Zorgplatform Web Browser Single-Sign-On 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

Het Zorgplatform ‘Web Browser Single-Sign-On protocol’ faciliteert Single-Sign-On en Context Sharing tussen het primaire informatie systeem van een zorgverlener en een web applicatie.

2 Belangrijke concepten en termen

XIS
Zorgverleners werken bij voorkeur vanuit 1 informatiesysteem. Afhankelijk van het type zorgverlener is dat bijvoorbeeld een Huisarts Informatie Systeem (HIS) of een Ziekenhuis Informatie Systeem (ZIS). De term 'XIS' wordt gebruikt als algemene term voor een primair informatiesysteem van een zorgverlener.

Single-Sign-On
Wanneer een zorgverlener naast zijn primaire XIS ook andere applicaties gebruikt bij het verlenen van zorg, is het wenselijk dat hij automatisch wordt ingelogd in die andere applicaties. Dit leidt tot een frictieloze ervaring en verkleint de kans op lekkage van inloggegevens.

Context Sharing
Wanneer een Zorgverlener naast zijn primaire XIS ook andere applicaties gebruikt bij het verlenen van zorg, is het wenselijk dat binnen die andere applicaties automatisch dezelfde patiënt (context) wordt geselecteerd als in het XIS. Dit leidt tot een frictieloze ervaring en verkleint de kans op patiëntverwisseling.

Visuele integratie
Andere applicaties (zoals web applicaties) kunnen visueel worden geïntegreerd binnen de user interface van het primaire informatie systeem (XIS). Het Zorgplatform Web Browser Single-Sign-On protocol vereist geen visuele integratie. Binnen de documentatie wordt echter wel visuele integratie voorondersteld.

Security Token
Ook wel 'Access Token'. Bevat security informatie, zoals identiteit, rol of toegangsrechten, over een persoon of systeem. Een Single-Sign-On token is één implementatie van een security token.

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

Single-Sign-On Token (SSO token)
Type security token dat wordt gebruikt om Single-Sign-On tussen systemen te creëren.

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 vertrouwt 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 de calls naar de Zorgplatform STS) worden voorzien van een security token conform de WS-Security standaard
WS-Trust 1.3	Opvragen van Single-Sign-On security tokens bij de Zorgplatform Security Token Service (STS)
SAML2.0	Zorgplatform gebruikt uitsluitend SAML2 assertions als security token
WS-Federation Passive Requestor Profile	Verstrekken van Single-Sign-On tokens aan web applicaties met behulp van HTTP Post
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

4 Usecase

Een Zorgverlener opent een web applicatie vanuit zijn XIS en:

- Wordt automatisch ingelogd in deze web applicatie (Single-Sign-On)
- De web applicatie selecteert automatisch de juiste (in het XIS actieve) patiënt (Context Sharing)

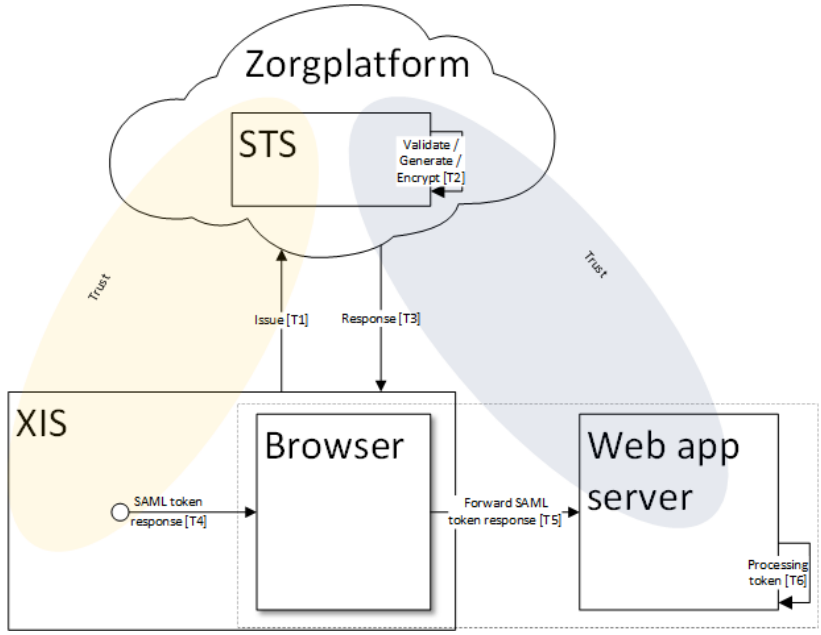
4.1 Relaties met andere Zorgplatform protocollen en use cases

Het Zorgplatform Web Browser Single-Sign-On protocol wordt in verschillende andere usecases en protocollen gebruikt:

- Het voorschrijven van apps
- Home monitoring
- Et cetera

5 Systeem architectuur

Onderstaande afbeelding geeft een globale indruk van de samenhang en communicatie tussen de verschillende betrokken actoren.



Figuur 1: Samenhang en communicatie tussen verschillende betrokken actoren (Zorgplatform, XIS en Web app)

Het aanvragen en verwerken van een token verloopt globaal als volgt:

#	Omschrijving	Afhankelijke standaarden
T1	XIS vraagt een Single-Sign-On token aan bij de Zorgplatform STS	- WS-Trust RequestSecurityToken - WS-Security - SAML2.0
T2	Zorgplatform STS valideert het verzoek van XIS, genereert een Single-Sign-On token en versleutelt het token met de publieke key van web app server	
T3	Zorgplatform STS retourneert het gegenereerde token naar XIS	- WS-Trust RequestSecurityTokenResponse - SAML 2.0
T4	XIS stuurt het token naar de browser	- WS-Federation passive requestor profile
T5	De browser stuurt het token door naar de web app server	- WS-Federation passive requestor profile

T6	De web app server verwerkt het token	

6 Betrokken actoren

XIS
Primaire informatie systeem van de zorgverlener. XIS is verantwoordelijk voor de authenticatie van de zorgverlener, het aanvragen van een Single-Sign-On token bij de Zorgplatform STS en het doorsturen van het aangevraagde token naar de web applicatie.

Zorgplatform STS
Verantwoordelijk voor het uitgeven van een Single-Sign-On token op verzoek van XIS.

Er is sprake van een 'trust' relatie tussen XIS en STS; De Zorgplatform STS vertrouwd er op dat XIS de gebruiker correct (conform relevante wetgeving) authentiseert en de juiste identificerende gegevens meestuurt bij een verzoek om een Single-Sign-On token.

Browser
De user interface van een web applicatie is de browser. XIS zal Single-Sign-On tokens versturen naar de web applicatie via de browser.

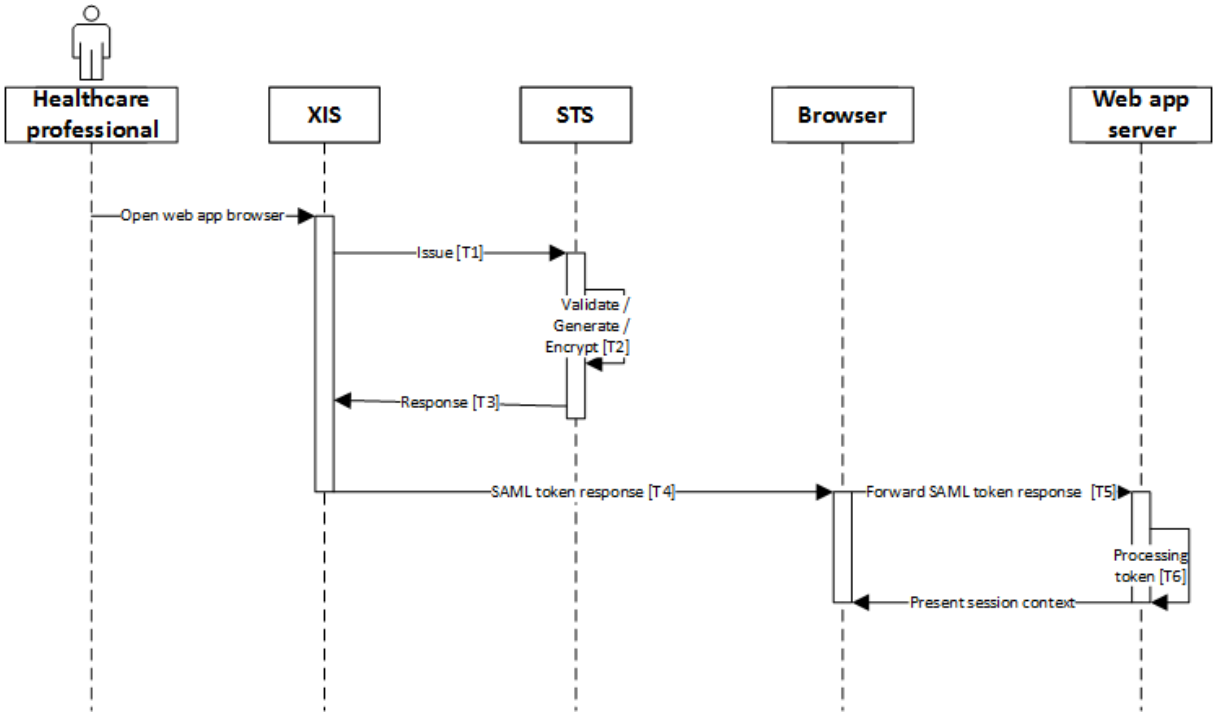
Web app server
De web app server bevat de serverzijde van de web applicatie. De web app server genereert de HTML/CSS/Javascript die door de browser wordt gebruikt om de user interface te tonen. De web app server is verantwoordelijk voor het verwerken van door XIS (via de browser) verzonden Single-Sign-On tokens en het op basis van dat token aanmaken van een gebruiker-sessie en het selecteren / inschrijven van de juiste patiënt.

Er is sprake van een 'trust' relatie tussen web app server en STS:

- De Zorgplatform STS versleutelt Single-Sign-On tokens met de public key van de betreffende web app server. Hierdoor kan alleen die specifieke web app server de voor hem bedoelde tokens verwerken

- De Zorgplatform STS ondertekent het verstrekte Single-Sign-On token met een eigen private key. De web app server kan de herkomst van het token verifiëren met behulp van de public key van de Zorgplatform STS.

7 Happy flow



Figuur 2: Sequence diagram welke de transacties tussen verschillende actoren omschrijft.

7.1 Issue (T1)

XIS verzoekt de Zorgplatform STS om een SSO token af te geven voor de huidige gebruiker en de binnen XIS actieve patiënt. Hiertoe genereert XIS een WS-Trust 1.3 compliant RequestSecurityToken en roept de WS-Trust 'Issue' operatie aan op de Zorgplatform STS.

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 actieve gebruiker en patiënt beschrijven. De inhoud van de SAML2.0 assertion is door Zorgplatform voorgeschreven.

- De verstrekte assertion wordt door XIS 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 XIS wordt geregistreerd binnen Zorgplatform.

7.1.2 RequestSecurityToken in de Issue operatie

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

- Het verzoek moet een 'AppliesTo/Address' element met de URL van de web applicatie bevatten: https://partner-application.nl
- Het tokentype is SAML2.0

```
<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>[URL van webapplicatie]</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>
```

7.1.3 Single-Sign-On token in de Issue operatie

De Issue operatie wordt beveiligd m.b.v. WS-Security. Het door XIS gegenereerde SSO security 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 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 If provided, the Zorgplatform STS will copy the contents to the resulting token	O
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Full name of the user requesting the token If provided, the Zorgplatform STS will copy the contents to the resulting	O

	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. When not yet known, the Zorgplatform STS will register the patient email address as an alternate identity. 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	Required when requesting workflow specific tokens. If included, the Zorgplatform STS will copy this claim to the resulting token.	O

De issuer van het RST dient de HL7 OID van het ziekenhuis 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. In het geval van ChipSoft HiX wordt de nameID als volgt samen gesteld:

- Een locale user-id van de actieve gebruiker
- Gevolgd door een '@' symbool
- Gevolgd door de HL7 OID van de (op Zorgplatform aangesloten) organisatie waarbinnen de gebruiker op dat moment werkzaam is.

```
<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 URL van de web applicatie: https://partner-application.nl

```
```

```
<AudienceRestriction>
        <Audience>https://partner-application.nl</Audience>
</AudienceRestriction>
```

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

```
<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 XIS.

7.1.4 Voorbeeld

```
<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:99516cac-36ff-42a0-98d2-f66df7a4a6d2</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>2019-04-19T12:55:23.030Z</u:Created>
        <u:Expires>2019-04-19T13:00:23.030Z</u:Expires>
      </u:Timestamp>
      <Assertion ID="_e4d34804-b156-4bdf-9503-ed8cfcefa3e9" IssueInstant="2019-04-19T12:55:23.023Z" Version="2.0"
xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
        <Issuer>urn:oid:2.16.840.1.113883.2.4.3.124.8.50.8</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="#_e4d34804-b156-4bdf-9503-ed8cfcefa3e9">
              <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>f5DxtXL2LpTXWaPPfU1uCUfPpVPAHdhsGSpBAS4L1kE=</DigestValue>
          </Reference>
         </SignedInfo>
         <SignatureValue>[Base64 encoded]</SignatureValue>
         <KeyInfo>
          <X509Data>
           <X509Certificate>[Base64 Encoded]</X509Certificate>
          </X509Data>
         </KeyInfo>
        </Signature>
        <Subject>
         <NameID>USER1@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="2019-04-19T12:55:23.023Z" NotOnOrAfter="2019-04-19T13:07:23.023Z">
         <AudienceRestriction>
          <Audience>https://partner-application.nl</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="223366009" 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>DoctorJansen@chipsoft.nl</AttributeValue>
         </Attribute>
         <Attribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name">
          <AttributeValue>Jansen, Doctor</AttributeValue>
         </Attribute>
         <Attribute Name="http://sts.zorgplatform.online/ws/claims/2017/07/workflow/workflow-id">
          <AttributeValue> test123-workflow-id </AttributeValue>
         </Attribute>
        </AttributeStatement>
        <AuthnStatement AuthnInstant="2019-04-19T12:55:23.023Z">
         <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>[URL van web applicatie]</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/Encrypt (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. Vervolgens wordt ze versleutelt met de public key van de web app server.

7.3 Response (T3)

De Zorgplatform STS plaatst het in T2 gegenereerde token in een WS-Trust 1.3 compliant RequestSecurityTokenResponse (RSTR) en retourneert het RSTR base64 encoded aan XIS. XIS stuurt het token in T4 door naar de web app browser.

7.3.1 RequestSecurityTokenResponse als resultaat van de Issue operatie

Conform WS-Trust 1.3 retourneert de Zorgplatform STS een RequestSecurityTokenResponse (RSTR). Het RSTR heeft de volgende eigenschappen:

- Het AppliesTo element bevat een Address element waarin het adres / domein van de web app server is opgenomen: https://partner-application.nl.

- Het RSTR bevat een Requested Security Token met een encrypted assertion (EncryptedAssertion element). De assertion is versleuteld met behulp van de public key van web app server.

- De assertion bevat een Issuer element waarin het adres van de Zorgplatform Security Token Service is opgenomen: https://zorgplatform.online/sts.

7.3.2 Single-Sign-On Token in het RequestSecurityTokenResponse

Het door de Zorgplatform STS geretourneerde 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 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 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 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. When not yet known, the Zorgplatform STS will register the patient email address as an alternate identity. 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	Required when requesting workflow specific tokens. If included, the Zorgplatform STS will copy this claim to the resulting token.	O

7.3.3 Voorbeeld

```
<t:RequestSecurityTokenResponse xmlns:t="http://docs.oasis-open.org/ws-sx/ws-trust/200512">
  <t:Lifetime>
    <wsu:Created xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">2019-04-19T15:48:34.354Z</wsu:Created>
    <wsu:Expires xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">2019-04-19T16:00:34.354Z</wsu:Expires>
```

```
  </t:Lifetime>
  <wsp:AppliesTo xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy">
    <EndpointReference xmlns="http://www.w3.org/2005/08/addressing">
      <Address>https://partner-application.nl/</Address>
    </EndpointReference>
  </wsp:AppliesTo>
  <t:RequestedSecurityToken>
    <EncryptedAssertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
      <xenc:EncryptedData Type="http://www.w3.org/2001/04/xmlenc#Element"
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
        <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc" />
        <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
          <e:EncryptedKey xmlns:e="http://www.w3.org/2001/04/xmlenc#">
            <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
              <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
            </e:EncryptionMethod>
            <KeyInfo>
              <o:SecurityTokenReference xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-
1.0.xsd">
                <X509Data>
                  <X509IssuerSerial>
                    <X509IssuerName>CN=partnerapplication - chipsoft-zorgplatform, OU=IO, O=Partner B.V., L=Amsterdam,
S=Utrecht, C=NL</X509IssuerName>
                    <X509SerialNumber>1553784972145</X509SerialNumber>
                  </X509IssuerSerial>
                </X509Data>
              </o:SecurityTokenReference>
            </KeyInfo>
            <e:CipherData>
              <e:CipherValue>[Base64 encoded]</e:CipherValue>
            </e:CipherData>
          </e:EncryptedKey>
        </KeyInfo>
        <xenc:CipherData>
          <xenc:CipherValue>[Base64 encoded]
        </xenc:CipherData>
      </xenc:EncryptedData>
    </EncryptedAssertion>
  </t:RequestedSecurityToken>
  <t:RequestedAttachedReference>
    <SecurityTokenReference d3p1:TokenType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0"
xmlns:d3p1="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd" xmlns="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
      <KeyIdentifier ValueType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLID">_9ff4bf18-dade-
4060-b1a9-de370aad3b01</KeyIdentifier>
    </SecurityTokenReference>
  </t:RequestedAttachedReference>
  <t:RequestedUnattachedReference>
    <SecurityTokenReference d3p1:TokenType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0"
xmlns:d3p1="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd" xmlns="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
      <KeyIdentifier ValueType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLID">_9ff4bf18-dade-
4060-b1a9-de370aad3b01</KeyIdentifier>
    </SecurityTokenReference>
  </t:RequestedUnattachedReference>
  <t:TokenType>http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0</t:TokenType>
  <t:RequestType>http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue</trust:RequestType>
  <t:KeyType>http://docs.oasis-open.org/ws-sx/ws-trust/200512/Bearer</trust:KeyType>
</t:RequestSecurityTokenResponse>
```

7.4 RSTR versturen naar browser (T4)

XIS stuurt het van de Zorgplatform STS ontvangen RequestSecurityTokenResponse (RSTR) door naar de web app browser.

XIS genereert daartoe een HTML form met een hidden field met de naam 'SAMLResponse'. Het RSTR wordt Base64 encoded als waarde van dit hidden field toegevoegd waarna het form naar de server wordt gepost.

7.5 RSTR doorsturen naar web app server (T5)

De web app browser stuurt de HTML form met het RSTR in het hidden field 'SAMLResponse' door naar de web app server.

7.6 Verwerken RSTR door Web application Server (T6)

De web app server verwerkt het ontvangen RequestSecurityTokenResponse als volgt:

- De EncryptedAssertion in de RSTR wordt ontsleuteld met behulp van de daartoe bestemde private key van de Web Application Server
- De ondertekening van de assertion wordt gevalideerd met behulp van de public key van de Zorgplatform STS
- De vervaltijd van het token wordt gevalideerd: is het token op het moment van gebruik nog geldig?
- De AudienceRestriction in de assertion wordt gevalideerd: is het token voor deze URL bestemd?
- De issuer in de assertion wordt gevalideerd: is dit token afkomstig van de Zorgplatform STS?
- Subject/NameID uit de assertion worden gebruikt om de betreffende gebruiker in te loggen en eventueel in te schrijven
- De resource-id claim wordt gebruikt om de juiste patiënt te selecteren
- Eventuele andere benodigde attributes (claims) worden verwerkt.

8 Unhappy flows

8.1 Web app ontvangt security token welke bedoeld is voor een andere partij

Indien de web app het security token ontvangt welke bedoeld is voor een andere web app, zal de web app server het RequestSecurityTokenResponse niet kunnen verwerken:

- De EncryptedAssertion in de RSTR kan niet ontsleuteld worden
- De URL in de AudienceRestriction in de assertion komt niet overeen met de URL van de ontvangende partnerapplicatie

8.2 Web app ontvangt security token welke niet van Zorgplatform STS afkomstig is

Indien de web app een security token ontvangt welke niet afkomstig is van Zorgplatform STS, zal de web app server het RequestSecurityTokenResponse niet kunnen verwerken:

- De ondertekening van de assertion komt niet overeen met de public key van de Zorgplatform STS