# *Zorgplatform Service authenticatie protocol*

**ChipSoft B.V.**
• Orlyplein 10, 1043 DP Amsterdam
• Postbus 37039, 1030 AA Amsterdam
• Tel: +31 (0)20 4939000 • Fax: +31 (0)20 6331975
• www.chipsoft.nl • marketing@chipsoft.nl

• K.V.K. nummer Amsterdam: 33.205.099 • IBAN: NL35ABNA089583083 • BIC: ABNANL2A

# Inhoudsopgave


1 Inleiding ..... 5
2 Belangrijke concepten en termen ..... 6
3 Gebruikte standaarden ..... 7
4 Usecase ..... 7
4.1 Relaties met andere use cases en protocollen ..... 7
5 Systeem architectuur ..... 8
6 Betrokken actoren ..... 9
7 Happy flow ..... 9
7.1 Issue (T1) ..... 10
7.1.1 Beveiliging ..... 10
7.1.2 RequestSecurityToken in de Issue operatie ..... 10
7.1.3 HealthCare Professional token (HCP token) in de Issue operatie ..... 11
7.1.4 Voorbeeld voor HCP token Request ..... 13
7.1.5 Application token in de Issue operatie ..... 15
7.1.6 Voorbeeld voor Application token Request ..... 16
7.2 Validate / Generate (T2) ..... 18
7.3 Response (T3) ..... 18
7.3.1 RequestSecurityTokenResponse als resultaat van de Issue operatie ..... 18
7.3.2 HealthCare Professional token (HCP token) in het RequestSecurityTokenResponse ..... 18
7.3.3 Voorbeeld voor HCP token Response ..... 19
7.3.4 Application token in het RequestSecurityTokenResponse ..... 21
7.3.5 Voorbeeld voor Application token Response ..... 22
7.4 Verwerken RSTR (T4) ..... 24
7.5 Call naar Zorgplatform Resource server (T5) ..... 24
8 Unhappy flow ..... 24

# 1 Inleiding

Het Zorgplatform ‘Service authenticatie’ protocol faciliteert authenticatie van een applicatie van een derde partij, al dan niet namens een zorgverlener.

# 2 Belangrijke concepten en termen

**Partnerapplicatie**
Een partnerapplicatie is een applicatie die wordt aangesloten op Zorgplatform.

**Security Token**
Ook wel 'Access Token'. Bevat security informatie, zoals identiteit, rol of toegangsrechten, over een persoon of systeem. Er zijn meerdere implementaties van deze abstracte term, waarvan Healthcare professional token en Application token twee types van implementaties zijn.

**Workflow specific token**
Een security token kan de eigenschap 'Workflow specific' hebben. Zorgplatform tokens beperken de toegang tot resources (services) gerelateerd aan een specifieke patiënt of aan een specifieke workflow. Deze laatste tokens worden 'workflow specific tokens' genoemd. Alle Zorgplatform token-types kunnen als workflow specific token ingezet worden.

**Healthcare Professional token (HCP token)**
Dit betreft een security token dat door een applicatie wordt aangevraagd uit naam van de (actieve) gebruiker om toegang te krijgen tot Zorgplatform services voor een specifieke patiënt. In dit document wordt doorgaans de afkorting HCP token gebruikt.

**Application token**
Dit betreft een security token dat door een applicatie zelf wordt aangevraagd en niet uit naam van de (actieve) gebruiker. Een application token wordt gebruikt in het geval van automatische processen, zoals bijvoorbeeld processen die automatisch opstarten op bepaalde tijden of naar aanleiding van een ander geautomatiseerd event.

**Security Token Service (STS)**
Systeem dat verantwoordelijk is voor het uitgeven (en vernieuwen of intrekken) van security tokens.

**Trust relationship**
Binnen een 'trust relationship' vertrouwt een systeem een bepaalde security taak toe aan een ander systeem. Systeem 'A' kan bijvoorbeeld het authentiseren van gebruikers toevertrouwen aan (uitsluitend) systeem 'B'. Dit betekent dat als systeem B 'beweert' dat een gebruiker 'user1' geauthentiseerd is, systeem A erop vertrouwd dat systeem B de authenticatie correct (volgens een afgesproken policy) heeft uitgevoerd.

Hoe weet systeem A nu of de bewerking 'user1 is geauthentiseerd' afkomstig is van systeem B? En niet bijvoorbeeld van systeem C of van een 'man in the middle' die een door systeem B afgegeven bewering heeft aangepast? Binnen een trust relationship wordt public key cryptografie gebruikt om een onweerlegbare relatie tussen de systemen te creëren. Systeem B kan bijvoorbeeld de bewering 'user1 is geauthentiseerd' digitaal ondertekenen met een private key zodat systeem A kan verifiëren dat de bewering inderdaad afkomstig is van systeem B.

# 3 Gebruikte standaarden

| Standaard/ protocol | Gebruik |
|---|---|
| WS-Security | Alle SOAP calls naar Zorgplatform (waaronder calls naar de Zorgplatform STS) worden voorzien van een security token conform de WS-Security standaard |
| WS-Trust 1.3 | Opvragen van Healthcare Professional token (HCP token) of Application tokens bij de Zorgplatform Security Token Service (STS) |
| SAML2.0 | Zorgplatform gebruikt uitsluitend SAML2 assertions als security token |
| IHE-XUA | Zorgplatform SAML 2.0 assertions voldoen aan het IHE XUA integration profile |
| IHE-ATNA | Conform IHE ATNA maakt Zorgplatform gebruik van dubbelzijdig TLS met client authenticatie. Dit speelt bij het opvragen van security tokens bij de Zorgplatform STS |
| HTTP | Zorgplatform RESTful APIs maken gebruiken van de HTTP Authorization header voor de authenticatie van partnerapplicatie calls. |

# 4 Usecase

Een token wordt aangevraagd door een partnerapplicatie bij de Zorgplatform STS en wordt gebruikt om toegang te krijgen tot Zorgplatform services voor een specifieke patiënt. Het token wordt aangevraagd voor de applicatie zelf (een Application token) of voor een specifieke (actieve) gebruiker (een Healthcare Professional Token).

Het opgevraagde token wordt meegegeven bij het aanroepen van de Zorgplatform SOAP en/ of RESTful (FHIR) API's.

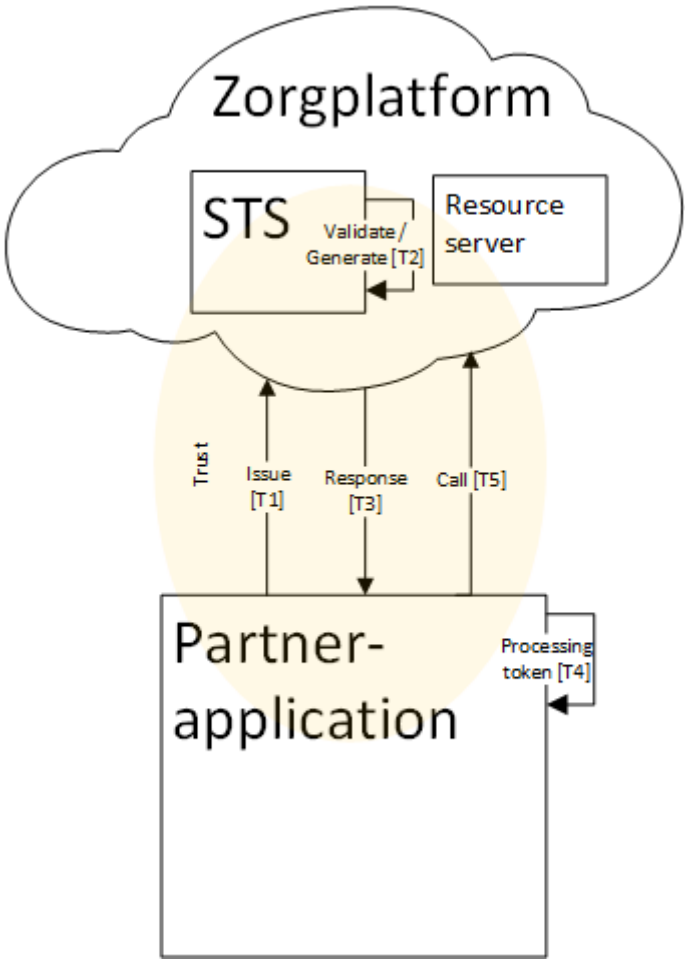
## 4.1 Relaties met andere use cases en protocollen

Het Zorgplatform Service authenticatie protocol wordt in verschillende andere protocollen gebruikt:

- Home monitoring
- Et cetera

Dit protocol kan in combinatie met het Zorgplatform Web Browser Single-Sign-On protocol gebruikt worden wanneer er een Single-Sign-On tussen twee partnerapplicaties wordt opgezet.

# 5 Systeem architectuur




Het aanvragen en verwerken van een HCP token of Application token werkt globaal als volgt:

| # | Omschrijving | Afhankelijke standaarden |
|---|---|---|
| T1 | De partnerapplicatie vraagt een HCP token of een Application token aan bij de Zorgplatform STS | - WS-Trust RequestSecurityToken<br>- WS-Security<br>- SAML2.0<br>- IHE-XUA<br>- IHE-ATNA |
| T2 | Zorgplatform STS valideert het verzoek van de partnerapplicatie, genereert een HCP token of een application token en ondertekent deze. | |
| T3 | Zorgplatform STS retourneert het gegenereerde token naar de partnerapplicatie | - WS-Trust RequestSecurityTokenResponse<br>- WS-Security<br>- SAML 2.0<br>- IHE-XUA<br>- IHE-ATNA |
| T4 | De partnerapplicatie verwerkt het token | |
| T5 | De partnerapplicatie voert een call uit naar Zorgplatform Resource server, waarbij de HCP token of Application token als security item meegestuurd | - WS-Trust<br>- WS-Security<br>- SAML 2.0 |

| | | |
|---|---|---|
| | wordt. | - IHE-XUA<br>- IHE-ATNA<br>- HTTP |

# 6 Betrokken actoren

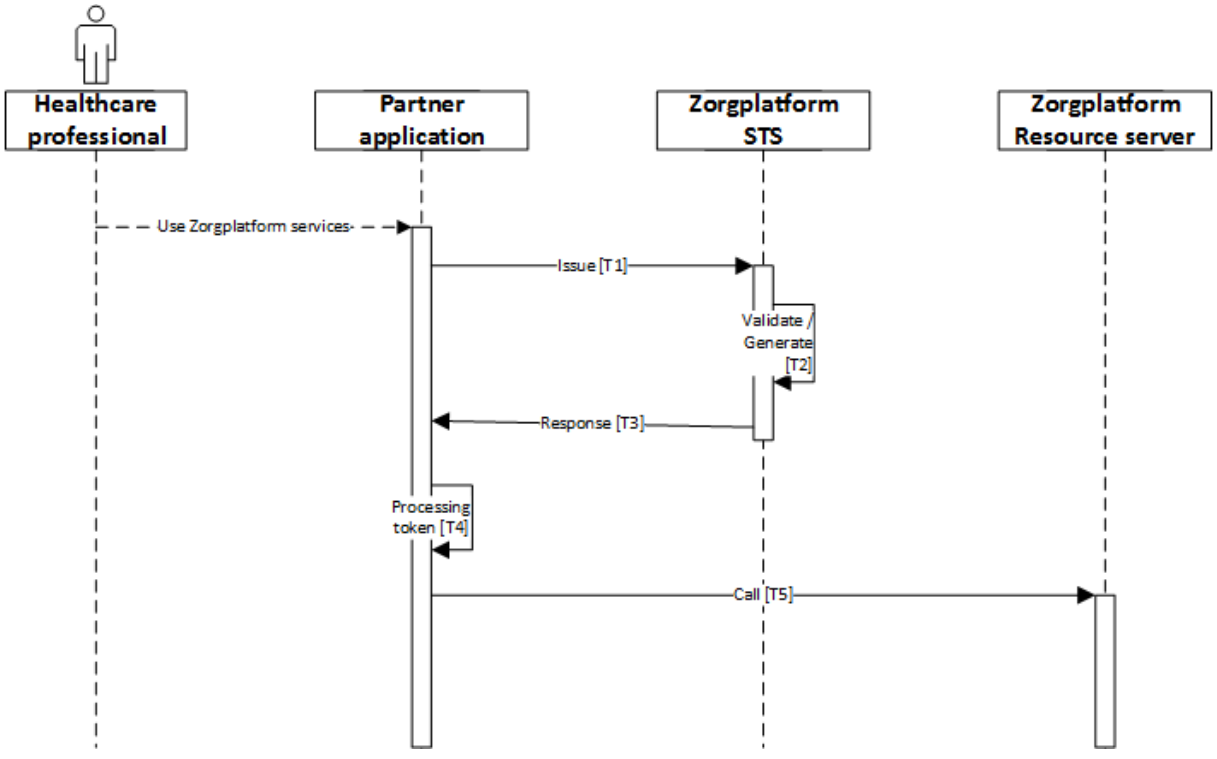
**Partner application**
Een partnerapplicatie is een applicatie die wordt aangesloten op Zorgplatform.

**Zorgplatform STS**
Verantwoordelijk voor het uitgeven van een HCP token of Application token op verzoek van de partnerapplicatie.

Er is sprake van een 'trust' relatie tussen de partnerapplicatie en STS; de Zorgplatform STS vertrouwt er op dat de partnerapplicatie de gebruiker correct (conform relevante wetgeving) authentiseert en de juiste identificerende gegevens meestuurt bij een verzoek om een HCP token of Application token.

**Zorgplatform Resource server**
Zorgplatform ontsluit meerdere SOAP en/of RESTful APIs, waar de partnerapplicaties resources kunnen opvragen.

# 7 Happy flow



## 7.1 Issue (T1)

De partnerapplicatie verzoekt de Zorgplatform STS om een token af te geven voor een specifieke patiënt. Hiertoe genereert de partnerapplicatie een WS-Trust 1.3 compliant RequestSecurityToken en roept de WS-Trust 'Issue' operatie aan op de Zorgplatform STS.

Er kunnen in deze stap van deze use case twee verschillende soorten security tokens aangevraagd worden. In het geval dat de partnerapplicatie geauthentiseerd wordt om namens een zorgverlener toegang te krijgen tot Zorgplatform services, wordt er een HCP token aangevraagd. Wanneer de partnerapplicatie geauthentiseerd wordt om toegang te krijgen zonder tussenkomst van een zorgverlener, zoals bij automatische processen het geval is, dan wordt er een application token aangevraagd.

### 7.1.1 Beveiliging

De Issue operatie is een SOAP call en wordt op de volgende wijze beveiligd:

- De SOAP security header bevat een SAML2.0 assertion met attributes die de patiënt beschrijven en eventueel de zorgverlener. De inhoud van de SAML2.0 assertion is door Zorgplatform voorgeschreven.

- De verstrekte assertion wordt door de partnerapplicatie gesigned met een daartoe bestemde private key. De bijbehorende public key wordt geregistreerd binnen Zorgplatform.

- De connectie wordt beveiligd m.b.v. dubbelzijdig TLS. De public TLS client key van de partnerapplicatie wordt geregistreerd binnen Zorgplatform.

### 7.1.2 RequestSecurityToken in de Issue operatie

Conform WS-Trust verzendt de partnerapplicatie een RequestSecurityToken (RST) naar de Zorgplatform STS. Het RST dient te voldoen aan de volgende voorwaarden:

- Het verzoek moet een 'AppliesTo/Address' element met de URL van Zorgplatform bevatten.

```
<trust:RequestSecurityToken xmlns:trust="http://docs.oasis-open.org/ws-sx/ws-trust/200512">
    <wsp:AppliesTo xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy">
      <wsa:EndpointReference xmlns:wsa="http://www.w3.org/2005/08/addressing">
        <wsa:Address>https://zorgplatform.online/</wsa:Address>
      </wsa:EndpointReference>
    </wsp:AppliesTo>
    <trust:KeyType>http://docs.oasis-open.org/ws-sx/ws-trust/200512/Bearer</trust:KeyType>
    <trust:RequestType>http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue</trust:RequestType>
    <trust:TokenType>http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-
1.1#SAMLV2.0</trust:TokenType>
</trust:RequestSecurityToken>
```

- Het tokentype en daarmee de volgorde van de elementen in de assertion is conform SAMLV2.0.

```
<element name="Assertion" type="saml:AssertionType"/>
<complexType name="AssertionType">
    <sequence>
        <element ref="saml:Issuer"/>
        <element ref="ds:Signature" minOccurs="0"/>
        <element ref="saml:Subject" minOccurs="0"/>
        <element ref="saml:Conditions" minOccurs="0"/>
                <element ref="saml:Advice" minOccurs="0"/>
                <choice minOccurs="0" maxOccurs="unbounded">
                        <element ref="saml:Statement"/>
                        <element ref="saml:AuthnStatement"/>
                        <element ref="saml:AuthzDecisionStatement"/>
                        <element ref="saml:AttributeStatement"/>
                </choice>
    </sequence>
    <attribute name="Version" type="string" use="required"/>
    <attribute name="ID" type="ID" use="required"/>
    <attribute name="IssueInstant" type="dateTime" use="required"/>
</complexType>
```

### 7.1.3 HealthCare Professional token (HCP token) in de Issue operatie

De Issue operatie wordt beveiligd m.b.v. ws-security. Het door de partnerapplicatie gegenereerde HCP token is een SAML2.0 assertion en bevat de volgende attributen/ claims:

| Name | Valid values | R/O |
|---|---|---|
| urn:oasis:names:tc:xspa:1.0:subject:purposeofuse | TREATMENT | R |
| urn:oasis:names:tc:xacml:2.0:subject:role | Any SNOMEDCT concept that is a child of 223366009 → Healthcare professional (occupation) | R |
| urn:oasis:names:tc:xacml:1.0:resource:resource-id | Unique identifier of the patient. For Dutch organizations this will be the patients BSN | R |
| urn:oasis:names:tc:xspa:1.0:subject:organization-id | Unique ID of the trusted partner (healthcare organization or service provider requesting the token (HL7 OID) | R |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress | Email address of the user requesting the token | O |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name | Full name of the user | O |

| | | |
|---|---|---|
| | requesting the token | |
| http://sts.zorgplatform.online/ws/claims/2017/07/identity/patient-email | Email address of the patient. Included because many patient-facing healthcare applications use the patient email address as a unique identifier.<br><br>When not yet known, the Zorgplatform STS will register the patient email address as an alternate identity. | O |
| http://sts.zorgplatform.online/ws/claims/2017/07/workflow/workflow-id | If included, the Zorgplatform STS will copy this claim to the resulting token. Required when requesting workflow specific tokens. | O |

Het issuer element van de assertion dient HL7 OID van de partnerapplicatie te bevatten.

```
<Issuer>urn:oid:2.16.840.1.113883.2.4.3.124.8.50.8</Issuer>
```

Het subject/nameID element van de assertion dient een gebruikers-id te bevatten die te herleiden is tot een unieke gebruiker binnen de aangesloten organisatie.

```
<Subject>
        <NameID>user1@123456.891011.12.13.1.4</NameID>
        <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"/>
</Subject>
```

De assertion dient een audience restriction te bevatten met de waarde ‘https://zorgplatform.online’

```
<AudienceRestriction>
         <Audience>https://zorgplatform.online</Audience>
</AudienceRestriction>
```

De organization-id in de assertion dient het HL7 OID te bevatten van de partnerapplicatie.

```
<Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:organization-id">
        <AttributeValue>urn:oid:2.16.840.1.113883.2.4.3.124.8.50.8</AttributeValue>
</Attribute>
```

De workflow-id in de assertion dient het identificerende nummer te bevatten van een workflow wat binnen Zorgplatform bekend is.

```
<Attribute Name="http://sts.zorgplatform.online/ws/claims/2017/07/workflow/workflow-id">
        <AttributeValue> test123-workflow-id </AttributeValue>
</Attribute>
```

De assertion dient te worden ondertekend met de daartoe bestemde private key van de partnerapplicatie.

### 7.1.4 Voorbeeld voor HCP token Request

```
<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope" xmlns:a="http://www.w3.org/2005/08/addressing"
xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
  <s:Header>
    <a:Action s:mustUnderstand="1">http://docs.oasis-open.org/ws-sx/ws-trust/200512/RST/Issue</a:Action>
    <a:MessageID>urn:uuid:cd9f16b0-8f62-4a35-bf68-fd4e4f98db87</a:MessageID>
    <a:ReplyTo>
      <a:Address>http://www.w3.org/2005/08/addressing/anonymous</a:Address>
    </a:ReplyTo>
    <a:To s:mustUnderstand="1">https://zorgplatform.online/sts</a:To>
    <o:Security s:mustUnderstand="1" xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-
1.0.xsd">
      <u:Timestamp u:Id="_0">
        <u:Created>2019-04-23T09:17:21.608Z</u:Created>
        <u:Expires>2019-04-23T09:22:21.608Z</u:Expires>
      </u:Timestamp>
      <Assertion ID="_980101bf-50fc-411a-bef9-0ffc38a09713" IssueInstant="2019-04-23T09:17:21.597Z" Version="2.0"
xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
        <Issuer>urn:oid:[HL7 OID van aanvragende organisatie]</Issuer>
        <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
          <SignedInfo>
            <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
            <Reference URI="#_980101bf-50fc-411a-bef9-0ffc38a09713">
              <Transforms>
                <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
              </Transforms>
              <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
              <DigestValue>9wnEdpnmqtHL0wb1ie0omPQXw01j+aZGq4Eq3+P2qZ4=</DigestValue>
            </Reference>
          </SignedInfo>
          <SignatureValue>[Base64 Encoded]</SignatureValue>
          <KeyInfo>
            <X509Data>
```

```
            <X509Certificate>[Base64 Encoded]</X509Certificate>
          </X509Data>
        </KeyInfo>
      </Signature>
      <Subject>
        <NameID>doctor@2.16.840.1.113883.2.4.3.124.8.50.8</NameID>
        <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"/>
      </Subject>
      <Conditions NotBefore="2019-04-23T09:17:21.597Z" NotOnOrAfter="2019-04-23T09:32:21.597Z">
        <AudienceRestriction>
          <Audience>https://zorgplatform.online</Audience>
        </AudienceRestriction>
      </Conditions>
      <AttributeStatement>
        <Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:purposeofuse">
          <AttributeValue>
            <PurposeOfUse code="TREATMENT" codeSystem="2.16.840.1.113883.3.18.7.1" codeSystemName="nhin-purpose"
displayName="" xmlns="urn:hl7-org:v3"/>
          </AttributeValue>
        </Attribute>
        <Attribute Name="urn:oasis:names:tc:xacml:2.0:subject:role">
          <AttributeValue>
            <Role code="158970007" codeSystem="2.16.840.1.113883.6.96" codeSystemName="SNOMED_CT" displayName=""
xmlns="urn:hl7-org:v3"/>
          </AttributeValue>
        </Attribute>
        <Attribute Name="urn:oasis:names:tc:xacml:1.0:resource:resource-id">
          <AttributeValue>
            <InstanceIdentifier root="2.16.840.1.113883.2.4.6.3" extension="999999205" xmlns="urn:hl7-org:v3"/>
          </AttributeValue>
        </Attribute>
        <Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:organization-id">
          <AttributeValue>urn:oid:2.16.840.1.113883.2.4.3.124.8.50.8</AttributeValue>
        </Attribute>
        <Attribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress">
          <AttributeValue>doctor@zkh1.nl</AttributeValue>
        </Attribute>
        <Attribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name">
          <AttributeValue>Loog, Nefro</AttributeValue>
        </Attribute>
        <Attribute Name="http://sts.zorgplatform.online/ws/claims/2017/07/identity/patient-email">
          <AttributeValue>testpatient@testpatient.be</AttributeValue>
        </Attribute>
        <Attribute Name="http://sts.zorgplatform.online/ws/claims/2017/07/workflow/workflow-id">
          <AttributeValue>test123-workflow-id</AttributeValue>
        </Attribute>
      </AttributeStatement>
      <AuthnStatement AuthnInstant="2019-04-23T09:17:21.597Z">
        <AuthnContext>
          <AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:X509</AuthnContextClassRef>
        </AuthnContext>
      </AuthnStatement>
    </Assertion>
  </o:Security>
 </s:Header>
 <s:Body>
  <trust:RequestSecurityToken xmlns:trust="http://docs.oasis-open.org/ws-sx/ws-trust/200512">
    <wsp:AppliesTo xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy">
      <wsa:EndpointReference xmlns:wsa="http://www.w3.org/2005/08/addressing">
        <wsa:Address>https://zorgplatform.online/</wsa:Address>
      </wsa:EndpointReference>
    </wsp:AppliesTo>
    <trust:KeyType>http://docs.oasis-open.org/ws-sx/ws-trust/200512/Bearer</trust:KeyType>
    <trust:RequestType>http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue</trust:RequestType>
```

```
    <trust:TokenType>http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0</trust:TokenType>
  </trust:RequestSecurityToken>
 </s:Body>
</s:Envelope>
```

### 7.1.5 Application token in de Issue operatie

Wanneer er een application token wordt aangevraagd in de Issue operatie in plaats van een HCP token, dan dienen de volgende attributes toegevoegd te worden aan de assertion:

| Name | Valid values |
|---|---|
| urn:oasis:names:tc:xspa:1.0:subject:purposeofuse | OPERATIONS |
| urn:oasis:names:tc:xacml:2.0:subject:role | SnomedCT concept identifier depending on the usecase. The following SnomedCT concept identifiers are allowed for now:<br>- 182777000 \| Monitoring of patient<br>- 710920002 \| Provision of privacy |
| urn:oasis:names:tc:xacml:1.0:resource:resource-id | Unique identifier of the patient |
| urn:oasis:names:tc:xspa:1.0:subject:organization-id | Unique ID of the trusted partner (healthcare organization or service provider requesting the token (HL7 OID) |
| http://sts.zorgplatform.online/ws/claims/2017/07/workflow/workflow-id | Must be present when the token is a workflow-token. |

Het issuer element van de assertion dient de HL7 OID van de partnerapplicatie te bevatten.

```
<Issuer>urn:oid:2.16.840.1.113883.2.4.3.124.8.50.8</Issuer>
```

Het subject/nameID element van de assertion dient een HL7 OID van de partnerapplicatie te bevatten.

```
<Subject>
        <NameID>urn:oid:[HL7 OID van de partnerapplicatie]</NameID>
        <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"/>
</Subject>
```

De assertion dient een audience restriction te bevatten met de waarde ‘https://zorgplatform.online’

```

```

```
<AudienceRestriction>
        <Audience>https://zorgplatform.online</Audience>
</AudienceRestriction>
```

De organization-id in de assertion dient het HL7 OID te bevatten van de partnerapplicatie.

```
<Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:organization-id">
        <AttributeValue>urn:oid:2.16.840.1.113883.2.4.3.124.8.50.8</AttributeValue>
</Attribute>
```

De workflow-id in de assertion dient het identificerende nummer te bevatten van een workflow wat binnen Zorgplatform bekend is.

```
<Attribute Name="http://sts.zorgplatform.online/ws/claims/2017/07/workflow/workflow-id">
        <AttributeValue> test123-workflow-id </AttributeValue>
</Attribute>
```

De assertion dient te worden ondertekend met de daartoe bestemde private key van de partnerapplicatie.

### 7.1.6 Voorbeeld voor Application token Request

```
<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope" xmlns:a="http://www.w3.org/2005/08/addressing"
xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
  <s:Header>
    <a:Action s:mustUnderstand="1">http://docs.oasis-open.org/ws-sx/ws-trust/200512/RST/Issue</a:Action>
    <a:MessageID>urn:uuid:ff869887-9bda-417b-8e43-9e6204579004</a:MessageID>
    <a:ReplyTo>
      <a:Address>http://www.w3.org/2005/08/addressing/anonymous</a:Address>
    </a:ReplyTo>
    <a:To s:mustUnderstand="1">https://zorgplatform.online/sts</a:To>
    <o:Security s:mustUnderstand="1" xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-
1.0.xsd">
      <u:Timestamp u:Id="_0">
        <u:Created>2019-04-23T09:18:37.803Z</u:Created>
        <u:Expires>2019-04-23T09:23:37.803Z</u:Expires>
      </u:Timestamp>
      <Assertion ID="_71184905-a5c5-4b91-9f13-b70a8605f149" IssueInstant="2019-04-23T09:18:37.783Z" Version="2.0"
xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
        <Issuer> urn:oid:[HL7 OID van aanvragende organisatie]</Issuer>
        <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
          <SignedInfo>
            <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
            <Reference URI="#_71184905-a5c5-4b91-9f13-b70a8605f149">
              <Transforms>
```

```
            <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
            <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
           </Transforms>
           <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
           <DigestValue>DzQOz04lwzLoPc/FwhgTF0ep8htUGPPbglOJlCjigOY=</DigestValue>
          </Reference>
         </SignedInfo>
         <SignatureValue>[Base64 Encoded]</SignatureValue>
         <KeyInfo>
          <X509Data>
           <X509Certificate>[Base64 Encoded]</X509Certificate>
          </X509Data>
         </KeyInfo>
        </Signature>
        <Subject>
         <NameID>urn:oid:[HL7 OID van partnerapplicatie]</NameID>
         <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"/>
        </Subject>
        <Conditions NotBefore="2019-04-23T09:18:37.783Z" NotOnOrAfter="2019-04-23T09:33:37.783Z">
         <AudienceRestriction>
          <Audience>https://zorgplatform.online</Audience>
         </AudienceRestriction>
        </Conditions>
        <AttributeStatement>
         <Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:purposeofuse">
          <AttributeValue>
           <PurposeOfUse code="OPERATIONS" codeSystem="2.16.840.1.113883.3.18.7.1" codeSystemName="nhin-purpose"
displayName="" xmlns="urn:hl7-org:v3"/>
          </AttributeValue>
         </Attribute>
         <Attribute Name="urn:oasis:names:tc:xacml:2.0:subject:role">
          <AttributeValue>
           <Role code="182777000" codeSystem="2.16.840.1.113883.6.96" codeSystemName="SNOMED_CT" displayName=""
xmlns="urn:hl7-org:v3"/>
          </AttributeValue>
         </Attribute>
         <Attribute Name="urn:oasis:names:tc:xacml:1.0:resource:resource-id">
          <AttributeValue>
           <InstanceIdentifier root="2.16.840.1.113883.2.4.6.3" extension="999999205" xmlns="urn:hl7-org:v3"/>
          </AttributeValue>
         </Attribute>
         <Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:organization-id">
          <AttributeValue>urn:oid:2.16.840.1.113883.2.4.3.124.8.50.8</AttributeValue>
         </Attribute>
         <Attribute Name="http://sts.zorgplatform.online/ws/claims/2017/07/workflow/workflow-id">
          <AttributeValue>ABC-233-DEF</AttributeValue>
         </Attribute>
        </AttributeStatement>
        <AuthnStatement AuthnInstant="2019-04-23T09:18:37.783Z">
         <AuthnContext>
          <AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:X509</AuthnContextClassRef>
         </AuthnContext>
        </AuthnStatement>
       </Assertion>
      </o:Security>
     </s:Header>
     <s:Body>
      <trust:RequestSecurityToken xmlns:trust="http://docs.oasis-open.org/ws-sx/ws-trust/200512">
       <wsp:AppliesTo xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy">
        <wsa:EndpointReference xmlns:wsa="http://www.w3.org/2005/08/addressing">
         <wsa:Address>https://zorgplatform.online/</wsa:Address>
        </wsa:EndpointReference>
       </wsp:AppliesTo>
       <trust:KeyType>http://docs.oasis-open.org/ws-sx/ws-trust/200512/Bearer</trust:KeyType>
```

```
    <trust:RequestType>http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue</trust:RequestType>
    <trust:TokenType>http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0</trust:TokenType>
  </trust:RequestSecurityToken>
 </s:Body>
</s:Envelope>
```

## 7.2 Validate / Generate (T2)

De Zorgplatform STS valideert het RequestSecurityToken en genereert een nieuw SAML 2.0 Security Token. Het token wordt gesigned met de private key van de Zorgplatform STS. Anders dan in het geval van een Web Single-Sign-On token, wordt het token niet versleuteld.

## 7.3 Response (T3)

De Zorgplatform STS genereert een WS-Trust 1.3 compliant RequestSecurityTokenResponseCollection, met daarin een RequestSecurityTokenResponse en plaatst het in T2 gegenereerde token in het response. Zorgplatform STS retourneert de RequestSecurityTokenResponseCollection aan de partnerapplicatie.

### 7.3.1 RequestSecurityTokenResponse als resultaat van de Issue operatie

Conform WS-Trust retourneert de Zorgplatform STS een RequestSecurityTokenResponse (RSTR). Het RSTR heeft de volgende eigenschap:

- Het AppliesTo/Address element moet de waarde https://zorgplatform.online bevatten.
- De AudienceRestriction moet waarde https://zorgplatform.online bevatten.
- De assertion bevat een Issuer element waarin de waarde https://zorgplatform.online/sts is opgenomen.

### 7.3.2 HealthCare Professional token (HCP token) in het RequestSecurityTokenResponse

Het door de Zorgplatform Security Token Service geretourneerde HCP token is een SAML2.0 assertion en bevat de volgende attributen/ claims:

| Name | Valid values | R/O |
|---|---|---|
| urn:oasis:names:tc:xspa:1.0:subject:purposeofuse | TREATMENT | R |
| urn:oasis:names:tc:xacml:2.0:subject:role | Any SNOMEDCT concept that is a child of 223366009 → Healthcare professional (occupation) | R |
| urn:oasis:names:tc:xacml:1.0:resource:resource-id | Unique identifier of the patient (BSN for Dutch patients) | R |
| urn:oasis:names:tc:xspa:1.0:subject:organization-id | Unique ID of the trusted partner (healthcare | R |

| | | |
|---|---|---|
| | organization or service provider requesting the token (HL7 OID) | |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress | Email address of the user requesting the token<br><br>If provided, the Zorgplatform STS will copy the contents to the resulting token | O |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name | Fullname of the user requesting the token<br><br>If provided, the Zorgplatform STS will copy the contents to the resulting token | O |
| http://sts.zorgplatform.online/ws/claims/2017/07/identity/patient-email | Email address of the patient. Included because many patient-facing healthcare applications use the patient email address as a unique identifier.<br><br>When not yet known, the Zorgplatform STS will register the patient email address as an alternate identity.<br><br>If provided, the Zorgplatform STS will copy the contents to the resulting token | O |
| http://sts.zorgplatform.online/ws/claims/2017/07/workflow/workflow-id | If included, the Zorgplatform STS will copy this claim to the resulting token. Required when requesting workflow specific tokens. | O |

### 7.3.3 Voorbeeld voor HCP token Response

```
<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope" xmlns:a="http://www.w3.org/2005/08/addressing"
xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
  <s:Header>
    <a:Action s:mustUnderstand="1">http://docs.oasis-open.org/ws-sx/ws-trust/200512/RSTRC/IssueFinal</a:Action>
    <a:RelatesTo>urn:uuid:cd9f16b0-8f62-4a35-bf68-fd4e4f98db87</a:RelatesTo>
    <o:Security s:mustUnderstand="1" xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-
1.0.xsd">
      <u:Timestamp u:Id="_0">
        <u:Created>2019-04-23T09:17:49.167Z</u:Created>
        <u:Expires>2019-04-23T09:22:49.167Z</u:Expires>
      </u:Timestamp>
    </o:Security>
  </s:Header>
```

```
 <s:Body>
  <trust:RequestSecurityTokenResponseCollection xmlns:trust="http://docs.oasis-open.org/ws-sx/ws-trust/200512">
   <trust:RequestSecurityTokenResponse>
    <trust:Lifetime>
     <wsu:Created xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">2019-
04-23T09:17:49.165Z</wsu:Created>
     <wsu:Expires xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">2019-04-
23T09:29:49.165Z</wsu:Expires>
    </trust:Lifetime>
    <wsp:AppliesTo xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy">
     <wsa:EndpointReference xmlns:wsa="http://www.w3.org/2005/08/addressing">
      <wsa:Address>https://zorgplatform.online/</wsa:Address>
     </wsa:EndpointReference>
    </wsp:AppliesTo>
    <trust:RequestedSecurityToken>
     <Assertion ID="_c26cef7e-4086-43c4-a352-9e783508a32a" IssueInstant="2019-04-23T09:17:49.166Z" Version="2.0"
xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
      <Issuer>https://zorgplatform.online/sts</Issuer>
      <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
       <SignedInfo>
        <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
        <Reference URI="#_c26cef7e-4086-43c4-a352-9e783508a32a">
         <Transforms>
          <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
          <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
         </Transforms>
         <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
         <DigestValue>38K0xeIRoWMz9pqMTr3tBCfjET/yFOrvDYSIczJ3VDQ=</DigestValue>
        </Reference>
       </SignedInfo>
       <SignatureValue>[Base64 Encoded]</SignatureValue>
       <KeyInfo>
        <X509Data>
         <X509Certificate>[Base64 Encoded]</X509Certificate>
        </X509Data>
       </KeyInfo>
      </Signature>
      <Subject>
       <NameID>doctor@2.16.840.1.113883.2.4.3.124.8.50.8</NameID>
       <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"/>
      </Subject>
      <Conditions NotBefore="2019-04-23T09:17:49.165Z" NotOnOrAfter="2019-04-23T09:29:49.165Z">
       <AudienceRestriction>
        <Audience>https://zorgplatform.online/</Audience>
       </AudienceRestriction>
      </Conditions>
      <AttributeStatement>
       <Attribute Name="urn:ihe:iti:xca:2010:homeCommunityId">
        <AttributeValue>urn:oid:2.16.840.1.113883.2.4.3.124.8.22</AttributeValue>
       </Attribute>
       <Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:purposeofuse" a:OriginalIssuer=" urn:oid:[HL7 OID van
aanvragende organisatie]" xmlns:a="http://schemas.xmlsoap.org/ws/2009/09/identity/claims">
        <AttributeValue>
         <PurposeOfUse code="TREATMENT" codeSystem="2.16.840.1.113883.3.18.7.1" codeSystemName="nhin-purpose"
displayName="" xmlns="urn:hl7-org:v3"/>
        </AttributeValue>
       </Attribute>
       <Attribute Name="urn:oasis:names:tc:xacml:2.0:subject:role" a:OriginalIssuer=" urn:oid:[HL7 OID van aanvragende
organisatie]" xmlns:a="http://schemas.xmlsoap.org/ws/2009/09/identity/claims">
        <AttributeValue>
         <Role code="158970007" codeSystem="2.16.840.1.113883.6.96" codeSystemName="SNOMED_CT" displayName=""
xmlns="urn:hl7-org:v3"/>
        </AttributeValue>
```

```
            </Attribute>
            <Attribute Name="urn:oasis:names:tc:xacml:1.0:resource:resource-id" a:OriginalIssuer=" urn:oid:[HL7 OID van
aanvragende organisatie]" xmlns:a="http://schemas.xmlsoap.org/ws/2009/09/identity/claims">
              <AttributeValue>
                <InstanceIdentifier root="2.16.840.1.113883.2.4.6.3" extension="999999205" xmlns="urn:hl7-org:v3"/>
              </AttributeValue>
            </Attribute>
            <Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:organization-id" a:OriginalIssuer=" urn:oid:[HL7 OID van
aanvragende organisatie]" xmlns:a="http://schemas.xmlsoap.org/ws/2009/09/identity/claims">
              <AttributeValue>urn:oid:2.16.840.1.113883.2.4.3.124.8.50.8</AttributeValue>
            </Attribute>
            <Attribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress" a:OriginalIssuer="
urn:oid:[HL7 OID van aanvragende organisatie]" xmlns:a="http://schemas.xmlsoap.org/ws/2009/09/identity/claims">
              <AttributeValue>doctor@zkh1.nl</AttributeValue>
            </Attribute>
            <Attribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name" a:OriginalIssuer=" urn:oid:[HL7 OID
van aanvragende organisatie]" xmlns:a="http://schemas.xmlsoap.org/ws/2009/09/identity/claims">
              <AttributeValue>Loog, Nefro</AttributeValue>
            </Attribute>
            <Attribute Name="http://sts.zorgplatform.online/ws/claims/2017/07/identity/patient-id">
              <AttributeValue>b9114ce8-ff6d-4314-ac58-6c236fd7193e</AttributeValue>
            </Attribute>
            <Attribute Name="http://sts.zorgplatform.online/ws/claims/2017/07/identity/patient-connectionTypeId">
              <AttributeValue>c0b98bf2-de02-4b97-94fb-ffffd57b058a</AttributeValue>
            </Attribute>
          </AttributeStatement>
          <AuthnStatement AuthnInstant="2019-04-23T09:17:21.597Z">
            <AuthnContext>
              <AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:X509</AuthnContextClassRef>
            </AuthnContext>
          </AuthnStatement>
        </Assertion>
      </trust:RequestedSecurityToken>
      <trust:RequestedAttachedReference>
        <SecurityTokenReference b:TokenType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0"
xmlns="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:b="http://docs.oasis-
open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd">
          <KeyIdentifier ValueType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLID">_c26cef7e-4086-
43c4-a352-9e783508a32a</KeyIdentifier>
        </SecurityTokenReference>
      </trust:RequestedAttachedReference>
      <trust:RequestedUnattachedReference>
        <SecurityTokenReference b:TokenType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0"
xmlns="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:b="http://docs.oasis-
open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd">
          <KeyIdentifier ValueType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLID">_c26cef7e-4086-
43c4-a352-9e783508a32a</KeyIdentifier>
        </SecurityTokenReference>
      </trust:RequestedUnattachedReference>
      <trust:TokenType>http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0</trust:TokenType>
      <trust:RequestType>http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue</trust:RequestType>
      <trust:KeyType>http://docs.oasis-open.org/ws-sx/ws-trust/200512/Bearer</trust:KeyType>
    </trust:RequestSecurityTokenResponse>
  </trust:RequestSecurityTokenResponseCollection>
 </s:Body>
</s:Envelope>
```


### 7.3.4 Application token in het RequestSecurityTokenResponse

Het door de Zorgplatform Security Token Service geretourneerde Application token is een SAML2.0 assertion en bevat de volgende attributen/ claims:

| Name | Valid values | R/O |
|---|---|---|
| urn:oasis:names:tc:xspa:1.0:subject:purposeofuse | OPERATIONS | R |
| urn:oasis:names:tc:xacml:2.0:subject:role | Any SNOMEDCT concept that is a child of 223366009 → Healthcare professional (occupation) | R |
| urn:oasis:names:tc:xacml:1.0:resource:resource-id | Unique identifier of the patient (BSN for Dutch patients) | R |
| urn:oasis:names:tc:xspa:1.0:subject:organization-id | Unique ID of the trusted partner (healthcare organization or service provider requesting the token (HL7 OID) | R |
| http://sts.zorgplatform.online/ws/claims/2017/07/workflow/workflow-id | Must be present when the token is a workflow-token. | O |

### 7.3.5 Voorbeeld voor Application token Response

```
<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope" xmlns:a="http://www.w3.org/2005/08/addressing"
xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
  <s:Header>
    <a:Action s:mustUnderstand="1">http://docs.oasis-open.org/ws-sx/ws-trust/200512/RSTRC/IssueFinal</a:Action>
    <a:RelatesTo>urn:uuid:ff869887-9bda-417b-8e43-9e6204579004</a:RelatesTo>
    <o:Security s:mustUnderstand="1" xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-
1.0.xsd">
      <u:Timestamp u:Id="_0">
        <u:Created>2019-04-23T09:18:57.418Z</u:Created>
        <u:Expires>2019-04-23T09:23:57.418Z</u:Expires>
      </u:Timestamp>
    </o:Security>
  </s:Header>
  <s:Body>
    <trust:RequestSecurityTokenResponseCollection xmlns:trust="http://docs.oasis-open.org/ws-sx/ws-trust/200512">
      <trust:RequestSecurityTokenResponse>
        <trust:Lifetime>
          <wsu:Created xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">2019-
04-23T09:18:57.417Z</wsu:Created>
          <wsu:Expires xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">2019-04-
23T09:30:57.417Z</wsu:Expires>
        </trust:Lifetime>
        <wsp:AppliesTo xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy">
          <wsa:EndpointReference xmlns:wsa="http://www.w3.org/2005/08/addressing">
            <wsa:Address>https://zorgplatform.online/</wsa:Address>
          </wsa:EndpointReference>
        </wsp:AppliesTo>
        <trust:RequestedSecurityToken>
          <Assertion ID="_4034f4ea-d45c-4cf0-9180-5659db9ce4d5" IssueInstant="2019-04-23T09:18:57.418Z" Version="2.0"
xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
            <Issuer>https://zorgplatform.online/sts</Issuer>
            <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
              <SignedInfo>
                <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
                <Reference URI="#_4034f4ea-d45c-4cf0-9180-5659db9ce4d5">
                  <Transforms>
                    <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                    <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                  </Transforms>
                  <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                  <DigestValue>8CmyBccrs4ox+iFxdzjPGkJ0DdpyVNJHWaX3hQj+66A=</DigestValue>
```

```
            </Reference>
           </SignedInfo>
           <SignatureValue>[Base64 Encoded]</SignatureValue>
           <KeyInfo>
            <X509Data>
             <X509Certificate>[Base64 Encoded]</X509Certificate>
            </X509Data>
           </KeyInfo>
          </Signature>
          <Subject>
           <NameID> urn:oid:[HL7 OID van aanvragende organisatie]</NameID>
           <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"/>
          </Subject>
          <Conditions NotBefore="2019-04-23T09:18:57.417Z" NotOnOrAfter="2019-04-23T09:30:57.417Z">
           <AudienceRestriction>
            <Audience>https://zorgplatform.online/</Audience>
           </AudienceRestriction>
          </Conditions>
          <AttributeStatement>
           <Attribute Name="urn:ihe:iti:xca:2010:homeCommunityId">
            <AttributeValue>urn:oid:2.16.840.1.113883.2.4.3.124.8.22</AttributeValue>
           </Attribute>
           <Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:purposeofuse" a:OriginalIssuer=" urn:oid:[HL7 OID van
aanvragende organisatie]" xmlns:a="http://schemas.xmlsoap.org/ws/2009/09/identity/claims">
            <AttributeValue>
             <PurposeOfUse code="OPERATIONS" codeSystem="2.16.840.1.113883.3.18.7.1" codeSystemName="nhin-purpose"
displayName="" xmlns="urn:hl7-org:v3"/>
            </AttributeValue>
           </Attribute>
           <Attribute Name="urn:oasis:names:tc:xacml:2.0:subject:role" a:OriginalIssuer=" urn:oid:[HL7 OID van aanvragende
organisatie]" xmlns:a="http://schemas.xmlsoap.org/ws/2009/09/identity/claims">
            <AttributeValue>
             <Role code="182777000" codeSystem="2.16.840.1.113883.6.96" codeSystemName="SNOMED_CT" displayName=""
xmlns="urn:hl7-org:v3"/>
            </AttributeValue>
           </Attribute>
           <Attribute Name="urn:oasis:names:tc:xacml:1.0:resource:resource-id" a:OriginalIssuer=" urn:oid:[HL7 OID van
aanvragende organisatie]" xmlns:a="http://schemas.xmlsoap.org/ws/2009/09/identity/claims">
            <AttributeValue>
             <InstanceIdentifier root="2.16.840.1.113883.2.4.6.3" extension="999999205" xmlns="urn:hl7-org:v3"/>
            </AttributeValue>
           </Attribute>
           <Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:organization-id" a:OriginalIssuer=" urn:oid:[HL7 OID van
aanvragende organisatie]" xmlns:a="http://schemas.xmlsoap.org/ws/2009/09/identity/claims">
            <AttributeValue>urn:oid:2.16.840.1.113883.2.4.3.124.8.50.8</AttributeValue>
           </Attribute>
           <Attribute Name="http://sts.zorgplatform.online/ws/claims/2017/07/workflow/workflow-id" a:OriginalIssuer="
urn:oid:[HL7 OID van aanvragende organisatie]" xmlns:a="http://schemas.xmlsoap.org/ws/2009/09/identity/claims">
            <AttributeValue>ABC-233-DEF</AttributeValue>
           </Attribute>
           <Attribute Name="http://sts.zorgplatform.online/ws/claims/2017/07/identity/patient-id">
            <AttributeValue>b9114ce8-ff6d-4314-ac58-6c236fd7193e</AttributeValue>
           </Attribute>
           <Attribute Name="http://sts.zorgplatform.online/ws/claims/2017/07/identity/patient-connectionTypeId">
            <AttributeValue>c0b98bf2-de02-4b97-94fb-ffffd57b058a</AttributeValue>
           </Attribute>
          </AttributeStatement>
          <AuthnStatement AuthnInstant="2019-04-23T09:18:37.783Z">
           <AuthnContext>
            <AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:X509</AuthnContextClassRef>
           </AuthnContext>
          </AuthnStatement>
         </Assertion>
        </trust:RequestedSecurityToken>
```

```
      <trust:RequestedAttachedReference>
        <SecurityTokenReference b:TokenType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0"
xmlns="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:b="http://docs.oasis-
open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd">
          <KeyIdentifier ValueType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLID">_4034f4ea-d45c-
4cf0-9180-5659db9ce4d5</KeyIdentifier>
        </SecurityTokenReference>
      </trust:RequestedAttachedReference>
      <trust:RequestedUnattachedReference>
        <SecurityTokenReference b:TokenType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0"
xmlns="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:b="http://docs.oasis-
open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd">
          <KeyIdentifier ValueType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLID">_4034f4ea-d45c-
4cf0-9180-5659db9ce4d5</KeyIdentifier>
        </SecurityTokenReference>
      </trust:RequestedUnattachedReference>
      <trust:TokenType>http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0</trust:TokenType>
      <trust:RequestType>http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue</trust:RequestType>
      <trust:KeyType>http://docs.oasis-open.org/ws-sx/ws-trust/200512/Bearer</trust:KeyType>
    </trust:RequestSecurityTokenResponse>
  </trust:RequestSecurityTokenResponseCollection>
 </s:Body>
</s:Envelope>
```

### 7.4 Verwerken RSTR (T4)

De partnerapplicatie verwerkt het ontvangen RequestSecurityTokenResponse door de ondertekening van de Assertion te valideren met behulp van de public key van de Zorgplatform STS.

### 7.5 Call naar Zorgplatform Resource server (T5)

De partnerapplicatie roept een Zorgplatform Resource server aan en authentiseert zichzelf met het in de voorgaande stappen verstrekte SAML2 token.

In het geval van een SOAP operatie wordt de assertion geplaatst in de SOAP security header conform WS-Security.

In het geval van een RESTful (FHIR) API wordt de assertion als BASE64 encoded string in de HTTP Authorization header geplaatst. Als type credentials wordt ‘Saml’ gebruikt:

```
Authorization: Saml YWxhZGRpbjpvcGVuc2VzYW1l……..
```

# 8 Unhappy flow

TBD