< IH Berichtauthenticatie Transactietoken t.b.v. FHIR

Datum: 2 Oktober 2020
Publicatie: V9.0.1.0

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) en het koppelvlak tussen de VZVZ DVZA (LSP+) en het landelijk schakelpunt (LSP) voor wat betreft de toe te passen technieken voor de authenticatie van zorgverleners, medewerkers en patiënten.

De scope betreft een eerste PoC voor het beschikbaar stellen van BG(G)Z gegevens door op AORTA aangesloten bronsystemen. Het betreft hier alleen beschikbaarstelling van gegevens voor de patiënt via LSP+. Hierbij wordt een FHIR-search vanuit LSP+ in combinatie met het hier beschreven transactietoken doorgestuurd naar het LSP. Het LSP zal deze FHIR-search in combinatie met het transactietoken doorzetten naar het juiste bronsysteem. Het transactietoken zal in de loop van de PoC of aan het eind van de PoC aan verandering onderhevig kunnen zijn.

1.2 Doelgroep voor dit document

De doelgroep voor dit document betreft binnen VZVZ, LSP- en LSP+-leverancier de betrokken productmanagers, architecten en testers. Daarnaast is dit document bedoeld voor alle betrokken bij de XIS-leverancier van de voor deze usecase op het LSP aan te sluiten XIS-applicatie. Het is wenselijk om dit document niet breder te verspreiden dan deze doelgroep.

1.3 Documenthistorie

Versie	Datum	Omschrijving
v8.0.2.0	31-januari-2018	Initieel document.
v8.0.3.0	15-nov-2018	Opgenomen in publicatie 8.0.3.0
v8.1.0.0	26-juni-2019	INI-8877: Aanpassing ten behoeve van de conditionele query
V8.1.0.0	13-september-2019	INI-9019: Optioneel gebruik BSN
V8.1.1.0	30-januari-2020	In hoofdstuk 3.1 verduidelijkt hoe om te gaan met het ondertekenen met een servcertificaat.
V8.1.1.0	30-januari-2020	Op verschillende plekken in het document aangescherpt dat er ook ondertekend kan worden met een UZI-servercertificaat.
V8.2.0.0	22-juli-2020	Controle op overseer in hoofstuk 4.1 aangepast.
V9.0.0.0	2-oktober-2020	Toevoegen transactietokengeneratie door LSP+.
V9.0.1.0	29-oktober-2020	Aanpassingen n.a.v. overleg technologiepartners.

2 Het SAML transactietoken

In dit hoofdstuk wordt de inhoud van het SAML transactietoken besproken die bij berichtauthenticatie met behulp van de UZI-pas/servercertificaat wordt gebruikt. Het SAML transactietoken bevat informatie over de toegepaste authenticatie en identificatie van de zorgverlener/medewerker/organisatie. Het SAML transactietoken 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 transactietoken en het aanbieden van dit token aan het LSP worden de volgende profielen gebruikt:

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

Dit profiel raakt het koppelvlak:

- Goed beheerd zorgsysteem (GBZ) – het landelijk schakelpunt (LSP);
- LSP+) - het landelijk schakelpunt (LSP);
- Het landelijk schakelpunt (LSP) - Goed beheerd zorgsysteem (GBZ).

Dit profiel wordt in de volgende paragrafen verder uitgewerkt.

2.1 Structuur

Het SAML transactietoken is een afgegeven SAML assertion die gebruikt wordt bij berichtauthenticatie met behulp van de UZI-pas/UZI-servercertificaat of PKIo-servercertificaat (van LSP+/LSP). 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 uitgifte van de Assertion.
Issuer	1	Bevat het OrganisatieID van de zendende applicatie. In het geval van een bevraging door een PGO, zal hier de organisatieID van LSP+ (autorisatieserver) komen te staan.
@NameQualifier	0	Niet gebruiken
@SPNameQualifier	0	Niet gebruiken
@Format	1	Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"

Element/@Attribute	0..1	Omschrijving
@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 (N) van de medewerker. De handtekening dient geplaatst te zijn met behulp van het authenticatie certificaat op de pas. Alleen in het geval van een conditionele query en in het geval van opvraag door LSP+ zal de handetekening gezet worden met het UZI/PKIo-servercertificaat (van de autorisatieserver) van de applicatie.
Subject	1	De zorgverlener/medewerker die zich authenticeert. In het geval van een bevraging door een PGO zal dit de burger zijn.
BaseID	0	Niet gebruiken
NameID	1	Bevat zowel de UZI van de geauthenticeerde zorgverlener/medewerker alsmede diens rolcode. Alleen in het geval van de conditionele query en in het geval het token wordt aangemaakt door het LSP mag dit veld leeggelaten worden. In het geval het token van LSP+/LSP afkomstig is zal dit de BSN van de burger zijn met als rolcode 'P' van patiënt.
EncryptedID	0	Niet gebruiken
SubjectConfirmation	1	Moet aanwezig zijn
@Method	1	'urn:oasis:names:tc:SAML:2.0:cm:holder-of-key' In het geval het token van LSP+ afkomstig is 'urn:oasis:names:tc:SAML:2.0:cm:bearer'
SubjectConfirmationData	1	Moet aanwezig zijn
@Recipient	0	Niet gebruiken
@NotOnOrAfter	0..1	Moet aanwezig zijn indien @Method is 'urn:oasis:names:tc:SAML:2.0:cm:bearer'. De waarde mag maximal 15 minuten bedragen. Niet gebruiken indien de @Method is 'urn:oasis:names:tc:SAML:2.0:cm:holder-of-key' .
@InResponseTo	0	Niet gebruiken
@NotBefore	0	Niet gebruiken
@Address	0	Niet gebruiken
KeyInfo	0..1	Indien de @Method is 'urn:oasis:names:tc:SAML:2.0:cm:holder-of-key' dan bevat de X509 Issuer.serial van de zorgverlener-/medewerkerspas of het servercertificaat. Niet gebruiken indien @Method is 'urn:oasis:names:tc:SAML:2.0:cm:bearer'.
Conditions	1	Moet aanwezig zijn
@NotBefore	1	Moet aanwezig zijn.
@NotOnOrAfter	1	Moet aanwezig zijn. Mag maximaal 90 minuten na @NotBefore liggen.
Condition	0	Niet gebruiken
AudienceRestriction	1	Moet aanwezig zijn
Audience	1..*	Hier moet in ieder geval de ZIM als audience worden opgenomen urn:IIroot:2.16.840.1.113883.2.4.6.6:IIext:1 (is de ZIM) . Indien het token ook naar achterliggende systemen wordt gestuurd, dan dienen ook deze systemen als audience worden opgenomen.
ProxyRestriction	0	Niet gebruiken
Advice	0	Niet gebruiken
AuthnStatement	1	Moet aanwezig zijn

Element/@Attribute	0..1	Omschrijving
@AuthnInstant	1	Tijdstip van authenticatie van de gebruiker (Subject) of applicatie
@SessionIndex	0	Niet gebruiken
AuthnContext	1	Moet aanwezig zijn
AuthnContextClassRef	1	Ingeval van ondertekening met pas: urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI Ingeval van ondertekening met servercertificaat: urn:oasis:names:tc:SAML:2.0:ac:classes:X509
AttributeStatement	1	Moet aanwezig zijn
Attribute	0..1	Moet aanwezig zijn indien bericht aan één patient is gerelateerd.
@Name	1	Vaste waarde: “burgerServiceNummer”
AttributeValue	0..1	Het BSN van de patient.
Attribute	0..1	Moet aanwezig zijn indien het token wordt verstuurd i.c.m. HL7v3 messaging. Niet gebruiken indien het token wordt verstuurd i.c.m. FHIR.
@Name	1	Vaste waarde: “messageIdRoot”
AttributeValue	1	De waarde van de messageIdRoot bijvoorbeeld:2.16.528.1.1007.3.3.1234567.1
Attribute	0..1	Moet aanwezig zijn indien het token wordt verstuurd i.c.m. HL7v3 messaging. Niet gebruiken indien het token wordt verstuurd i.c.m. FHIR.
@Name	1	Vaste waarde: “messageIdExt”
AttributeValue	1	Het MessageId van het bericht.
Attribute	0..1	Moet aanwezig zijn indien het token wordt verstuurd i.c.m. HL7v3 messaging. Niet gebruiken indien het token wordt verstuurd i.c.m. FHIR.
@Name	1	Vaste waarde: “InteractionId”
AttributeValue	1	Het InteractionId van het Bericht (het extension-element).
Attribute	0..1	Moet aanwezig zijn indien het token wordt verstuurd i.c.m. FHIR. Niet gebruiken indien het token wordt verstuurd i.c.m. HL7v3 messaging
@Name	1	Vaste waarde: “Scope”
AttributeValue	1	De scope waarbinnen de bevraging plaatsvindt.
Attribute	0..1	Moet aanwezig zijn bij de Generieke Query. ~~In het geval van bevraging door een PGO alleen aanwezig indien er gebruik wordt gemaakt van een FHIR-operation.~~
@Name	1	Vaste waarde: “contextCodeSystem”
AttributeValue	1	2.16.840.1.113883.2.4.3.111.15.1
Attribute	0..1	Moet aanwezig zijn bij de Generieke Query
@Name	1	Vaste waarde: “contextCode”
AttributeValue	1	De contextcode uit de Generieke query.
Attribute	0..1	Moet aanwezig zijn indien gebruik gemaakt is van een mandaat
@Name	1	Vaste waarde: “autorisatieregel/context”
AttributeValue	1	URI waar de autorisatieregel/context gevonden kan worden waarbinnen het mandaat gegeven wordt.
Attribute	0..1	Moet aanwezig zijn indien gebruikt wordt binnen AORTA infrastructuur

Element/@Attribute	0..1	Omschrijving
@Name	1	Vaste waarde: “applicationID”
AttributeValue	1	ApplicatieID van de agerende applicatie Indien LSP+ zal hier de applicatieID van de resource server staan.
Attribute	0..1	Moet aanwezig zijn indien het token wordt verstuurd i.c.m. FHIR. Niet gebruiken indien het token wordt verstuurd i.c.m. HL7v3 messaging
@Name	1	Vaste waarde: “tokenversie”
AttributeValue	1	VersieID van het token
Attribute	0..1	Moet aanwezig zijn indien het token wordt verstuurd i.c.m. FHIR. Niet gebruiken indien het token wordt verstuurd i.c.m. HL7v3 messaging
@Name	1	Vaste waarde: “tokensoort”
AttributeValue	1	Vaste waard: “AORTA_Transactietoken”

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 transactietoken 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.

2.3 Inhoud

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

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

Het SAML transactietoken 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_ 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 assertion mag slechts eenmalig 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) 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".

2.3.2 Afzender

```
<saml:Issuer>
 <!-- De Issuer verwijst naar de organisatie van waaruit het totale bericht
verstuurd wordt.-->
     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

De OrganisatieID van LSP+ wordt uitgedrukt als een id onder het identificatiesysteem "….". De organisatieID wordt toegekend door VZVZ en betreft de vaste waarde …. .

2.3.3 Onderwerp

```
<saml:Subject>
  <saml:NameID>
   123456789:01.015
  </saml:NameID>
  <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:holder-of-key">
     <saml:SubjectConfirmationData>
       <saml:KeyInfo>
         <ds:X509Data>
           <ds:X509IssuerSerial>
             <ds:X509IssuerName>CN=...,...,O=...,C=NL</ds:X509IssuerName>
             <ds:X509SerialNumber>...834756977854956...</ds:X509SerialNumber>
           </ds:X509IssuerSerial>
         </ds:X509Data>
       </saml:KeyInfo>
     </saml:SubjectConfirmationData>
  </saml:SubjectConfirmation>
</saml:Subject>
```

De `Subject` verwijst naar de UZI van de zorgverlener/medewerker die de assertion heeft gegenereerd in combinatie met de rolcode van diezelfde zorgverlener/medewerker gescheiden door een dubbele punt (:). Indien het token afkomstig is van LSP+, dan zal hier de burger worden opgenomen met het BSN als id en rolcode 'P' gescheiden door een dubbele punt (:).

Alleen in het geval van een conditionele query (een query die automatisch door het systeem verstuurd wordt) en in het geval het token wordt aangemaakt door het LSP mag het nameID-element leeg gelaten worden.

In het geval van een conditionele query dient tevens een Mandaattoken [Mandaattoken] en een Inschrijftoken [Inschrijftoken] in het bericht opgenomen te zijn.

Vervolgens moet de SubjectConfirmation / SubjectConfirmationData / KeyInfo nog toegevoegd worden. Deze KeyInfo dient te verwijzen naar het certificaat waarmee het token ondertekend is.

Voor een beschrijving van de opbouw van de KeyInfo wordt verwezen naar hoofdstuk 4.4.3 Certificaatverwijzingen in document [IH tokens generiek].

2.3.4 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 maximaal toegestane verschil is 90 minuten voor transactietokens aangemaakt door GBZ-en. Dit maximum dient voor berichten die niet direct, maar bijvoorbeeld 's nachts verzonden worden, of kort voor de aanvang van een consult, zodat er iets ruimere mogelijkheden voor batchgewijze processen zijn. Het wordt sterk aanbevolen de SAML assertion direct (binnen 5 minuten) te gebruiken voor berichten die verzonden worden (dus terwijl de zorgverlener of medewerker 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. Voor het een transactietoken aangemaakt door LSP+ geldt de maximum van 15 minuten. Deze tijd is gebaseerd op de geldigheidsduur van het access token zoals uitgegeven is door de autorisatieserver.

De geldigheidsduur van een token (*NotOnOrAfter* minus *NotBefore*) mag niet langer dan 90 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.

De geldigheidsduur van een token (*NotOnOrAfter* minus *NotBefore*) mag niet langer dan 15 minuten zijn indien het token van LSP+ afkomstig is.

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 UZI-pas.

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 vaste waarden voor de ZIM. Indien het token ook moet worden verstuurd naar achterliggende systemen dan geldt dat bij de audience ook de applicatieID ingevuld dient te worden van het betreffende ontvangende systeem (urn:IIroot:2.16.840.1.113883.2.4.6.6:IIext:{applicatieID}).

```
<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 het achterliggende systeem -->
  <saml:Audience>urn:IIroot:2.16.840.1.113883.2.4.6.6:IIext:300</saml:Audience>
</saml:AudienceRestriction>
```

Voor de `<Audience>` parameter is (ook) gekozen voor URN, zie voor opbouw paragraaf 2.3.2 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 zorgverlener of medewerker, 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>
```

Als het transactietoken ondertekend is met het servercertificaat dan dient de `AuthnContextClassRef` de waarde `urn:oasis:names:tc:SAML:2.0:ac:classes:X509` te krijgen.

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.

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

Afsluiting authentication statement.

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 of gegevens die extra toegevoegd zijn bij een FHIR-search. 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.

InteractionId

```
<saml:Attribute Name="interactionId">
  <saml:AttributeValue>QURX_IN990011NL</saml:AttributeValue>
</saml:Attribute>
```

Het attribuut interactionId wordt altijd meegetekend. De interactionId geeft een directe relatie met het berichttype. 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.

In het geval dat het transactietoken wordt meegestuurd met een FHIR-search, dan wordt hier geen invulling aangegeven.

Scope

```
<saml:Attribute Name="scope">
  <saml:AttributeValue>’medmij.gegevensdienst.6’</saml:AttributeValue>
</saml:Attribute>
```

Indien het transactietoken is bijgesloten bij een FHIR-search vanuit LSP+, dan zal dit veld gevuld moeten worden met de ‘scope’ waarbinnen de bevraging geldig is. De waarde bevat een string met de tekst gescheiden door punten: ‘medmij.gegevensdienst.<*identifier van de gegevensdienst*>’.

contextCode

```
<saml:Attribute Name="contextCodeSystem">
  <saml:AttributeValue>2.16.840.1.113883.2.4.3.111.15.1</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="contextCode">
  <saml:AttributeValue>KZDI</saml:AttributeValue>
</saml:Attribute>
```

In het geval er sprake is van een opvraag op basis van een context dient ook de contextCode meegetekend te worden. Dit is in principe alleen het geval bij de generiekeQueryZorggegevens. Bij deze generieke query is het trigger event niet meer voldoende om de intentie van de verzender aan te geven, aangezien deze altijd gelijk is. Door het toevoegen van de contextCode wordt deze intentie wel weer expliciet gemaakt. De codes zijn te vinden in het vocab bestand 2.16.840.1.113883.2.4.3.111.15.1.xml.

In het geval dat het transactietoken wordt meegestuurd met een FHIR-operation, dan is het mogelijk om de ‘operation’ hierin op te nemen. Vooralsnog wordt dit niet gebruikt.

```
<saml:Attribute Name="contextCode">
  <saml:AttributeValue>'Operation'</saml:AttributeValue>
</saml:Attribute>
```

messageId

```
<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.

In het geval dat het transactietoken wordt meegestuurd met een FHIR-search, dan wordt hier geen invulling aangegeven.

burgerServiceNummer

```
<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. Hierbij zijn twee situaties te onderscheiden:

- Logistieke berichten; het bericht betreft géén informatie gerelateerd tot een specifieke patiënt;
- Medische berichten; het bericht betreft medische informatie gerelateerd tot een specifieke patiënt(en), maar waarvan het BSN niet bekend is. In de implementatiehandleiding van een zorgtoepassing zal bij de betreffende interactie expliciet benoemd staan, dat een patiëntidentificatie niet voorkomt of optioneel is.

autorisatieregel/context

Alleen indien gebruik gemaakt wordt van een mandaat dient het volgende attribuut toegevoegd te worden:

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

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

In het voorbeeld is voor een URL gekozen.

applicationID

Indien het transactietoken gebruikt wordt binnen de AORTA infrastructuur is het applicatieID verplicht:

```
<saml:Attribute Name="applicationID">
      <!-- Applicatie-id van de GBZ-applicatie, zoals toegekend bij aansluiting.-->
      <saml:AttributeValue>urn:IIroot:2.16.840.1.113883.2.4.6.6:IIext:?
      </saml:attributeValue>
</saml:Attribute>
```

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 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 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
```

Tokenversie

Indien het transactietoken verstuurd wordt in combinatie met een FHIR-search dan dient er een attribuut opgenomen te worden waar het versienummer van het token in is opgenomen. Het gaat hierbij om een tweenummerig versienummer (X.Y). Bij een wijziging in het token, waarvan de wijziging niet backwards compatibel is, zal het eerste nummer (X) opgehoogd worden. In het geval een token wel backwards compatibel is, dan zal het tweede nummer (Y) opgehoogd worden.

```
<saml:Attribute Name="tokenversie">
      <!—Versie van het token -->
      <saml:AttributeValue>2.3</saml:attributeValue>
</saml:Attribute>
```

Tokensoort

Indien het transactietoken verstuurd wordt in combinatie met een FHIR-search dan dient er een attribuut opgenomen te worden waar het soort token in is opgenomen. In dit veld zal de vaste waarde "AORTA_Transactietoken" kunnen voorkomen.

```
<saml:Attribute Name="tokensoort">
      <!—Soort token -->
      <saml:AttributeValue>"AORTA_Transactietoken"</saml:attributeValue>
</saml:Attribute>
```

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="interactionId">
   <saml:AttributeValue>QURX_IN990011NL</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:Attribute Name="autorisatieregel/context">
<saml:AttributeValue>https://goedbeheerdziekenhuis/autorisatieregels/medicatieconte
xt/v2</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute Name="applicationID">
   <saml:AttributeValue>urn:IIroot:2.16.840.1.113883.2.4.6.6:IIext:300
   </saml:AttributeValue>
  </saml:Attribute>
</saml:AttributeStatement>
```

Tenslotte wordt het attributen statement blok afgesloten met

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

Een transactietoken die meegestuurd wordt met een FHIR-search ziet er bijvoorbeeld als volgt uit:

```
<saml:AttributeStatement>
  <saml:Attribute Name="scope">
   <saml:AttributeValue>'medmij.gegevensdienst.6'</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute Name="burgerServiceNummer">
```

```
    <saml:AttributeValue>950052413</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute Name="applicationID">
    <saml:AttributeValue>urn:IIroot:2.16.840.1.113883.2.4.6.6:IIext:5
    </saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute Name="tokenversie">
    <saml:AttributeValue>2.3</saml:attributeValue>
  </saml:Attribute>
  <saml:Attribute Name="tokensoort">
     <saml:AttributeValue>”AORTA_Transactietoken”</saml:attributeValue>
  </saml:Attribute>
</saml:AttributeStatement>
```

2.4 Algoritmes

Om de integriteit en onweerlegbaarheid van het SAML transactietoken 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 persoons- of organisatiegebonden PKIoverheid-certificaat van de verzender en de CA certificaten zoals verstrekt door PKIoverheid, onomstotelijk vaststellen dat het SAML transactietoken ondertekend is met de privé sleutel behorend bij het gebruikte certificaat van de zorgmedewerker of de organisatie.

De XML Signature van het SAML transactietoken die gebruikt wordt bij berichtauthenticatie met behulp van een UZI-certificaat 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 transactietoken en in het SAML transactietoken geplaatst wordt, moet er een "enveloped-signature" transformatie uitgevoerd worden die de Signature tags uit het SAML transactietoken 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 transactietoken – 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 transactietoken. 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>
      <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 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.

2.5.2 Plaats van het SAML token en de digitale handtekening

De plaats van de SAML-token is afhankelijk van de berichtstandaard.

Voor HL7v3-berichten wordt het SAML transactietoken met daarin de digitale handtekening 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>
```

Voor FHIR-searches wordt het SAML transactietoken met daarin de digitale handtekening in de HTTP-header opgenomen.

3 Certificaten

3.1 Te gebruiken certificaat en attributen

De UZI-pas/certificaat kent een aantal modellen:

Tabel AORTA.STK.t3210 – UZI pastype

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

De pas of het certificaat die gebruikt wordt voor het ondertekenen van een transactietoken moet een zorgverlenerpas,een medewerkerpas op naam zijn of een servercertificaat. 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. Indien de verzender van het transactietoken LSP+ is, dan zal er gebruik worden gemaakt van een PKIo-servercertificaat.

Indien i.h.k.v. de conditionele query gebruik gemaakt wordt van een servercertificaat, dan geldt het volgende: een GBZ dient voor transportbeveiliging bij voorkeur een ander servercertificaat te gebruiken dan voor berichtauthenticatie. Dit is met name van toepassing wanneer ondertekening niet via een zelfde key-store verloopt dan dat van de TLS-verbinding. De verschillende certificaten horen daarbij in verschillende componenten ondergebracht te zijn in de architectuur van het XIS.

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-certificaten zijn:

Tabel AORTA.STK.t3220 – DN attributen van UZI-certificaten

Attribuut	Omschrijving	Waarde
CN	Issuer.commonName	*Derde generatie:* UZI-register Zorgverlener CA G3 Voor mogelijke volgende generaties wordt verwezen naar het UZI-register: 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.

Om de digitale handtekening bij het LSP en bij een ontvangende GBx 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 en UZI-testcertificaten 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 transactietoken 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.

Voor het transactietoken in combinatie met het FHIR-search zijn op sommige velden geen controles vereist, dit heeft onder ander te maken dat het transatietoken in dat geval het doel van gegevensdrager van de gegevens richting de GBZ heeft. Indien dat het geval is, dan zal dat hieronder bij de controles vermeld staan.

De ontvanger controleert of de WS-Security SOAP Header voor hem bestemd is, zie soap attribuut actor. Indien in het geval van een FHIR-search de SOAP Header ontbreekt, dan kan de ontvanger er vanuit gaan dat het token voor hem bedoeld is.

Het SAML transactietoken wordt door de ontvanger uit de HTTP-header, of 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 transactietoken moet de ontvanger controleren of:

- Het attribuut ID van het Assertion element een unieke waarde heeft, welke slechts eenmalig gebruikt mag worden, zie paragaaf 2.3.1 Uniekheid;
- De aanduiding voor de versie van SAML gedefinieerd is op "2.0", zie paragaaf 2.3.1 Uniekheid;
- De juiste organisatieID is opgenomen die deze assertion heeft gecreëerd en de gebruiker heeft geauthenticeerd, zie paragraaf 2.3.2 Afzender. Het zorgaanbiederID in het token dient overeen te komen met de zorgaanbiederID in het bericht. Voor het transactietoken in het FHIR-search dient alleen gecontroleerd te worden op correctheid van het veld in het token;
- Indien Conditionele Query (token is ondertekend met een certificaat met certificaattype “S”): de NameID van het Subject is wel aanwezig maar leeg, zie paragraaf 2.3.3 Onderwerp; Tevens dient er een mandaattoken en inschrijftoken aanwezig te zijn; In overige gevallen: Het UZI-nummer en rolcode van het authenticatiecertificaat, gebruikt voor de ondertekening van de Assertion, overeenkomt met de NameID van het Subject en met de authorOrPerformer in het bericht zie paragraaf 2.3.3 Onderwerp;
- De Assertion correct is ondertekend door de Signature te valideren met het gerefereerde authenticatiecertificaat.
- Het gebruikte certificaat en de relevante certificaatketen te valideren op geldigheid, inclusief revocatie.
- Het bericht ontvangen is binnen de geldigheidsperiode van het token, zie paragraaf 2.3.4 Geldigheid;
- De afnemer van het SAML transactietoken (audience) de ZIM is, zie paragraaf 2.3.5 Ontvanger. Indien het transactietoken ontvangen wordt door een GBZ, dan dient deze te controleren of een applicatie opgenomen in het ‘audience’-veld overeenkomt met de door de applicatie gebruikte applicatieID;
- Indien gebruik gemaakt is van een mandaat, dan dient er een getekend mandaattoken te zijn opgenomen in de SOAP-header (zie [Mandaattoken]). Het attribuut `"autorisatieregel/context"` dient identiek te zijn aan het overeenkomstige attribuut in het mandaattoken. Daarnaast dient de organisatieID in beide tokens overeen te komen.

- Indien geen Conditionele Query: De zorgverlener/zorgmedewerker is geauthenticeerd via het voorgedefinieerde authenticatiemiddel, de SmartCardPKI, zoals beschreven in paragraaf 2.3.6 Authenticatie;
- Indien Conditionele Query of een FHIR-search afkomstig van LSP+: Het systeem is geauthenticeerd via het voorgedefinieerde authenticatiemiddel, Het X509 servercertificaat, zoals beschreven in paragraaf 2.3.6 Authenticatie;
- 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;
- Alleen die attributen zijn gedefinieerd, die zijn beschreven in paragraaf 2.3.7 Attributen;
- In het geval van een HLv3-bericht de attribuutwaarde van interactionId overeenkomt met *het extension-element* van het HLv3 bericht, zie paragraaf 2.3.7 Attributen.
- In het geval van een transactietoken dat is meegestuurd met een FHIR-search dient er een scope opgenomen te zijn;
- In het geval van een generieke query dient er een contextcode te zijn opgenomen. De contextcode dient overeen te komen met de contextcode in het bericht, zie paragraaf 2.3.7 Attributen;.
- De attribuutwaarden van messageIdRoot en messageIdExt overeenkomt met de gebruikte HL7v3 message.id. In het geval van een FHIR-search worden deze velden niet gevuld, zie paragraaf 2.3.7 Attributen;
- Indien de interactie patient-specifiek is: de attribuutwaarde van burgerServiceNummer overeenkomt met het BSN in het HL7v3 bericht of de FHIR search. Ofwel dat de gegevens in het bericht daadwerkelijk betrekking hebben op de persoon, zie paragraaf 2.3.7 Attributen. De volgende situaties zijn hierbij te onderscheiden:
    - Wel BSN in token en in bericht; er is sprake van een goedsituatie indien BSN overeenkomt. Indien dat niet het geval is, is er sprake van een foutsituatie;
    - Wel BSN in token en niet in het bericht; er is sprake van een foutsituatie;
    - Geen BSN in token en wel in bericht; er is sprake van een foutsituatie;
    - Geen BSN in token en geen BSN in het bericht; er is sprake van een goedsituatie.
- Indien het token gebruikt wordt binnen de AORTA infrastructuur moet de juiste applicatieID zijn vastgelegd die deze assertion heeft gecreëerd en de gebruiker heeft geauthenticeerd. In het geval van een HL7v3-bericht dient hetapplicatieID overeen te komen met de Message/sender/device/id in de transmission wrapper van het HL7v3 bericht;

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 of een HTTP-foutmelding in het geval van een FHIR-search, zie foutafhandeling in [IH tokens generiek].

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

Bijlage A Referenties

Referentie	Document	Versie
[IH tokens generiek]	AORTA_Auth_IH_Security_tokens_generiek	8.2.0.0
[Mandaattoken]	AORTA_Auth_IH_Mandaattoken	8.2.0.0
[Inschrijftoken]	AORTA_Auth_IH_Inschrijftoken	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