IMPLEMENTATIEHANDLEIDING MITZ

Berichtauthenticatie

Versie: 3.8.0
Status: Definitief
Datum: 21 juni 2021

WIJZIGINGENBEHEER

Versie	Hoofdstuk	Auteur	Opmerkingen
3.6.0.0		DD	Concept versie Berichtauthenticatie OID voor Mitz toegevoegd KeyInfo in de vorm van X509Issuer.serial; BSN als resource-id. Issuer in de vorm van een URL toegestaan
3.6.0.0		FS	Ter goedkeuring versie 3.6.0.0 release na interne review
3.6.0.0		AV	Definitieve versie 3.6.0.0
3.6.1		AV	Definitieve versie 3.6.1
3.6.2		AV	Definitieve versie 3.6.2
3.7.0.TV		FS	Uitwerking migratie interne review v3.7.0
3.7.0.TG		FS	Uitwerking migratie externe review v3.7.0
3.7.0		FS	Definitieve versie 3.7.0
3.8.0.TV		FS	Uitwerking toestemmingsknop v3.8.0 interne review
3.8.0.TG		FS	Uitwerking toestemmingsknop v3.8.0 externe review
3.8.0		FS	Definitieve versie 3.8.0

DOEL

Dit document heeft tot doel een handleiding te geven voor de implementatie van het transactietoken die op het koppelvlak tussen Mitz en US door de zender meegestuurd wordt met het bericht. Daarnaast wordt de afhandeling van het transactietoken door de ontvanger beschreven.

Dit document is bedoeld voor softwareontwikkelaars die berichten willen uitrusten met het SAML transactietoken. Daarnaast wordt het plaatsen van de digitale handtekening besproken (zie ook [IH Security Tokens Generiek]).

INHOUDSOPGAVE

1 INTRODUCTIE

Het programma “Online Toestemmingsvoorziening (OTV)” streeft naar het gebruik van open standaarden, omdat daardoor een open koppelvlak ontstaat waarop de leveranciers die dat wensen hun producten en diensten kunnen koppelen. Daarnaast zijn open standaarden van belang omdat componenten die al gebouwd en gebaseerd zijn op deze standaarden, hergebruikt kunnen worden en dat is efficiënter en goedkoper dan maatwerk ontwikkelen en bouwen. In die situatie zouden bijvoorbeeld bestaande internationale componenten ‘slechts’ geconfigureerd hoeven te worden voor de Nederlandse situatie, in plaats van volledig opnieuw geprogrammeerd.

Dit document beschrijft de implementatie van het transactietoken die op het koppelvlak tussen Mitz en US door de zender meegestuurd wordt met het bericht.

2 HET SAML TRANSACTIETOKEN

In dit hoofdstuk wordt de inhoud van het SAML transactietoken besproken die bij berichtauthenticatie wordt gebruikt. Het SAML transactietoken bevat informatie over de toegepaste authenticatie en identificatie. 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.

2.1 STRUCTUUR

Het SAML transactietoken is een afgegeven SAML assertion die gebruikt wordt bij berichtauthenticatie. 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.
@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 het PKIo-servercertificaat van de Issuer. De handtekening dient geplaatst te zijn met behulp van een ander servercertificaat dan waarmee de TLS-sessie wordt opgezet.
Subject	1	Bevat het OrganisatieID van de zendende applicatie.
BaseID	0	Niet gebruiken
NameID	0	
EncryptedID	0	Niet gebruiken
SubjectConfirmation	1	Moet aanwezig zijn
@Method	1	'urn:oasis:names:tc:SAML:2.0:cm:holder-of-key'

Element / @Attribute	0..1	Omschrijving
SubjectConfirmationData	0	Niet gebruiken
@Recipient	0	Niet gebruiken
@NotOnOrAfter	0	Niet gebruiken
@InResponseTo	0	Niet gebruiken
@NotBefore	0	Niet gebruiken
@Address	0	Niet gebruiken
KeyInfo	1	Bevat het servercertificaat.
Conditions	1	Moet aanwezig zijn
@NotBefore	1	Moet aanwezig zijn.
@NotOnOrAfter	1	Moet aanwezig zijn. Mag maximaal 10 minuten na @NotBefore liggen.
Condition	0	Niet gebruiken
AudienceRestriction	1	Moet aanwezig zijn
Audience	1	Verwijzing naar de ontvanger(s) van het token.
ProxyRestriction	0	Niet gebruiken
Advice	0	Niet gebruiken
AuthnStatement	1	Moet aanwezig zijn
@AuthnInstant	1	Tijdstip van authenticatie van de Subject
@SessionIndex	0	Niet gebruiken
AuthnContext	1	Moet aanwezig zijn
AuthnContextClassRef	1	Ingeval van ondertekening met servercertificaat: urn:oasis:names:tc:SAML:2.0:ac:classes:X509
AttributeStatement	1	Moet aanwezig zijn
Attribute	1	Moet aanwezig zijn
@Name	1	Vaste waarde: “burgerServiceNummer”
AttributeValue	1	Het BSN van de patiënt.

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

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 Security 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 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:oid:2.16.840.1.113883.2.4.3.111.2.1
</saml:Issuer>
```

De OrganisatieID wordt uitgedrukt met behulp van een URN (Uniform Resource Name) of met behulp van een URL (Uniform Resource Locator).

Indien een URN gebruikt wordt dan is de URN opgebouwd uit:

```
"urn:oid:"<OID voor organisatieId>"
```

OrganisatieID's worden uitgedrukt als een Object Identifier (OID). De OID uit het voorbeeld verwijst naar de organisatie Mitz.

Indien een URL gebruikt wordt dan ziet het voorbeeld van de Issuer er als volgt uit:

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

NB.: het voorbeeld is fictief. De string "https://mijnmitz.nl/mitz" dient nog een uiteindelijke waarde te krijgen.

2.3.3 ONDERWERP

```
<saml:Subject>
  <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:holder-of-key">
     <saml:SubjectConfirmationData>
       <saml:KeyInfo>
                <ds:X509Data>
                    <!-- Het certificaat -->
                    <ds:X509Certificate>MIIFd...PZaIvdgXOQ==</X509Certificate>
               </ds:X509Data>
        </saml:KeyInfo>
      </saml:SubjectConfirmationData>
  </saml:SubjectConfirmation>
</saml:Subject>
```

Het `Subject` verwijst naar de entiteit die de assertion heeft gegenereerd.

Vervolgens moet de SubjectConfirmation / SubjectConfirmationData / KeyInfo nog toegevoegd worden. In deze KeyInfo dient het certificaat waarmee het token ondertekend is als base64 string opgenomen te zijn.

Voor een beschrijving van de opbouw van de KeyInfo wordt verwezen naar hoofdstuk 4.4.2 Certificaat meezenden als KeyInfo in document [IH tokens generiek].

2.3.4 GELDIGHEID

```
<saml:Conditions
 NotBefore="2009-06-24T11:47:34Z"
 NotOnOrAfter="2009-06-24T11:57:34Z">
```

Het attribuut *NotBefore* is de tijd waarop de SAML assertion geldig wordt.

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. Het maximaal toegestane verschil is 10 minuten.

De geldigheidsduur van een token (*NotOnOrAfter* minus *NotBefore*) mag niet langer dan 10 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 **Fout! Verwijzingsbron niet gevonden. Fout! Verwijzingsbron niet gevonden.**.

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

2.3.5 ONTVANGER

```
<saml:AudienceRestriction>
  <!-- Root en extensie van het ontvangende US -->
  <saml:Audience>urn:oid:2.16.840.1.113883.2.4.3.111.2.1</saml:Audience>
</saml:AudienceRestriction>
```

In de `AudienceRestriction` wordt beschreven aan wie de SAML assertion is gericht. De `<Audience>` parameter wordt uitgedrukt met behulp van een URN (Uniform Resource Name) of met behulp van een URL (Uniform Resource Locator), zie voor opbouw paragraaf **Fout! Verwijzingsbron niet gevonden.** REF _Ref284431491 \h **Fout! Verwijzingsbron niet gevonden.**.

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 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:X509
  </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 componenten.

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

Afsluiting authentication statement.

2.3.7 ATTRIBUTEN

```
<saml:AttributeStatement>
```

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

burgerServiceNummer

```
<saml:Attribute Name="urn:oasis:names:tc:xacml:1.0:resource:resource-id">
  <saml:AttributeValue><InstanceIdentifier root="2.16.840.1.113883.2.4.6.3"
extension="950052413" xmlns="urn:hl7-org:v3"/></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.

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="urn:oasis:names:tc:xacml:1.0:resource:resource-id">
              <saml:AttributeValue>
<InstanceIdentifier root="2.16.840.1.113883.2.4.6.3" extension="950052413" xmlns="urn:hl7-
org:v3"/>
</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 Security Tokens Generiek]. Na plaatsen van de XML Signature kan de ontvanger onomstotelijk vaststellen dat het SAML transactietoken ondertekend is met de privé sleutel behorend bij het gebruikte certificaat van de afzender van het bericht.

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>
                    <!-- Het certificaat -->
                    <ds:X509Certificate>MIIFd...PZaIvdgXOQ==</X509Certificate>
               </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 Base64 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 het certificaat in het KeyInfo blok op, in de vorm van een Base64 string.

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

Het SAML transactietoken met daarin de digitale handtekening wordt in het WS-Security SOAP Header gezet indien het een SOAP bericht betreft. Indien het een FHIR bericht betreft wordt het SAML token (de SAML assertion) in de HTTP-header geplaatst. Het token is optioneel. Op het `<wss:Security>` element zal een `soap:mustUnderstand="1"` vlag opgenomen worden, die aangeeft dat de ontvanger dit security element **moet** verwerken.

```
<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.mijnmitz.nl/actor/mitz" 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

Het certificaat dat gebruikt wordt voor het ondertekenen van een transactietoken moet een servercertificaat zijn. Dit servercertificaat moet een ander certificaat zijn dan waarmee de TLS-sessie wordt opgezet. De signature wordt gezet met de sleutel voor authenticiteit (keyUsage=digitalSignature, hexadecimaal 0x80).

De attributen in het certificaat worden gegeven in de vorm van een *Distinguished Name (*DN), zie [IH Security Tokens Generiek].

De waarden van deze attributen voor de relevante certificaten zijn:

Attribuut	**Omschrijving**	**Waarde**
CN	Issuer.commonName	
O	Issuer.organisationName	
C	Issuer.countryName	NL

TABEL AORTA.STK.T3220 – DN ATTRIBUTEN VAN CERTIFICATEN

Om de digitale handtekening te verifiëren, moet de ontvanger over de bijbehorende publieke sleutel beschikken, zie [IH Security Tokens Generiek].

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 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 Header voor hem bestemd is.

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

- 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, zie paragraaf **Fout! V erwijzingsbron niet gevonden. Fout! Verwijzingsbron niet gevonden.**. Het zorgaanbiederID in het token dient overeen te komen zorgaanbiederID die de TLS-tunnel heeft opgezet;
- Het servercertificaat waarmee de ondertekening heeft plaatsgevonden is niet hetzelfde als het servercertificaat waarmee de TLS tunnel is opgezet.
- De Assertion correct is ondertekend door de Signature te valideren met het gerefereerde authenticatie certificaat.
- Het gebruikte certificaat uit het token ook in de certificate store voorkomt.
- 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 **Fout! V erwijzingsbron niet gevonden. Fout! Verwijzingsbron niet gevonden.**;
- Alleen die attributen zijn gedefinieerd, die zijn beschreven in paragraaf **Fout! Verwijzingsbron niet g evonden. Fout! Verwijzingsbron niet gevonden.**;
- de attribuutwaarde van burgerServiceNummer overeenkomt met het BSN in het bericht ofwel dat de gegevens in het bericht daadwerkelijk betrekking hebben op de persoon, zie paragraaf **Fout! V erwijzingsbron niet gevonden. Fout! Verwijzingsbron niet gevonden.**.

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

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

BIJLAGE A REFERENTIES

Referentie	Document	Versie
[IH Security Tokens Generiek]	VZVZ_Mitz_Implementatiehandleiding_Security_Tokens_Generiek	3.8.0
[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