Signature tags uit het SAML authenticatietoken verwijderd.

2.5 Opbouw

2.5.1 De headers

Eerst wordt het SAML authenticatietoken – 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 authenticatietoken. 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">
  ... Zie paragraaf 2.3 Inhoud ...
  <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>
      <ds:X509Data>
      ...
      </ds:X509Data>
    </ds:KeyInfo>
  </ds:Signature>  ...
</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.

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

Voor authenticatie doeleinden mag er niet meer dan één SAML assertion voorkomen met 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. 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 ... >
    ... Zie paragraaf 2.3 Inhoud ...
      <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>
       <saml:Assertion ... >
  </wss:Security>
</soap:Header>
```

3 Certificaten

3.1 Te gebruiken certificaat en attributen

Voor het tekenen van het SAML authenticatietoken worden persoonsgebonden authenticiteitcertificaten uit de PKIoverheid hiërarchie gebruikt. Dit certificaat bevat een RSA publieke sleutel. Met de privé sleutel wordt de digitale handtekening gegenereerd.

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

Tabel AORTA.STK.t3310 – Certificaat attributen

Attribuut	Omschrijving	Waarde
CN	Subject.commonName	<Volledige naam van de persoon, zie [CP PKIO] deel 3a>
OU	Subject.organizationalUnitName	Klantenloket
O	Subject.organizationName	Vereniging van Zorgaanbieders voor Zorgcommunicatie
C	Subject.countryName	C=NL <zie [CP PKIO] deel 3a>
Serienummer	SerialNumber. Wordt door de certificaatdienstverlener vastgelegd	<zie [CP PKIO] deel 3a>

De issuer.commonName verschilt per 'generatie' PKIO-passen.
De root en de domeinen die het SHA-1 algoritme gebruiken, worden aangemerkt als G1, waarbij G staat voor generatie. De root en de domeinen die eind 2010 het SHA-256 algoritme gaan gebruiken, worden aangemerkt als G2. De Issuer DN kan alleen dynamisch afgeleid worden uit het gebruikte authenticatie certificaat. De verschillende generaties PKIO-passen kunnen bij een klantenloket naast elkaar gebruikt worden.

Het serialNumber van het authenticiteitscertificaat van de pas wordt gebruikt in combinatie met de attributen O en OU om een klantenloketmedewerker te identificeren.

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 door het certificaat met de publieke sleutel mee te zenden in KeyInfo van het SAML authenticatietoken, zie ook [IH tokens generiek].

Noot: In samenspraak met Nictiz en andere betrokken partijen kan de keuze voor het meezenden van het certificaat nog heroverwogen worden.

Noot: In het testtraject worden ook PKIO-passen gebruikt.

4 Token afhandeling

4.1 Verificatie van het bericht

Het is belangrijk vast te stellen dat de velden in het SAML authenticatietoken overeenstemmen met die in het HL7v3 bericht 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 authenticatietoken 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 authenticatietoken moet de ontvanger controleren of:

- Het attribuut ID van het Assertion element op een unieke wijze het uiteindelijk gebruikte HL7v3 message.Id identificeert, zie paragaaf 2.3.1 Uniekheid;
- De aanduiding voor de versie van SAML gedefinieerd is op "2.0", zie paragaaf 2.3.1 Uniekheid;
- Het bericht ontvangen is binnen de geldigheidsperiode van het token, zie paragraaf 2.3.3 Geldigheid;
- Het serienummer van het authenticatie certificaat overeenkomt met de NameID van het Subject, zie paragraaf 2.3.2 Onderwerp;
- De juiste afzender is vastgelegd die deze assertion heeft gecreëerd en de gebruiker heeft geauthenticeerd, zie paragraaf 2.3.4 Afzender;
- De afnemer van het SAML authenticatietoken (audience) het LSP is, zie paragraaf 2.3.5 Ontvanger;
- De klantenloketmedewerker is geauthenticeerd via het voorgedefinieerde authenticatiemiddel, de SmartCardPKI, zoals beschreven in paragraaf 2.3.6 Authenticatie;
- Alleen die attributen zijn gedefinieerd, die zijn beschreven in paragraaf 2.3.7 Attributen;
- De attribuutwaarde van TriggerEventId overeenkomt met het berichttype van het HLv3 bericht, zie paragraaf 2.3.7 Attributen;
- De attribuutwaarden van messageIdRoot en messageIdExt overeenkomt met de gebruikte HL7v3 message.id, zie paragraaf 2.3.7 Attributen;
- De attribuutwaarde van burgerServiceNummer overeenkomt met het BSN in het HL7v3 bericht ofwel doordat de gegevens in het bericht daadwerkelijk betrekking hebben op de persoon, zie paragraaf 2.3.7 Attributen;

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	8.0.3.0
[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
[CP PKIO]	Certificate Policies	3.0 25 januari 2011