Frederick Hirsch 7/21/06 4:24 PM
Formatted: Numbering: Continuous

An OASIS White Paper

WS-SX Interop Scenarios

Scenarios for demonstration of WS-SX TC specifications

Version ED-04fjh

Marc A Goodner 7/18/06 4:21 PM
Deleted: 3

Editors Marc Goodner, Prateek Mishra
Contributors Darren Platt

For OASIS WS-SX TC

OASIS (Organization for the Advancement of Structured Information Standards) is a not-for-profit, international consortium that drives the development, convergence, and adoption of e-business standards. Members themselves set the OASIS technical agenda, using a lightweight, open process expressly designed to promote industry consensus and unite disparate efforts. The consortium produces open standards for Web services, security, e-business, and standardization efforts in the public sector and for application-specific markets. OASIS was founded in 1993. More information can be found on the OASIS website at http://www.oasis-open.org.

The purpose of the OASIS WS-SX TC is to define extensions to OASIS Web Services Security to enable trusted SOAP message exchanges involving multiple message exchanges and to define security policies that govern the formats and tokens of such messages. This work will be carried out through continued refinement of the Web Services SecureConversation, SecurityPolicy and Trust specifications submitted to the TC as referenced in this charter.

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 18 July 2006

Marc A Goodner 7/18/06 4:20 PM
Inserted: 18 July 2006

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 30 June 2006

Table of Contents

Frederick Hirsch 7/21/06 4:22 PM

Deleted: Introduction → 5
Namespaces → 5
WS-SX Interop Scenarios → 6
Preconditions → 6
Client and STS Security Bindings → 8
Username for SAML 1.1 HoK over HTTPS → 8
Username for SAML 1.1 Bearer Token, WSS 1.0 → 14
Certificate for SAML 1.1 HoK Token, WSS 1.0 → 20
Mutual Certificate, WSS1.0 → 25
Mutual Certificate, WSS1.1 → 36
Delegated SAML 2.0 with Certificate for SAML 2.0 HoK, WSS 1.1 → 48
Client and Service Security Bindings → 56
Issued SAML 1.1 Token over Transport → 56
Issued SAML 1.1 Token → 59
Issued SAML 1.1 Token for Certificate → 65
SecureConversation → 74
Issued SAML 2.0 Token → 81
WSDL → 82
STS → 82
Service → 83
References → 84
Normative → 84
Notes → 85
Revision History → 86

67

68

69

70

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 18 July 2006

Marc A Goodner 7/18/06 4:20 PM
Inserted: 18 July 2006

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 30 June 2006

1. Introduction

This document contains basic interoperability scenarios for services and clients that use WS-Trust and WS-SecureConversation. In each scenario there are Client, Service and Security Token Service (STS). The message flow is common across all scenarios.

Client issues a request to STS and exchanges an X509 or a Username Token representing Client's identity for a SAML1.1 token with client's identity claims.

Client uses SAML Token to authenticate to the Service.

Specific security protection mechanisms vary across scenarios.

Note that where policy expressions are provided, they are informative.

1.1. Namespaces

Unless overridden by a namespace declaration inside an XML fragment, this document uses the following namespaces:

Prefix	Namespace
s	http://schemas.xmlsoap.org/soap/envelope
a	http://schemas.xmlsoap.org/ws/2004/08/addressing
d	http://www.w3.org/2000/09/xmldsig#
e	http://www.w3.org/2001/04/xmlenc#
k	http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd
o	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd
u	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd
saml	urn:oasis:names:tc:SAML:1.0:assertion
sc	http://docs.oasis-open.org/ws-sx/ws-secureconversation/200512
T	http://docs.oasis-open.org/ws-sx/ws-trust/200512
sp	http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200512
wsp	http://schemas.xmlsoap.org/ws/2004/09/policy

Frederick Hirsch 7/21/06 4:21 PM
Formatted: Bullets and Numbering

Frederick Hirsch 7/21/06 4:37 PM
Formatted Table

Marc A Goodner 7/18/06 4:28 PM
Deleted: http://docs.oasis-open.org/wss/2005/xx/oasis-2005xx-wss-wssecurity-secext-1.1.xsd

Frederick Hirsch 7/21/06 4:48 PM
Formatted Table

Frederick Hirsch 7/21/06 5:04 PM
Formatted: Normal, No widow/orphan control, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Frederick Hirsch 7/21/06 5:05 PM
Formatted: Tabs: 1.73", Left

Frederick Hirsch 7/21/06 4:24 PM
Formatted: Numbering: Continuous

2. WS-SX Interop Scenarios

The scenarios here iterate over different configurations of 3-way Token Issuance. When two different WS-Trust implementations participate in WS-Trust Token Issuance scenario three scenario roles (the Client, Service and STS) can be distributed across the two implementations. The scenarios have the following possible combinations of participants. Note that only combination A below is valid for transport dependent scenarios (1 and 7).

Frederick Hirsch 7/21/06 4:37 PM
Formatted Table

Participant Combination	Client	STS	Service
A (Client1, STS2, Service2)	Implementation 1	Implementation 2	Implementation 2
B (Client1, STS1, Service2)	Implementation 1	Implementation 1	Implementation 2
C (Client1, STS2, Service1)	Implementation 1	Implementation 2	Implementation 1

The following scenarios were chosen to cover different combinations of parameters discussed below.

Frederick Hirsch 7/21/06 4:38 PM
Formatted: Font color: Auto

Frederick Hirsch 7/21/06 4:38 PM
Formatted Table

Unknown
Field Code Changed

Frederick Hirsch 7/21/06 4:38 PM
Formatted: Font color: Auto

Unknown
Field Code Changed

	Client and STS Security binding	Client and Service Security Binding
1	Username for SAML 1.1 HoK over HTTPS	Issued SAML 1.1 Token over Transport
2	Username for SAML 1.1 Bearer Token, WSS 1.0	Issued SAML 1.1 Token for Certificate, WSS 1.0
3	Certificate for SAML 1.1 HoK Token, WSS 1.0	Issued SAML 1.1 Token for Certificate, WSS 1.0
4	Mutual Certificate, WSS1.0	Issued SAML 1.1 Token for Certificate, WSS 1.0
5	Mutual Certificate, WSS1.1	Issued SAML 1.1 Token for Certificate, WSS 1.1
6	Mutual Certificate, WSS1.1	SecureConversation
7	Delegated SAML 2.0 with Certificate for SAML 2.0 HoK, WSS 1.1	Issued SAML 2.0 Token

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 18 July 2006

Marc A Goodner 7/18/06 4:22 PM
Inserted: 18 July 2006

2.1. Preconditions

WSDL

See the WSDL section at the end of this document for the STS and Service WSDL.

User Name and Password

The client and STS must agree on a list of acceptable user names and passwords. At a minimum a user name of joe and password of eoj should be supported by clients and STS to minimize necessary configuration tasks.

Certificates

The following certificates are associated with roles used across scenarios.

- Client: Alice
- STS: WssIP
- Service: Bob

Trust and Proof Keys

In all scenarios a trust relationship between the STS and Service is established by providing (out-of-band) the STS with the public key of the Service's X509 certificate and Service with the public key of the STS's X509 certificate.

In all Scenarios the STS will issue a symmetric proof-of-possession key associated with the SAML token. The key length can be requested by the Client via RequestSecurityToken/KeySize element, or is 256 by default.

Frederick Hirsch 7/21/06 4:39 PM
Deleted: \

The SAML token contains this proof-of-possession key encrypted for the Service's X509 certificate.

3. Client and STS Security Bindings

Frederick Hirsch 7/21/06 4:21 PM
Formatted: Bullets and Numbering

Each Scenario defined above will use one of the following security bindings for message exchanges between the Client and STS. This section provides an overview of the flow of those messages.

This STS contract covers a request/response MEP over the http binding. SOAP 1.1 MUST be used. As required by SOAP 1.1, the SOAPAction http header MUST be present. Any value, including a null string may be used. The recipient SHOULD ignore the value.

The Client sends the STS a single SOAP message with body containing a RST element; the STS responds with a single SOAP message containing either (1) SOAP fault (2) RSTR element.

The sections below detail the specific requirements for each Client and STS binding.

3.1. Username for SAML 1.1 HoK over HTTPS

Frederick Hirsch 7/21/06 4:20 PM
Formatted: Bullets and Numbering

This binding is used in Scenario 1.

Username Token is used to authenticate the Client. The STS's certificate is used to authenticate the service. Secure transport (HTTPS) is used for message protection.

Expected Security Properties

Use of the service is restricted to authorized parties who can present a valid user name and password.

Agreements

This section describes the agreements that must be made, directly or indirectly between parties who wish to interoperate beyond the common preconditions noted for all scenarios.

Acceptable <wsa:EndpointReference> Values

The requestor and the STS must agree on at least one <wsa:EndpointReference> value on receipt of which the STS can issue a SAML HoK assertion.

Request Message

Message Creation

Security

The Security element MUST contain the mustUnderstand="1" attribute.

UserName

The security element MUST contain a username element with a UserName and Password sub-elements.

Body

RequestSecurityToken

TokenType

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 18 July 2006

Marc A Goodner 7/18/06 4:22 PM
Inserted: 18 July 2006

If present, the <t:TokenType> element value MUST be equal to http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0#SAMLV1.1

RequestType

The <t:RequestType> element value MUST be equal to http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue

AppliesTo

If present, this element MUST include an <wsa:EndpointReference> element with a <wsa:Address> sub-element. The value of the <wsa:Address> element should be known to the STS.

KeyType

The <t:KeyType> element value MUST be equal to http://docs.oasis-open.org/ws-sx/wstrust/200512/SymmetricKey

Message Processing

This section describes the processing performed by the STS. The STS checks the name and password found in the SOAP header. If it can find the name and password pair in its local lists, it creates a RSTR message with a SAML 1.1 assertion. . It verifies that its local policy permits the issuance of a SAML bearer assertion for the value of the <wsa:EndpointReference> found in the message. The <SubjectConfirmation>/<ConfirmationMethod> element in the returned SAML assertion should be set to urn:oasis:names:tc:SAML:1.0:cm:holder-of-key.

If an error is detected, the STS MUST cease processing the message and report the fault with a value of t:FailedAuthentication (name or password are unacceptable) or t:RequestFailed (other reasons for failure).

Example (Non-normative)

Here is an example request.

```
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope"
  xmlns:a="http://schemas.xmlsoap.org/ws/2004/08/addressing"
  xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd"
  xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd"
  xmlns:t="http://docs.oasis-open.org/ws-sx/ws-trust/200512"
>
  <s:Header>
    <a:Action s:mustUnderstand="1" u:Id="_3">
      http://docs.oasis-open.org/ws-sx/ws-trust/200512/RST/Issue
    </a:Action>
    <a:MessageID u:Id="_4">
      urn:uuid:85836182-3ef8-4efc-a93f-06466277053e
    </a:MessageID>
    <a:ReplyTo u:Id="_5">
      <a:Address>
        http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous
      </a:Address>
    </a:ReplyTo>
```

```
    <a:To s:mustUnderstand="1" u:Id="_6">
      http://server.example.com/STS/Scenario1
    </a:To>
    <o:Security s:mustUnderstand="1">
      <u:Timestamp u:Id="uuid-c3cdb38b-e4aa-4467-9d0e-dd30f081e08d-5">
        <u:Created>2005-10-24T15:51:44.664Z</u:Created>
        <u:Expires>2005-10-24T15:56:44.664Z</u:Expires>
      </u:Timestamp>
      <o:UsernameToken u:Id='Me'>
        <o:Username>joe</o:Username>
        <o:Password>eoj</o:Password>
      </o:UsernameToken>
    </o:Security>
  </s:Header>
  <s:Body>
    <t:RequestSecurityToken>
      <t:RequestType>
        http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue
      </t:RequestType>
      <t:Entropy>
        <t:BinarySecret u:Id="uuid-4acf589c-0076-4a83-8b66-5f29341514b7-3"
          Type="http://docs.oasis-open.org/ws-sx/ws-trust/200512/Nonce">
          Uv38QLxDQM9gLoDZ6OwYDiFk094nmwu3Wmay7EdKmhw=
        </t:BinarySecret>
      </t:Entropy>
      <t:KeyType>
        http://docs.oasis-open.org/ws-sx/ws-trust/200512/SymmetricKey
      </t:KeyType>
      <t:KeySize>
        256
      </t:KeySize>
      <t:ComputedKeyAlgorithm>
        http://docs.oasis-open.org/ws-sx/ws-trust/200512/CK/PSHA1
      </t:ComputedKeyAlgorithm>
    </t:RequestSecurityToken>
  </s:Body>
</s:Envelope>
```

Request Policy

Since there are no requirements for client authentication using HTTPS, the TransportBinding assertion alone is adequate to capture the requirement to use HTTPS to secure the channel.

The policy corresponding to the request requirements may be written:

```
<wsp:Policy>
  <sp:TransportBinding />
  <sp:UsernameToken
      sp:IncludeToken='http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200512/IncludeToken/Always' />
</wsp:Policy>
```

Frederick Hirsch 7/21/06 4:56 PM
Formatted: Body Text

Frederick Hirsch 7/21/06 5:00 PM
Formatted: Code,c

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 18 July 2006

Marc A Goodner 7/18/06 4:22 PM
Inserted: 18 July 2006

Response Message

Message Creation

Body

RequestSecurityTokenResponseCollection/RequestSecurityTokenResponse

TokenType

The <t:TokenType> element value MUST be equal to http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0#SAMLV1.1

AppliesTo

If present, the <wsp:AppliesTo> element contents MUST be identical to that found in the RST message.

Lifetime

A <t:Lifetime> element MUST be present and include a <wsu:Created> and <wsu:Expires> sub-element

RequestedSecurityToken

Assertion

A SAML 1.1 Assertion MUST be returned; the assertion MUST contain a statement with <saml:ConfirmationMethod> set to urn:oasis:names:tc:SAML:1.0:cm:holder-of-key. The assertion MUST be signed and include a <ds:Signature> element as part of an enveloped signature.

Message Processing

The requestor must check to see if all elements noted as mandatory are present in the response. It must further verify that values for <t:TokenType> and <wsp:AppliesTo> are set as required above.

Typically, requestors will not process the contents of the SAML assertion; instead, the assertion is used to secure an exchange with a recipient. However, it is suggested that requestors check the value of the <saml:ConfirmationMethod> and also ensure that the assertion contains an enveloped signature.

Example (Non-normative)

Here is an example response.

```
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope"
  xmlns:a="http://schemas.xmlsoap.org/ws/2004/08/addressing"
  xmlns:e="http://www.w3.org/2001/04/xmlenc#"
  xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd"
  xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
  xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd"
  xmlns:t="http://docs.oasis-open.org/ws-sx/ws-trust/200512"
  >
  <s:Header>
```

```
    <a:Action s:mustUnderstand="1" u:Id="_3">
      http://docs.oasis-open.org/ws-sx/ws-trust/200512/RSTRC/IssueFinal
    </a:Action>
    <a:MessageID u:Id="_4">
      urn:uuid:85836182-3ef8-4efc-a93f-06466277053e
    </a:MessageID>
    <a:ReplyTo u:Id="_5">
      <a:Address>
        http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous
      </a:Address>
    </a:ReplyTo>
    <a:To s:mustUnderstand="1" u:Id="_6">
      http://client.example.com/STS/Scenario1
    </a:To>
    <o:Security s:mustUnderstand="1">
      <u:Timestamp u:Id="uuid-c3cdb38b-e4aa-4467-9d0e-dd30f081e08d-5">
        <u:Created>2005-10-24T15:51:44.664Z</u:Created>
        <u:Expires>2005-10-24T15:56:44.664Z</u:Expires>
      </u:Timestamp>
    </o:Security>
  </s:Header>
  <s:Body>
   <t:RequestSecurityTokenResponseCollection>
    <t:RequestSecurityTokenResponse>
      <t:TokenType>
        http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-
1.1#SAMLV1.1
      </t:TokenType>
      <t:KeySize>
        256
      </t:KeySize>
      <t:RequestedAttachedReference>
        <o:SecurityTokenReference>
          <o:KeyIdentifier
            ValueType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-
profile-1.0#SAMLAssertionID">
            uuid-8222b7a2-3874-4884-bdb5-9c2ddd4b86b5-16
          </o:KeyIdentifier>
        </o:SecurityTokenReference>
      </t:RequestedAttachedReference>
      <t:RequestedUnattachedReference>
        <o:SecurityTokenReference>
          <o:KeyIdentifier
            ValueType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-
profile-1.0#SAMLAssertionID">
```

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 18 July 2006

Marc A Goodner 7/18/06 4:22 PM
Inserted: 18 July 2006

```
            uuid-8222b7a2-3874-4884-bdb5-9c2ddd4b86b5-16
          </o:KeyIdentifier>
        </o:SecurityTokenReference>
      </t:RequestedUnattachedReference>
      <t:Lifetime>
        <u:Created>2005-10-24T20:19:26.526Z</u:Created>
        <u:Expires>2005-10-25T06:24:26.526Z</u:Expires>
      </t:Lifetime>
      <t:RequestedSecurityToken>
        <saml:Assertion MajorVersion="1" MinorVersion="1"
          AssertionID="uuid-8222b7a2-3874-4884-bdb5-9c2ddd4b86b5-16"
          Issuer="Test STS"
          IssueInstant="2005-10-24T20:24:26.526Z">
          <saml:Conditions NotBefore="2005-10-24T20:19:26.526Z"
NotOnOrAfter="2005-10-25T06:24:26.526Z"/>
          <saml:Advice/>
          <saml:AttributeStatement>
            <saml:Subject>
              <saml:SubjectConfirmation>
                <saml:ConfirmationMethod>
                  urn:oasis:names:tc:SAML:1.0:cm:holder-of-key
                </saml:ConfirmationMethod>
                <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
                  <e:EncryptedKey>
                    <e:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p"/>
                    <KeyInfo>
                      <o:SecurityTokenReference>
                        <o:KeyIdentifier
                          ValueType="http://docs.oasis-open.org/wss/oasis-
wss-wssecurity-secext-1.1.xsd#ThumbprintSHA1">
                          NQM0IBvuplAtETQvk+6gn8C13wE=
                        </o:KeyIdentifier>
                      </o:SecurityTokenReference>
                    </KeyInfo>
                    <e:CipherData>
                      <e:CipherValue>
EEcYjwNoYcJ+20xTYE5e/fixl5KOgzgrfaYAxkDFv/VXiuKfl084h8PmogTfM+azcgAfmArVQvOyK
WXRb5vmXYfVHLlhZTbXacy+nowSUNnEjp37VDbI3RJ5k6tBHF+ow0NM/P6GPNZ9ZqJi11GDgWJkFs
JzNZXNbbMgwuFu3cA=
                      </e:CipherValue>
                    </e:CipherData>
                  </e:EncryptedKey>
                </KeyInfo>
              </saml:SubjectConfirmation>
```

Marc A Goodner 7/18/06 4:35 PM
Deleted: http://docs.oasis-open.org/wss/2005/xx/oasis-2005xx-wss-soap-message-security-1.1

```
            </saml:Subject>
          </saml:AttributeStatement>
          <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/2000/09/xmldsig#rsa-sha1"/>
              <Reference URI="#uuid-8222b7a2-3874-4884-bdb5-9c2ddd4b86b5-16">
                <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/2000/09/xmldsig#sha1"/>
                <DigestValue>7nHBrFPsm+LEFAoV4NoQPoEl5Lk=</DigestValue>
              </Reference>
            </SignedInfo>
            <SignatureValue>
TugV4pTIwCH87bLD4jiMgVGtkbRBt1tRlHXJArL34A/YfA4AnGBLXB4pJdUsUxMUtbQl4PoGgEsdL
Ng8C77peARELGP1/Tqw7T3u5zBYHxCHCiV2FWBBfeOmwJmqoaBf8XZJ4AlyqPq61P61jrQjZJafpH
uYpAZnZQSvsiJaBPQ=
            </SignatureValue>
            <KeyInfo>
              <o:SecurityTokenReference>
                <o:KeyIdentifier
                  ValueType="http://docs.oasis-open.org/wss/oasis-wss-
wssecurity-secext-1.1.xsd#ThumbprintSHA1">
                  NQM0IBvuplAtETQvk+6gn8C13wE=
                </o:KeyIdentifier>
              </o:SecurityTokenReference>
            </KeyInfo>
          </Signature>
        </saml:Assertion>
      </t:RequestedSecurityToken>
      <t:RequestedProofToken>
        <t:BinarySecret u:Id="uuid-8222b7a2-3874-4884-bdb5-9c2ddd4b86b5-14">
          zT8LWAUwUrIVKA/rkCr0kxlEmKAEhcB6TGWJuAgucBM=
        </t:BinarySecret>
      </t:RequestedProofToken>
    </t:RequestSecurityTokenResponse>
  </t:RequestSecurityTokenResponseCollection>
 </s:Body>
</s:Envelope>
```

Marc A Goodner 7/18/06 4:35 PM
Deleted: http://docs.oasis-open.org/wss/2005/xx/oasis-2005xx-wss-soap-message-security-1.1

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 18 July 2006

Marc A Goodner 7/18/06 4:22 PM
Inserted: 18 July 2006

3.2. Username for SAML 1.1 Bearer Token, WSS 1.0

This binding is used in scenario 2.

The requestor sends the STS a message over HTTP requesting issuance of a SAML token. The RST message is secured by a WSS 1.1 UserNameToken placed in the SOAP security header. The STS responds with a RSTR within an RSTRC message with a SAML bearer token. The SAML token is signed by the STS. The certificate used to sign the SAML token is included in the <ds:KeyInfo> element of the assertion.

Frederick Hirsch 7/21/06 6:36 PM
Deleted: RSTR

Frederick Hirsch 7/21/06 4:40 PM
Deleted: keyinfo

Expected Security Properties

Use of the service is restricted to authorized parties that can present valid user name and password.

Agreements

This section describes the agreements that must be made, directly or indirectly between parties who wish to interoperate beyond the common preconditions noted for all scenarios.

Acceptable <wsa:EndpointReference> Values

The requestor and the STS must agree on at least one <wsa:EndpointReference> value on receipt of which the STS can issue a SAML bearer assertion.

Request Message

Message Creation

Security

The Security element MUST contain the mustUnderstand="1" attribute.

UserName

The security element MUST contain a username element with a UserName and Password sub-elements.

Body

RequestSecurityToken

TokenType

The <t:TokenType> element value MUST be equal to http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0#SAMLV1.1

RequestType

The <t:RequestType> element value MUST be equal to http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue

AppliesTo

This element MUST include an <wsa:EndpointReference> element with a <wsa:Address> sub-element. The value of the <wsa:Address> element should be known to the STS.

436 KeyType

437 The <t:KeyType> element value MUST be equal to http://docs.oasis-open.org/ws-
438 sx/wstrust/200512/Bearer

439 ***Message Processing***

440 This section describes the processing performed by the STS. The STS checks the name and password
441 found in the SOAP header. If it can find the name and password pair in its local lists, it creates a RSTR
442 message with a SAML 1.1 assertion. . It verifies that its local policy permits the issuance of a SAML
443 bearer assertion for the value of the <wsa:EndpointReference> found in the message. The
444 <SubjectConfirmation>/<ConfirmationMethod> element in the returned SAML assertion should be set to
445 urn:oasis:names:tc:SAML:1.0:cm:bearer.

446 If an error is detected, the STS MUST cease processing the message and report the fault with a value of
447 t:FailedAuthentication (name or password are unacceptable) or t:RequestFailed (other reasons for
448 failure).

449 ***Example (Non-normative)***

450 Here is an example request.

```
451 <?xml version="1.0" encoding="utf-8" ?>
452 <soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
453 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
454 xmlns:xsd="http://www.w3.org/2001/XMLSchema"
455 xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
456 wssecurity-secext-1.0.xsd"
457 xmlns:wst="http://docs.oasis-open.org/ws-sx/ws-trust/200512"
458 >
459  <soap:Header>
460   <wsse:Security soap:mustUnderstand="1">
461      <wsse:UserNameToken>
462          <wsse:UserName>Joe</UserName><wsse:Password>eoj</Password>
463      </wsse:UserNameToken>
464   </wsse:Security>
465  </soap:Header>
466  <soap:Body>
467 <t:RequestSecurityToken>
468     <t:TokenType>
469        http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-
470 1.0#SAMLV1.1
471     </t:TokenType>
472     <t:RequestType>
473       http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue
474     </t:RequestType>
475     <wsp:AppliesTo
476 xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/03/addressing">
477             <wsa:EndpointReference>
478                <wsa:Address>http://www.example.org/</wsa:Address>
```

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 18 July 2006

Marc A Goodner 7/18/06 4:22 PM
Inserted: 18 July 2006

```
            </wsa:EndpointReference>
    </wsp:Appliesto>
    <t:KeyType>
         http://docs.oasis-open.org/ws-sx/wstrust/200512/Bearer
     </t:KeyType>
</t:RequestSecurityToken>
</soap:Body>
</soap:Envelope>
```

Policy

Same as previous case.

Response Message

Message Creation

Body

RequestSecurityTokenResponseCollection/RequestSecurityTokenResponse

TokenType

The <t:TokenType> element value MUST be equal to http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0#SAMLV1.1

AppliesTo

The <wsp:AppliesTo> element contents MUST be identical to that found in the RST message.

Lifetime

A <t:Lifetime> element MUST be present and include a <wsu:Created> and <wsu:Expires> sub-element

RequestedSecurityToken

Assertion

A SAML 1.1 Assertion MUST be returned; the assertion MUST contain a statement with <saml:ConfirmationMethod> set to urn:oasis:names:tc:SAML:1.0:cm:bearer. The assertion MUST be signed and include a <ds:Signature> element as part of an enveloped signature.

Message Processing

The requestor must check to see if all elements noted as mandatory are present in the response. It must further verify that values for <t:TokenType> and <wsp:AppliesTo> are set as required above.

Typically, requestors will not process the contents of the SAML assertion; instead, the assertion is used to secure an exchange with a recipient. However, it is suggested that requestors check the value of the <saml:ConfirmationMethod> and also ensure that the assertion contains an enveloped signature.

Example (Non-normative)

Here is an example response.

```
<?xml version="1.0" encoding="utf-8" ?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
xmlns:wst="http://docs.oasis-open.org/ws-sx/ws-trust/200512"
 xmlns:xsd="http://www.w3.org/2001/XMLSchema">
 <soap:Header>
 </soap:Header>
 <soap:Body wsu:Id="body"
xmlns:wsu="http://schemas.xmlsoap.org/ws/2003/06/utility">
   <t:RequestSecurityTokenResponseCollection>
      <t:RequestSecurityTokenResponse>
         <t:TokenType>
     http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0#SAMLV1.1
         </t:TokenType>
        <wsp:AppliesTo
xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/03/addressing">
            <wsa:EndpointReference>
               <wsa:Address>http://www.example.org/</wsa:Address>
            </wsa:EndpointReference>
        <wsp:AppliesTo>
       <t:Lifetime>
         <wsu:Created>"2005-04-17T00:46:02Z"</wsu:Created>
         <wsu:Expires>"2005-04-17T00:51:02Z"> </wsu:Expires>
        </t:Lifetime>

       <t:RequestedSecurityToken>
         <saml:Assertion
              AssertionID="_a75adf55-01d7-40cc-929f-dbd8372ebdfc"
              IssueInstant="2005-04-17T00:46:02Z"
              Issuer="www.opensaml.org"
              MajorVersion="1"
              MinorVersion="1"
              Xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
              xmlns:xsd="http://www.w3.org/2001/XMLSchema"
             xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <saml:Conditions
             NotBefore="2005-04-17T00:46:02Z"
             NotOnOrAfter="2005-04-17T00:51:02Z">
         </saml:Conditions>
     <saml:AuthenticationStatement
         AuthenticationInstant="2003-04-17T00:46:00Z"
         AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:password">
     <saml:Subject>
       <saml:NameIdentifier
              Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:emailAddress">
```

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 18 July 2006

Marc A Goodner 7/18/06 4:22 PM
Inserted: 18 July 2006

```
        scott@example.org</NameIdentifier>
       <saml:SubjectConfirmation>
         <saml:ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:bearer
        </saml:ConfirmationMethod>
        </saml:SubjectConfirmation>
     </saml:Subject>
     </saml:AuthenticationStatement>
<ds:Signature
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
<ds:SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<ds:Reference
URI="#_a75adf55-01d7-40cc-929f-dbd8372ebdfc">
<ds:Transforms>
<ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
<ds:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
<InclusiveNamespaces
PrefixList="#default saml samlp ds xsd xsi"
xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"/>
</ds:Transform>
</ds:Transforms>
<ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<ds:DigestValue>Kclet6XcaOgOWXM4gty6/UNdviI=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>
hq4zk+ZknjggCQgZm7ea8fI79gJEsRy3E8LHDpYXWQIgZpkJN9CMLG8ENR4Nrw+n
7iyzixBvKXX8P53BTCT4VghPBWhFYSt9tHWu/AtJfOTh6qaAsNdeCyG86jmtp3TD
MWuL/cBUj2OtBZOQMFn7jQ9YB7klIz3RqVL+wNmeWI4=</ds:SignatureValue>
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate>
MIICyjCCAjOgAwIBAgICAnUwDQYJKoZIhvcNAQEEBQAwgakxCzAJBgNVBAYTAlVT
MRIwEAYDVQQIEwlXaXNjb25zaW4xEDAOBgNVBAcTB01hZGlzb24xIDAeBgNVBAoT
F1VuaXZlcnNpdHkgb2YgV2lzY29uc2luMSswKQYDVQQLEyJEaXZpc2lvbiBvZiBJ
bmZvcm1hdGlvbiBUZWNobm9sb2d5MSUwIwYDVQQDExxIRVBLSSBTZXJ2ZXIgQ0Eg
LS0gMjAwMjA3MDFBMB4XDTAyMDcyNjA3Mjc1MVoXDTA2MDkwNDA3Mjc1MVowgYsx
CzAJBgNVBAYTAlVTMREwDwYDVQQIEwhNaWNoaWdhbjESMBAGA1UEBxMJQW5uIEFy
Ym9yMQ4wDAYDVQQKEwVVQ0FJRDEcMBoGA1UEAxMTc2hpYjEuaW50ZXJuZXQyLmVk
```

```
dTEnMCUGCSqGSIb3DQEJARYYcm9vdEBzaGliMS5pbnRlcm5ldDIuZWR1MIGfMA0G
CSqGSIb3DQEBAQUAA4GNADCBiQKBgQDZSAb2sxvhAXnXVIVTx8vuRay+x50z7GJj
IHRYQgIv6IqaGG04eTcyVMhoekE0b45QgvBIaOAPSZBl13R6+KYiE7x4XAWIrCP+
c2MZVeXeTgV3Yz+USLg2Y1on+Jh4HxwkPFmZBctyXiUr6DxF8rvoP9W7O27rhRjE
pmqOIfGTWQIDAQABox0wGzAMBgNVHRMBAf8EAjAAMAsGA1UdDwQEAwIFoDANBgkq
hkiG9w0BAQQFAAOBgQBfDqEW+OI3jqBQHIBzhujN/PizdN7s/z4D5d3pptWDJf2n
qgi7lFV6MDkhmTvTqBtjmNk3No7v/dnP6Hr7wHxvCCRwubnmIfZ6QZAv2FU78pLX
8I3bsbmRAUg4UP9hH6ABVq4KQKMknxu1xQxLhpR1ylGPdiowMNTrEG8cCx3w/w==
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</ds:signature>
     </saml:Assertion>
     </t:RequestedSecurityToken>
     </t:SecurityTokenResponse>
   <t:RequestSecurityTokenResponseCollection>
 </soap:Body>
</soap:Envelope>
```

3.3. Certificate for SAML 1.1 HoK Token, WSS 1.0

This binding is used in scenario 3.

The requestor sends the STS a message over HTTP requesting issuance of a SAML token. The RST message includes a WSS 1.1 X.509 BinarySecurityToken in the SOAP security header. The STS responds with a RSTR message with a SAML Holder of Key (HoK) Assertion. The SAML assertion is signed by the STS. The certificate used to sign the SAML token is included in the <ds:KeyInfo> element of the assertion.

Frederick Hirsch 7/21/06 4:41 PM
Deleted: keyinfo

NOTE: In most use-cases, there may be an authentication or proof step associated with the certificate provided in the header. This may take the form of a digital signature or a SSL handshake. This step is omitted in this scenario.

Expected Security Properties

Use of the service is restricted to authorized parties that can present valid WSS 1.1 X.509 BinarySecurityToken.

Agreements

This section describes the agreements that must be made, directly or indirectly between parties who wish to interoperate beyond the common preconditions noted for all scenarios.

Acceptable <wsa:EndpointReference> Values

The requestor and the STS must agree on at least one <wsa:EndpointReference> value on receipt of which the STS can issue a SAML HoK assertion.

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 18 July 2006

Marc A Goodner 7/18/06 4:22 PM
Inserted: 18 July 2006

Request Message

Message Creation

Security

The Security element MUST contain the mustUnderstand="1" attribute.

BinarySecurityToken

The security element MUST contain a BinarySecurityToken with a X.509 certificate that is encoded as Base64 sequence. The ValueType attribute MUST be set to #X509v3.

Body

RequestSecurityToken

TokenType

If present, the <t:TokenType> element value MUST be equal to http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0#SAMLV1.1

RequestType

The <t:RequestType> element value MUST be equal to http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue

AppliesTo

If present. this element MUST include an <wsa:EndpointReference> element with a <wsa:Address> sub-element. The value of the <wsa:Address> element should be known to the STS.

KeyType

The <t:KeyType> element value MUST be equal to http://docs.oasis-open.org/ws-sx/wstrust/200512/PublicKey

Message Processing

This section describes the processing performed by the STS. It verifies that its local policy permits the issuance of a SAML HoK assertion for the value of the <wsa:EndpointReference> found in the message.

The value of the <SubjectConfirmation>/<ds:KeyInfo> element in the SAML assertion is a <ds:X.509Data> element with a <ds:X509Certificate> sub-element. The base-64 certificate value is taken from the security header of the request message. The <SubjectConfirmation>/<ConfirmationMethod> element is set to urn:oasis:names:tc:SAML:1.0:cm:holder-of-key.

If an error is detected, the STS MUST cease processing the message and report the fault with a value of t:RequestFailed (other reasons for failure).

Example (Non-normative)

Here is an example request.

```
<?xml version="1.0" encoding="utf-8" ?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
```

```
xmlns:wsse=”http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd”
xmlns:wst=”http://docs.oasis-open.org/ws-sx/ws-trust/200512”
>


 <soap:Header>
  <wsse:Security soap:mustUnderstand=“1”>
          <wsse:BinarySecurityToken
                    wsu:Id="binarytoken"
                    ValueType="…#X509v3"
                    EncodingType="…#Base64Binary">
                          MIIEZzCCA9CgAwIBAgIQEmtJZc0…
          </wsse:BinarySecurityToken>
  </wsse:Security>
 </soap:Header>
 <soap:Body>
<t:RequestSecurityToken>
    <t:TokenType>
       http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-
1.0#SAMLV1.1
    </t:TokenType>
    <t:RequestType>
      http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue
    </t:RequestType>
    <wsp:AppliesTo
xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/03/addressing">
            <wsa:EndpointReference>
               <wsa:Address>http://www.example.org/</wsa:Address>
            </wsa:EndpointReference>
    </wsp:Appliesto>
    <t:KeyType>
         http://docs.oasis-open.org/ws-sx/wstrust/200512/PublicKey
     </t:KeyType>
</t:RequestSecurityToken>
</soap:Body>
</soap:Envelope>
```

Policy

Note this policy statement assumes the use of SSL as indicated in the Note above.

```
<wsp:Policy>
  <sp:TransportBinding />
  <sp:X509Token
     sp:IncludeToken='http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200512/IncludeToken/Always' />
    <wsp:Policy>
```

Frederick Hirsch 7/21/06 5:12 PM
Formatted: Body Text

Frederick Hirsch 7/21/06 5:16 PM
Formatted: Code,c

Unknown
Field Code Changed

Frederick Hirsch 7/21/06 5:16 PM
Formatted: Font:Courier New, 10 pt

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 18 July 2006

Marc A Goodner 7/18/06 4:22 PM
Inserted: 18 July 2006

```
      <sp:WssX509V3Token11 />
    </wsp:Policy>
  </sp:X509Token>
</wsp:Policy>
```

Response Message

Message Creation

Body

RequestSecurityTokenResponseCollection/RequestSecurityTokenResponse

TokenType

The <t:TokenType> element value MUST be equal to http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0#SAMLV1.1

AppliesTo

The <wsp:AppliesTo> element contents MUST be identical to that found in the RST message.

Lifetime

A <t:Lifetime> element MUST be present and include a <wsu:Created> and <wsu:Expires> sub-element

RequestedSecurityToken

Assertion

A SAML 1.1 Assertion MUST be returned; the assertion MUST contain a statement with <saml:ConfirmationMethod> set to urn:oasis:names:tc:SAML:1.0:cm: holder-of-key. The value of the <SubjectConfirmation>/<ds:KeyInfo> element in the SAML assertion is a <ds:X.509Data> element with a <ds:X509Certificate> sub-element. The base-64 certificate value is taken from the BinarySecurityToken element in the request message. The assertion MUST be signed and include a <ds:Signature> element as part of an enveloped signature.

Message Processing

The requestor must check to see if all elements noted as mandatory are present in the response. It must further verify that values for <t:TokenType> and <wsp:AppliesTo> are set as required above.

Typically, requestors will not process the contents of the SAML assertion; instead, the assertion is used to secure an exchange with a recipient. However, it is suggested that requestors check the value of the <saml:ConfirmationMethod> and also ensure that the assertion contains an enveloped signature.

Example (Non-normative)

Here is an example response.

```
<?xml version="1.0" encoding="utf-8" ?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
xmlns:wst=”http://docs.oasis-open.org/ws-sx/ws-trust/200512”
 xmlns:xsd="http://www.w3.org/2001/XMLSchema">
 <soap:Header>
```

```
 </soap:Header>
 <soap:Body wsu:Id="body"
xmlns:wsu="http://schemas.xmlsoap.org/ws/2003/06/utility">
   <t:RequestSecurityTokenResponseCollection>
      <t:RequestSecurityTokenResponse>
         <t:TokenType>
     http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0#SAMLV1.1
         </t:TokenType>
        <wsp:AppliesTo
xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/03/addressing">
            <wsa:EndpointReference>
               <wsa:Address>http://www.example.org/</wsa:Address>
            </wsa:EndpointReference>
        </wsp:AppliesTo>
       <t:Lifetime>
         <wsu:Created>"2005-04-17T00:46:02Z"</wsu:Created>
         <wsu:Expires>"2005-04-17T00:51:02Z"</wsu:Expires>
        </t:Lifetime>

       <t:RequestedSecurityToken>
         <saml:Assertion
              AssertionID="_a75adf55-01d7-40cc-929f-dbd8372ebdfc"
              IssueInstant="2005-04-17T00:46:02Z"
              Issuer="www.opensaml.org"
              MajorVersion="1"
              MinorVersion="1"
              Xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
              xmlns:xsd="http://www.w3.org/2001/XMLSchema"
             xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <saml:Conditions
             NotBefore="2005-04-17T00:46:02Z"
             NotOnOrAfter="2005-04-17T00:51:02Z">
         </saml:Conditions>
     <saml:AuthenticationStatement
         AuthenticationInstant="2003-04-17T00:46:00Z"
         AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:Unspecified">
     <saml:Subject>
       <saml:NameIdentifier
               Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:emailAddress">
        scott@example.org</NameIdentifier>
       <saml:SubjectConfirmation>
         <saml:ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:holder-of-
key
        </saml:ConfirmationMethod>
       <ds:KeyInfo>
```

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 18 July 2006

Marc A Goodner 7/18/06 4:22 PM
Inserted: 18 July 2006

```
        <ds:KeyValue>
        <ds:X509Data><ds:X509Certificate> MIIEZzCCA9CgAwIBAgIQEmtJZc0…
                     <ds:X509Certificate>
       <ds:X509Data>
       </ds:KeyValue>
       </ds:KeyInfo>
        </saml:SubjectConfirmation>
     </saml:Subject>
     </saml:AuthenticationStatement>
<ds:Signature
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
<ds:SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<ds:Reference
URI="#_a75adf55-01d7-40cc-929f-dbd8372ebdfc">
<ds:Transforms>
<ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
<ds:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
<InclusiveNamespaces
PrefixList="#default saml samlp ds xsd xsi"
xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"/>
</ds:Transform>
</ds:Transforms>
<ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<ds:DigestValue>Kclet6XcaOgOWXM4gty6/UNdviI=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>
hq4zk+ZknjggCQgZm7ea8fI79gJEsRy3E8LHDpYXWQIgZpkJN9CMLG8ENR4Nrw+n
7iyzixBvKXX8P53BTCT4VghPBWhFYSt9tHWu/AtJfOTh6qaAsNdeCyG86jmtp3TD
MWuL/cBUj2OtBZOQMFn7jQ9YB7klIz3RqVL+wNmeWI4=</ds:SignatureValue>
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate>
MIICyjCCAjOgAwIBAgICAnUwDQYJKoZIhvcNAQEEBQAwgakxCzAJBgNVBAYTAlVT
MRIwEAYDVQQIEwlXaXNjb25zaW4xEDAOBgNVBAcTB01hZGlzb24xIDAeBgNVBAoT
F1VuaXZlcnNpdHkgb2YgV2lzY29uc2luMSswKQYDVQQLEyJEaXZpc2lvbiBvZiBJ
bmZvcm1hdGlvbiBUZWNobm9sb2d5MSUwIwYDVQQDExxIRVBLSSBTZXJ2ZXIgQ0Eg
LS0gMjAwMjA3MDFBMB4XDTAyMDcyNjA3Mjc1MVoXDTA2MDkwNDA3Mjc1MVowgYsx
CzAJBgNVBAYTAlVTMREwDwYDVQQIEwhNaWNoaWdhbjESMBAGA1UEBxMJQW5uIEFy
```

```
Ym9yMQ4wDAYDVQQKEwVVQ0FJRDEcMBoGA1UEAxMTc2hpYjEuaW50ZXJuZXQyLmVk
dTEnMCUGCSqGSIb3DQEJARYYcm9vdEBzaGliMS5pbnRlcm5ldDIuZWR1MIGfMA0G
CSqGSIb3DQEBAQUAA4GNADCBiQKBgQDZSAb2sxvhAXnXVIVTx8vuRay+x50z7GJj
IHRYQgIv6IqaGG04eTcyVMhoekE0b45QgvBIaOAPSZBl13R6+KYiE7x4XAWIrCP+
c2MZVeXeTgV3Yz+USLg2Y1on+Jh4HxwkPFmZBctyXiUr6DxF8rvoP9W7O27rhRjE
pmqOIfGTWQIDAQABox0wGzAMBgNVHRMBAf8EAjAAMAsGA1UdDwQEAwIFoDANBgkq
hkiG9w0BAQQFAAOBgQBfDqEW+OI3jqBQHIBzhujN/PizdN7s/z4D5d3pptWDJf2n
qgi7lFV6MDkhmTvTqBtjmNk3No7v/dnP6Hr7wHxvCCRwubnmIfZ6QZAv2FU78pLX
8I3bsbmRAUg4UP9hH6ABVq4KQKMknxu1xQxLhpR1ylGPdiowMNTrEG8cCx3w/w==
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</ds:signature>
     </saml:Assertion>
     </t:RequestedSecurityToken>
     </t:RequestSecurityTokenResponse>
   <t:RequestSecurityTokenResponseCollection>
 </soap:Body>
</soap:Envelope>
```

3.4. Mutual Certificate, WSS1.0

This binding is used in Scenario 4.

Client and STS X509 certificates are used to authenticate client and STS respectively. Client sends Request to STS signed using Client's X509 certificate, then encrypted using ephemeral key K protected (wrapped) for STS's X509 Certificate. Signing token is attached in the request, wrapping token is unattached. STS signs the response using STS's X509 certificate and encrypts using ephemeral key K2 protected for the client certificate. Both signing and wrapping tokens are unattached in the response.

Expected Security Properties

Use of the service is restricted to authorized parties that can present a valid WSS 1.0 X.509 BinarySecurityToken.

Agreements

This section describes the agreements that must be made, directly or indirectly between parties who wish to interoperate beyond the common preconditions noted for all scenarios.

Acceptable <wsa:EndpointReference> Values

The requestor and the STS must agree on at least one <wsa:EndpointReference> value on receipt of which the STS can issue a SAML HoK token.

Request Message

Message Creation

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 18 July 2006
Marc A Goodner 7/18/06 4:22 PM
Inserted: 18 July 2006

Security

The Security element MUST contain the mustUnderstand="1" attribute.

BinarySecurityToken

The security element MUST contain a BinarySecurityToken with a X.509 certificate that is encoded as Base64 sequence. The ValueType attribute MUST be set to #X509v3.

Body

RequestSecurityToken

TokenType

If present, the <t:TokenType> element value MUST be equal to http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0#SAMLV1.1.

RequestType

The <t:RequestType> element value MUST be equal to http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue

AppliesTo

If present. this element MUST include an <wsa:EndpointReference> element with a <wsa:Address> sub-element. The value of the <wsa:Address> element should be known to the STS.

KeyType

The <t:KeyType> element value MUST be equal to http://docs.oasis-open.org/ws-sx/wstrust/200512/SymmetricKey

Message Processing

This section describes the processing performed by the STS. It verifies that its local policy permits the issuance of a SAML HoK assertion for the value of the <wsa:EndpointReference> found in the message.

If an error is detected, the STS MUST cease processing the message and report the fault with a value of t:RequestFailed (other reasons for failure).

Example (Non-normative)

Here is an example request.

```
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope"
  xmlns:a="http://schemas.xmlsoap.org/ws/2004/08/addressing"
  xmlns:e="http://www.w3.org/2001/04/xmlenc#"
  xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd"
  xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd"
  >
  <s:Header>
    <a:Action s:mustUnderstand="1" u:Id="_3">
      http://docs.oasis-open.org/ws-sx/ws-trust/200512/RST/Issue
    </a:Action>
```

```
    <a:MessageID u:Id="_4">
      urn:uuid:85836182-3ef8-4efc-a93f-06466277053e
    </a:MessageID>
    <a:ReplyTo u:Id="_5">
      <a:Address>
        http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous
      </a:Address>
    </a:ReplyTo>
    <a:To s:mustUnderstand="1" u:Id="_6">
      http://server.example.com/STS/Scenario4
    </a:To>
    <o:Security s:mustUnderstand="1">
      <u:Timestamp u:Id="uuid-c3cdb38b-e4aa-4467-9d0e-dd30f081e08d-5">
        <u:Created>2005-10-24T15:51:44.664Z</u:Created>
        <u:Expires>2005-10-24T15:56:44.664Z</u:Expires>
      </u:Timestamp>
      <o:BinarySecurityToken u:Id="uuid-c3cdb38b-e4aa-4467-9d0e-dd30f081e08d-
2"
        ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
x509-token-profile-1.0#X509v3"
        EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wss-soap-message-security-1.0#Base64Binary">
MIIDDDCCAfSgAwIBAgIQM6YEf7FVYx/tZyEXgVComTANBgkqhkiG9w0BAQUFADAwMQ4wDAYDVQQKD
AVPQVNJUzEeMBwGA1UEAwwVT0FTSVMgSW50ZXJvcCBUZXN0IENBMB4XDTA1MDMxOTAwMDAwMFoXDT
E4MDMxOTIzNTk1OVowQjEOMAwGA1UECgwFT0FTSVMxIDAeBgNVBAsMF09BU0lTIEludGVyb3AgVGV
zdCBDZXJ0MQ4wDAYDVQQDDAVBbGljZTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAoqi99By1
VYo0aHrkKCNT4DkIgPL/SgahbeKdGhrbu3K2XG7arfD9tqIBIKMfrX4Gp90NJa85AV1yiNsEyvq+m
UnMpNcKnLXLOjkTmMCqDYbbkehJlXPnaWLzve+mW0pJdPxtf3rbD4PS/cBQIvtpjmrDAU8VsZKT8D
N5Kyz+EZsCAwEAAaOBkzCBkDAJBgNVHRMEAjAAMDMGA1UdHwQsMCowKKImhiRodHRwOi8vaW50ZXJ
vcC5iYnRlc3QubmV0L2NybC9jYS5jcmwwDgYDVR0PAQH/BAQDAgSwMB0GA1UdDgQWBBQK4l0TUHZ1
QV3V2QtlLNDm+PoxiDAfBgNVHSMEGDAWgBTAnSj8wes1oR3WqqqgHBpNwkkPDzANBgkqhkiG9w0BA
QUFAAOCAQEABTqpOpvW+6yrLXyUlP2xJbEkohXHI5OWwKWleOb9hlkhWntUalfcFOJAgUyH30TTpH
ldzx1+vK2LPzhoUFKYHE1IyQvokBN2JjFO64BQukCKnZhldLRPxGhfkTdxQgdf5rCK/wh3xVsZCNT
fuMNmlAM6lOAg8QduDah3WFZpEA0s2nwQaCNQTNMjJC8tav1CBr6+E5FAmwPXP7pJxn9Fw9OXRyqb
RA4v2y7YpbGkG2GI9UvOHw6SGvf4FRSthMMO35YbpikGsLix3vAsXWWi4rwfVOYzQK0OFPNi9RMCU
dSH06m9uLWckiCxjos0FQODZE9l4ATGy9s9hNVwryOJTw==
      </o:BinarySecurityToken>
      <e:EncryptedKey Id="_0">
        <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-
oaep-mgf1p"/>
        <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
          <o:SecurityTokenReference>
            <o:KeyIdentifier
              ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wss-x509-token-profile-1.0#X509SubjectKeyIdentifier">
              Xeg55vRyK3ZhAEhEf+YT0z986L0=
            </o:KeyIdentifier>
          </o:SecurityTokenReference>
```

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 18 July 2006

Marc A Goodner 7/18/06 4:22 PM
Inserted: 18 July 2006

```
        </KeyInfo>
        <e:CipherData>
          <e:CipherValue>

WNcUubWi8BGtzjt9BFnEcr53ktqQiEkJWjkkxIkRnE3oEWRcceluOrwAVDxobKLO2Xz8x3NjQ1iRi
HQlMCuykFgACHIxcy7+odeW5deWSDf7nw1g/9iaVC+bUuYttuhHVc3uw3z+J143LQr4gwL5tnzzCB
Ux9WOkA6AShPbtEL8=
          </e:CipherValue>
        </e:CipherData>
        <e:ReferenceList>
          <e:DataReference URI="#_2"/>
        </e:ReferenceList>
      </e:EncryptedKey>
      <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/2000/09/xmldsig#rsa-
sha1"/>
          <Reference URI="#_1">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>Ha9+qHnkvikYdjG/XJjQZqAxVCA=</DigestValue>
          </Reference>
          <Reference URI="#_3">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>FwiFAUuqNDo9SDkk5A28Mg7Pa8Q=</DigestValue>
          </Reference>
          <Reference URI="#_4">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>jtGbn/BVKmfw6r9SP4a8jDKOzhI=</DigestValue>
          </Reference>
```

```
          <Reference URI="#_5">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>KIK3vklFN1QmMdQkplq2azfzrzg=</DigestValue>
          </Reference>
          <Reference URI="#_6">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>APDst42iUyZB8B+3UcRfv9fR0dU=</DigestValue>
          </Reference>
          <Reference URI="#uuid-c3cdb38b-e4aa-4467-9d0e-dd30f081e08d-5">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>4a8Vc8wN+esJrUNSumktT4GGHnw=</DigestValue>
          </Reference>
        </SignedInfo>
        <SignatureValue>
Gj8zD5HubAVSpPxJ72auHS+Wb7E7J3LETvqufcg/cyGNoAhiXO3ql26KwR9P1HchF9XU6ofaqcMDu
/THkHYFQwOytEme4lzggN/aDMbVW03XzES+GtuWSifYmszufYu9C0C5Vb7liFw1oxPCXhFDj7sN+M
5TYbQG1l2FoR6GQIQ=
        </SignatureValue>
        <KeyInfo>
          <o:SecurityTokenReference>
            <o:Reference
              ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wss-x509-token-profile-1.0#X509v3"
              URI="#uuid-c3cdb38b-e4aa-4467-9d0e-dd30f081e08d-2"/>
          </o:SecurityTokenReference>
        </KeyInfo>
      </Signature>
    </o:Security>
  </s:Header>
  <s:Body u:Id="_1">
    <e:EncryptedData Id="_2" Type="http://www.w3.org/2001/04/xmlenc#Content">
```

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 18 July 2006

Marc A Goodner 7/18/06 4:22 PM
Inserted: 18 July 2006

```
      <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-
cbc"/>
      <e:CipherData>
        <e:CipherValue>
          <!-- base64 encoded octets with encrypted RST request-->
          <!-- Unencrypted form:  -->
          <!--
    <t:RequestSecurityToken>
      <t:RequestType>
        http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue
      </t:RequestType>
      <t:Entropy>
        <t:BinarySecret u:Id="uuid-4acf589c-0076-4a83-8b66-5f29341514b7-3"
Type="http://docs.oasis-open.org/ws-sx/ws-
trust/200512/Nonce">Uv38QLxDQM9gLoDZ6OwYDiFk094nmwu3Wmay7EdKmhw=</t:BinarySec
ret>
      </t:Entropy>
      <t:KeyType>http://docs.oasis-open.org/ws-sx/ws-
trust/200512/SymmetricKey</t:KeyType>
      <t:KeySize>256</t:KeySize>
      <t:ComputedKeyAlgorithm>
        http://docs.oasis-open.org/ws-sx/ws-trust/200512/CK/PSHA1
      </t:ComputedKeyAlgorithm>
    </t:RequestSecurityToken>
          -->
        </e:CipherValue>
      </e:CipherData>
    </e:EncryptedData>
  </s:Body>
</s:Envelope>
```

Policy

Note, client token is not sent in request, only wrapped key according to note above. Note also that no algorithms were specified for this interop, so policy makes no statements.

```
<wsp:Policy>
<sp:SymmetricBinding>
    <wsp:Policy>
      <sp:ProtectionToken>
        <wsp:Policy>
          <sp:X509Token
            sp:IncludeToken='http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200512/IncludeToken/Never' />
            <wsp:Policy>
```

Frederick Hirsch 7/21/06 6:20 PM
Comment: Does it make sense in this case to specify X509v3 and token profile 11? Is it appropriate to specify the IncludeToken property?

Frederick Hirsch 7/21/06 5:35 PM
Formatted: Code,c

```
                <sp:WssX509V3Token11 />
            </wsp:Policy>
          </wsp:Policy>
        </sp:ProtectionToken>
        <sp:SignBeforeEncrypting />
        <sp:EncryptSignature />
      </wsp:Policy>
    </sp:SymmetricBinding>
</wsp:Policy>
```

Frederick Hirsch 7/21/06 5:35 PM
Formatted: Code,c

Response Message

Message Creation

Body

RequestSecurityTokenResponseCollection/RequestSecurityTokenResponse

TokenType

The <t:TokenType> element value MUST be equal to http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0#SAMLV1.1

Unknown
Field Code Changed

AppliesTo

If present, the <wsp:AppliesTo> element contents MUST be identical to that found in the RST message.

Lifetime

A <t:Lifetime> element MUST be present.

RequestedSecurityToken

A SAML 1.1 Assertion MUST be returned.

Message Processing

The requestor must check to see if all elements noted as mandatory are present in the response. It must further verify that values for <t:TokenType> and <wsp:AppliesTo> are set as required above.

Example (Non-normative)

Here is an example response.

```
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope"
  xmlns:a="http://schemas.xmlsoap.org/ws/2004/08/addressing"
  xmlns:e="http://www.w3.org/2001/04/xmlenc#"
  xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd"
  xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd"
  >
  <s:Header>
    <a:Action s:mustUnderstand="1" u:Id="_3">
```

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 18 July 2006

Marc A Goodner 7/18/06 4:22 PM
Inserted: 18 July 2006

```
      http://docs.oasis-open.org/ws-sx/ws-trust/200512/RSTRC/IssueFinal
    </a:Action>
    <a:RelatesTo u:Id="_4">
      urn:uuid:85836182-3ef8-4efc-a93f-06466277053e
    </a:RelatesTo>
    <a:To s:mustUnderstand="1" u:Id="_5">
      http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous
    </a:To>
    <o:Security s:mustUnderstand="1">
      <u:Timestamp u:Id="uuid-78c746a2-3ec4-4cf8-a913-50d2f7334cf9-34">
        <u:Created>2005-10-24T15:51:47.025Z</u:Created>
        <u:Expires>2005-10-24T15:56:47.025Z</u:Expires>
      </u:Timestamp>
      <e:EncryptedKey Id="_0" >
        <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-
oaep-mgf1p"/>
        <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
          <o:SecurityTokenReference>
            <o:KeyIdentifier
              ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wss-x509-token-profile-1.0#X509SubjectKeyIdentifier"
              EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-soap-message-security-1.0#Base64Binary">
              CuJdE1B2dUFd1dkLZSzQ5vj6MYg=
            </o:KeyIdentifier>
          </o:SecurityTokenReference>
        </KeyInfo>
        <e:CipherData>
          <e:CipherValue>

Mvb294ZmtQu7pA4YAyRxPYeEUFMB8ZDIDhsActVzF2kFacaVMHo2IlloBOC17CWDix1NI3qiA9wvt
FDsQzK2unaSULI+KzjEwAkIWma7eH/j2xKvhaRsQjxcF+A6VuEWA7fXoY1AZRt1cwACiVqKtdqSYF
EWvxxdTaHjVG2o80k=
          </e:CipherValue>
        </e:CipherData>
        <e:ReferenceList>
          <e:DataReference URI="#_2"/>
        </e:ReferenceList>
      </e:EncryptedKey>
      <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/2000/09/xmldsig#rsa-
sha1"/>
          <Reference URI="#_1">
```

```
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>o2h+mu3Hj7xU/6RHqDhb57oJpJU=</DigestValue>
          </Reference>
          <Reference URI="#_3">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>627rTKmQ6nuQSHGO+I5uyKXh2yY=</DigestValue>
          </Reference>
          <Reference URI="#_4">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>bt5N+ngBdN+BsJlowpaRrntL3X8=</DigestValue>
          </Reference>
          <Reference URI="#_5">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>VEzxbS+q/5Oj04P4Ywk/YZmQvxo=</DigestValue>
          </Reference>
          <Reference URI="#uuid-78c746a2-3ec4-4cf8-a913-50d2f7334cf9-34">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>oQ15WMehxnMzOSRUt4A/lOz8wHY=</DigestValue>
          </Reference>
        </SignedInfo>
        <SignatureValue>
```

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 18 July 2006

Marc A Goodner 7/18/06 4:22 PM
Inserted: 18 July 2006

```
f13OH+2aHcff0izaj+zc2NXue3mIgnM4W+cNT4TXPvNmOunWHWXij55YcPEjq8tXBQ2xSVkk0iii/
PUiXpZ/awiJbgTxe7EX0nJrNA81UYOCZsAkcA8La5lNzd3f6jZXFqZj6p2DwjKmHg7bPZDy+sn8Ri
yveevoPIVqSqTF2po=
        </SignatureValue>
        <KeyInfo>
          <o:SecurityTokenReference>
            <o:KeyIdentifier
              ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wss-x509-token-profile-1.0#X509SubjectKeyIdentifier"
              EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-soap-message-security-1.0#Base64Binary">
              Xeg55vRyK3ZhAEhEf+YT0z986L0=
            </o:KeyIdentifier>
          </o:SecurityTokenReference>
        </KeyInfo>
      </Signature>
    </o:Security>
  </s:Header>
  <s:Body u:Id="_1">
    <e:EncryptedData Id="_2" Type="http://www.w3.org/2001/04/xmlenc#Content">
      <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-
cbc"/>
      <e:CipherData>
        <e:CipherValue>
          <!--base64 encoded octets of encrypted RSTR-->
          <!--
   <t:RequestSecurityTokenResponseCollection>
     <t:RequestSecurityTokenResponse>
      <t:TokenType>http://docs.oasis-open.org/wss/oasis-wss-saml-token-
profile-1.1#SAMLV1.1</t:TokenType>
      <t:KeySize>256</t:KeySize>
      <t:RequestedAttachedReference>
        <o:SecurityTokenReference>
          <o:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/oasis-
wss-saml-token-profile-1.0#SAMLAssertionID">uuid-8222b7a2-3874-4884-bdb5-
9c2ddd4b86b5-16</o:KeyIdentifier>
        </o:SecurityTokenReference>
      </t:RequestedAttachedReference>
      <t:RequestedUnattachedReference>
        <o:SecurityTokenReference>
          <o:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/oasis-
wss-saml-token-profile-1.0#SAMLAssertionID">uuid-8222b7a2-3874-4884-bdb5-
9c2ddd4b86b5-16</o:KeyIdentifier>
        </o:SecurityTokenReference>
      </t:RequestedUnattachedReference>
```

```
      <t:Lifetime>
        <u:Created>2005-10-24T20:19:26.526Z</u:Created>
        <u:Expires>2005-10-25T06:24:26.526Z</u:Expires>
      </t:Lifetime>
      <t:RequestedSecurityToken>
        <saml:Assertion MajorVersion="1" MinorVersion="1" AssertionID="uuid-
8222b7a2-3874-4884-bdb5-9c2ddd4b86b5-16" Issuer="Test STS"
IssueInstant="2005-10-24T20:24:26.526Z"
xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion">
          <saml:Conditions NotBefore="2005-10-24T20:19:26.526Z"
NotOnOrAfter="2005-10-25T06:24:26.526Z">
          </saml:Conditions>
          <saml:Advice>
          </saml:Advice>
          <saml:AttributeStatement>
            <saml:Subject>
              <saml:SubjectConfirmation>

<saml:ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:holder-of-
key</saml:ConfirmationMethod>
                <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">
                    </e:EncryptionMethod>
                    <KeyInfo>
                      <o:SecurityTokenReference xmlns:o="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
                        <o:KeyIdentifier ValueType="http://docs.oasis-
open.org/wss/oasis-wss-wssecurity-secext-
1.1.xsd#ThumbprintSHA1">NQM0IBvuplAtETQvk+6gn8C13wE=</o:KeyIdentifier>
                      </o:SecurityTokenReference>
                    </KeyInfo>
                    <e:CipherData>

<e:CipherValue>EEcYjwNoYcJ+20xTYE5e/fixl5KOgzgrfaYAxkDFv/VXiuKfl084h8PmogTfM+
azcgAfmArVQvOyKWXRb5vmXYfVHLlhZTbXacy+nowSUNnEjp37VDbI3RJ5k6tBHF+ow0NM/P6GPNZ
9ZqJi11GDgWJkFsJzNZXNbbMgwuFu3cA=</e:CipherValue>
                    </e:CipherData>
                  </e:EncryptedKey>
                </KeyInfo>
              </saml:SubjectConfirmation>
            </saml:Subject>
          </saml:AttributeStatement>
          <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
            <SignedInfo>
```

Marc A Goodner 7/18/06 4:35 PM
Deleted: http://docs.oasis-open.org/wss/2005/xx/oasis-2005xx-wss-soap-message-security-1.1

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 18 July 2006

Marc A Goodner 7/18/06 4:22 PM
Inserted: 18 July 2006

```
              <CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
              </CanonicalizationMethod>
              <SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1">
              </SignatureMethod>
              <Reference URI="#uuid-8222b7a2-3874-4884-bdb5-9c2ddd4b86b5-16">
                <Transforms>
                  <Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature">
                  </Transform>
                  <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#">
                  </Transform>
                </Transforms>
                <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
                </DigestMethod>
                <DigestValue>7nHBrFPsm+LEFAoV4NoQPoEl5Lk=</DigestValue>
              </Reference>
            </SignedInfo>

<SignatureValue>TugV4pTIwCH87bLD4jiMgVGtkbRBt1tRlHXJArL34A/YfA4AnGBLXB4pJdUsU
xMUtbQl4PoGgEsdLNg8C77peARELGP1/Tqw7T3u5zBYHxCHCiV2FWBBfeOmwJmqoaBf8XZJ4AlyqP
q61P61jrQjZJafpHuYpAZnZQSvsiJaBPQ=</SignatureValue>
            <KeyInfo>
              <o:SecurityTokenReference xmlns:o="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
                <o:KeyIdentifier ValueType="http://docs.oasis-
open.org/wss/oasis-wss-wssecurity-secext-
1.1.xsd#ThumbprintSHA1">NQM0IBvuplAtETQvk+6gn8C13wE=</o:KeyIdentifier>
              </o:SecurityTokenReference>
            </KeyInfo>
          </Signature>
        </saml:Assertion>
      </t:RequestedSecurityToken>
      <t:RequestedProofToken>
        <t:BinarySecret u:Id="uuid-8222b7a2-3874-4884-bdb5-9c2ddd4b86b5-
14">zT8LWAUwUrIVKA/rkCr0kxlEmKAEhcB6TGWJuAgucBM=</t:BinarySecret>
      </t:RequestedProofToken>
    </t:RequestSecurityTokenResponse>
   </t:RequestSecurityTokenResponseCollection>
                  -->
        </e:CipherValue>
      </e:CipherData>
    </e:EncryptedData>
```

Marc A Goodner 7/18/06 4:35 PM
Deleted: http://docs.oasis-open.org/wss/2005/xx/oasis-2005xx-wss-soap-message-security-1.1

```
  </s:Body>
</s:Envelope>
```

3.5. Mutual Certificate, WSS1.1

This binding is used in Scenarios 5 and 6.

This mode requires WS-Security 1.1.

Client and STS X509 certificates are used to authenticate client and STS respectively. Client sends Request to STS signed using DKT1(K), then encrypted using a DKT2(K), K is ephemeral key protected for STS's Certificate, DKT1(K) and DKT2(K) represent keys derived from K per WS-SecureConversation. Signature corresponding to DKT1(K) is signed using Client's certificate. Response is signed using DKT3(K), encrypted using DKT4(K).

Expected Security Properties

Use of the service is restricted to authorized parties that can present a valid WSS 1.1 X.509 BinarySecurityToken.

Agreements

This section describes the agreements that must be made, directly or indirectly between parties who wish to interoperate beyond the common preconditions noted for all scenarios.

Acceptable <wsa:EndpointReference> Values

The requestor and the STS must agree on at least one <wsa:EndpointReference> value on receipt of which the STS can issue a SAML HoK assertion or SecureConversationToken.

Request Message

Message Creation

Security

The Security element MUST contain the mustUnderstand="1" attribute.

BinarySecurityToken

The security element MUST contain a BinarySecurityToken with a X.509 certificate that is encoded as Base64 sequence. The ValueType attribute MUST be set to #X509v3.

Body

RequestSecurityToken

TokenType

If present, the <t:TokenType> element value MUST be equal to http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0#SAMLV1.1 or http://docs.oasis-open.org/ws-sx/ws-secureconversation/200512/sct

RequestType

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 18 July 2006

Marc A Goodner 7/18/06 4:22 PM
Inserted: 18 July 2006

The <t:RequestType> element value MUST be equal to http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue

AppliesTo

If present. this element MUST include an <wsa:EndpointReference> element with a <wsa:Address> sub-element. The value of the <wsa:Address> element should be known to the STS.

KeyType

The <t:KeyType> element value MUST be equal to http://docs.oasis-open.org/ws-sx/wstrust/200512/SymmetricKey

Message Processing

This section describes the processing performed by the STS. It verifies that its local policy permits the issuance of a SAML HoK assertion or SCT for the value of the <wsa:EndpointReference> found in the message.

If an error is detected, the STS MUST cease processing the message and report the fault with a value of t:RequestFailed (other reasons for failure).

Example (Non-normative)

Here is an example request.

```
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope"
  xmlns:a="http://schemas.xmlsoap.org/ws/2004/08/addressing"
  xmlns:e="http://www.w3.org/2001/04/xmlenc#"
  xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
  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" u:Id="_3">
      http://docs.oasis-open.org/ws-sx/ws-trust/200512/RST/Issue
    </a:Action>
    <a:MessageID u:Id="_4">
      urn:uuid:04d386bf-f850-459e-918b-ad80f3d1e088
    </a:MessageID>
    <a:ReplyTo u:Id="_5">
      <a:Address>
        http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous
      </a:Address>
    </a:ReplyTo>
    <a:To s:mustUnderstand="1" u:Id="_6">
      http://server.example.com/STS/Scenarios5-6
    </a:To>
    <o:Security s:mustUnderstand="1">
      <u:Timestamp u:Id="uuid-40f5bac7-f9af-4384-80db-cfab34263849-10">
```

```
        <u:Created>2005-10-25T00:47:36.144Z</u:Created>
        <u:Expires>2005-10-25T00:52:36.144Z</u:Expires>
      </u:Timestamp>
      <e:EncryptedKey Id="uuid-40f5bac7-f9af-4384-80db-cfab34263849-9">
        <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-
oaep-mgf1p"/>
        <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
          <o:SecurityTokenReference>
            <o:KeyIdentifier
              ValueType="_http://docs.oasis-open.org/wss/oasis-wss-
wssecurity-secext-1.1.xsd#ThumbprintSHA1">
              NQM0IBvuplAtETQvk+6gn8C13wE=
            </o:KeyIdentifier>
          </o:SecurityTokenReference>
        </KeyInfo>
        <e:CipherData>
          <e:CipherValue>
            <!--base64 encoded cipher-->
          </e:CipherValue>
        </e:CipherData>
      <e:ReferenceList>
        <e:DataReference URI="#_2"/>
      </e:ReferenceList>      </e:EncryptedKey>
      <o:BinarySecurityToken u:Id="uuid-40f5bac7-f9af-4384-80db-cfab34263849-
6"
        ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
x509-token-profile-1.0#X509v3"
        EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wss-soap-message-security-1.0#Base64Binary">

MIIDDDCCAfSgAwIBAgIQM6YEf7FVYx/tZyEXgVComTANBgkqhkiG9w0BAQUFADAwMQ4wDAYDVQQKD
AVPQVNJUzEeMBwGA1UEAwwVT0FTSVMgSW50ZXJvcCBUZXN0IENBMB4XDTA1MDMxOTAwMDAwMFoXDT
E4MDMxOTIzNTk1OVowQjEOMAwGA1UECgwFT0FTSVMxIDAeBgNVBAsMF09BU0lTIEludGVyb3AgVGV
zdCBDZXJ0MQ4wDAYDVQQDDAVBbGljZTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAoqi99By1
VYo0aHrkKCNT4DkIgPL/SgahbeKdGhrbu3K2XG7arfD9tqIBIKMfrX4Gp90NJa85AV1yiNsEyvq+m
UnMpNcKnLXLOjkTmMCqDYbbkehJlXPnaWLzve+mW0pJdPxtf3rbD4PS/cBQIvtpjmrDAU8VsZKT8D
N5Kyz+EZsCAwEAAaOBkzCBkDAJBgNVHRMEAjAAMDMGA1UdHwQsMCowKKImhiRodHRwOi8vaW50ZXJ
vcC5iYnRlc3QubmV0L2NybC9jYS5jcmwwDgYDVR0PAQH/BAQDAgSwMB0GA1UdDgQWBBQK4l0TUHZ1
QV3V2QtlLNDm+PoxiDAfBgNVHSMEGDAWgBTAnSj8wes1oR3WqqqgHBpNwkkPDzANBgkqhkiG9w0BA
QUFAAOCAQEABTqpOpvW+6yrLXyUlP2xJbEkohXHI5OWwKWleOb9hlkhWntUalfcFOJAgUyH30TTpH
ldzx1+vK2LPzhoUFKYHE1IyQvokBN2JjFO64BQukCKnZhldLRPxGhfkTdxQgdf5rCK/wh3xVsZCNT
fuMNmlAM6lOAg8QduDah3WFZpEA0s2nwQaCNQTNMjJC8tav1CBr6+E5FAmwPXP7pJxn9Fw9OXRyqb
RA4v2y7YpbGkG2GI9UvOHw6SGvf4FRSthMMO35YbpikGsLix3vAsXWWi4rwfVOYzQK0OFPNi9RMCU
dSH06m9uLWckiCxjos0FQODZE9l4ATGy9s9hNVwryOJTw==
      </o:BinarySecurityToken>
      <Signature Id="_0" xmlns="http://www.w3.org/2000/09/xmldsig#">
        <SignedInfo>
```

Marc A Goodner 7/18/06 4:31 PM
Deleted: http://docs.oasis-open.org/wss/2005/xx/oasis-2005xx-wss-soap-message-security-1.1

Marc A Goodner 7/18/06 4:38 PM
Deleted:

Marc A Goodner 7/18/06 4:38 PM
Deleted: <e:ReferenceList> <e:DataReference URI="#_2"/> </e:ReferenceList>

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 18 July 2006

Marc A Goodner 7/18/06 4:22 PM
Inserted: 18 July 2006

```
          <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-
exc-c14n#"/>
          <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#hmac-
sha1"/>
          <Reference URI="#_1">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>VX1fCPwCzVsSc1hZf0BSbCgW2hM=</DigestValue>
          </Reference>
          <Reference URI="#_3">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>FwiFAUuqNDo9SDkk5A28Mg7Pa8Q=</DigestValue>
          </Reference>
          <Reference URI="#_4">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>oM59PsOTpmrDdOcwXYQzjVUl0xw=</DigestValue>
          </Reference>
          <Reference URI="#_5">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>KIK3vklFN1QmMdQkplq2azfzrzg=</DigestValue>
          </Reference>
          <Reference URI="#_6">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
```

```
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>RJEe3hrcyCD6PzFJo6fyut6biVg=</DigestValue>
          </Reference>
          <Reference URI="#uuid-40f5bac7-f9af-4384-80db-cfab34263849-10">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>zQdN5XpejfqXn0WKo0m51ZYiasE=</DigestValue>
          </Reference>
        </SignedInfo>
        <SignatureValue>iHGJ+xV2VZTjMlRc7AQJrwLY/aM=</SignatureValue>
        <KeyInfo>
          <o:SecurityTokenReference>
            <o:Reference
              ValueType="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-
secext-1.1.xsd#EncryptedKey"
              URI="#uuid-40f5bac7-f9af-4384-80db-cfab34263849-9"/>
          </o:SecurityTokenReference>
        </KeyInfo>
      </Signature>
      <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/2000/09/xmldsig#rsa-
sha1"/>
          <Reference URI="#_0">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>UZKtShk8q6iu9WR5uQZp04iAitg=</DigestValue>
          </Reference>
        </SignedInfo>
        <SignatureValue>

Ovxdeg4KQcfQlT/hEBJz+Z8dQUAfChaWIcmG3xGLZYcc8tbmCtZFuQz9tnW35Lmst6vIHFI23mg8U
3lRefuPA7ewRLYORAOjf92SxMbeVTlrIxQbIQNw0bs4SBSLfAo14=
        </SignatureValue>
        <KeyInfo>
```

Marc A Goodner 7/18/06 4:32 PM
Deleted: http://docs.oasis-open.org/wss/2005/xx/oasis-2005xx-wss-soap-message-security-1.1

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 18 July 2006

Marc A Goodner 7/18/06 4:22 PM
Inserted: 18 July 2006

```
          <o:SecurityTokenReference>
            <o:Reference
              ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wss-x509-token-profile-1.0#X509v3"
              URI="#uuid-40f5bac7-f9af-4384-80db-cfab34263849-6"/>
          </o:SecurityTokenReference>
        </KeyInfo>
      </Signature>
    </o:Security>
  </s:Header>
  <s:Body u:Id="_1">
    <e:EncryptedData Id="_2" Type="http://www.w3.org/2001/04/xmlenc#Content">
      <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-
cbc"/>
      <e:CipherData>
        <e:CipherValue>
          <!-- base64 encoded octets with encrypted RST request-->
          <!-- Unencrypted form:  -->
          <!--
    <t:RequestSecurityToken>
      <t:RequestType>
        http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue
      </t:RequestType>
      <t:Entropy>
        <t:BinarySecret u:Id="uuid-4acf589c-0076-4a83-8b66-5f29341514b7-3"
Type="http://docs.oasis-open.org/ws-sx/ws-
trust/200512/Nonce">Uv38QLxDQM9gLoDZ6OwYDiFk094nmwu3Wmay7EdKmhw=</t:BinarySec
ret>
      </t:Entropy>
      <t:KeyType>http://docs.oasis-open.org/ws-sx/ws-
trust/200512/SymmetricKey</t:KeyType>
      <t:KeySize>256</t:KeySize>
      <t:ComputedKeyAlgorithm>
        http://docs.oasis-open.org/ws-sx/ws-trust/200512/CK/PSHA1
      </t:ComputedKeyAlgorithm>
    </t:RequestSecurityToken>
                    -->
        </e:CipherValue>
      </e:CipherData>
    </e:EncryptedData>
  </s:Body>
```

</s:Envelope>

Policy

This policy statement must note that two derived keys are used, one for signing and one for encryption.
QUESTION: HOW TO STATE THIS IN POLICY. Policy same as previous for now.

Assuming signed then encrypted as in previous case, though not stated.

Frederick Hirsch 7/21/06 5:53 PM
Formatted: Font:Italic

```
<wsp:Policy>
<sp:SymmetricBinding>
    <wsp:Policy>
      <sp:ProtectionToken>
        <wsp:Policy>
          <sp:X509Token
            sp:IncludeToken='http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200512/IncludeToken/Never' />
            <wsp:Policy>
               <sp:WssX509V3Token11 />
          </wsp:Policy>
        </wsp:Policy>
      </sp:ProtectionToken>
      <sp:SignBeforeEncrypting />
      <sp:EncryptSignature />
    </wsp:Policy>
  </sp:SymmetricBinding>
</wsp:Policy>
```

Response Message

Message Creation

Body

RequestSecurityTokenResponseCollection/RequestSecurityTokenResponse

TokenType

The <t:TokenType> element value MUST be equal to http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0#SAMLV1.1 or http://docs.oasis-open.org/ws-sx/ws-secureconversation/200512/sct

AppliesTo

If present, the <wsp:AppliesTo> element contents MUST be identical to that found in the RST message.

Lifetime

A <t:Lifetime> element MUST be present.

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 18 July 2006

Marc A Goodner 7/18/06 4:22 PM
Inserted: 18 July 2006

RequestedSecurityToken

A SAML 1.1 Assertion or SecureConversationToken MUST be returned

Message Processing

The requestor must check to see if all elements noted as mandatory are present in the response. It must further verify that values for <t:TokenType> and <wsp:AppliesTo> are set as required above.

Example (Non-normative)

Here is an example response.

```
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope"
  xmlns:a="http://schemas.xmlsoap.org/ws/2004/08/addressing"
  xmlns:e="http://www.w3.org/2001/04/xmlenc#"
  xmlns:k="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-
1.1.xsd"
  xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd"
  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" u:Id="_4">
      http://docs.oasis-open.org/ws-sx/ws-trust/200512/RSTRC/IssueFinal
    </a:Action>
    <a:RelatesTo u:Id="_5">
      urn:uuid:04d386bf-f850-459e-918b-ad80f3d1e088
    </a:RelatesTo>
    <a:To s:mustUnderstand="1" u:Id="_6">
      http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous
    </a:To>
    <o:Security s:mustUnderstand="1">
      <u:Timestamp u:Id="uuid-0c947d47-f527-410a-a674-753a9d7d97f7-18">
        <u:Created>2005-10-25T00:47:38.718Z</u:Created>
        <u:Expires>2005-10-25T00:52:38.718Z</u:Expires>
      </u:Timestamp>
      <e:ReferenceList>
        <e:DataReference URI="#_3"/>
      </e:ReferenceList>
      <k:SignatureConfirmation u:Id="_0"
Value="iHGJ+xV2VZTjMlRc7AQJrwLY/aM="/>
      <k:SignatureConfirmation u:Id="_1"

Value="Ovxdeg4KQcfQlT/hEBJz+Z8dQUAfChaWIcmG3xGLZYcc8tbmCtZFuQz9tnW35Lmst6vRef
uPA7ewRLYORAOjf92SxMbeVTlrIxQx5Il71rcK+XBy+wm5Tl2D1qcTq+dMZW5oiom7J/1sibIQNw0
bs4SBSLfAo14="/>
      <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
```

Marc A Goodner 7/18/06 4:28 PM
Deleted: http://docs.oasis-open.org/wss/2005/xx/oasis-2005xx-wss-wssecurity-secext-1.1.xsd

```
        <SignedInfo>
          <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-
exc-c14n#"/>
          <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#hmac-
sha1"/>
          <Reference URI="#_2">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>kKx5bpLLlyucgXQ6exv/PbjsFlA=</DigestValue>
          </Reference>
          <Reference URI="#_4">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>LB+VGn4fP2z45jg0Mdzyo8yTAwQ=</DigestValue>
          </Reference>
          <Reference URI="#_5">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>izHLxm6V4Lc3PSs9Y6VRv3I5RPw=</DigestValue>
          </Reference>
          <Reference URI="#_6">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>6LS4X08vC/GMGay2vwmD8fL7J2U=</DigestValue>
          </Reference>
          <Reference URI="#uuid-0c947d47-f527-410a-a674-753a9d7d97f7-18">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
```

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 18 July 2006

Marc A Goodner 7/18/06 4:22 PM
Inserted: 18 July 2006

```
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>uXGSpCBfbT1fLNBLdGMgy6DGDio=</DigestValue>
          </Reference>
          <Reference URI="#_0">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>z86w+GrzqRZF56ciuz6ogzVXAUA=</DigestValue>
          </Reference>
          <Reference URI="#_1">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>Z9TfD20a5aGngsyOPEvQuE0urvQ=</DigestValue>
          </Reference>
        </SignedInfo>
        <SignatureValue>Q7HhboPUaZyXqUKgG7NCYlhMTXI=</SignatureValue>
        <KeyInfo>
          <o:SecurityTokenReference>
            <o:KeyIdentifier
              ValueType="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-
secext-1.1.xsd#EncryptedKeySHA1">
              CixQW5yEb3mw6XYqD8Ysvrf8cwI=
            </o:KeyIdentifier>
          </o:SecurityTokenReference>
        </KeyInfo>
      </Signature>
    </o:Security>
  </s:Header>
  <s:Body u:Id="_2">
    <e:EncryptedData Id="_3" Type="http://www.w3.org/2001/04/xmlenc#Content">
      <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-
cbc"/>
      <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
        <o:SecurityTokenReference>
          <o:KeyIdentifier
            ValueType="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-
secext-1.1.xsd#EncryptedKeySHA1">
            CixQW5yEb3mw6XYqD8Ysvrf8cwI=
```

Marc A Goodner 7/18/06 4:32 PM
Deleted: http://docs.oasis-open.org/wss/2005/xx/oasis-2005xx-wss-soap-message-security-1.1

Marc A Goodner 7/18/06 4:32 PM
Deleted: http://docs.oasis-open.org/wss/2005/xx/oasis-2005xx-wss-soap-message-security-1.1

```
          </o:KeyIdentifier>
        </o:SecurityTokenReference>
      </KeyInfo>
      <e:CipherData>
        <e:CipherValue>
          <!--base64 encoded octets of encrypted RSTR-->
          <!--
   <t:RequestSecurityTokenResponseCollection>
    <t:RequestSecurityTokenResponse>
      <t:TokenType>http://docs.oasis-open.org/wss/oasis-wss-saml-token-
profile-1.1#SAMLV1.1</t:TokenType>
      <t:KeySize>256</t:KeySize>
      <t:RequestedAttachedReference>
        <o:SecurityTokenReference>
          <o:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/oasis-
wss-saml-token-profile-1.0#SAMLAssertionID">uuid-8222b7a2-3874-4884-bdb5-
9c2ddd4b86b5-16</o:KeyIdentifier>
        </o:SecurityTokenReference>
      </t:RequestedAttachedReference>
      <t:RequestedUnattachedReference>
        <o:SecurityTokenReference>
          <o:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/oasis-
wss-saml-token-profile-1.0#SAMLAssertionID">uuid-8222b7a2-3874-4884-bdb5-
9c2ddd4b86b5-16</o:KeyIdentifier>
        </o:SecurityTokenReference>
      </t:RequestedUnattachedReference>
      <t:Lifetime>
        <u:Created>2005-10-24T20:19:26.526Z</u:Created>
        <u:Expires>2005-10-25T06:24:26.526Z</u:Expires>
      </t:Lifetime>
      <t:RequestedSecurityToken>
        <saml:Assertion MajorVersion="1" MinorVersion="1" AssertionID="uuid-
8222b7a2-3874-4884-bdb5-9c2ddd4b86b5-16" Issuer="Test STS"
IssueInstant="2005-10-24T20:24:26.526Z"
xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion">
          <saml:Conditions NotBefore="2005-10-24T20:19:26.526Z"
NotOnOrAfter="2005-10-25T06:24:26.526Z">
          </saml:Conditions>
          <saml:Advice>
          </saml:Advice>
          <saml:AttributeStatement>
            <saml:Subject>
              <saml:SubjectConfirmation>

<saml:ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:holder-of-
key</saml:ConfirmationMethod>
```

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 18 July 2006

Marc A Goodner 7/18/06 4:22 PM
Inserted: 18 July 2006

```
                <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">
                    </e:EncryptionMethod>
                    <KeyInfo>
                      <o:SecurityTokenReference xmlns:o="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
                        <o:KeyIdentifier ValueType="http://docs.oasis-
open.org/wss/oasis-wss-wssecurity-secext-
1.1.xsd#ThumbprintSHA1">NQM0IBvuplAtETQvk+6gn8C13wE=</o:KeyIdentifier>
                      </o:SecurityTokenReference>
                    </KeyInfo>
                    <e:CipherData>

<e:CipherValue>EEcYjwNoYcJ+20xTYE5e/fixl5KOgzgrfaYAxkDFv/VXiuKfl084h8PmogTfM+
azcgAfmArVQvOyKWXRb5vmXYfVHLlhZTbXacy+nowSUNnEjp37VDbI3RJ5k6tBHF+ow0NM/P6GPNZ
9ZqJi11GDgWJkFsJzNZXNbbMgwuFu3cA=</e:CipherValue>
                    </e:CipherData>
                  </e:EncryptedKey>
                </KeyInfo>
              </saml:SubjectConfirmation>
            </saml:Subject>
          </saml:AttributeStatement>
          <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
            <SignedInfo>
              <CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
              </CanonicalizationMethod>
              <SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1">
              </SignatureMethod>
              <Reference URI="#uuid-8222b7a2-3874-4884-bdb5-9c2ddd4b86b5-16">
                <Transforms>
                  <Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature">
                  </Transform>
                  <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#">
                  </Transform>
                </Transforms>
                <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
                </DigestMethod>
                <DigestValue>7nHBrFPsm+LEFAoV4NoQPoEl5Lk=</DigestValue>
              </Reference>
```

Marc A Goodner 7/18/06 4:36 PM
Deleted: http://docs.oasis-open.org/wss/2005/xx/oasis-2005xx-wss-soap-message-security-1.1

```
            </SignedInfo>

<SignatureValue>TugV4pTIwCH87bLD4jiMgVGtkbRBt1tRlHXJArL34A/YfA4AnGBLXB4pJdUsU
xMUtbQl4PoGgEsdLNg8C77peARELGP1/Tqw7T3u5zBYHxCHCiV2FWBBfeOmwJmqoaBf8XZJ4AlyqP
q61P61jrQjZJafpHuYpAZnZQSvsiJaBPQ=</SignatureValue>
            <KeyInfo>
              <o:SecurityTokenReference xmlns:o="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
                <o:KeyIdentifier ValueType="http://docs.oasis-
open.org/wss/oasis-wss-wssecurity-secext-
1.1.xsd#ThumbprintSHA1">NQM0IBvuplAtETQvk+6gn8C13wE=</o:KeyIdentifier>
              </o:SecurityTokenReference>
            </KeyInfo>
          </Signature>
        </saml:Assertion>
      </t:RequestedSecurityToken>
      <t:RequestedProofToken>
        <t:BinarySecret u:Id="uuid-8222b7a2-3874-4884-bdb5-9c2ddd4b86b5-
14">zT8LWAUwUrIVKA/rkCr0kxlEmKAEhcB6TGWJuAgucBM=</t:BinarySecret>
      </t:RequestedProofToken>
    </t:RequestSecurityTokenResponse>
   </t:RequestSecurityTokenResponseCollection>
                  -->
        </e:CipherValue>
      </e:CipherData>
    </e:EncryptedData>
  </s:Body>
</s:Envelope>
```

Marc A Goodner 7/18/06 4:33 PM
Deleted: http://docs.oasis-open.org/wss/2005/xx/oasis-2005xx-wss-soap-message-security-1.1

3.6. Delegated SAML 2.0 with Certificate for SAML 2.0 HoK, WSS 1.1

This binding is used in Scenario 7.

This mode requires WS-Security 1.1.

The requestor sends the STS a message over HTTP requesting issuance of a SAML token. The RST message includes a WSS 1.1 X.509 BinarySecurityToken in the SOAP security header.

The <t:OnBehalfOf> element includes a SAML 2.0 assertion describing the user. The <t:DelegateTo> element includes an STR describing the entity which will use the SAML assertion.The STS responds with a RSTR message with a SAML 2.0 holder of key assertion.

NOTE: In most use-cases, there may be an authentication or proof step associated with the certificate provided in the header. This may take the form of a digital signature or a SSL handshake. This step is omitted in this scenario.

The <SubjectConfirmation>/<ds:KeyInfo> element in the SAML assertion includes the issuer and serial number of the requestors X.509 certificate. The <SubjectConfirmation>/<NameId> element has value equal to the SubjectDN of the requestors certificate and has format attribute set to urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName. The <NameId> element is used to

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 18 July 2006

Marc A Goodner 7/18/06 4:22 PM
Inserted: 18 July 2006

signal delegated use in SAML 2.0. The Method attribute of the <SubjectConfirmation> element is set to urn:oasis:names:tc:SAML:2.0:cm:holder-of-key.

The SAML assertion is signed by the STS. The certificate used to sign the SAML token is included in the <ds:KeyInfo> element of the assertion.

Frederick Hirsch 7/21/06 4:41 PM
Deleted: keyinfo

Expected Security Properties

Agreements

This section describes the agreements that must be made, directly or indirectly between parties who wish to interoperate beyond the common preconditions noted for all scenarios.

Acceptable <wsa:EndpointReference> Values

The requestor and the STS must agree on at least one <wsa:EndpointReference> value on receipt of which the STS can issue a delegated SAML HoK assertion.

Request Message

Message Creation

Security

The Security element MUST contain the mustUnderstand="1" attribute.

BinarySecurityToken

The security element MUST contain a BinarySecurityToken with a X.509 certificate that is encoded as Base64 sequence. The ValueType attribute MUST be set to #X509v3.

Body

TokenType

The <t:TokenType> element value MUST be equal to http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0#SAMLV1.1

RequestType

The <t:RequestType> element value MUST be equal to http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue

AppliesTo

This element MUST include an <wsa:EndpointReference> element with a <wsa:Address> sub-element. The value of the <wsa:Address> element should be known to the STS.

KeyType

The <t:KeyType> element value MUST be equal to http://docs.oasis-open.org/ws-sx/wstrust/200512/PublicKey

OnBehalfOf

The <t:OnBehalfOf> element MUST include a SAML 2.0 bearer assertion.

DelegateTO

The <t:DelegateTo> element MUST include a STR direct reference to X.509 certificate found in the SOAP security header.

Message Processing

This section describes the processing performed by the STS. It verifies that its local policy permits the issuance of a SAML HoK assertion for the value of the <wsa:EndpointReference> found in the message.

The value of the <SubjectConfirmation>/<ds:KeyInfo> element in the SAML assertion is a <ds:X.509Data> element with a <ds:X509Certificate> sub-element. The base-64 certificate value is taken from the security header of the request message. The <SubjectConfirmation>/<NameId> element has value equal to the SubjectDN of the X.509 certificate and has format attribute set to urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName. The <SubjectConfirmation>/<ConfirmationMethod> element is set to urn:oasis:names:tc:SAML:1.0:cm:holder-of-key.

If an error is detected, the STS MUST cease processing the message and report the fault with a value of t:RequestFailed (other reasons for failure).

Example (Non-normative)

Here is an example request.

```
<?xml version="1.0" encoding="utf-8" ?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd=”http://www.w3.org/2001/XMLSchema”
xmlns:wsse=”http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd”
xmlns:wst=”http://docs.oasis-open.org/ws-sx/ws-trust/200512”
>

 <soap:Header>
  <wsse:Security soap:mustUnderstand=“1”>
          <wsse:BinarySecurityToken
                    wsu:Id="binarytoken"
                    ValueType="…#X509v3"
                    EncodingType="…#Base64Binary">
                          MIIEZzCCA9CgAwIBAgIQEmtJZc0…
          </wsse:BinarySecurityToken>
  </wsse:Security>
 </soap:Header>
 <soap:Body>
<t:RequestSecurityToken>
    <t:TokenType>
```

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 18 July 2006

Marc A Goodner 7/18/06 4:22 PM
Inserted: 18 July 2006

```
        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
    </t:RequestType>
    <wsp:AppliesTo
xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/03/addressing">
            <wsa:EndpointReference>
               <wsa:Address>http://www.example.org/</wsa:Address>
            </wsa:EndpointReference>
    </wsp:Appliesto>
    <t:KeyType>
         http://docs.oasis-open.org/ws-sx/wstrust/200512/PublicKey
     </t:KeyType>
     <t:OnBehalfOf>

                          <saml:Assertion ID="_a75adf55-01d7-40cc-929f-
dbd8372ebdfc"
                                  IssueInstant="2003-04-17T00:46:02Z"
Version="2.0"

Xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
                 <saml:Issuer>https://www.opensaml.org/IDP</Issuer>
                 <saml:Subject>
                 <saml:NameID
                 Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:emailAddress">
                   scott@example.org
                </saml:NameID>
                <saml:SubjectConfirmation
                     Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"/>
                  </saml:Subject>
             <saml:Conditions NotBefore="2003-04-17T00:46:02Z"
             NotOnOrAfter="2003-04-17T00:51:02Z">
              </saml:Conditions>
            </saml:Assertion>
     </t:OnBehalfOf>
     <t:DelegateTo>
               <wsse:SecurityTokenReference wsu:Id="...">
                    <wsse:Reference URI="#binarytoken"/>
                </wsse:SecurityTokenReference>
     </t:DelegateTo>
</t:RequestSecurityToken>
</soap:Body>
</soap:Envelope>
```

Policy

Same as 3.5 but require WSS 1.1.

Frederick Hirsch 7/21/06 6:20 PM
Comment: or does this case have additional requirements?

```
<wsp:Policy>
 <sp:SymmetricBinding>
    <wsp:Policy>
      <sp:ProtectionToken>
        <wsp:Policy>
          <sp:X509Token
            sp:IncludeToken='http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200512/IncludeToken/Never' />
            <wsp:Policy>
               <sp:WssX509V3Token11 />
          </wsp:Policy>
        </wsp:Policy>
      </sp:ProtectionToken>
      <sp:SignBeforeEncrypting />
      <sp:EncryptSignature />
    </wsp:Policy>
 </sp:SymmetricBinding>
 <sp:wss11 />
</wsp:Policy>
```

Response Message

Message Creation

Body

RequestSecurityTokenResponseCollection/RequestSecurityTokenResponse

TokenType

The <t:TokenType> element value MUST be equal to http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0#SAMLV1.1

AppliesTo

The <wsp:AppliesTo> element contents MUST be identical to that found in the RST message.

Lifetime

A <t:Lifetime> element MUST be present and include a <wsu:Created> and <wsu:Expires> sub-element

RequestedSecurityToken

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 18 July 2006

Marc A Goodner 7/18/06 4:22 PM
Inserted: 18 July 2006

Assertion

A SAML 2.0 Assertion MUST be returned; the assertion MUST contain a statement with <saml:ConfirmationMethod> set to urn:oasis:names:tc:SAML:1.0:cm: holder-of-key. The value of the <SubjectConfirmation>/<ds:KeyInfo> element in the SAML assertion MUST be a <ds:X.509Data> element with a <ds:X509Certificate> sub-element. The base-64 certificate value is taken from the BinarySecurityToken element in the request message. The <SubjectConfirmation>/<NameId> element MUST have value equal to the SubjectDN of the X.509 certificate and has format attribute set to urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName. The assertion MUST be signed and include a <ds:Signature> element as part of an enveloped signature.

Message Processing

The requestor must check to see if all elements noted as mandatory are present in the response. It must further verify that values for <t:TokenType> and <wsp:AppliesTo> are set as required above.

Typically, requestors will not process the contents of the SAML assertion; instead, the assertion is used to secure an exchange with a recipient. However, it is suggested that requestors check the value of the <saml:ConfirmationMethod> and also ensure that the assertion contains an enveloped signature.

Example (Non-normative)

Here is an example response.

```
<?xml version="1.0" encoding="utf-8" ?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
xmlns:wst="http://docs.oasis-open.org/ws-sx/ws-trust/200512"
 xmlns:xsd="http://www.w3.org/2001/XMLSchema">
 <soap:Header>
 </soap:Header>
 <soap:Body wsu:Id="body"
xmlns:wsu="http://schemas.xmlsoap.org/ws/2003/06/utility">
      <t:RequestSecurityTokenResponse>
         <t:TokenType>
        http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0
         </t:TokenType>
        <wsp:AppliesTo
xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/03/addressing">
            <wsa:EndpointReference>
               <wsa:Address>http://www.example.org/</wsa:Address>
            </wsa:EndpointReference>
        <wsp:AppliesTo>
       <t:Lifetime>
         <wsu:Created>"2005-04-17T00:46:02Z"</wsu:Created>
         <wsu:Expires>"2005-04-17T00:51:02Z"</wsu:Expires>
        </t:Lifetime>

       <t:RequestedSecurityToken>
             <saml:Assertion ID="_xw5adf55-01d7-40cc-ayp2-dbd8372ebdfc"
                 IssueInstant="2005-04-17T00:46:02Z" Version="2.0"
                 xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
```

```
                <saml:Issuer>https://www.example.org/STS</Issuer>
<ds:Signature
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
<ds:SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<ds:Reference
URI="#_a75adf55-01d7-40cc-929f-dbd8372ebdfc">
<ds:Transforms>
<ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
<ds:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
<InclusiveNamespaces
PrefixList="#default saml samlp ds xsd xsi"
xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"/>
</ds:Transform>
</ds:Transforms>
<ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<ds:DigestValue>Kclet6XcaOgOWXM4gty6/UNdviI=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>
hq4zk+ZknjggCQgZm7ea8fI79gJEsRy3E8LHDpYXWQIgZpkJN9CMLG8ENR4Nrw+n
7iyzixBvKXX8P53BTCT4VghPBWhFYSt9tHWu/AtJfOTh6qaAsNdeCyG86jmtp3TD
MWuL/cBUj2OtBZOQMFn7jQ9YB7klIz3RqVL+wNmeWI4=</ds:SignatureValue>
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate>
MIICyjCCAjOgAwIBAgICAnUwDQYJKoZIhvcNAQEEBQAwgakxCzAJBgNVBAYTAlVT
MRIwEAYDVQQIEwlXaXNjb25zaW4xEDAOBgNVBAcTB01hZGlzb24xIDAeBgNVBAoT
F1VuaXZlcnNpdHkgb2YgV2lzY29uc2luMSswKQYDVQQLEyJEaXZpc2lvbiBvZiBJ
bmZvcm1hdGlvbiBUZWNobm9sb2d5MSUwIwYDVQQDExxIRVBLSSBTZXJ2ZXIgQ0Eg
LS0gMjAwMjA3MDFBMB4XDTAyMDcyNjA3Mjc1MVoXDTA2MDkwNDA3Mjc1MVowgYsx
CzAJBgNVBAYTAlVTMREwDwYDVQQIEwhNaWNoaWdhbjESMBAGA1UEBxMJQW5uIEFy
Ym9yMQ4wDAYDVQQKEwVVQ0FJRDEcMBoGA1UEAxMTc2hpYjEuaW50ZXJuZXQyLmVk
dTEnMCUGCSqGSIb3DQEJARYYcm9vdEBzaGliMS5pbnRlcm5ldDIuZWR1MIGfMA0G
CSqGSIb3DQEBAQUAA4GNADCBiQKBgQDZSAb2sxvhAXnXVIVTx8vuRay+x50z7GJj
IHRYQgIv6IqaGG04eTcyVMhoekE0b45QgvBIaOAPSZBl13R6+KYiE7x4XAWIrCP+
c2MZVeXeTgV3Yz+USLg2Y1on+Jh4HxwkPFmZBctyXiUr6DxF8rvoP9W7O27rhRjE
pmqOIfGTWQIDAQABox0wGzAMBgNVHRMBAf8EAjAAMAsGA1UdDwQEAwIFoDANBgkq
```

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 18 July 2006

Marc A Goodner 7/18/06 4:22 PM
Inserted: 18 July 2006

```
hkiG9w0BAQQFAAOBgQBfDqEW+OI3jqBQHIBzhujN/PizdN7s/z4D5d3pptWDJf2n
qgi7lFV6MDkhmTvTqBtjmNk3No7v/dnP6Hr7wHxvCCRwubnmIfZ6QZAv2FU78pLX
8I3bsbmRAUg4UP9hH6ABVq4KQKMknxu1xQxLhpR1ylGPdiowMNTrEG8cCx3w/w==
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</ds:signature>
</ds:Signature>
        <saml:Subject>
            <saml:NameID
             Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:emailAddress">
                joes@example.org
            </saml:NameID>
             <saml:SubjectConfirmation
                        Method="urn:oasis:names:tc:SAML:2.0:cm: holder-of-
key">

              <saml:NameId Format=" urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName"
                                  C=US, S=WA, L=Woodinville, O=Contoso,
CN=FinanceServer
               </saml:NameId>
              <ds:KeyInfo>
              <ds:KeyValue>
                <ds:X509Data><ds:X509Certificate>
MIIEZzCCA9CgAwIBAgIQEmtJZc0…
                     <ds:X509Certificate>
                <ds:X509Data>
             </ds:KeyValue>
             </ds:KeyInfo>
             </saml:SubjectConfirmation>
            <saml:Conditions NotBefore="2005-04-17T00:46:02Z"
                      NotOnOrAfter="2005-04-17T00:51:02Z">
            </saml:Conditions>
            <saml:AttributeStatement>
            <saml:Attribute
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
               Name="Division"
        <saml:AttributeValue
xsi:type="xs:string">Development</AttributeValue>
       </saml:Attribute>
       </saml:AttributeStatement>
     </saml:Assertion>
     </t:RequestedSecurityToken>
     </t:SecurityTokenResponse>
 </soap:Body>
</soap:Envelope>
```

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 18 July 2006

Marc A Goodner 7/18/06 4:22 PM
Inserted: 18 July 2006

4. Client and Service Security Bindings

Frederick Hirsch 7/21/06 4:21 PM
Formatted: Bullets and Numbering

Each scenario defined above will use one of the following security bindings for message exchanges between the Client and Service.

4.1. Issued SAML 1.1 Token over Transport

This binding is used in Scenario 1.

SAML HoK token issued to the Client by the STS is used to authenticate the Client. The Service's X509 certificate is used to authenticate the Service. Secure transport (HTTPS) is used to protect messages.

Request Message

Example (Non-normative)

Here is an example request.

```
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope"
  xmlns:a="http://schemas.xmlsoap.org/ws/2004/08/addressing"
  xmlns:d="http://www.w3.org/2000/09/xmldsig#"
  xmlns:e="http://www.w3.org/2001/04/xmlenc#"
  xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd"
  xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
  xmlns:sc="http://docs.oasis-open.org/ws-sx/ws-secureconversation/200512"
  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" u:Id="_4">
      http://example.org/Ping
    </a:Action>
    <a:MessageID u:Id="_5">
      urn:uuid:b6345ac8-dfc4-4174-a985-2f69cf4ac54e
    </a:MessageID>
    <a:ReplyTo u:Id="_6">
      <a:Address>
        http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous
      </a:Address>
    </a:ReplyTo>
    <a:To s:mustUnderstand="1" u:Id="_7">
      http://server.example.com/Ping/Scenario1
    </a:To>
    <o:Security s:mustUnderstand="1">
      <u:Timestamp u:Id="uuid-c3cdb38b-e4aa-4467-9d0e-dd30f081e08d-10">
        <u:Created>2005-10-24T15:51:46.791Z</u:Created>
        <u:Expires>2005-10-24T15:56:46.791Z</u:Expires>
      </u:Timestamp>
      <saml:Assertion MajorVersion="1" MinorVersion="1"
        AssertionID="uuid-78c746a2-3ec4-4cf8-a913-50d2f7334cf9-32"
        Issuer="Test STS"
        IssueInstant="2005-10-24T15:51:47.025Z">
        <saml:Conditions NotBefore="2005-10-24T15:46:47.025Z"
NotOnOrAfter="2005-10-25T01:51:47.025Z"/>
```

```
        <saml:Advice/>
        <saml:AttributeStatement>
          <saml:Subject>
            <saml:SubjectConfirmation>
              <saml:ConfirmationMethod>
                urn:oasis:names:tc:SAML:1.0:cm:holder-of-key
              </saml:ConfirmationMethod>
              <d:KeyInfo>
                <e:EncryptedKey>
                  <e:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p"/>
                  <d:KeyInfo>
                    <o:SecurityTokenReference>
                      <o:KeyIdentifier
                        ValueType="http://docs.oasis-open.org/wss/oasis-wss-
wssecurity-secext-1.1.xsd#ThumbprintSHA1">
                        NQM0IBvuplAtETQvk+6gn8C13wE=
                      </o:KeyIdentifier>
                    </o:SecurityTokenReference>
                  </d:KeyInfo>
                  <e:CipherData>
                    <e:CipherValue>
cb7+JW2idPNSarK9quqCe9PQwmW2hoUghuyKRe+I9zOts6HaMcg73LqCWuK/jtdpvNl6GT/ZDYfcA
J7NLyMGxSiwi4DUlTOShqS6OTYBIKgUKiA+zXNl2koVSy7amcUhPMIT6/fohH+6MZDA4t6jomcyhl
CiW8d9IAzSWFkfg2k=
                    </e:CipherValue>
                  </e:CipherData>
                </e:EncryptedKey>
              </d:KeyInfo>
            </saml:SubjectConfirmation>
          </saml:Subject>
        </saml:AttributeStatement>
        <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/2000/09/xmldsig#rsa-sha1"/>
            <Reference URI="#uuid-78c746a2-3ec4-4cf8-a913-50d2f7334cf9-32">
              <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/2000/09/xmldsig#sha1"/>
              <DigestValue>WubDx7buehNvSvpCoGr/3tKmcyg=</DigestValue>
            </Reference>
          </SignedInfo>
          <SignatureValue>
Cag6FeoBeoHrRpv9h8Evx58rXp6G5vKOK4BgMnJiq/wUp2sQyOjeCVnij/g+gbIi+2ZGa75zhMykv
+9O/jXhlYtRNrNGFTWhEznsU0olKBoezJ/FHhDNytVUeDHiTChf/kwP8COZ4atCDtaQUN3ZXLaxbp
FBYewpoh+OABMTBlo=
          </SignatureValue>
```

Marc A Goodner 7/18/06 4:33 PM
Deleted: http://docs.oasis-open.org/wss/2005/xx/oasis-2005xx-wss-soap-message-security-1.1

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 18 July 2006

Marc A Goodner 7/18/06 4:22 PM
Inserted: 18 July 2006

```
          <KeyInfo>
            <o:SecurityTokenReference>
              <o:KeyIdentifier ValueType="http://docs.oasis-
open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd#ThumbprintSHA1">
                NQM0IBvuplAtETQvk+6gn8C13wE=
              </o:KeyIdentifier>
            </o:SecurityTokenReference>
          </KeyInfo>
        </Signature>
      </saml:Assertion>
      <sc:DerivedKeyToken u:Id="_0">
        <o:SecurityTokenReference>
          <o:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/oasis-
wss-saml-token-profile-1.0#SAMLAssertionID">
            uuid-78c746a2-3ec4-4cf8-a913-50d2f7334cf9-32
          </o:KeyIdentifier>
        </o:SecurityTokenReference>
        <sc:Offset>
          0
        </sc:Offset>
        <sc:Length>
          24
        </sc:Length>
        <sc:Nonce>
          flvBVmEJTyhdYLlf8qDxBg==
        </sc:Nonce>
      </sc:DerivedKeyToken>
      <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/2000/09/xmldsig#hmac-
sha1"/>
          <Reference URI="#uuid-c3cdb38b-e4aa-4467-9d0e-dd30f081e08d-10">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>Tj0yGTMhbgonlFR9JUsLZpZ2TQY=</DigestValue>
          </Reference>
        </SignedInfo>
        <SignatureValue>DYf5TKftfZSzjz7x8+srho1Z3nU=</SignatureValue>
        <KeyInfo>
          <o:SecurityTokenReference>
            <o:Reference URI="#_0"/>
          </o:SecurityTokenReference>
        </KeyInfo>
      </Signature>
    </o:Security>
  </s:Header>
  <s:Body>
    <Ping xmlns="http://example.org/Ping">Ping</Ping>
```

Marc A Goodner 7/18/06 4:33 PM
Deleted: http://docs.oasis-open.org/wss/2005/xx/oasis-2005xx-wss-soap-message-security-1.1

```
  </s:Body>
</s:Envelope>
```

Service Policy

This is the service policy.

```
<wsp:Policy>
  <sp:TransportBinding />
  <sp:SamlToken sp:IncludeToken='http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200512/IncludeToken/Always' >
    <wsp:Policy>
      <sp:WssSamlV11Token11 />
    </wsp:Policy>
  </sp:SamlToken>
</wsp:Policy>
```

Frederick Hirsch 7/21/06 6:20 PM
Comment: Did I get the version of the SAML Token Profile correct? Where/how do I state holder of key requirement, does this mean an issue for SP?

Frederick Hirsch 7/21/06 6:08 PM
Formatted: Body Text

Response Message

Example (Non-normative)

Here is an example response.

```
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope"
  xmlns:a="http://schemas.xmlsoap.org/ws/2004/08/addressing"
  xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd"
  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" u:Id="_4">
          http://example.org/PingResponse
        </a:Action>
        <a:MessageID u:Id="_5">
          urn:uuid:b6345ac8-dfc4-4174-a985-2f69cf4ac54e
        </a:MessageID>
        <a:RelatesTo u:Id="_6">
            urn:uuid:b6345ac8-dfc4-4174-a985-2f69cf4ac54e
        </a:RelatesTo>
        <a:To s:mustUnderstand="1" u:Id="_7">
          http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous
        </a:To>
        <o:Security s:mustUnderstand="1">
            <u:Timestamp u:Id="uuid-c3cdb38b-e4aa-4467-9d0e-dd30f081e08d-10">
                <u:Created>2005-10-24T15:51:46.791Z</u:Created>
                <u:Expires>2005-10-24T15:56:46.791Z</u:Expires>
            </u:Timestamp>
        </o:Security>
    </s:Header>
    <s:Body>
        <PingResponse xmlns="http://example.org/Ping">Ping</PingResponse>
    </s:Body>
</s:Envelope>
```

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 18 July 2006

Marc A Goodner 7/18/06 4:22 PM
Inserted: 18 July 2006

4.2. Issued SAML 1.1 Token for Certificate, WSS 1.0

This binding is used in Scenarios 2, 3 and 4.

SAML token issued to the Client by STS is used to authenticate the Client. Messages are signed then encrypted using symmetric keys derived from the symmetric proof-of-possession key Sx associated with the SAML token.

Service Policy

This is the service policy.

```
<wsp:Policy>
  <sp:SymmetricBinding>
    <wsp:Policy>
      <sp:ProtectionToken>
        <wsp:Policy>
          <sp:SamlToken sp:IncludeToken='http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200512/IncludeToken/Always' >
            <wsp:Policy>
              <sp:WssSamlV11Token11 />
            </wsp:Policy>
          </sp:SamlToken>
        </wsp:Policy>
      </sp:ProtectionToken>
      <sp:SignBeforeEncrypting />
      <sp:EncryptSignature />
    </wsp:Policy>
  </sp:SymmetricBinding>
</wsp:Policy>
```

Request Message

Example (Non-normative)

Here is an example request.

```
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope"
  xmlns:a="http://schemas.xmlsoap.org/ws/2004/08/addressing"
  xmlns:e="http://www.w3.org/2001/04/xmlenc#"
  xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
  xmlns:sc="http://docs.oasis-open.org/ws-sx/ws-secureconversation/200512"
  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" u:Id="_4">
      http://example.org/Ping
    </a:Action>
```

```
    <a:MessageID u:Id="_5">
      urn:uuid:b6345ac8-dfc4-4174-a985-2f69cf4ac54e
    </a:MessageID>
    <a:ReplyTo u:Id="_6">
      <a:Address>
        http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous
      </a:Address>
    </a:ReplyTo>
    <a:To s:mustUnderstand="1" u:Id="_7">
      http://server.example.com/Ping/Scenario2-3-4
    </a:To>
    <o:Security s:mustUnderstand="1" >
      <u:Timestamp u:Id="uuid-c3cdb38b-e4aa-4467-9d0e-dd30f081e08d-10">
        <u:Created>2005-10-24T15:51:46.791Z</u:Created>
        <u:Expires>2005-10-24T15:56:46.791Z</u:Expires>
      </u:Timestamp>
      <e:EncryptedData Id="_3">
        <e:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>
        <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
          <!-- encrypted Key K-->
          <e:EncryptedKey>
            <e:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p"/>
            <KeyInfo>
              <o:SecurityTokenReference>
                <o:KeyIdentifier
                  ValueType="http://docs.oasis-open.org/wss/oasis-wss-
wssecurity-secext-1.1.xsd#ThumbprintSHA1">
                  NQM0IBvuplAtETQvk+6gn8C13wE=
                </o:KeyIdentifier>
              </o:SecurityTokenReference>
            </KeyInfo>
            <e:CipherData>
              <e:CipherValue>
cb7+JW2idPNSarK9quqCe9PQwmW2hoUghuyKRe+I9zOts6HaMcg73LqCWuK/jtdpvNl6GT/ZDYfcA
J7NLyMGxSiwi4DUlTOShqS6OTYBIKgUKiA+zXNl2koVSy7amcUhPMIT6/fohH+6MZDA4t6jomcyhl
CiW8d9IAzSWFkfg2k=
              </e:CipherValue>
            </e:CipherData>
          </e:EncryptedKey>
        </KeyInfo>
        <e:CipherData>
          <e:CipherValue>
RDolD6Fl/Oewj36sjiinWLKObqsMneMhkt0toCmH6YxyszC0/M+q3CMDfwmOd0AoEeudo0NpMyjki
YG9KylkWoPeTfPL+K52j2J6enttCQ8=
          </e:CipherValue>
        </e:CipherData>
      </e:EncryptedData>
      <sc:DerivedKeyToken u:Id="_0">
        <o:SecurityTokenReference>
          <o:KeyIdentifier
            ValueType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-
profile-1.0#SAMLAssertionID">
            uuid-78c746a2-3ec4-4cf8-a913-50d2f7334cf9-32
```

Marc A Goodner 7/18/06 4:34 PM
Deleted: http://docs.oasis-open.org/wss/2005/xx/oasis-2005xx-wss-soap-message-security-1.1

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 18 July 2006

Marc A Goodner 7/18/06 4:22 PM
Inserted: 18 July 2006

```
          </o:KeyIdentifier>
        </o:SecurityTokenReference>
        <sc:Offset>0</sc:Offset>
        <sc:Length>24</sc:Length>
        <sc:Nonce>flvBVmEJTyhdYLlf8qDxBg==</sc:Nonce>
      </sc:DerivedKeyToken>
      <sc:DerivedKeyToken u:Id="_1">
        <o:SecurityTokenReference>
          <o:KeyIdentifier
            ValueType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-
profile-1.0#SAMLAssertionID">
            uuid-78c746a2-3ec4-4cf8-a913-50d2f7334cf9-32
          </o:KeyIdentifier>
        </o:SecurityTokenReference>
        <sc:Nonce>
          OJha4PKuTZbrdYoRG+wGdQ==
        </sc:Nonce>
      </sc:DerivedKeyToken>
      <e:ReferenceList>
        <e:DataReference URI="#_3"/>
      </e:ReferenceList>
      <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/2000/09/xmldsig#hmac-
sha1"/>
          <Reference URI="#_2">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>vbmdUSQRkAxqvUZpmIdO4sVvJtc=</DigestValue>
          </Reference>
          <Reference URI="#_4">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>tHsRP4mIFpGxuenN8F228dLQFgY=</DigestValue>
          </Reference>
          <Reference URI="#_5">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>O0W235qGMKd6vRjlAYnT/wzwNUU=</DigestValue>
          </Reference>
          <Reference URI="#_6">
```

```
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>yxG97lENThCdELIX9DBR6DeuEcc=</DigestValue>
          </Reference>
          <Reference URI="#_7">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>JTKMjWSZwz8Eda+SELo67k1So7U=</DigestValue>
          </Reference>
          <Reference URI="#uuid-c3cdb38b-e4aa-4467-9d0e-dd30f081e08d-10">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>Tj0yGTMhbgonlFR9JUsLZpZ2TQY=</DigestValue>
          </Reference>
        </SignedInfo>
        <SignatureValue>DYf5TKftfZSzjz7x8+srho1Z3nU=</SignatureValue>
        <KeyInfo>
          <o:SecurityTokenReference>
            <o:Reference URI="#_0"/>
          </o:SecurityTokenReference>
        </KeyInfo>
      </Signature>
    </o:Security>
  </s:Header>
  <s:Body u:Id="_2">
    <e:EncryptedData Id="_3">
      <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-
cbc"/>
      <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
        <o:SecurityTokenReference>
          <o:Reference URI="#_1"/>
        </o:SecurityTokenReference>
      </KeyInfo>
      <e:CipherData>
        <e:CipherValue>

RDolD6Fl/Oewj36sjiinWLKObqsMneMhkt0toCmH6YxyszC0/M+q3CMDfwmOd0AoEeudo0NpMyjki
YG9KylkWoPeTfPL+K52j2J6enttCQ8=
        </e:CipherValue>
      </e:CipherData>
    </e:EncryptedData>
  </s:Body>
</s:Envelope>
```

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 18 July 2006

Marc A Goodner 7/18/06 4:22 PM
Inserted: 18 July 2006

Response Message

Example (Non-normative)

Here is an example response.

```
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope"
  xmlns:a="http://schemas.xmlsoap.org/ws/2004/08/addressing"
  xmlns:e="http://www.w3.org/2001/04/xmlenc#"
  xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd"
  xmlns:sc="http://docs.oasis-open.org/ws-sx/ws-secureconversation/200512"
  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" u:Id="_4">
      http://example.org/PingResponse
    </a:Action>
    <a:RelatesTo u:Id="_5">
      urn:uuid:b6345ac8-dfc4-4174-a985-2f69cf4ac54e
    </a:RelatesTo>
    <a:To s:mustUnderstand="1" u:Id="_6">
      http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous
    </a:To>
    <o:Security s:mustUnderstand="1">
      <u:Timestamp u:Id="uuid-ad2ee057-8538-4e26-9b32-fc2cbf309f65-21">
        <u:Created>2005-10-24T15:51:47.244Z</u:Created>
        <u:Expires>2005-10-24T15:56:47.244Z</u:Expires>
      </u:Timestamp>
      <sc:DerivedKeyToken u:Id="_0" >
        <o:SecurityTokenReference>
          <o:KeyIdentifier
            ValueType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-
profile-1.0#SAMLAssertionID">
            uuid-78c746a2-3ec4-4cf8-a913-50d2f7334cf9-32
          </o:KeyIdentifier>
        </o:SecurityTokenReference>
        <sc:Offset>0</sc:Offset>
        <sc:Length>24</sc:Length>
        <sc:Nonce>NSL/hWMxr06TuqM9TWw62g==</sc:Nonce>
      </sc:DerivedKeyToken>
      <sc:DerivedKeyToken u:Id="_1">
        <o:SecurityTokenReference>
          <o:KeyIdentifier
            ValueType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-
profile-1.0#SAMLAssertionID">
            uuid-78c746a2-3ec4-4cf8-a913-50d2f7334cf9-32
          </o:KeyIdentifier>
        </o:SecurityTokenReference>
        <sc:Nonce>j9ELMPom+TqmOSCwKWwkhQ==</sc:Nonce>
      </sc:DerivedKeyToken>
      <e:ReferenceList>
        <e:DataReference URI="#_3"/>
      </e:ReferenceList>
      <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/2000/09/xmldsig#hmac-
sha1"/>
          <Reference URI="#_2">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>BahfbtbT6EJYYlsuGAN9Yu9AdJQ=</DigestValue>
          </Reference>
          <Reference URI="#_4">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>aIgoXzibEYVtNdiea5ozAxp8bcc=</DigestValue>
          </Reference>
          <Reference URI="#_5">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>/zXTjjyUnWZONNIrgOaBOs/qJ3E=</DigestValue>
          </Reference>
          <Reference URI="#_6">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>6LS4X08vC/GMGay2vwmD8fL7J2U=</DigestValue>
          </Reference>
          <Reference URI="#uuid-ad2ee057-8538-4e26-9b32-fc2cbf309f65-21">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>t407ttquWCqTsJGFTk7YWiodT/U=</DigestValue>
          </Reference>
        </SignedInfo>
        <SignatureValue>JrFIQ92/JCCn4QhpTHLv7sADuz8=</SignatureValue>
        <KeyInfo>
          <o:SecurityTokenReference>
            <o:Reference URI="#_0"/>
          </o:SecurityTokenReference>
```

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 18 July 2006

Marc A Goodner 7/18/06 4:22 PM
Inserted: 18 July 2006

```
        </KeyInfo>
      </Signature>
    </o:Security>
  </s:Header>
  <s:Body u:Id="_2">
    <e:EncryptedData Id="_3" Type="http://www.w3.org/2001/04/xmlenc#Content">
      <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-
cbc"/>
      <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
        <o:SecurityTokenReference >
          <o:Reference URI="#_1"/>
        </o:SecurityTokenReference>
      </KeyInfo>
      <e:CipherData>
        <e:CipherValue>
          NdMch9ybfaSJDiZGh...
        </e:CipherValue>
      </e:CipherData>
    </e:EncryptedData>
  </s:Body>
</s:Envelope>
```

4.3. Issued SAML 1.1 Token for Certificate, WSS 1.1

This binding is used for Scenario 5.

This mode requires WS-Security 1.1.

SAML token issued to the Client by STS is used to authenticate the Client. Service's X509 certificate is used to authenticate the Service. Client sends Request to the Service signed using DKT1(K), then encrypted using a DKT2(K), K is ephemeral key protected for STS's Certificate, DKT1(K) and DKT2(K) represent keys derived from K per WS-SecureConversation. Signature corresponding to DKT1(K) is signed using a key DKT(Sx) derived from symmetric proof-of-possession key Sx associated with the SAML token issued to the client by STS. SAML token is included in the message.

Service Policy

This is the service policy.

Frederick Hirsch 7/21/06 6:20 PM
Comment: Same question about how to specify use of two derived keys in policy,

```
<wsp:Policy>
  <sp:SymmetricBinding>
    <wsp:Policy>
      <sp:ProtectionToken>
        <wsp:Policy>
          <sp:SamlToken sp:IncludeToken='http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200512/IncludeToken/Always' >
            <wsp:Policy>
              <sp:WssSamlV11Token11 />
            </wsp:Policy>
          </sp:SamlToken>
        </wsp:Policy>
```

```
      </sp:ProtectionToken>
      <sp:SignBeforeEncrypting />
      <sp:EncryptSignature />
    </wsp:Policy>
  </sp:SymmetricBinding>
</wsp:Policy>
```

Request Message

Example (Non-normative)

Here is an example request.

```
<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope"
  xmlns:a="http://schemas.xmlsoap.org/ws/2004/08/addressing"
  xmlns:e="http://www.w3.org/2001/04/xmlenc#"
  xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd"
  xmlns:sc="http://docs.oasis-open.org/ws-sx/ws-secureconversation/200512"
  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" u:Id="_5">
      http://example.org/Ping
    </a:Action>
    <a:MessageID u:Id="_6">
      urn:uuid:a859eb17-1855-4d4f-8f73-85e4cba3e423
    </a:MessageID>
    <a:ReplyTo u:Id="_7">
      <a:Address>
        http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous
      </a:Address>
    </a:ReplyTo>
    <a:To s:mustUnderstand="1" u:Id="_8">
      http://server.example.com/Scenarios5
    </a:To>
    <o:Security s:mustUnderstand="1">
      <u:Timestamp u:Id="uuid-40f5bac7-f9af-4384-80db-cfab34263849-14">
        <u:Created>2005-10-25T00:47:38.222Z</u:Created>
        <u:Expires>2005-10-25T00:52:38.222Z</u:Expires>
      </u:Timestamp>
      <e:EncryptedKey Id="uuid-40f5bac7-f9af-4384-80db-cfab34263849-4">
        <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-
oaep-mgf1p"/>
        <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
```

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 18 July 2006

Marc A Goodner 7/18/06 4:22 PM
Inserted: 18 July 2006

```
          <o:SecurityTokenReference>
            <o:KeyIdentifier
              ValueType="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-
secext-1.1.xsd#ThumbprintSHA1">
              NQM0IBvuplAtETQvk+6gn8C13wE=
            </o:KeyIdentifier>
          </o:SecurityTokenReference>
        </KeyInfo>
        <e:CipherData>
          <e:CipherValue>
            <!-- base64 encoded octets of encrypted key K -->
          </e:CipherValue>
        </e:CipherData>
      </e:EncryptedKey>
      <sc:DerivedKeyToken u:Id="_0" >
        <o:SecurityTokenReference>
          <o:Reference URI="#uuid-40f5bac7-f9af-4384-80db-cfab34263849-4"/>
        </o:SecurityTokenReference>
        <sc:Offset>0</sc:Offset>
        <sc:Length>24</sc:Length>
        <sc:Nonce>7hI6Ul6OHavffYgpquHWuQ==</sc:Nonce>
      </sc:DerivedKeyToken>
      <sc:DerivedKeyToken u:Id="_2">
        <o:SecurityTokenReference>
          <o:Reference URI="#uuid-40f5bac7-f9af-4384-80db-cfab34263849-4"/>
        </o:SecurityTokenReference>
        <sc:Nonce>OEu+WEeUxPFRQK7SCFAnEQ==</sc:Nonce>
      </sc:DerivedKeyToken>
      <e:ReferenceList>
        <e:DataReference URI="#_4"/>
      </e:ReferenceList>
      <!-- encrypted SAML assertion -->
      <e:EncryptedData Id="_3"
Type="http://www.w3.org/2001/04/xmlenc#Element">
        <e:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>
        <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
          <!-- encrypted Key K-->
          <e:EncryptedKey>
            <e:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p"/>
            <KeyInfo>
              <o:SecurityTokenReference>
                <o:KeyIdentifier
```

Marc A Goodner 7/18/06 4:34 PM
Deleted: http://docs.oasis-open.org/wss/2005/xx/oasis-2005xx-wss-soap-message-security-1.1

```
                  ValueType="http://docs.oasis-open.org/wss/oasis-wss-
wssecurity-secext-1.1.xsd#ThumbprintSHA1">
                  NQM0IBvuplAtETQvk+6gn8C13wE=
                </o:KeyIdentifier>
              </o:SecurityTokenReference>
            </KeyInfo>
            <e:CipherData>
              <e:CipherValue>

cb7+JW2idPNSarK9quqCe9PQwmW2hoUghuyKRe+I9zOts6HaMcg73LqCWuK/jtdpvNl6GT/ZDYfcA
J7NLyMGxSiwi4DUlTOShqS6OTYBIKgUKiA+zXNl2koVSy7amcUhPMIT6/fohH+6MZDA4t6jomcyhl
CiW8d9IAzSWFkfg2k=
              </e:CipherValue>
            </e:CipherData>
          </e:EncryptedKey>
        </KeyInfo>
        <e:CipherData>
          <e:CipherValue>
            <!-- base64 encoded octets from SAML assertion encrypted with the
encrypted key K above -->
            <!-- SAML assertion element is identical as received in RSTR ,
unencrypted form is omitted for brevity -->
            <!--.........-->
          </e:CipherValue>
        </e:CipherData>
      </e:EncryptedData>

      <sc:DerivedKeyToken u:Id="_9">
        <o:SecurityTokenReference>
          <o:KeyIdentifier
            ValueType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-
profile-1.0#SAMLAssertionID">
            uuid-0c947d47-f527-410a-a674-753a9d7d97f7-16
          </o:KeyIdentifier>
        </o:SecurityTokenReference>
        <sc:Offset>0</sc:Offset>
        <sc:Length>24</sc:Length>
        <sc:Nonce>pgnS/VDSzJn6SFz+Vy23JA==</sc:Nonce>
      </sc:DerivedKeyToken>
      <Signature Id="_1" 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/2000/09/xmldsig#hmac-
sha1"/>
          <Reference URI="#_3">
```

Marc A Goodner 7/18/06 4:34 PM
Deleted: http://docs.oasis-open.org/wss/2005/xx/oasis-2005xx-wss-soap-message-security-1.1

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 18 July 2006

Marc A Goodner 7/18/06 4:22 PM
Inserted: 18 July 2006

```
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>eQdQVGRkVI1YfKJBw7vOYCOeLQw=</DigestValue>
          </Reference>
          <Reference URI="#_5">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>xxyKpp5RZ2TebKca2IGOafIgcxk=</DigestValue>
          </Reference>
          <Reference URI="#_6">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>WyGDDyYbL/hQZJfE3Yx2aK3RkK8=</DigestValue>
          </Reference>
          <Reference URI="#_7">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>AEOH0t2KYR8mivgqUGDrgMtxgEQ=</DigestValue>
          </Reference>
          <Reference URI="#_8">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>y8n6Dxd3DbD6TR6d6H/oVWsV4yE=</DigestValue>
          </Reference>
          <Reference URI="#uuid-40f5bac7-f9af-4384-80db-cfab34263849-14">
            <Transforms>
```

```
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>/Cc+bGkkeQ6jlVXZx8PGgmF6MjI=</DigestValue>
          </Reference>
        </SignedInfo>
        <SignatureValue>
          <!--base64 encoded signature value -->
        </SignatureValue>
        <KeyInfo>
          <o:SecurityTokenReference>
            <o:Reference URI="#_0"/>
          </o:SecurityTokenReference>
        </KeyInfo>
      </Signature>
      <!-- signature over the primary signature above
            using the key derived from the proof-key associated with SAML
assertion-->
      <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/2000/09/xmldsig#hmac-
sha1"/>
          <Reference URI="#_1">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>TMSmLlgeUn8cxyb6OYe5Q2nUuxY=</DigestValue>
          </Reference>
        </SignedInfo>
        <SignatureValue>Fh4NyOpAi+NqVFiHBgHWyvzah9I=</SignatureValue>
        <KeyInfo>
          <o:SecurityTokenReference>
            <o:Reference URI="#_9"/>
          </o:SecurityTokenReference>
        </KeyInfo>
      </Signature>
    </o:Security>
  </s:Header>
```

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 18 July 2006

Marc A Goodner 7/18/06 4:22 PM
Inserted: 18 July 2006

```
  <s:Body u:Id="_3">
    <e:EncryptedData Id="_4" Type="http://www.w3.org/2001/04/xmlenc#Content">
      <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-
cbc"/>
      <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
        <o:SecurityTokenReference >
          <o:Reference URI="#_2"/>
        </o:SecurityTokenReference>
      </KeyInfo>
      <e:CipherData>
        <e:CipherValue>
          <!-- base64 encoded octets of encrypted body content-->
        </e:CipherValue>
      </e:CipherData>
    </e:EncryptedData>
  </s:Body>
</s:Envelope>
```

Response Message

Example (Non-normative)

Here is an example response.

```
<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope"
  xmlns:a="http://schemas.xmlsoap.org/ws/2004/08/addressing"
  xmlns:e="http://www.w3.org/2001/04/xmlenc#"
  xmlns:k="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-
1.1.xsd"
  xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd"
  xmlns:sc="http://docs.oasis-open.org/ws-sx/ws-secureconversation/200512"
  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" u:Id="_6">
      http://example.org/PingResponse
    </a:Action>
    <a:RelatesTo u:Id="_7">
      urn:uuid:a859eb17-1855-4d4f-8f73-85e4cba3e423
    </a:RelatesTo>
    <a:To s:mustUnderstand="1" u:Id="_8">
      http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous
    </a:To>
    <o:Security s:mustUnderstand="1">
      <u:Timestamp u:Id="uuid-24adda3a-247a-4fec-b4f7-fb3827496cee-16">
        <u:Created>2005-10-25T00:47:38.921Z</u:Created>
```

Marc A Goodner 7/18/06 4:28 PM
Deleted: http://docs.oasis-open.org/wss/2005/xx/oasis-2005xx-wss-wssecurity-secext-1.1.xsd

```
        <u:Expires>2005-10-25T00:52:38.921Z</u:Expires>
      </u:Timestamp>
      <sc:DerivedKeyToken u:Id="_0" >
        <o:SecurityTokenReference>
          <o:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/oasis-
wss-wssecurity-secext-
1.1.xsd#EncryptedKeySHA1">pDJlrSJLzIqi+AcQLUB4GjUuRLs=</o:KeyIdentifier>
        </o:SecurityTokenReference>
        <sc:Offset>0</sc:Offset>
        <sc:Length>24</sc:Length>
        <sc:Nonce>KFjy1Gb73BubLul0ZGgx+w==</sc:Nonce>
      </sc:DerivedKeyToken>
      <sc:DerivedKeyToken u:Id="_3">
        <o:SecurityTokenReference>
          <o:KeyIdentifier
            ValueType="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-
secext-
1.1.xsd#EncryptedKeySHA1">pDJlrSJLzIqi+AcQLUB4GjUuRLs=</o:KeyIdentifier>
        </o:SecurityTokenReference>
        <sc:Nonce>omyh+Eg6XIa8q3V5IkHiXg==</sc:Nonce>
      </sc:DerivedKeyToken>
      <e:ReferenceList>
        <e:DataReference URI="#_5"/>
      </e:ReferenceList>
      <k:SignatureConfirmation u:Id="_1"
Value="EyKUHUuffPUPE/ZjaFrMJJ5KLKY="/>
      <k:SignatureConfirmation u:Id="_2"
Value="Fh4NyOpAi+NqVFiHBgHWyvzah9I="/>
      <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/2000/09/xmldsig#hmac-
sha1"/>
          <Reference URI="#_4">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>y/oItF5TcTOFan7SavhZTTTv48M=</DigestValue>
          </Reference>
          <Reference URI="#_6">
            <Transforms>
```

Marc A Goodner 7/18/06 4:34 PM
Deleted: http://docs.oasis-open.org/wss/2005/xx/oasis-2005xx-wss-soap-message-security-1.1

Marc A Goodner 7/18/06 4:34 PM
Deleted: http://docs.oasis-open.org/wss/2005/xx/oasis-2005xx-wss-soap-message-security-1.1

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 18 July 2006

Marc A Goodner 7/18/06 4:22 PM
Inserted: 18 July 2006

```
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>X4UIaLWnaAWTriw4UJ/SFDgm090=</DigestValue>
          </Reference>
          <Reference URI="#_7">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>vqy8/D4CDCaI1nnd4wl1Qjyp+qM=</DigestValue>
          </Reference>
          <Reference URI="#_8">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>H11vLAr5g8pbZ6jfZ+2WNyiNjiM=</DigestValue>
          </Reference>
          <Reference URI="#uuid-24adda3a-247a-4fec-b4f7-fb3827496cee-16">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>dr0g6hycoc884i+BD8FYCJGbbbE=</DigestValue>
          </Reference>
          <Reference URI="#_1">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>Rv3N7VNfAqpn0khr3F/qQZmE/l4=</DigestValue>
          </Reference>
          <Reference URI="#_2">
            <Transforms>
```

```
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>X2pxEnYPM8cMLrbhNqPgs8xk+a4=</DigestValue>
          </Reference>
        </SignedInfo>
        <SignatureValue>I2jQuDTWWQiNJy/ziyg8AFYO/z4=</SignatureValue>
        <KeyInfo>
          <o:SecurityTokenReference>
            <o:Reference URI="#_0"/>
          </o:SecurityTokenReference>
        </KeyInfo>
      </Signature>
    </o:Security>
  </s:Header>
  <s:Body u:Id="_4">
    <e:EncryptedData Id="_5" Type="http://www.w3.org/2001/04/xmlenc#Content">
      <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-
cbc"/>
      <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
        <o:SecurityTokenReference>
          <o:Reference URI="#_3"/>
        </o:SecurityTokenReference>
      </KeyInfo>
      <e:CipherData>
        <e:CipherValue>
          <!--base64 encoded octets of encrypted body content-->
        </e:CipherValue>
      </e:CipherData>
    </e:EncryptedData>
  </s:Body>
</s:Envelope>
```

4.4. SecureConversation

This binding is used for Scenario 6.

Secure session key Sz is established following Secure Conversation. RequestSecurityToken and RequestSecurityTokenResponse are protected following IssuedTokenForCertificate binding described above. Application messages are protected using symmetric keys derived from Sz following Secure Conversation.

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 18 July 2006

Marc A Goodner 7/18/06 4:22 PM
Inserted: 18 July 2006

Service Policy

This is the service policy.

```
<wsp:Policy>
  <sp:SymmetricBinding>
    <wsp:Policy>
      <sp:ProtectionToken>
        <wsp:Policy>
          <sp:SecurityContextToken sp:IncludeToken='http://docs.oasis-
open.org/ws-sx/ws-securitypolicy/200512/IncludeToken/Always' />
        </wsp:Policy>
      </sp:ProtectionToken>
    </wsp:Policy>
  </sp:SymmetricBinding>
</wsp:Policy>
```

Request Message

Frederick Hirsch 7/21/06 6:17 PM
Deleted:

Example (Non-normative)

Here is an example request.

```
<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope"
  xmlns:a="http://schemas.xmlsoap.org/ws/2004/08/addressing"
  xmlns:e="http://www.w3.org/2001/04/xmlenc#"
  xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd"
  xmlns:sc="http://docs.oasis-open.org/ws-sx/ws-secureconversation/200512"
  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" u:Id="_2">
      http://example.org/Ping
    </a:Action>
    <a:MessageID u:Id="_3">
      urn:uuid:94e6ed8b-7084-48e1-bba7-85c4ea50c512
    </a:MessageID>
    <a:ReplyTo u:Id="_4">
    <a:Address>
      http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous
    </a:Address>
    </a:ReplyTo>
    <a:To s:mustUnderstand="1" u:Id="_5">
      http://server.example.com/Scenarios6
    </a:To>
```

```
    <o:Security s:mustUnderstand="1">
      <u:Timestamp u:Id="uuid-5df39133-c58e-4b83-9b86-e20bf5efe563-17">
        <u:Created>2005-11-02T23:38:05.175Z</u:Created>
        <u:Expires>2005-11-02T23:43:05.175Z</u:Expires>
      </u:Timestamp>
      <sc:SecurityContextToken u:Id="uuid-8930d45e-14b0-42f5-b415-
6b4ee115b943-7">
       <sc:Identifier>
          urn:uuid:8e6a3a95-fd1b-4c24-96d4-28e875025ff7
        </sc:Identifier>
      </sc:SecurityContextToken>
      <!-- START: Key derived from SCT-Key used for signing. -->
     <sc:DerivedKeyToken u:Id="uuid-5df39133-c58e-4b83-9b86-e20bf5efe563-12">
        <o:SecurityTokenReference>
          <o:Reference URI="#uuid-8930d45e-14b0-42f5-b415-6b4ee115b943-7" />
        </o:SecurityTokenReference>
        <sc:Offset>0</sc:Offset>
        <sc:Length>24</sc:Length>
        <sc:Nonce>lCO/qhHek2+0qiFPEwdeLw==</sc:Nonce>
      </sc:DerivedKeyToken>
      <!-- END: Key derived from SCT-Key used for signing. -->
      <!-- START: Key derived from SCT-Key used for encryption. -->
     <sc:DerivedKeyToken u:Id="uuid-5df39133-c58e-4b83-9b86-e20bf5efe563-13">
        <o:SecurityTokenReference>
          <o:Reference URI="#uuid-8930d45e-14b0-42f5-b415-6b4ee115b943-7" />
        </o:SecurityTokenReference>
        <sc:Nonce>rMICQZ+A6CWApF3/j6XauA==</sc:Nonce>
      </sc:DerivedKeyToken>
      <!-- END: Key derived from SCT-Key used for encryption. -->
      <e:ReferenceList xmlns:e="http://www.w3.org/2001/04/xmlenc#">
        <e:DataReference URI="#_1" />
      </e:ReferenceList>
      <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/2000/09/xmldsig#hmac-sha1" />
          <Reference URI="#_0">
           <Transforms>
            <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            </Transforms>
          <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
            <DigestValue>zXrQhCxRjuPxmhQB2iSzCDNp/fg=</DigestValue>
          </Reference>
          <Reference URI="#_1">
```

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 18 July 2006

Marc A Goodner 7/18/06 4:22 PM
Inserted: 18 July 2006

```
            <Transforms>
            <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            </Transforms>
          <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
            <DigestValue>zXrQhCxRjuPxmhQB2iSzCDNp/fg=</DigestValue>
          </Reference>
          <Reference URI="#_2">
            <Transforms>
            <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            </Transforms>
          <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
            <DigestValue>NQGQB5EcC5nODzdIHfvhYeqgxOE=</DigestValue>
          </Reference>
          <Reference URI="#_3">
            <Transforms>
            <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            </Transforms>
          <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
            <DigestValue>IBNjyw72JuzKU0plbF2eEWm0rHk=</DigestValue>
          </Reference>
          <Reference URI="#_4">
            <Transforms>
            <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            </Transforms>
          <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
            <DigestValue>IBNjyw72JuzKU0plbF2eEWm0rHk=</DigestValue>
          </Reference>
          <Reference URI="#_5">
            <Transforms>
            <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            </Transforms>
          <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
            <DigestValue>IBNjyw72JuzKU0plbF2eEWm0rHk=</DigestValue>
          </Reference>
          <Reference URI="#uuid-ff348436-ba42-41ea-bec2-2f1138f29623-17">
            <Transforms>
            <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            </Transforms>
          <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
            <DigestValue>jX1/gPMBRWBKgq7WNAjdFkIFPxI=</DigestValue>
          </Reference>
        </SignedInfo>
        <SignatureValue>j6nmdxEi4kTks81DqdxSPPZDiTw=</SignatureValue>
        <KeyInfo>
```

```
          <o:SecurityTokenReference>
          <o:Reference URI="#uuid-ff348436-ba42-41ea-bec2-2f1138f29623-12">
          </o:Reference>
          </o:SecurityTokenReference>
        </KeyInfo>
      </Signature>
    </o:Security>
  </s:Header>
  <s:Body u:Id="_0">
    <e:EncryptedData Id="_1" Type="http://www.w3.org/2001/04/xmlenc#Content">
<e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>
      <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
        <o:SecurityTokenReference >
          <o:Reference URI="#uuid-5df39133-c58e-4b83-9b86-e20bf5efe563-13" />
        </o:SecurityTokenReference>
      </KeyInfo>
      <e:CipherData>
        <e:CipherValue>...20X2ZX01grMOPbUMXYmeXXY</e:CipherValue>
      </e:CipherData>
    </e:EncryptedData>
  </s:Body>
</s:Envelope>
```

Response Message

```
<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope"
  xmlns:a="http://schemas.xmlsoap.org/ws/2004/08/addressing"
  xmlns:e="http://www.w3.org/2001/04/xmlenc#"
  xmlns:k="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-
1.1.xsd"
  xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd"
  xmlns:sc="http://docs.oasis-open.org/ws-sx/ws-secureconversation/200512"
  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" u:Id="_2">
      http://example.org/Ping
    </a:Action>
    <a:RelatesTo u:Id="_1">
      urn:uuid:94e6ed8b-7084-48e1-bba7-85c4ea50c512
    </a:RelatesTo>
    <a:To s:mustUnderstand="1" u:Id="_3">
      http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous
    </a:To>
```

Marc A Goodner 7/18/06 4:28 PM
Deleted: http://docs.oasis-open.org/wss/2005/xx/oasis-2005xx-wss-wssecurity-secext-1.1.xsd

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 18 July 2006

Marc A Goodner 7/18/06 4:22 PM
Inserted: 18 July 2006

```
    <o:Security s:mustUnderstand="1">
      <u:Timestamp u:Id="uuid-8930d45e-14b0-42f5-b415-6b4ee115b943-16">
        <u:Created>2005-11-02T23:38:05.253Z</u:Created>
        <u:Expires>2005-11-02T23:43:05.253Z</u:Expires>
      </u:Timestamp>
      <!-- START: Derived key SCT-Key1 used for signing. -->
     <sc:DerivedKeyToken u:Id="uuid-8930d45e-14b0-42f5-b415-6b4ee115b943-10">
        <o:SecurityTokenReference>
          <o:Reference URI="urn:uuid:8e6a3a95-fd1b-4c24-96d4-28e875025ff7"
ValueType="http://docs.oasis-open.org/ws-sx/ws-secureconversation/200512/sct"
/>
        </o:SecurityTokenReference>
        <sc:Offset>0</sc:Offset>
        <sc:Length>24</sc:Length>
        <sc:Nonce>ZakR9dMZmd4LBa7qLOY56w==</sc:Nonce>
      </sc:DerivedKeyToken>
      <!-- END: Derived key SCT-Key1 used for signing. -->
      <!-- START: Derived key SCT-Key2 used for encryption. -->
   <sc:DerivedKeyToken u:Id="uuid-8930d45e-14b0-42f5-b415-6b4ee115b943-11">
        <o:SecurityTokenReference>
          <o:Reference URI="urn:uuid:8e6a3a95-fd1b-4c24-96d4-28e875025ff7"
ValueType="http://docs.oasis-open.org/ws-sx/ws-secureconversation/200512/sct"
/>
        </o:SecurityTokenReference>
        <sc:Nonce>t+R+jHxI8T642/HLd0EHiA==</sc:Nonce>
      </sc:DerivedKeyToken>
      <!-- END: Derived key SCT-Key2 used for encryption. -->
      <e:ReferenceList>
        <e:DataReference URI="#_4" />
      </e:ReferenceList>

      <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
        <SignedInfo>
 <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
</CanonicalizationMethod>
    <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#hmac-sha1">
    </SignatureMethod>
          <Reference URI="#_0">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
              </Transform>
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
            </DigestMethod>
```

```
            <DigestValue>3gVmAaye1xmL7Y+rC2iGKxAsT6w=</DigestValue>
          </Reference>
          <Reference URI="#_1">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
              </Transform>
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
            </DigestMethod>
            <DigestValue>nHUD4Ojy3RPL1M7NFEkaF1SgRsI=</DigestValue>
          </Reference>
          <Reference URI="#_2">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
              </Transform>
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
            </DigestMethod>
            <DigestValue>Y7ZFX24xNjoNfJMnX1YvgPNdQd0=</DigestValue>
          </Reference>
          <Reference URI="#_3">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
              </Transform>
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
            </DigestMethod>
            <DigestValue>QgsDL8L8Nn0rI2wj44V5Wn6a7Vg=</DigestValue>
          </Reference>
          <Reference URI="#_7">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
              </Transform>
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
            </DigestMethod>
            <DigestValue>QgsDL8L8Nn0rI2wj44V5Wn6a7Vg=</DigestValue>
          </Reference>
          <Reference URI="#uuid-f96d9fdb-f7d3-4e14-95b8-503a8e163d45-16">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
              </Transform>
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
```

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 18 July 2006

Marc A Goodner 7/18/06 4:22 PM
Inserted: 18 July 2006

```
            </DigestMethod>
            <DigestValue>fUOV9sL3vcJtyC7agjaIvYG/bbw=</DigestValue>
          </Reference>
        </SignedInfo>
        <SignatureValue>DNxG4BukpgO8NJ6Rr7RXyZ15unM=</SignatureValue>
        <KeyInfo>
          <o:SecurityTokenReference>
            <o:Reference URI="#uuid-f96d9fdb-f7d3-4e14-95b8-503a8e163d45-10">
            </o:Reference>
          </o:SecurityTokenReference>
        </KeyInfo>
      </Signature>
    </o:Security>
  </s:Header>
  <s:Body u:Id="_7" >
    <e:EncryptedData Id="_3" Type="http://www.w3.org/2001/04/xmlenc#Content">
<e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>
      <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
        <o:SecurityTokenReference>
          <o:Reference URI="#uuid-8930d45e-14b0-42f5-b415-6b4ee115b943-11"/>
        </o:SecurityTokenReference>
      </KeyInfo>
      <e:CipherData>

<e:CipherValue>gRGx8V7NPorFrfQ2TnzdUPT7h6nZuFERLwt7G1N8Npi0lB0UjU7N27U5Fwqqw1
zsIzQyjxKtmwTop6ghczvGh8jleW25N0JK4Ef7qCPhiTIwof/8abZuvJI+ckw+4HEe</e:CipherV
alue>
      </e:CipherData>
    </e:EncryptedData>
  </s:Body>
</s:Envelope>
```

Example (Non-normative)

Here is an example response.

4.5. Issued SAML 2.0 Token

This binding is used in Scenario 7.

SAML token issued to the Client by STS is used to authenticate the Client. Messages are signed then encrypted using symmetric keys derived from the symmetric proof-of-possession key Sx associated with the SAML token.

Service Policy

This is the service policy, now with SAML 2.0 and WSS 1.1 SAML Token Profile

```
<wsp:Policy>
  <sp:SymmetricBinding>
    <wsp:Policy>
      <sp:ProtectionToken>
        <wsp:Policy>
          <sp:SamlToken sp:IncludeToken='http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200512/IncludeToken/Always' >
            <wsp:Policy>
              <sp:WssSamlV20Token11 />
            </wsp:Policy>
          </sp:SamlToken>
        </wsp:Policy>
      </sp:ProtectionToken>
      <sp:SignBeforeEncrypting />
      <sp:EncryptSignature />
    </wsp:Policy>
  </sp:SymmetricBinding>
</wsp:Policy>
```

Request Message

Frederick Hirsch 7/21/06 6:20 PM
Deleted:

Example (Non-normative)

Here is an example request.

Response Message

Example (Non-normative)

Here is an example response.

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 18 July 2006

Marc A Goodner 7/18/06 4:22 PM
Inserted: 18 July 2006

5. WSDL

Frederick Hirsch 7/21/06 4:21 PM
Formatted: Bullets and Numbering

5.1. STS

```
<?xml version="1.0" encoding="utf-8"?>
<wsdl:definitions name="SecurityTokenService"
  targetNamespace="http://tempuri.org/"
  xmlns:tns="http://tempuri.org/"
  xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
  xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/"
  xmlns:t="http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust">
  <wsdl:import namespace="http://docs.oasis-open.org/ws-sx/ws-
trust/200512/ws-trust"
               location="http://www.oasis-open.org/apps/org/workgroup/ws-
sx/download.php/16291/oasis-wssx-ws-trust-1.0.wsdl"/>
  <wsdl:binding name="SecurityTokenService" type="t:SecurityTokenService">
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="ProcessRequestSecurityToken">
      <soap12:operation soapAction="http://docs.oasis-open.org/ws-sx/ws-
trust/200512/ws-trust/RST/Issue" style="document"/>
      <wsdl:input>
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <soap12:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
  </wsdl:binding>
  <wsdl:binding name="SecurityTokenService1" type="t:SecurityTokenService">
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="ProcessRequestSecurityToken">
      <soap12:operation soapAction="http://docs.oasis-open.org/ws-sx/ws-
trust/200512/ws-trust/RST/Issue" style="document"/>
      <wsdl:input>
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <soap12:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
  </wsdl:binding>
  <wsdl:service name="SecurityTokenService">
    <wsdl:port name="SecurityTokenService_port"
binding="tns:SecurityTokenService">
```

```
      <soap12:address location="http://example.org/Sts/MutualCertificate11"/>
    </wsdl:port>
    <wsdl:port name="SecurityTokenService1_port"
binding="tns:SecurityTokenService1">
      <soap12:address location="http://example.org/Sts/MutualCertificate10"/>
    </wsdl:port>
  </wsdl:service>
</wsdl:definitions>
```

5.2. Service

```
<?xml version="1.0" encoding="utf-8"?>
<wsdl:definitions name="PingService"
  targetNamespace="http://tempuri.org/"
  xmlns:tns="http://tempuri.org/"
  xmlns:i0="http://example.org/Ping"
  xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
  xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/"
  >
  <wsdl:import namespace="http://example.org/Ping"
location="service_portType.wsdl"/>
  <wsdl:types/>
  <wsdl:binding name="IPingService" type="i0:IPingService">
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="Ping">
      <soap12:operation soapAction="http://example.org/Ping"
style="document"/>
      <wsdl:input name="PingRequest">
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output name="PingResponse">
        <soap12:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
  </wsdl:binding>
  <wsdl:service name="PingService">
    <wsdl:port name="IPingService_port" binding="tns:IPingService">
      <soap12:address location="http://example.org/PingService"/>
    </wsdl:port>
  </wsdl:service>
</wsdl:definitions>
```

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 18 July 2006

Marc A Goodner 7/18/06 4:22 PM
Inserted: 18 July 2006

6. References

Frederick Hirsch 7/21/06 4:21 PM
Formatted: Bullets and Numbering

6.1. Normative

[RFC2119] S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*, http://www.ietf.org/rfc/rfc2119.txt, IETF RFC 2119, March 1997.

7. Notes

Frederick Hirsch 7/21/06 4:21 PM
Formatted: Bullets and Numbering

Frederick Hirsch 7/19/06 8:10 AM
Deleted: 18 July 2006

Marc A Goodner 7/18/06 4:22 PM
Inserted: 18 July 2006

Frederick Hirsch 7/21/06 4:21 PM
Formatted: Bullets and Numbering

8. Revision History

Rev	Date	By Whom	What
00	2006-04-25	Marc Goodner	First merge of previous interop scenarios contributed to SX TC from Marc Goodner and Prateek Mishra.
01	2006-04-25	Prateek Mishra	Added detailed message flows for scenario #3; scenarios 1-3 are now complete.
02	2006-05-02	Marc Goodner	This revision is the merged version of all contributed scenarios. XML examples exist for most scenarios. There is still additional work needed around explaining those examples in prose as well as adding the missing XML examples.
03	2006-06-27	Marc Goodner	Removed SOAP 1.2 option Updated RSTR message examples with RSTRC Added SC message example Updated incomplete scenario descriptions Cleaned up document, removed table of XLM structure in favor of message examples (just one source to edit/review), normalized use of wst and t namespace prefixes
04	2006-07-18	Marc Goodner	Correction from Jan Alexander comments to TC list.