

1 An OASIS White Paper

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

2 WS-SX Interop Scenarios

3 Scenarios for demonstration of WS-SX TC specifications

4 Version ED-04 [fih](#)

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

5 Editors Marc Goodner, Prateek Mishra  
6 Contributors Darren Platt

7 For OASIS WS-SX TC





8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20

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

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

33

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**

34 Table of Contents

35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65  
66

- [1. Introduction ..... 5](#)
- [1.1. Namespaces..... 5](#)
- [2. WS-SX Interop Scenarios ..... 6](#)
- [2.1. Preconditions ..... 7](#)
- [3. Client and STS Security Bindings ..... 8](#)
- [3.1. Username for SAML 1.1 HoK over HTTPS ..... 8](#)
- [3.2. Username for SAML 1.1 Bearer Token, WSS 1.0 ..... 15](#)
- [3.3. Certificate for SAML 1.1 HoK Token, WSS 1.0 ..... 20](#)
- [3.4. Mutual Certificate, WSS1.0 ..... 26](#)
- [3.5. Mutual Certificate, WSS1.1 ..... 38](#)
- [3.6. Delegated SAML 2.0 with Certificate for SAML 2.0 HoK, WSS 1.1 ..... 50](#)
- [4. Client and Service Security Bindings ..... 59](#)
- [4.1. Issued SAML 1.1 Token over Transport..... 59](#)
- [4.2. Issued SAML 1.1 Token for Certificate, WSS 1.0..... 63](#)
- [4.3. Issued SAML 1.1 Token for Certificate, WSS 1.1..... 69](#)
- [4.4. SecureConversation ..... 78](#)
- [4.5. Issued SAML 2.0 Token ..... 85](#)
- [5. WSDL ..... 87](#)
- [5.1. STS ..... 87](#)
- [5.2. Service ..... 88](#)
- [6. References ..... 89](#)
- [6.1. Normative ..... 89](#)
- [7. Notes ..... 90](#)
- [8. Revision History ..... 91](#)

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**

71 1. Introduction

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

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

77 Client uses SAML Token to authenticate to the Service.

78 Specific security protection mechanisms vary across scenarios.

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

80 **1.1. Namespaces**

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

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

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

83

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

## 84 2. WS-SX Interop Scenarios

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

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

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

90  
91 The following scenarios were chosen to cover different combinations of parameters discussed below.

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

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

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

92 **2.1. Preconditions**

93 **WSDL**

94 See the [WSDL section](#) at the end of this document for the [STS](#) and [Service](#) WSDL.

95 **User Name and Password**

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

99 **Certificates**

100 The following certificates are associated with roles used across scenarios.

- 101 • Client: Alice
- 102 • STS: WssIP
- 103 • Service: Bob

104 **Trust and Proof Keys**

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

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

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

Frederick Hirsch 7/21/06 4:39 PM

Deleted: \

### 112 3. Client and STS Security Bindings

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

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

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

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

#### 121 3.1. Username for SAML 1.1 HoK over HTTPS

122 This binding is used in Scenario 1.

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

##### 125 **Expected Security Properties**

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

##### 127 **Agreements**

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

##### 130 **Acceptable <wsa:EndpointReference> Values**

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

##### 133 **Request Message**

##### 134 **Message Creation**

##### 135 **Security**

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

##### 137 **UserName**

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

##### 139 **Body**

##### 140 **RequestSecurityToken**

141 TokenType

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

Frederick Hirsch 7/21/06 4:20 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



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

144 RequestType

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

147 AppliesTo

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

150 KeyType

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

### 153 **Message Processing**

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

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

### 163 **Example (Non-normative)**

164 Here is an example request.

```
165 <s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope"  
166   xmlns:a="http://schemas.xmlsoap.org/ws/2004/08/addressing"  
167   xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-  
168   wssecurity-secext-1.0.xsd"  
169   xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-  
170   wssecurity-utility-1.0.xsd"  
171   xmlns:t="http://docs.oasis-open.org/ws-sx/ws-trust/200512"  
172 >  
173   <s:Header>  
174     <a:Action s:mustUnderstand="1" u:Id="_3">  
175       http://docs.oasis-open.org/ws-sx/ws-trust/200512/RST/Issue  
176     </a:Action>  
177     <a:MessageID u:Id="_4">  
178       urn:uuid:85836182-3ef8-4efc-a93f-06466277053e  
179     </a:MessageID>  
180     <a:ReplyTo u:Id="_5">  
181       <a:Address>  
182         http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous  
183       </a:Address>  
184     </a:ReplyTo>
```

```

185 <a:To s:mustUnderstand="1" u:Id=" 6">
186   http://server.example.com/STS/Scenario1
187 </a:To>
188 <o:Security s:mustUnderstand="1">
189   <u:Timestamp u:Id="uuid-c3cdb38b-e4aa-4467-9d0e-dd30f081e08d-5">
190     <u:Created>2005-10-24T15:51:44.664Z</u:Created>
191     <u:Expires>2005-10-24T15:56:44.664Z</u:Expires>
192   </u:Timestamp>
193   <o:UsernameToken u:Id='Me'>
194     <o:Username>joe</o:Username>
195     <o:Password>eoj</o:Password>
196   </o:UsernameToken>
197 </o:Security>
198 </s:Header>
199 <s:Body>
200   <t:RequestSecurityToken>
201     <t:RequestType>
202       http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue
203     </t:RequestType>
204     <t:Entropy>
205       <t:BinarySecret u:Id="uuid-4acf589c-0076-4a83-8b66-5f29341514b7-3"
206         Type="http://docs.oasis-open.org/ws-sx/ws-trust/200512/Nonce">
207         Uv38QLxDQM9gLoDZ6OwYDiFk094nmwu3Wmay7EdKmhW=
208       </t:BinarySecret>
209     </t:Entropy>
210     <t:KeyType>
211       http://docs.oasis-open.org/ws-sx/ws-trust/200512/SymmetricKey
212     </t:KeyType>
213     <t:KeySize>
214       256
215     </t:KeySize>
216     <t:ComputedKeyAlgorithm>
217       http://docs.oasis-open.org/ws-sx/ws-trust/200512/CK/PSHA1
218     </t:ComputedKeyAlgorithm>
219   </t:RequestSecurityToken>
220 </s:Body>
221 </s:Envelope>

```

222 [Request Policy](#)

223 [Since there are no requirements for client authentication using HTTPS, the TransportBinding assertion](#)  
 224 [alone is adequate to capture the requirement to use HTTPS to secure the channel.](#)

225 [The policy corresponding to the request requirements may be written:](#)

```

227 <wsp:Policy>
228   <sp:TransportBinding />
229   <sp:UsernameToken
230     sp:IncludeToken='http://docs.oasis-open.org/ws-sx/ws-
231     securitypolicy/200512/IncludeToken/Always' />
232 </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

233 **Response Message**

234 **Message Creation**

235 **Body**

236 **RequestSecurityTokenResponseCollection/RequestSecurityTokenResponse**

237 **TokenType**

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

240 **AppliesTo**

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

242 **Lifetime**

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

244 **RequestedSecurityToken**

245 **Assertion**

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

249 **Message Processing**

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

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

255 **Example (Non-normative)**

256 Here is an example response.

```
257 <s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope"  
258   xmlns:a="http://schemas.xmlsoap.org/ws/2004/08/addressing"  
259   xmlns:e="http://www.w3.org/2001/04/xmlenc#"  
260   xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-  
261 wssecurity-secext-1.0.xsd"  
262   xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"  
263   xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-  
264 wssecurity-utility-1.0.xsd"  
265   xmlns:t="http://docs.oasis-open.org/ws-sx/ws-trust/200512"  
266   >  
267 <s:Header>
```

```

268 <a:Action s:mustUnderstand="1" u:Id="_3">
269   http://docs.oasis-open.org/ws-sx/ws-trust/200512/RSTRC/IssueFinal
270 </a:Action>
271 <a:MessageID u:Id="_4">
272   urn:uuid:85836182-3ef8-4efc-a93f-06466277053e
273 </a:MessageID>
274 <a:ReplyTo u:Id="_5">
275   <a:Address>
276     http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous
277   </a:Address>
278 </a:ReplyTo>
279 <a:To s:mustUnderstand="1" u:Id="_6">
280   http://client.example.com/STS/Scenario1
281 </a:To>
282 <o:Security s:mustUnderstand="1">
283   <u:Timestamp u:Id="uuid-c3cdb38b-e4aa-4467-9d0e-dd30f081e08d-5">
284     <u:Created>2005-10-24T15:51:44.664Z</u:Created>
285     <u:Expires>2005-10-24T15:56:44.664Z</u:Expires>
286   </u:Timestamp>
287 </o:Security>
288 </s:Header>
289 <s:Body>
290   <t:RequestSecurityTokenResponseCollection>
291     <t:RequestSecurityTokenResponse>
292       <t:TokenType>
293         http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-
294 1.1#SAMLV1.1
295       </t:TokenType>
296       <t:KeySize>
297         256
298       </t:KeySize>
299       <t:RequestedAttachedReference>
300         <o:SecurityTokenReference>
301           <o:KeyIdentifier
302             ValueType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-
303 profile-1.0#SAMLAssertionID">
304             uuid-8222b7a2-3874-4884-bdb5-9c2ddd4b86b5-16
305           </o:KeyIdentifier>
306         </o:SecurityTokenReference>
307       </t:RequestedAttachedReference>
308       <t:RequestedUnattachedReference>
309         <o:SecurityTokenReference>
310           <o:KeyIdentifier
311             ValueType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-
312 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

```

313         uuid-8222b7a2-3874-4884-bdb5-9c2ddd4b86b5-16
314     </o:KeyIdentifier>
315 </o:SecurityTokenReference>
316 </t:RequestedUnattachedReference>
317 <t:Lifetime>
318     <u:Created>2005-10-24T20:19:26.526Z</u:Created>
319     <u:Expires>2005-10-25T06:24:26.526Z</u:Expires>
320 </t:Lifetime>
321 <t:RequestedSecurityToken>
322     <saml:Assertion MajorVersion="1" MinorVersion="1"
323         AssertionID="uuid-8222b7a2-3874-4884-bdb5-9c2ddd4b86b5-16"
324         Issuer="Test STS"
325         IssueInstant="2005-10-24T20:24:26.526Z">
326         <saml:Conditions NotBefore="2005-10-24T20:19:26.526Z"
327 NotOnOrAfter="2005-10-25T06:24:26.526Z"/>
328         <saml:Advice/>
329         <saml:AttributeStatement>
330             <saml:Subject>
331                 <saml:SubjectConfirmation>
332                     <saml:ConfirmationMethod>
333                         urn:oasis:names:tc:SAML:1.0:cm:holder-of-key
334                     </saml:ConfirmationMethod>
335                     <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
336                         <e:EncryptedKey>
337                             <e:EncryptionMethod
338 Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p"/>
339                             <KeyInfo>
340                                 <o:SecurityTokenReference>
341                                     <o:KeyIdentifier
342                                         ValueType="http://docs.oasis-open.org/wss/oasis-
343 wss-wssecurity-secext-1.1.xsd#ThumbprintSHA1">
344                                         NQM0IBvuplAtETQvk+6gn8C13wE=
345                                     </o:KeyIdentifier>
346                                 </o:SecurityTokenReference>
347                             </KeyInfo>
348                             <e:CipherData>
349                                 <e:CipherValue>
350 EEcYjwNoYcJ+20xTYE5e/fixl5K0gzgrfaYAxkDFv/VXiuKf1084h8PmogTfM+azcgAfmArVQvOyK
351 WXRb5vmXYfVHLlhZTbXacy+nowSUNnEjp37VDbI3RJ5k6tBHF+ow0NM/P6GPNZ9ZqJi11GDgWJkFs
352 JzNXNbbMgwuFu3cA=
353                                 </e:CipherValue>
354                             </e:CipherData>
355                         </e:EncryptedKey>
356                     </KeyInfo>
357                 </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

```

358     </saml:Subject>
359   </saml:AttributeStatement>
360   <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
361     <SignedInfo>
362       <CanonicalizationMethod
363 Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
364       <SignatureMethod
365 Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
366       <Reference URI="#uuid-8222b7a2-3874-4884-bdb5-9c2ddd4b86b5-16">
367         <Transforms>
368           <Transform
369 Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
370           <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
371 c14n#" />
372         </Transforms>
373         <DigestMethod
374 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
375         <DigestValue>7nHBrFPsm+LEFAoV4NoQPoEl5Lk=</DigestValue>
376       </Reference>
377     </SignedInfo>
378     <SignatureValue>
379 TugV4pTIwCH87bLD4jiMgVGtkbRBt1tRlHXJArL34A/YfA4AnGBLXB4pJdUsUxMUtbQl4PoGgEsdL
380 Ng8C77peARELGPl/Tqw7T3u5zBYHxCHCiV2FWBBfeOmwJmqaBf8XZJ4AlyqPq61P61jrQjZJafpH
381 uYpAZnZQSvsiJaBPQ=
382     </SignatureValue>
383     <KeyInfo>
384       <o:SecurityTokenReference>
385         <o:KeyIdentifier
386           ValueType="http://docs.oasis-open.org/wss/oasis-wss-
387 wssecurity-secext-1.1.xsd#ThumbprintSHA1">
388           NQM0IBvuplAtETQvk+6gn8C13wE=
389         </o:KeyIdentifier>
390       </o:SecurityTokenReference>
391     </KeyInfo>
392   </Signature>
393 </saml:Assertion>
394 </t:RequestedSecurityToken>
395 <t:RequestedProofToken>
396   <t:BinarySecret u:Id="uuid-8222b7a2-3874-4884-bdb5-9c2ddd4b86b5-14">
397     zT8LWAUwUrIVKA/rkCr0kxlEmKAehcB6TGWJuAgucBM=
398   </t:BinarySecret>
399 </t:RequestedProofToken>
400 </t:RequestSecurityTokenResponse>
401 </t:RequestSecurityTokenResponseCollection>
402 </s:Body>
403 </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

### 404 3.2. Username for SAML 1.1 Bearer Token, WSS 1.0

405 This binding is used in scenario 2.

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

Frederick Hirsch 7/21/06 6:36 PM

Deleted: RSTR

Frederick Hirsch 7/21/06 4:40 PM

Deleted: keyinfo

#### 411 Expected Security Properties

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

#### 413 Agreements

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

#### 416 Acceptable <wsa:EndpointReference> Values

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

#### 419 Request Message

##### 420 Message Creation

##### 421 Security

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

##### 423 UserName

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

##### 425 Body

##### 426 RequestSecurityToken

##### 427 TokenType

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

##### 430 RequestType

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

##### 433 AppliesTo

434 This element MUST include an <wsa:EndpointReference> element with a <wsa:Address> sub-element.  
435 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-](http://docs.oasis-open.org/ws-sx/wstrust/200512/Bearer)  
438 [sx/wstrust/200512/Bearer](http://docs.oasis-open.org/ws-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



```
479     </wsa:EndpointReference>
480   </wsp:AppliesTo>
481   <t:KeyType>
482     http://docs.oasis-open.org/ws-sx/wstrust/200512/Bearer
483   </t:KeyType>
484 </t:RequestSecurityToken>
485 </soap:Body>
486 </soap:Envelope>
```

487 [Policy](#)

488 [Same as previous case.](#)

489 **Response Message**

490 **Message Creation**

491 **Body**

492 **RequestSecurityTokenResponseCollection/RequestSecurityTokenResponse**

493 TokenType

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

496 AppliesTo

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

498 Lifetime

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

500 RequestedSecurityToken

501 Assertion

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

505 **Message Processing**

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

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

511 **Example (Non-normative)**

512 Here is an example response.

```
513 <?xml version="1.0" encoding="utf-8" ?>
514 <soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
515 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance
516 xmlns:wst="http://docs.oasis-open.org/ws-sx/ws-trust/200512"
517 xmlns:xsd="http://www.w3.org/2001/XMLSchema">
518 <soap:Header>
519 </soap:Header>
520 <soap:Body wsu:Id="body"
521 xmlns:wsu="http://schemas.xmlsoap.org/ws/2003/06/utility">
522 <t:RequestSecurityTokenResponseCollection>
523 <t:RequestSecurityTokenResponse>
524 <t:TokenType>
525 http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0#SAMLV1.1
526 </t:TokenType>
527 <wsp:AppliesTo
528 xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/03/addressing">
529 <wsa:EndpointReference>
530 <wsa:Address>http://www.example.org/</wsa:Address>
531 </wsa:EndpointReference>
532 <wsp:AppliesTo>
533 <t:Lifetime>
534 <wsu:Created>"2005-04-17T00:46:02Z"</wsu:Created>
535 <wsu:Expires>"2005-04-17T00:51:02Z"> </wsu:Expires>
536 </t:Lifetime>
537 <t:RequestedSecurityToken>
538 <saml:Assertion
539 <saml:Assertion
540 AssertionID="_a75adf55-01d7-40cc-929f-dbd8372ebdfc"
541 IssueInstant="2005-04-17T00:46:02Z"
542 Issuer="www.opensaml.org"
543 MajorVersion="1"
544 MinorVersion="1"
545 Xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
546 xmlns:xsd="http://www.w3.org/2001/XMLSchema"
547 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
548 <saml:Conditions
549 NotBefore="2005-04-17T00:46:02Z"
550 NotOnOrAfter="2005-04-17T00:51:02Z">
551 </saml:Conditions>
552 <saml:AuthenticationStatement
553 AuthenticationInstant="2003-04-17T00:46:00Z"
554 AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:password">
555 <saml:Subject>
556 <saml:NameIdentifier
557 Format="urn:oasis:names:tc:SAML:1.1:nameid-
558 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

559       scott@example.org</NameIdentifier>  
560       <saml:SubjectConfirmation>  
561        <saml:ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:bearer  
562        </saml:ConfirmationMethod>  
563        </saml:SubjectConfirmation>  
564       </saml:Subject>  
565       </saml:AuthenticationStatement>  
566 <ds:Signature  
567 xmlns:ds="http://www.w3.org/2000/09/xmldsig#">  
568   <ds:SignedInfo>  
569    <ds:CanonicalizationMethod  
570    Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />  
571    <ds:SignatureMethod  
572    Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />  
573    <ds:Reference  
574    URI="#\_a75adf55-01d7-40cc-929f-dbd8372ebdfc">  
575      <ds:Transforms>  
576      <ds:Transform  
577      Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />  
578      <ds:Transform  
579      Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />  
580      <InclusiveNamespaces  
581      PrefixList="#default saml samlp ds xsd xsi"  
582      xmlns="http://www.w3.org/2001/10/xml-exc-c14n#" />  
583      </ds:Transform>  
584      </ds:Transforms>  
585      <ds:DigestMethod  
586      Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />  
587      <ds:DigestValue>Kclet6XcaOgOWXM4gty6/UNdviI=</ds:DigestValue>  
588      </ds:Reference>  
589      </ds:SignedInfo>  
590      <ds:SignatureValue>  
591      hq4zk+ZknjggCQgZm7ea8fI79gJEsRy3E8LHDpYXWQIgZpkJN9CMLG8ENR4Nrw+n  
592      7iyzixBvKXX8P53BTCT4VghPBWhFYSt9tHWu/AtJfOTh6qaAsNdeCyG86jmt3TD  
593      MWuL/cBUj2OtBZOQMFN7jQ9YB7klIz3RqVL+wNmEwi4=</ds:SignatureValue>  
594      <ds:KeyInfo>  
595      <ds:X509Data>  
596      <ds:X509Certificate>  
597      MIICyCCAJQgAwIBAgICAnUwDQYJKoZIhvcNAQEEBQAwgakkCzAJBgNVBAYTA1VT  
598      MRlWEAYDVQQQIEwlcXZlbn25zaW4xEDAObgNVBACTB01hZG1zb24xIDAeBgNVBAoT  
599      FlVuaXZlcnNpdHk2YyV21zY29uc2luMSswKQYDVQQLEyJEaXZpc2lubiBvZiBJ  
600      bmZvcmlhdG1vb1BUZWN0bm9sb2d5MSUwIwYDVQQDExxIRVBLSsBTZXJ2ZXIqQ0Eg  
601      LS0gMjAwMjA3MDFBMB4XDyMDcyNjA3Mjc1MVoXDTA2MDkwNDA3Mjc1MVoqYsxCz  
602      AJBgNVBAYTA1VTMRlWEAYDVQQQIEwlcXZlbn25zaW4xEDAObgNVBACTB01hZG1zb24x  
603      IDZ1Z3RqVL+wNmEwi4=</ds:X509Certificate>  
597      MIICyCCAJQgAwIBAgICAnUwDQYJKoZIhvcNAQEEBQAwgakkCzAJBgNVBAYTA1VT  
598      MRlWEAYDVQQQIEwlcXZlbn25zaW4xEDAObgNVBACTB01hZG1zb24xIDAeBgNVBAoT  
599      FlVuaXZlcnNpdHk2YyV21zY29uc2luMSswKQYDVQQLEyJEaXZpc2lubiBvZiBJ  
600      bmZvcmlhdG1vb1BUZWN0bm9sb2d5MSUwIwYDVQQDExxIRVBLSsBTZXJ2ZXIqQ0Eg  
601      LS0gMjAwMjA3MDFBMB4XDyMDcyNjA3Mjc1MVoXDTA2MDkwNDA3Mjc1MVoqYsxCz  
602      AJBgNVBAYTA1VTMRlWEAYDVQQQIEwlcXZlbn25zaW4xEDAObgNVBACTB01hZG1zb24x  
603      IDZ1Z3RqVL+wNmEwi4=</ds:X509Certificate>

```

604 dTEncUCUGCSqGSIB3DQeJARYYcm9vdEBzaG1iMS5pbmRlcm5ldDIuZWRLMIGfMA0G
605 CSqGSIB3DQeEBAQUAA4GNADCBiQKBgQDZSAb2sxxvhAXnXVIVTx8vuRay+x50z7GJj
606 IHRYQgIv6IqaGG04eTcyVMhoeke0b45QgvBiaOAPSZB113R6+KYiE7x4XAWIrCP+
607 c2MZVeXeTgV3Yz+USLg2Y1on+Jh4HxwkPFmZBctyXiUr6DxF8rvoP9W7O27rhRjE
608 pmqOIfGTWQIDAQABox0wGzAMBgNVHRMBAf8EAjAAMAsGA1UdDwQEAwIFoDANBgkq
609 hkiG9w0BAQQFAAOBgQBfDqEW+OI3jqBQHIBzhujN/Pizdn7s/z4D5d3pptWDJf2n
610 qgi7lFV6MDkhmTvTqBtjmNk3No7v/dnP6Hr7wHxvCCRwubnmIfZ6QZAv2FU78pLX
611 8I3bsbmRAUg4UP9hH6ABVq4KQKMknxulxQxLhpRly1GPdiowMNTREg8cCx3w/w==
612 </ds:X509Certificate>
613 </ds:X509Data>
614 </ds:KeyInfo>
615 </ds:signature>
616     </saml:Assertion>
617     </t:RequestedSecurityToken>
618     </t:SecurityTokenResponse>
619     <t:RequestSecurityTokenResponseCollection>
620 </soap:Body>
621 </soap:Envelope>

```

622

### 623 3.3. Certificate for SAML 1.1 HoK Token, WSS 1.0

624 This binding is used in scenario 3.

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

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

#### 633 Expected Security Properties

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

#### 636 Agreements

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

#### 639 Acceptable <wsa:EndpointReference> Values

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

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

642 **Request Message**

643 **Message Creation**

644 **Security**

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

646 **BinarySecurityToken**

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

649 **Body**

650 **RequestSecurityToken**

651 **TokenType**

652 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>

654 **RequestType**

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

657 **AppliesTo**

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

660 **KeyType**

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

663 **Message Processing**

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

666 The value of the <SubjectConfirmation>/<ds:KeyInfo> element in the SAML assertion is a  
667 <ds:X509Data> element with a <ds:X509Certificate> sub-element. The base-64 certificate value is taken  
668 from the security header of the request message. The <SubjectConfirmation>/<ConfirmationMethod>  
669 element is set to urn:oasis:names:tc:SAML:1.0:cm:holder-of-key.

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

672 **Example (Non-normative)**

673 Here is an example request.

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

```

678 xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
679 wssecurity-secext-1.0.xsd"
680 xmlns:wst="http://docs.oasis-open.org/ws-sx/ws-trust/200512"
681 >
682
683 <soap:Header>
684   <wsse:Security soap:mustUnderstand="1">
685     <wsse:BinarySecurityToken
686       wsu:Id="binarytoken"
687       ValueType="...#X509v3"
688       EncodingType="...#Base64Binary">
689       MIIEZzCCA9CgAwIBAgIQEmtJZc0...
690     </wsse:BinarySecurityToken>
691   </wsse:Security>
692 </soap:Header>
693 <soap:Body>
694 <t:RequestSecurityToken>
695   <t:TokenType>
696     http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-
697 1.0#SAMLV1.1
698   </t:TokenType>
699   <t:RequestType>
700     http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue
701   </t:RequestType>
702   <wsp:AppliesTo
703 xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/03/addressing">
704     <wsa:EndpointReference>
705       <wsa:Address>http://www.example.org/</wsa:Address>
706     </wsa:EndpointReference>
707   </wsp:Appliesto>
708   <t:KeyType>
709     http://docs.oasis-open.org/ws-sx/wstrust/200512/PublicKey
710   </t:KeyType>
711 </t:RequestSecurityToken>
712 </soap:Body>
713 </soap:Envelope>

```

714 [Policy](#)

715 [Note this policy statement assumes the use of SSL as indicated in the Note above.](#)

```

716
717 <wsp:Policy>
718   <sp:TransportBinding />
719   <sp:X509Token
720     sp:IncludeToken='http://docs.oasis-open.org/ws-sx/ws-
721 securitypolicy/200512/IncludeToken/Always' />
722 </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

```
723 <sp:WssX509V3Token11 />
724 </wsp:Policy>
725 </sp:X509Token>
726 </wsp:Policy>
```

## 727 Response Message

### 728 Message Creation

#### 729 Body

#### 730 RequestSecurityTokenResponseCollection/RequestSecurityTokenResponse

#### 731 TokenType

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

#### 734 AppliesTo

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

#### 736 Lifetime

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

#### 738 RequestedSecurityToken

#### 739 Assertion

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

### 746 Message Processing

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

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

### 752 Example (Non-normative)

753 Here is an example response.

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

```

760 </soap:Header>
761 <soap:Body wsu:Id="body"
762 xmlns:wsu="http://schemas.xmlsoap.org/ws/2003/06/utility">
763 <t:RequestSecurityTokenResponseCollection>
764 <t:RequestSecurityTokenResponse>
765 <t:TokenType>
766 http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0#SAMLV1.1
767 </t:TokenType>
768 <wsp:AppliesTo
769 xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/03/addressing">
770 <wsa:EndpointReference>
771 <wsa:Address>http://www.example.org/</wsa:Address>
772 </wsa:EndpointReference>
773 <wsp:AppliesTo>
774 <t:Lifetime>
775 <wsu:Created>"2005-04-17T00:46:02Z"</wsu:Created>
776 <wsu:Expires>"2005-04-17T00:51:02Z"</wsu:Expires>
777 </t:Lifetime>
778
779 <t:RequestedSecurityToken>
780 <saml:Assertion
781 AssertionID="_a75adf55-01d7-40cc-929f-dbd8372ebdfc"
782 IssueInstant="2005-04-17T00:46:02Z"
783 Issuer="www.opensaml.org"
784 MajorVersion="1"
785 MinorVersion="1"
786 Xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
787 xmlns:xsd="http://www.w3.org/2001/XMLSchema"
788 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
789 <saml:Conditions
790 NotBefore="2005-04-17T00:46:02Z"
791 NotOnOrAfter="2005-04-17T00:51:02Z">
792 </saml:Conditions>
793 <saml:AuthenticationStatement
794 AuthenticationInstant="2003-04-17T00:46:00Z"
795 AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:Unspecified">
796 <saml:Subject>
797 <saml:NameIdentifier
798 Format="urn:oasis:names:tc:SAML:1.1:nameid-
799 format:emailAddress">
800 scott@example.org</NameIdentifier>
801 <saml:SubjectConfirmation>
802 <saml:ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:holder-of-
803 key
804 </saml:ConfirmationMethod>
805 <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





```

852 Ym9yMQ4wDAYDVQQKEwVVQ0FJRDEcMBoGAlUEAxMTc2hpYjEuaW50ZXJuZXQyLmVk
853 dTEhMCUGCSqGSIB3DQEJARYYcm9vdEBzaGlMS5pbhR1cm5ldDIuZWRR1MIGfMA0G
854 CSqGSIB3DQEBAQUAA4GNADCBiQKBgQDZSAb2sxvhAXnXVIVTx8vuRay+x50z7GJj
855 IHRYQgIv6IqaGG04eTcyVMhoeke0b45QgvBiaOAPSZB113R6+KYiE7x4XAWIrCP+
856 c2MZVeXeTgV3Yz+USLg2Y1on+Jh4HxwkPFmZBctyXiUr6DxF8rvoP9W7O27rhRjE
857 pmqOI fGTWQIDAQABox0wGzAMBgNVHRMBAf8EAjAAMAsGA1UdDwQEAwIFoDANBgkq
858 hkiG9w0BAQQFAAOBgQBfDqEW+OI3jqBQHIBzhujN/PizdN7s/z4D5d3pptWDJf2n
859 qgi7lFV6MDkhhTvtqBtjmNk3No7v/dnP6Hr7wHxvCCRwubnmIfZ6QZAv2FU78pLX
860 8I3bsbmRAUg4UP9hH6ABVq4KQKMknxulxQxLhpR1y1GPdiowMNTREg8cCx3w/w==
861 </ds:X509Certificate>
862 </ds:X509Data>
863 </ds:KeyInfo>
864 </ds:signature>
865     </saml:Assertion>
866     </t:RequestedSecurityToken>
867     </t:RequestSecurityTokenResponse>
868     <t:RequestSecurityTokenResponseCollection>
869 </soap:Body>
870 </soap:Envelope>

```

### 871 3.4. Mutual Certificate, WSS1.0

872 This binding is used in Scenario 4.

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

#### 878 Expected Security Properties

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

#### 881 Agreements

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

#### 884 Acceptable <wsa:EndpointReference> Values

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

#### 887 Request Message

#### 888 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

889 *Security*

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

891 **BinarySecurityToken**

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

894 **Body**

895 **RequestSecurityToken**

896 **TokenType**

897 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>.

899 **RequestType**

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

902 **AppliesTo**

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

905 **KeyType**

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

908 *Message Processing*

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

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

913 *Example (Non-normative)*

914 Here is an example request.

```
915 <s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope"
916   xmlns:a="http://schemas.xmlsoap.org/ws/2004/08/addressing"
917   xmlns:e="http://www.w3.org/2001/04/xmlenc#"
918   xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
919   wssecurity-utility-1.0.xsd"
920   xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
921   wssecurity-secext-1.0.xsd"
922 >
923   <s:Header>
924     <a:Action s:mustUnderstand="1" u:Id="_3">
925       http://docs.oasis-open.org/ws-sx/ws-trust/200512/RST/Issue
926     </a:Action>
```

```

927 <a:MessageID u:Id="_4">
928 urn:uuid:85836182-3ef8-4efc-a93f-06466277053e
929 </a:MessageID>
930 <a:ReplyTo u:Id="_5">
931 <a:Address>
932 http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous
933 </a:Address>
934 </a:ReplyTo>
935 <a:To s:mustUnderstand="1" u:Id="_6">
936 http://server.example.com/STS/Scenario4
937 </a:To>
938 <o:Security s:mustUnderstand="1">
939 <u:Timestamp u:Id="uuid-c3cdb38b-e4aa-4467-9d0e-dd30f081e08d-5">
940 <u:Created>2005-10-24T15:51:44.664Z</u:Created>
941 <u:Expires>2005-10-24T15:56:44.664Z</u:Expires>
942 </u:Timestamp>
943 <o:BinarySecurityToken u:Id="uuid-c3cdb38b-e4aa-4467-9d0e-dd30f081e08d-
944 2"
945 ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
946 x509-token-profile-1.0#X509v3"
947 EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
948 wss-soap-message-security-1.0#Base64Binary">
949 MIIDDDCCAfSgAwIBAgIQM6YEf7FVYx/tZyEXgVComTANBgkqhkiG9w0BAQUFADAwMQ4wDAYDVQQKD
950 AVPQVNJUZeEMBwGA1UEAwVTOFTSVMgSW50ZXJvcCBUZXN0IENBMB4XDTA1MDMxOTAwMDAwMFoXDT
951 E4MDMxOTIzNTk1OVowQjEOMAwGA1UECgwFT0FTSVMxIDAeBgNVBAsMF09BU01TIEludGVyb3AgVG
952 zdCBDZXR0MjQ4wDAYDVQDDAVBGljZTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwGyKCGYEAoqi99Byl
953 VYo0aHrkKCNT4DkIgL/SgahbeKdGhrbu3K2XG7arFD9tqIBIKMfrX4Gp90NJa85AVlyiNsEyyq+m
954 UnMpNcKnLXL0jkTmMCQDYbbkehJlXPnaWLzve+mW0pJdPxtf3rbd4PS/cBQIvtpjmrDAU8VsZKT8D
955 N5Kyz+EZsCAwEAAaOBkzCBkDAJBGNVHRMEAjaAMDMGA1UdHwQSMCowKkImhiRodHRwoi8vaW50ZXJ
956 vcC5iYnRlc3QubmV0L2NybC9jYS5jcmwwDgYDVR0PAQH/BAQDAgSwMBOGA1UdDgQWBQBK410TUHZ1
957 QV3V2Qt1LNDm+PoxiDAfBgNVHSMEGDAwBTAnSj8wes1oR3WqqgqgHBpNwkkPDzANBgkqhkiG9w0BA
958 QUFAAOCAQEABTqpOpvW+6yrLXyUlP2xJbEkohXHI5OWwKW1eOb9h1khWntUalfcFOJAgUyH30TPh
959 ldzx1+vK2LPzhoUFKYHE1IyQvokBN2JjFO64BQuCKnZhlDLRpXGhfktDxQgdf5rCK/wh3xVsZCNT
960 fuMNmlAM61OAg8QduDah3WFZpEA0s2nwQaCNQTMjJC8tav1CB6r6+E5FAMwPXP7pJxn9Fw9OXRYqb
961 RA4v2y7YpbGkG2GI9UvOHw6SGvf4FRsthMMO35YbpikGsLix3vAsXWwi4rwwfVOYzQK0OFPNi9RMCU
962 dSH06m9uLWckiCxjos0FQODZE914ATGy9s9hNVwryOJTw==
963 </o:BinarySecurityToken>
964 <e:EncryptedKey Id="_0">
965 <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-
966 oaep-mgf1p"/>
967 <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
968 <o:SecurityTokenReference>
969 <o:KeyIdentifier
970 ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
971 wss-x509-token-profile-1.0#X509SubjectKeyIdentifier">
972 Xeg55vRyK3ZhAEhEf+YT0z986L0=
973 </o:KeyIdentifier>
974 </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

```

975     </KeyInfo>
976     <e:CipherData>
977         <e:CipherValue>
978
979 WncUubWi8BGtzjt9BFnEcr53ktqQiEkJWjkkxIkRnE3oEWRcceluOrwAVDxobKLO2Xz8x3NjQliRi
980 Hq1MCuykFgACHIXcy7+odeW5deWSDf7nwlg/9iaVC+bUuYttuhHVC3uw3z+J143LQr4gwL5tnzzCB
981 Ux9WOkA6AShPbtEL8=
982         </e:CipherValue>
983     </e:CipherData>
984     <e:ReferenceList>
985         <e:DataReference URI="#_2"/>
986     </e:ReferenceList>
987 </e:EncryptedKey>
988 <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
989     <SignedInfo>
990         <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-
991 exc-c14n#" />
992         <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
993 sha1" />
994         <Reference URI="#_1">
995             <Transforms>
996                 <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
997 c14n#" />
998             </Transforms>
999             <DigestMethod
1000 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
1001                 <DigestValue>Ha9+qHnkvikYdjG/XJjQZqAxVCA=</DigestValue>
1002             </Reference>
1003             <Reference URI="#_3">
1004                 <Transforms>
1005                     <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
1006 c14n#" />
1007                 </Transforms>
1008                 <DigestMethod
1009 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
1010                     <DigestValue>FwiFAUuqNDo9SDkk5A28Mg7Pa8Q=</DigestValue>
1011                 </Reference>
1012             <Reference URI="#_4">
1013                 <Transforms>
1014                     <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
1015 c14n#" />
1016                 </Transforms>
1017                 <DigestMethod
1018 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
1019                     <DigestValue>jtGbn/BVKmfw6r9SP4a8jDKOzhI=</DigestValue>
1020                 </Reference>

```

```

1021     <Reference URI="#_5">
1022         <Transforms>
1023             <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
1024 c14n#"/>
1025         </Transforms>
1026         <DigestMethod
1027 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
1028             <DigestValue>KIK3vklFN1QmMdQkplq2azfzrzg=</DigestValue>
1029         </Reference>
1030     <Reference URI="#_6">
1031         <Transforms>
1032             <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
1033 c14n#"/>
1034         </Transforms>
1035         <DigestMethod
1036 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
1037             <DigestValue>APDSt42iUyZB8B+3UcRfv9fR0dU=</DigestValue>
1038         </Reference>
1039     <Reference URI="#uuid-c3cdb38b-e4aa-4467-9d0e-dd30f081e08d-5">
1040         <Transforms>
1041             <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
1042 c14n#"/>
1043         </Transforms>
1044         <DigestMethod
1045 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
1046             <DigestValue>4a8Vc8wN+esJrUNSumktT4GGHnw=</DigestValue>
1047         </Reference>
1048     </SignedInfo>
1049     <SignatureValue>
1050 Gj8zD5HubAVSpPxJ72auHS+Wb7E7J3LETvqufcg/cyGNoAhiXO3q126KwR9P1HchF9XU6ofaqcMDu
1051 /THkHYFQwOytEme4lzggN/aDMbVW03XzES+GtuWSifYmszufYu9C0C5Vb7liFw1oxPCXhFDj7sN+M
1052 5TYbQG1l2FoR6GGQIQ=
1053     </SignatureValue>
1054     <KeyInfo>
1055         <o:SecurityTokenReference>
1056             <o:Reference
1057                 ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
1058 wss-x509-token-profile-1.0#X509v3"
1059                 URI="#uuid-c3cdb38b-e4aa-4467-9d0e-dd30f081e08d-2"/>
1060             </o:SecurityTokenReference>
1061         </KeyInfo>
1062     </Signature>
1063 </o:Security>
1064 </s:Header>
1065 <s:Body u:Id="_1">
1066     <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

```

1067 <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-
1068 cbc"/>
1069 <e:CipherData>
1070 <e:CipherValue>
1071 <!-- base64 encoded octets with encrypted RST request-->
1072 <!-- Unencrypted form: -->
1073 <!--
1074 <t:RequestSecurityToken>
1075 <t:RequestType>
1076 http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue
1077 </t:RequestType>
1078 <t:Entropy>
1079 <t:BinarySecret u:Id="uuid-4acf589c-0076-4a83-8b66-5f29341514b7-3"
1080 Type="http://docs.oasis-open.org/ws-sx/ws-
1081 trust/200512/Nonce">Uv38QLxDQM9gLoDZ6OwYDiFk094nmwu3Wmay7EdKmhw=</t:BinarySec
1082 ret>
1083 </t:Entropy>
1084 <t:KeyType>http://docs.oasis-open.org/ws-sx/ws-
1085 trust/200512/SymmetricKey</t:KeyType>
1086 <t:KeySize>256</t:KeySize>
1087 <t:ComputedKeyAlgorithm>
1088 http://docs.oasis-open.org/ws-sx/ws-trust/200512/CK/PSHA1
1089 </t:ComputedKeyAlgorithm>
1090 </t:RequestSecurityToken>
1091 -->
1092 </e:CipherValue>
1093 </e:CipherData>
1094 </e:EncryptedData>
1095 </s:Body>
1096 </s:Envelope>

```

## 1097 [Policy](#)

1098 [Note, client token is not sent in request, only wrapped key according to note above. Note also that no](#)  
1099 [algorithms were specified for this interop, so policy makes no statements.](#)

```

1100
1101 <wsp:Policy>
1102 <sp:SymmetricBinding>
1103 <wsp:Policy>
1104 <sp:ProtectionToken>
1105 <wsp:Policy>
1106 <sp:X509Token
1107 sp:IncludeToken='http://docs.oasis-open.org/ws-sx/ws-
1108 securitypolicy/200512/IncludeToken/Never' />
1109 </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

```
1110     <sp:WssX509V3Token11 />
1111     </wsp:Policy>
1112 </wsp:Policy>
1113 </sp:ProtectionToken>
1114 <sp:SignBeforeEncrypting />
1115 <sp:EncryptSignature />
1116 </wsp:Policy>
1117 </sp:SymmetricBinding>
1118 </wsp:Policy>
```

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

#### 1119 Response Message

#### 1120 Message Creation

#### 1121 Body

#### 1122 RequestSecurityTokenResponseCollection/RequestSecurityTokenResponse

#### 1123 TokenType

1124 The <t:TokenType> element value MUST be equal to [http://docs.oasis-open.org/wss/oasis-wss-saml-](http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0#SAMLV1.1)  
1125 [token-profile-1.0#SAMLV1.1](http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0#SAMLV1.1)

Unknown  
Field Code Changed

#### 1126 AppliesTo

1127 If present, the <wsp:AppliesTo> element contents MUST be identical to that found in the RST message.

#### 1128 Lifetime

1129 A <t:Lifetime> element MUST be present.

#### 1130 RequestedSecurityToken

1131 A SAML 1.1 Assertion MUST be returned.

#### 1132 Message Processing

1133 The requestor must check to see if all elements noted as mandatory are present in the response. It must  
1134 further verify that values for <t:TokenType> and <wsp:AppliesTo> are set as required above.

#### 1135 Example (Non-normative)

1136 Here is an example response.

```
1137 <s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope"
1138   xmlns:a="http://schemas.xmlsoap.org/ws/2004/08/addressing"
1139   xmlns:e="http://www.w3.org/2001/04/xmlenc#"
1140   xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
1141   wssecurity-utility-1.0.xsd"
1142   xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
1143   wssecurity-secext-1.0.xsd"
1144 >
1145 <s:Header>
1146 <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



```

1147     http://docs.oasis-open.org/ws-sx/ws-trust/200512/RSTRC/IssueFinal
1148 </a:Action>
1149 <a:RelatesTo u:Id="_4">
1150     urn:uuid:85836182-3ef8-4efc-a93f-06466277053e
1151 </a:RelatesTo>
1152 <a:To s:mustUnderstand="1" u:Id="_5">
1153     http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous
1154 </a:To>
1155 <o:Security s:mustUnderstand="1">
1156     <u:Timestamp u:Id="uuid-78c746a2-3ec4-4cf8-a913-50d2f7334cf9-34">
1157         <u:Created>2005-10-24T15:51:47.025Z</u:Created>
1158         <u:Expires>2005-10-24T15:56:47.025Z</u:Expires>
1159     </u:Timestamp>
1160     <e:EncryptedKey Id="_0" >
1161         <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-
1162 oaep-mgf1p"/>
1163         <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
1164             <o:SecurityTokenReference>
1165                 <o:KeyIdentifier
1166                     ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
1167 wss-x509-token-profile-1.0#X509SubjectKeyIdentifier"
1168                     EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-
1169 200401-wss-soap-message-security-1.0#Base64Binary">
1170                         CuJdE1B2dUFd1dkLZSzQ5vj6MYg=
1171                     </o:KeyIdentifier>
1172                 </o:SecurityTokenReference>
1173             </KeyInfo>
1174             <e:CipherData>
1175                 <e:CipherValue>
1176 Mvb294ZmtQu7pA4YAyRxPYeEUFMB8ZDIIDhsActVzF2kFacaVMHo2I1loBOC17CWDix1NI3qiA9wvt
1177 FDsQzK2unaSULI+KzjEwAkIWma7eH/j2xKvhaRsQjxcF+A6VuEWA7fXoY1A2Rt1cwACiVqKtdqSYF
1178 EWvxxdTahjVG2o80k=
1179                 </e:CipherValue>
1180             </e:CipherData>
1181             <e:ReferenceList>
1182                 <e:DataReference URI="#_2"/>
1183             </e:ReferenceList>
1184         </e:EncryptedKey>
1185     <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
1186         <SignedInfo>
1187             <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-
1188 exc-c14n#"/>
1189             <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
1190 sha1"/>
1191             <Reference URI="#_1">

```

```
1193     <Transforms>
1194         <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
1195 c14n#" />
1196     </Transforms>
1197     <DigestMethod
1198 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
1199     <DigestValue>o2h+mu3Hj7xU/6RHqDhb57oJpJU=</DigestValue>
1200 </Reference>
1201 <Reference URI="#_3">
1202     <Transforms>
1203         <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
1204 c14n#" />
1205     </Transforms>
1206     <DigestMethod
1207 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
1208     <DigestValue>627rTKmQ6nuQSHGO+I5uyKXh2yY=</DigestValue>
1209 </Reference>
1210 <Reference URI="#_4">
1211     <Transforms>
1212         <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
1213 c14n#" />
1214     </Transforms>
1215     <DigestMethod
1216 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
1217     <DigestValue>bt5N+ngBdN+BsJlowpaRrntL3X8=</DigestValue>
1218 </Reference>
1219 <Reference URI="#_5">
1220     <Transforms>
1221         <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
1222 c14n#" />
1223     </Transforms>
1224     <DigestMethod
1225 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
1226     <DigestValue>VEzxbS+q/5Oj04P4Ywk/YZmQvxo=</DigestValue>
1227 </Reference>
1228 <Reference URI="#uuid-78c746a2-3ec4-4cf8-a913-50d2f7334cf9-34">
1229     <Transforms>
1230         <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
1231 c14n#" />
1232     </Transforms>
1233     <DigestMethod
1234 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
1235     <DigestValue>oQ15WMehxnMzOSRut4A/1Oz8wHY=</DigestValue>
1236 </Reference>
1237 </SignedInfo>
1238 <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

```

1239 f130H+2aHcff0izaj+zc2NXue3mIgnM4W+cNT4TXPvNmOunWHWXij55YcPEjq8tXBQ2xSVkk0iii/
1240 PUiXpZ/awiJbgTxe7EX0nJrNA81UYOCZsAkca8La5lNzd3f6jZXFqZj6p2DwjKmHg7bPZDy+sn8Ri
1242 yveevoPIVqSqTF2po=
1243     </SignatureValue>
1244     <KeyInfo>
1245         <o:SecurityTokenReference>
1246             <o:KeyIdentifier
1247                 ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
1248 wss-x509-token-profile-1.0#X509SubjectKeyIdentifier"
1249                 EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-
1250 200401-wss-soap-message-security-1.0#Base64Binary">
1251                     Xeg55vRyK3ZhAEhEf+YT0z986L0=
1252                 </o:KeyIdentifier>
1253             </o:SecurityTokenReference>
1254         </KeyInfo>
1255     </Signature>
1256 </o:Security>
1257 </s:Header>
1258 <s:Body u:Id="_1">
1259     <e:EncryptedData Id="_2" Type="http://www.w3.org/2001/04/xmlenc#Content">
1260     <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-
1261 cbc"/>
1262     <e:CipherData>
1263     <e:CipherValue>
1264         <!--base64 encoded octets of encrypted RSTR-->
1265         <!--
1266     <t:RequestSecurityTokenResponseCollection>
1267     <t:RequestSecurityTokenResponse>
1268     <t:TokenType>http://docs.oasis-open.org/wss/oasis-wss-saml-token-
1269 profile-1.1#SAMLV1.1</t:TokenType>
1270     <t:KeySize>256</t:KeySize>
1271     <t:RequestedAttachedReference>
1272     <o:SecurityTokenReference>
1273     <o:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/oasis-
1274 wss-saml-token-profile-1.0#SAMLAssertionID">uuid-8222b7a2-3874-4884-bdb5-
1275 9c2ddd4b86b5-16</o:KeyIdentifier>
1276     </o:SecurityTokenReference>
1277     </t:RequestedAttachedReference>
1278     <t:RequestedUnattachedReference>
1279     <o:SecurityTokenReference>
1280     <o:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/oasis-
1281 wss-saml-token-profile-1.0#SAMLAssertionID">uuid-8222b7a2-3874-4884-bdb5-
1282 9c2ddd4b86b5-16</o:KeyIdentifier>
1283     </o:SecurityTokenReference>
1284     </t:RequestedUnattachedReference>

```

```

1285     <t:Lifetime>
1286         <u:Created>2005-10-24T20:19:26.526Z</u:Created>
1287         <u:Expires>2005-10-25T06:24:26.526Z</u:Expires>
1288     </t:Lifetime>
1289     <t:RequestedSecurityToken>
1290         <saml:Assertion MajorVersion="1" MinorVersion="1" AssertionID="uuid-
1291 8222b7a2-3874-4884-bdb5-9c2ddd4b86b5-16" Issuer="Test STS"
1292 IssueInstant="2005-10-24T20:24:26.526Z"
1293 xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion">
1294         <saml:Conditions NotBefore="2005-10-24T20:19:26.526Z"
1295 NotOnOrAfter="2005-10-25T06:24:26.526Z">
1296             </saml:Conditions>
1297             <saml:Advice>
1298             </saml:Advice>
1299             <saml:AttributeStatement>
1300                 <saml:Subject>
1301                     <saml:SubjectConfirmation>
1302
1303 <saml:ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:holder-of-
1304 key</saml:ConfirmationMethod>
1305                 <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
1306                     <e:EncryptedKey
1307 xmlns:e="http://www.w3.org/2001/04/xmlenc#">
1308                         <e:EncryptionMethod
1309 Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
1310                         </e:EncryptionMethod>
1311                         <KeyInfo>
1312                             <o:SecurityTokenReference xmlns:o="http://docs.oasis-
1313 open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
1314                                 <o:KeyIdentifier ValueType="http://docs.oasis-
1315 open.org/wss/oasis-wss-wssecurity-secext-
1316 1.1.xsd#ThumbprintSHA1">NQMOIBvuplAtETQvk+6gn8C13wE=</o:KeyIdentifier>
1317                             </o:SecurityTokenReference>
1318                         </KeyInfo>
1319                         <e:CipherData>
1320
1321 <e:CipherValue>EEcYjwNoYcJ+20xTYE5e/fixl5K0gzgrfaYAxDfV/VXiuKf1084h8PmogTfM+
1322 azcgAfmArVQvOyKwXRb5vmXYfVHLlhZTbXacy+nowSUNnEjp37VDbI3RJ5k6tBHF+ow0NM/P6GPNZ
1323 9ZqJiilGDgWJkFsJzNZXNbbMgwuFu3cA=</e:CipherValue>
1324                         </e:CipherData>
1325                     </e:EncryptedKey>
1326                 </KeyInfo>
1327             </saml:SubjectConfirmation>
1328         </saml:Subject>
1329     </saml:AttributeStatement>
1330     <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
1331         <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

```

1332         <CanonicalizationMethod
1333 Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
1334         </CanonicalizationMethod>
1335         <SignatureMethod
1336 Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1">
1337         </SignatureMethod>
1338         <Reference URI="#uuid-8222b7a2-3874-4884-bdb5-9c2ddd4b86b5-16">
1339         <Transforms>
1340         <Transform
1341 Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature">
1342         </Transform>
1343         <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
1344 c14n#">
1345         </Transform>
1346         </Transforms>
1347         <DigestMethod
1348 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
1349         </DigestMethod>
1350         <DigestValue>7nHBrFPsm+LEFAoV4NoQPoEl5Lk=</DigestValue>
1351         </Reference>
1352     </SignedInfo>
1353     <SignatureValue>TugV4pTIwCH87bLD4jiMgVGtkbRBt1tRlHXJArL34A/YfA4AnGBLXB4pJdUsU
1354 xMUtbQl4PoGgEsdLNg8C77peARELGP1/Tqw7T3u5zBYHxCHCiV2FWBBfeOmwJmqoaBf8XZJ4AlyqP
1355 q6lP6ljrQjZJafpHuYpAZnZQsvsiJaBPQ=</SignatureValue>
1356     <KeyInfo>
1357     <o:SecurityTokenReference xmlns:o="http://docs.oasis-
1358 open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
1359     <o:KeyIdentifier ValueType="http://docs.oasis-
1360 open.org/wss/oasis-wss-wssecurity-secext-
1361 1.1.xsd#ThumbprintSHA1">NQM0IBvuplAtETQvk+6gn8C13wE=</o:KeyIdentifier>
1362     </o:SecurityTokenReference>
1363     </KeyInfo>
1364     </Signature>
1365     </saml:Assertion>
1366     </t:RequestedSecurityToken>
1367     <t:RequestedProofToken>
1368     <t:BinarySecret u:Id="uuid-8222b7a2-3874-4884-bdb5-9c2ddd4b86b5-
1369 14">zT8LWAUwUrIVKA/rkCr0kxLEmKAehcB6TGWJuAgucBM=</t:BinarySecret>
1370     </t:RequestedProofToken>
1371     </t:RequestSecurityTokenResponse>
1372     </t:RequestSecurityTokenResponseCollection>
1373     -->
1374     </e:CipherValue>
1375     </e:CipherData>
1376     </e:EncryptedData>
1377

```

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

1378 </s:Body>  
1379 </s:Envelope>

### 1380 **3.5. Mutual Certificate, WSS1.1**

1381 This binding is used in Scenarios 5 and 6.

1382 This mode requires WS-Security 1.1.

1383 Client and STS X509 certificates are used to authenticate client and STS respectively. Client sends  
1384 Request to STS signed using DKT1(K), then encrypted using a DKT2(K), K is ephemeral key protected  
1385 for STS's Certificate, DKT1(K) and DKT2(K) represent keys derived from K per WS-SecureConversation.  
1386 Signature corresponding to DKT1(K) is signed using Client's certificate. Response is signed using  
1387 DKT3(K), encrypted using DKT4(K).

#### 1388 **Expected Security Properties**

1389 Use of the service is restricted to authorized parties that can present a valid WSS 1.1 X.509  
1390 BinarySecurityToken.

#### 1391 **Agreements**

1392 This section describes the agreements that must be made, directly or indirectly between parties who wish  
1393 to interoperate beyond the common preconditions noted for all scenarios.

#### 1394 **Acceptable <wsa:EndpointReference> Values**

1395 The requestor and the STS must agree on at least one <wsa:EndpointReference> value on receipt of  
1396 which the STS can issue a SAML HoK assertion or SecureConversationToken.

#### 1397 **Request Message**

##### 1398 **Message Creation**

##### 1399 **Security**

1400 The Security element MUST contain the mustUnderstand="1" attribute.

##### 1401 **BinarySecurityToken**

1402 The security element MUST contain a BinarySecurityToken with a X.509 certificate that is encoded as  
1403 Base64 sequence. The ValueType attribute MUST be set to #X509v3.

##### 1404 **Body**

##### 1405 **RequestSecurityToken**

##### 1406 **TokenType**

1407 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>

##### 1410 **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

1411 The <t:RequestType> element value MUST be equal to [http://docs.oasis-open.org/ws-sx/ws-](http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue)  
1412 [trust/200512/Issue](http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue)

1413 **AppliesTo**

1414 If present, this element MUST include an <wsa:EndpointReference> element with a <wsa:Address> sub-  
1415 element. The value of the <wsa:Address> element should be known to the STS.

1416 **KeyType**

1417 The <t:KeyType> element value MUST be equal to [http://docs.oasis-open.org/ws-](http://docs.oasis-open.org/ws-sx/wstrust/200512/SymmetricKey)  
1418 [sx/wstrust/200512/SymmetricKey](http://docs.oasis-open.org/ws-sx/wstrust/200512/SymmetricKey)

1419 **Message Processing**

1420 This section describes the processing performed by the STS. It verifies that its local policy permits the  
1421 issuance of a SAML HoK assertion or SCT for the value of the <wsa:EndpointReference> found in the  
1422 message.

1423 If an error is detected, the STS MUST cease processing the message and report the fault with a value of  
1424 t:RequestFailed (other reasons for failure).

1425 **Example (Non-normative)**

1426 Here is an example request.

```
1427 <s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope"  
1428   xmlns:a="http://schemas.xmlsoap.org/ws/2004/08/addressing"  
1429   xmlns:e="http://www.w3.org/2001/04/xmlenc#"  
1430   xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-  
1431   wssecurity-secext-1.0.xsd"  
1432   xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-  
1433   wssecurity-utility-1.0.xsd"  
1434   >  
1435   <s:Header>  
1436     <a:Action s:mustUnderstand="1" u:Id="_3">  
1437       http://docs.oasis-open.org/ws-sx/ws-trust/200512/RST/Issue  
1438     </a:Action>  
1439     <a:MessageID u:Id="_4">  
1440       urn:uuid:04d386bf-f850-459e-918b-ad80f3d1e088  
1441     </a:MessageID>  
1442     <a:ReplyTo u:Id="_5">  
1443       <a:Address>  
1444         http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous  
1445       </a:Address>  
1446     </a:ReplyTo>  
1447     <a:To s:mustUnderstand="1" u:Id="_6">  
1448       http://server.example.com/STS/Scenarios5-6  
1449     </a:To>  
1450     <o:Security s:mustUnderstand="1">  
1451       <u:Timestamp u:Id="uuid-40f5bac7-f9af-4384-80db-cfab34263849-10">
```

```

1452     <u:Created>2005-10-25T00:47:36.144Z</u:Created>
1453     <u:Expires>2005-10-25T00:52:36.144Z</u:Expires>
1454     </u:Timestamp>
1455     <e:EncryptedKey Id="uuid-40f5bac7-f9af-4384-80db-cfab34263849-9">
1456     <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-
1457     oaep-mgflp"/>
1458     <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
1459     <o:SecurityTokenReference>
1460     <o:KeyIdentifier
1461     Value="http://docs.oasis-open.org/wss/oasis-wss-
1462     wssecurity-secext-1.1.xsd#ThumbprintSHA1">
1463     NQM0IBvuplAtETQvk+6gn8C13wE=
1464     </o:KeyIdentifier>
1465     </o:SecurityTokenReference>
1466     </KeyInfo>
1467     <e:CipherData>
1468     <e:CipherValue>
1469     <!--base64 encoded cipher-->
1470     </e:CipherValue>
1471     </e:CipherData>
1472     <e:ReferenceList>
1473     <e:DataReference URI="# 2"/>
1474     </e:ReferenceList> </e:EncryptedKey>
1475     <o:BinarySecurityToken u:Id="uuid-40f5bac7-f9af-4384-80db-cfab34263849-
1476     6"
1477     Value="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
1478     x509-token-profile-1.0#X509v3"
1479     EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
1480     wss-soap-message-security-1.0#Base64Binary">
1481     MIIDDDCCafSgAwIBAgIQM6Yef7FVyx/tZyEXgVComTANBgkqhkiG9w0BAQUFADAwMQ4wDAYDVQQKD
1482     AVPQVNJUzEeMBwGA1UEAwV0FTSVMgSW50ZXJvcCBUZXR0IENBMB4XDTA1MDMxOTAwMDAwMFOXDT
1483     E4MDMxOTIzNTk1OVowQjEOMAwGA1UECgwFT0FTSVMxIDAeBgNVBAsMF09BU01TIEludGVyY3AgVGV
1484     zdCBDZlJ0MQ4wDAYDVQQDDAVBbG1jZTcBnzANBgkqhkiG9w0BAQEFAAOBjQAwYkCgYEAoqi99By1
1485     VYo0aHrkKcNT4DkIgpL/SgahbeKdGhrbu3K2XG7arfD9tqIBIKmfrX4Gp90NJa85AV1yiNsEyyq+m
1486     UnMpNcKnLXLOjkTmMCqDYbbkehJlXPnaWLzve+mW0pJdPxtf3rbD4PS/cBQIvtpjmrDAU8VsZKT8D
1487     N5Kyz+EZsCAwEAAaOBkzCBkDAJBGNVHRMEAJAAMDGA1UdHwQsMCowKKImhiRodHRwOi8vaW50ZXJ
1488     vcC5iYnRlc3QubmV0L2Nybc9jYS5jcmwwDgYDVDR0PAQH/BAQDAGSwMB0GA1UdDgQWBQBK410TUHZ1
1489     QV3V2Qt1LNDm+PoxiDAfBgNVHSMGDAWgBTAnSj8wes1oR3WqqgqgHBpNwkkPDzANBgkqhkiG9w0BA
1490     QUFAAOCAQEABTqpOpvW+6yrLXyU1P2xJbEkohXHI5OWwKW1eOb9h1khWntUalfcFOJAgUyH30TtPh
1491     ldzx1+vK2LPzhoUFKYHE1IyQvokBN2JjF064BQukCKnZhlDLRPxGhfktDxQgd5rCK/wh3xVsZCNT
1492     fuMNMlAM61OAg8QduDah3WFZpEA0s2nwQaCNQTNmjJC8tav1CBr6+E5FAMwPXP7pJxn9Fw9OXRyqb
1493     RA4v2y7YpbGkG2GI9UvOHw6SGvf4FRsthMMO35YbpikGsLix3vAsXWw14rxfVOYzQK00FPNi9RMCU
1494     dSH06m9uLWckiCjos0FQODZE914ATGy9s9hNVwryOJTw==
1495     </o:BinarySecurityToken>
1496     <Signature Id="_0" xmlns="http://www.w3.org/2000/09/xmldsig#">
1497     <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



```
1499     <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-
1500 exc-c14n#" />
1501     <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#hmac-
1502 sha1" />
1503         <Reference URI="#_1">
1504             <Transforms>
1505                 <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
1506 c14n#" />
1507             </Transforms>
1508             <DigestMethod
1509 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
1510                 <DigestValue>VX1fCPwCzVsSc1hZf0BSbCgW2hM=</DigestValue>
1511             </Reference>
1512             <Reference URI="#_3">
1513                 <Transforms>
1514                     <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
1515 c14n#" />
1516                 </Transforms>
1517                 <DigestMethod
1518 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
1519                     <DigestValue>FwiFAUuqNDo9SDkk5A28Mg7Pa8Q=</DigestValue>
1520                 </Reference>
1521                 <Reference URI="#_4">
1522                     <Transforms>
1523                         <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
1524 c14n#" />
1525                     </Transforms>
1526                     <DigestMethod
1527 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
1528                         <DigestValue>oM59PsOTpMrDdOcwXYQzjVU10xw=</DigestValue>
1529                     </Reference>
1530                     <Reference URI="#_5">
1531                         <Transforms>
1532                             <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
1533 c14n#" />
1534                         </Transforms>
1535                         <DigestMethod
1536 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
1537                             <DigestValue>KIK3vklFN1QmMdQkplq2azfzrzg=</DigestValue>
1538                         </Reference>
1539                         <Reference URI="#_6">
1540                             <Transforms>
1541                                 <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
1542 c14n#" />
1543                             </Transforms>
```

```

1544     <DigestMethod
1545 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
1546     <DigestValue>RJEe3hrCyCD6PzFJo6fyut6biVg=</DigestValue>
1547     </Reference>
1548     <Reference URI="#uuid-40f5bac7-f9af-4384-80db-cfab34263849-10">
1549       <Transforms>
1550         <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
1551 c14n#" />
1552       </Transforms>
1553     </Reference>
1554     <DigestMethod
1555 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
1556     <DigestValue>zQdN5XpejfqXn0Wko0m51ZYiasE=</DigestValue>
1557     </Reference>
1558 </SignedInfo>
1559 <SignatureValue>iHGJ+xV2VZTjMlRc7AQJrwLY/aM=</SignatureValue>
1560 <KeyInfo>
1561   <o:SecurityTokenReference>
1562     <o:Reference
1563       ValueType="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-
1564 secext-1.1.xsd#EncryptedKey"
1565       URI="#uuid-40f5bac7-f9af-4384-80db-cfab34263849-9"/>
1566     </o:SecurityTokenReference>
1567   </KeyInfo>
1568 </Signature>
1569 <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
1570   <SignedInfo>
1571     <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-
1572 exc-c14n#" />
1573     <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
1574 sha1"/>
1575     <Reference URI="#_0">
1576       <Transforms>
1577         <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
1578 c14n#" />
1579       </Transforms>
1580     </Reference>
1581     <DigestMethod
1582 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
1583     <DigestValue>UZKtShk8q6iu9WR5uQZp04iAitg=</DigestValue>
1584     </Reference>
1585   </SignedInfo>
1586   <SignatureValue>
1587     Ovxdg4KQcfQlT/hEBJz+Z8dQUAfChaWlcmG3xGLZYcc8tbmCtZFuQz9tnW35Lmst6vIHFI23mg8U
1588     3lRefuPA7ewRLYORA0jf92SxMbeVTlrIxQbIQNw0bs4SBSLfAo14=
1589   </SignatureValue>
1590 </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

```

1590     <o:SecurityTokenReference>
1591         <o:Reference
1592             ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
1593 wss-x509-token-profile-1.0#X509v3"
1594             URI="#uuid-40f5bac7-f9af-4384-80db-cfab34263849-6"/>
1595         </o:SecurityTokenReference>
1596     </KeyInfo>
1597 </Signature>
1598 </o:Security>
1599 </s:Header>
1600 <s:Body u:Id="_1">
1601     <e:EncryptedData Id="_2" Type="http://www.w3.org/2001/04/xmlenc#Content">
1602     <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-
1603 cbc"/>
1604     <e:CipherData>
1605     <e:CipherValue>
1606         <!-- base64 encoded octets with encrypted RST request-->
1607         <!-- Unencrypted form: -->
1608         <!--
1609     <t:RequestSecurityToken>
1610     <t:RequestType>
1611         http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue
1612     </t:RequestType>
1613     <t:Entropy>
1614     <t:BinarySecret u:Id="uuid-4acf589c-0076-4a83-8b66-5f29341514b7-3"
1615 Type="http://docs.oasis-open.org/ws-sx/ws-
1616 trust/200512/Nonce">Uv38QLxDQM9gLoDZ6OwYDiFk094nmwu3Wmay7EdKmhw=</t:BinarySec
1617 ret>
1618     </t:Entropy>
1619     <t:KeyType>http://docs.oasis-open.org/ws-sx/ws-
1620 trust/200512/SymmetricKey</t:KeyType>
1621     <t:KeySize>256</t:KeySize>
1622     <t:ComputedKeyAlgorithm>
1623         http://docs.oasis-open.org/ws-sx/ws-trust/200512/CK/PSHA1
1624     </t:ComputedKeyAlgorithm>
1625 </t:RequestSecurityToken>
1626         -->
1627     </e:CipherValue>
1628 </e:CipherData>
1629 </e:EncryptedData>
1630 </s:Body>

```

1631 </s:Envelope>

1632 **Policy**

1633 [This policy statement must note that two derived keys are used, one for signing and one for encryption.](#)

1634 [QUESTION: HOW TO STATE THIS IN POLICY. Policy same as previous for now.](#)

1635 [Assuming signed then encrypted as in previous case, though not stated.](#)

Frederick Hirsch 7/21/06 5:53 PM

Formatted: Font:Italic

```
1637 <wsp:Policy>
1638 <sp:SymmetricBinding>
1639   <wsp:Policy>
1640     <sp:ProtectionToken>
1641       <wsp:Policy>
1642         <sp:X509Token
1643           sp:IncludeToken='http://docs.oasis-open.org/ws-sx/ws-
1644 securitypolicy/200512/IncludeToken/Never' />
1645         <wsp:Policy>
1646           <sp:WssX509V3Token11 />
1647         </wsp:Policy>
1648       </wsp:Policy>
1649     </sp:ProtectionToken>
1650     <sp:SignBeforeEncrypting />
1651     <sp:EncryptSignature />
1652   </wsp:Policy>
1653 </sp:SymmetricBinding>
1654 </wsp:Policy>
```

1655

1656 **Response Message**

1657 **Message Creation**

1658 **Body**

1659 **RequestSecurityTokenResponseCollection/RequestSecurityTokenResponse**

1660 **TokenType**

1661 The <t:TokenType> element value MUST be equal to [http://docs.oasis-open.org/wss/oasis-wss-saml-](http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0#SAMLV1.1)

1662 [token-profile-1.0#SAMLV1.1](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>

1663 **AppliesTo**

1664 If present, the <wsp:AppliesTo> element contents MUST be identical to that found in the RST message.

1665 **Lifetime**

1666 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

1667 **RequestedSecurityToken**

1668 A SAML 1.1 Assertion or SecureConversationToken MUST be returned

1669 **Message Processing**

1670 The requestor must check to see if all elements noted as mandatory are present in the response. It must  
1671 further verify that values for <t:TokenType> and <wsp:AppliesTo> are set as required above.

1672 **Example (Non-normative)**

1673 Here is an example response.

```
1674 <s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope"  
1675   xmlns:a="http://schemas.xmlsoap.org/ws/2004/08/addressing"  
1676   xmlns:e="http://www.w3.org/2001/04/xmlenc#"  
1677   xmlns:k="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-  
1678   1.1.xsd"  
1679   xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-  
1680   wssecurity-secext-1.0.xsd"  
1681   xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-  
1682   wssecurity-utility-1.0.xsd"  
1683   >  
1684   <s:Header>  
1685     <a:Action s:mustUnderstand="1" u:Id="_4">  
1686       http://docs.oasis-open.org/ws-sx/ws-trust/200512/RSTRC/IssueFinal  
1687     </a:Action>  
1688     <a:RelatesTo u:Id="_5">  
1689       urn:uuid:04d386bf-f850-459e-918b-ad80f3d1e088  
1690     </a:RelatesTo>  
1691     <a:To s:mustUnderstand="1" u:Id="_6">  
1692       http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous  
1693     </a:To>  
1694     <o:Security s:mustUnderstand="1">  
1695       <u:Timestamp u:Id="uuid-0c947d47-f527-410a-a674-753a9d7d97f7-18">  
1696         <u:Created>2005-10-25T00:47:38.718Z</u:Created>  
1697         <u:Expires>2005-10-25T00:52:38.718Z</u:Expires>  
1698       </u:Timestamp>  
1699       <e:ReferenceList>  
1700         <e:DataReference URI="#_3"/>  
1701       </e:ReferenceList>  
1702       <k:SignatureConfirmation u:Id="_0"  
1703       Value="iHGJ+xV2VZTjMlRc7AQJrwLY/aM="/>  
1704       <k:SignatureConfirmation u:Id="_1"  
1705       Value="Ovxdeg4KQcfQ1T/hEBJz+Z8dQUAfChaWicmG3xGLZYcc8tbmCtZFuQz9tnW35Lmst6vRef  
1706       uPA7ewRLYORA0jf92SxMbeVTlrIxQx5I17lrcK+XBy+wm5Tl2DlqcTq+dMZW5oio7J/1sibIQNw0  
1707       bs4SBSLfAo14="/>  
1708       <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

```
1710     <SignedInfo>
1711         <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-
1712 exc-c14n#"/>
1713         <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#hmac-
1714 sha1"/>
1715         <Reference URI="#_2">
1716             <Transforms>
1717                 <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
1718 c14n#"/>
1719             </Transforms>
1720             <DigestMethod
1721 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
1722                 <DigestValue>kKx5bpLLlyucgXQ6exv/Pbj5f1A=</DigestValue>
1723             </Reference>
1724             <Reference URI="#_4">
1725                 <Transforms>
1726                     <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
1727 c14n#"/>
1728                 </Transforms>
1729                 <DigestMethod
1730 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
1731                     <DigestValue>LB+VGn4fP2z45jg0Mdzyo8yTAWQ=</DigestValue>
1732                 </Reference>
1733                 <Reference URI="#_5">
1734                     <Transforms>
1735                         <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
1736 c14n#"/>
1737                     </Transforms>
1738                     <DigestMethod
1739 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
1740                         <DigestValue>izHLxm6V4Lc3PSs9Y6VRv3I5RPw=</DigestValue>
1741                     </Reference>
1742                     <Reference URI="#_6">
1743                         <Transforms>
1744                             <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
1745 c14n#"/>
1746                         </Transforms>
1747                         <DigestMethod
1748 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
1749                             <DigestValue>6LS4X08vC/GMGay2vwmD8fL7J2U=</DigestValue>
1750                         </Reference>
1751                         <Reference URI="#uuid-0c947d47-f527-410a-a674-753a9d7d97f7-18">
1752                             <Transforms>
1753                                 <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
1754 c14n#"/>
1755                             </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

```

1756     <DigestMethod
1757 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
1758     <DigestValue>uXGSpCBfbT1fLNBLdGMgy6DGDio=</DigestValue>
1759     </Reference>
1760     <Reference URI="#_0">
1761     <Transforms>
1762     <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
1763 c14n#"/>
1764     </Transforms>
1765     <DigestMethod
1766 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
1767     <DigestValue>z86w+GrzqRZF56ciuz6ogzVXAUA=</DigestValue>
1768     </Reference>
1769     <Reference URI="#_1">
1770     <Transforms>
1771     <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
1772 c14n#"/>
1773     </Transforms>
1774     <DigestMethod
1775 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
1776     <DigestValue>Z9TfD20a5aGngsyOPEvQuE0urvQ=</DigestValue>
1777     </Reference>
1778 </SignedInfo>
1779 <SignatureValue>Q7HhboPUaZyXqUKgG7NCYlhMTXI=</SignatureValue>
1780 <KeyInfo>
1781 <o:SecurityTokenReference>
1782 <o:KeyIdentifier
1783 Value="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-
1784 secext-1.1.xsd#EncryptedKeySHA1">
1785 CixQW5yEb3mw6XYqD8Ysvrf8cwI=
1786 </o:KeyIdentifier>
1787 </o:SecurityTokenReference>
1788 </KeyInfo>
1789 </Signature>
1790 </o:Security>
1791 </s:Header>
1792 <s:Body u:Id="_2">
1793 <e:EncryptedData Id="_3" Type="http://www.w3.org/2001/04/xmlenc#Content">
1794 <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-
1795 cbc"/>
1796 <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
1797 <o:SecurityTokenReference>
1798 <o:KeyIdentifier
1799 Value="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-
1800 secext-1.1.xsd#EncryptedKeySHA1">
1801 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

```

1802     </o:KeyIdentifier>
1803     </o:SecurityTokenReference>
1804   </KeyInfo>
1805   <e:CipherData>
1806     <e:CipherValue>
1807       <!--base64 encoded octets of encrypted RSTR-->
1808       <!--
1809     <t:RequestSecurityTokenResponseCollection>
1810     <t:RequestSecurityTokenResponse>
1811       <t:TokenType>http://docs.oasis-open.org/wss/oasis-wss-saml-token-
1812 profile-1.1#SAMLV1.1</t:TokenType>
1813       <t:KeySize>256</t:KeySize>
1814       <t:RequestedAttachedReference>
1815         <o:SecurityTokenReference>
1816           <o:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/oasis-
1817 wss-saml-token-profile-1.0#SAMLAssertionID">uuid-8222b7a2-3874-4884-bdb5-
1818 9c2ddd4b86b5-16</o:KeyIdentifier>
1819           </o:SecurityTokenReference>
1820         </t:RequestedAttachedReference>
1821         <t:RequestedUnattachedReference>
1822           <o:SecurityTokenReference>
1823             <o:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/oasis-
1824 wss-saml-token-profile-1.0#SAMLAssertionID">uuid-8222b7a2-3874-4884-bdb5-
1825 9c2ddd4b86b5-16</o:KeyIdentifier>
1826             </o:SecurityTokenReference>
1827           </t:RequestedUnattachedReference>
1828           <t:Lifetime>
1829             <u:Created>2005-10-24T20:19:26.526Z</u:Created>
1830             <u:Expires>2005-10-25T06:24:26.526Z</u:Expires>
1831           </t:Lifetime>
1832           <t:RequestedSecurityToken>
1833             <saml:Assertion MajorVersion="1" MinorVersion="1" AssertionID="uuid-
1834 8222b7a2-3874-4884-bdb5-9c2ddd4b86b5-16" Issuer="Test STS"
1835 IssueInstant="2005-10-24T20:24:26.526Z"
1836 xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion">
1837               <saml:Conditions NotBefore="2005-10-24T20:19:26.526Z"
1838 NotOnOrAfter="2005-10-25T06:24:26.526Z">
1839                 </saml:Conditions>
1840                 <saml:Advice>
1841                   </saml:Advice>
1842                 <saml:AttributeStatement>
1843                   <saml:Subject>
1844                     <saml:SubjectConfirmation>
1845                       <saml:ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:holder-of-
1846 key</saml:ConfirmationMethod>
1847

```

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



```

1848         <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
1849             <e:EncryptedKey
1850 xmlns:e="http://www.w3.org/2001/04/xmlenc#">
1851                 <e:EncryptionMethod
1852 Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
1853                     </e:EncryptionMethod>
1854                 <KeyInfo>
1855                     <o:SecurityTokenReference xmlns:o="http://docs.oasis-
1856 open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
1857                         <o:KeyIdentifier ValueType="http://docs.oasis-
1858 open.org/wss/oasis-wss-wssecurity-secext-
1859 1.1.xsd#ThumbprintSHA1">NQM0IBvuplAtETQvk+6gn8C13wE=</o:KeyIdentifier>
1860                     </o:SecurityTokenReference>
1861                 </KeyInfo>
1862             <e:CipherData>
1863                 <e:CipherValue>EEcYjwNoYcJ+20xTYE5e/fixl5KOgzgrfaYAxkDFv/VXiuKf1084h8PmogTfM+
1864 azcgAfmArVQvOyKWXRb5vmXYfVHLLlhZTbXacy+nowSUNnEjp37VDbI3RJ5k6tBHF+ow0NM/P6GPNZ
1865 9ZqJi1lGDgWJkFsJzNZXNbbMgwuFu3cA=</e:CipherValue>
1866             </e:CipherData>
1867         </e:EncryptedKey>
1868     </KeyInfo>
1869 </saml:SubjectConfirmation>
1870 </saml:Subject>
1871 </saml:AttributeStatement>
1872 <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
1873     <SignedInfo>
1874         <CanonicalizationMethod
1875 Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
1876         </CanonicalizationMethod>
1877         <SignatureMethod
1878 Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1">
1879         </SignatureMethod>
1880         <Reference URI="#uuid-8222b7a2-3874-4884-bdb5-9c2ddd4b86b5-16">
1881             <Transforms>
1882                 <Transform
1883 Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature">
1884                 </Transform>
1885                 <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
1886 c14n#">
1887                 </Transform>
1888             </Transforms>
1889             <DigestMethod
1890 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
1891             </DigestMethod>
1892             <DigestValue>7nHBrFPsm+LEFAoV4NoQPoEl5Lk=</DigestValue>
1893         </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

```

1895         </SignedInfo>
1896
1897 <SignatureValue>TugV4pTIwCH87bLD4jiMgVGtkbRBt1tRlHXJArL34A/YfA4AnGBLXB4pJdUsU
1898 xMUTbQl4PoGgEsdLNg8C77peARELGP1/Tqw7T3u5zBYHxCHCiV2FWBBfeOmwJmgoaBf8XZJ4AlyqP
1899 q61P61jrQjZJafpHuYpAZnZQsvsiJaBPQ=</SignatureValue>
1900     <KeyInfo>
1901         <o:SecurityTokenReference xmlns:o="http://docs.oasis-
1902 open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
1903             <o:KeyIdentifier ValueType="http://docs.oasis-
1906 1.1.xsd#ThumbprintSHA1">NQM0IBvuplAtETQvk+6gn8C13wE=</o:KeyIdentifier>
1907         </o:SecurityTokenReference>
1908     </KeyInfo>
1909 </Signature>
1910 </saml:Assertion>
1911 </t:RequestedSecurityToken>
1912 <t:RequestedProofToken>
1913     <t:BinarySecret u:Id="uuid-8222b7a2-3874-4884-bdb5-9c2ddd4b86b5-
1914 14">zT8LWUwUrvIVKA/rkCr0kxlEmKAehcB6TGWJuAgucBM=</t:BinarySecret>
1915 </t:RequestedProofToken>
1916 </t:RequestSecurityTokenResponse>
1917 </t:RequestSecurityTokenResponseCollection>
1918     -->
1919 </e:CipherValue>
1920 </e:CipherData>
1921 </e:EncryptedData>
1922 </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>

### 1923 3.6. Delegated SAML 2.0 with Certificate for SAML 2.0 HoK, WSS 1.1

1924 This binding is used in Scenario 7.

1925 This mode requires WS-Security 1.1.

1926 The requestor sends the STS a message over HTTP requesting issuance of a SAML token. The RST  
1927 message includes a WSS 1.1 X.509 BinarySecurityToken in the SOAP security header.

1928 The <t:OnBehalfOf> element includes a SAML 2.0 assertion describing the user. The <t:DelegateTo>  
1929 element includes an STR describing the entity which will use the SAML assertion. The STS responds with  
1930 a RSTR message with a SAML 2.0 holder of key assertion.

1931 NOTE: In most use-cases, there may be an authentication or proof step associated with the certificate  
1932 provided in the header. This may take the form of a digital signature or a SSL handshake. This step is  
1933 omitted in this scenario.

1934 The <SubjectConfirmation>/<ds:KeyInfo> element in the SAML assertion includes the issuer and serial  
1935 number of the requestors X.509 certificate. The <SubjectConfirmation>/<NameID> element has value  
1936 equal to the SubjectDN of the requestors certificate and has format attribute set to  
1937 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

1938 signal delegated use in SAML 2.0. The Method attribute of the <SubjectConfirmation> element is set to  
1939 urn:oasis:names:tc:SAML:2.0:cm:holder-of-key.

1940

1941 The SAML assertion is signed by the STS. The certificate used to sign the SAML token is included in the  
1942 <ds:KeyInfo> element of the assertion.

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

#### 1943 **Expected Security Properties**

#### 1944 **Agreements**

1945 This section describes the agreements that must be made, directly or indirectly between parties who wish  
1946 to interoperate beyond the common preconditions noted for all scenarios.

#### 1947 **Acceptable <wsa:EndpointReference> Values**

1948 The requestor and the STS must agree on at least one <wsa:EndpointReference> value on receipt of  
1949 which the STS can issue a delegated SAML HoK assertion.

#### 1950 **Request Message**

#### 1951 **Message Creation**

#### 1952 **Security**

1953 The Security element MUST contain the mustUnderstand="1" attribute.

#### 1954 **BinarySecurityToken**

1955 The security element MUST contain a BinarySecurityToken with a X.509 certificate that is encoded as  
1956 Base64 sequence. The ValueType attribute MUST be set to #X509v3.

#### 1957 **Body**

#### 1958 **TokenType**

1959 The <t:TokenType> element value MUST be equal to [http://docs.oasis-open.org/wss/oasis-wss-saml-  
1960 token-profile-1.0#SAMLV1.1](http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0#SAMLV1.1)

#### 1961 **RequestType**

1962 The <t:RequestType> element value MUST be equal to [http://docs.oasis-open.org/ws-sx/ws-  
1963 trust/200512/Issue](http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue)

#### 1964 **AppliesTo**

1965 This element MUST include an <wsa:EndpointReference> element with a <wsa:Address> sub-element.  
1966 The value of the <wsa:Address> element should be known to the STS.

#### 1967 **KeyType**

1968 The <t:KeyType> element value MUST be equal to [http://docs.oasis-open.org/ws-  
1969 sx/wstrust/200512/PublicKey](http://docs.oasis-open.org/ws-sx/wstrust/200512/PublicKey)

1970 **OnBehalfOf**

1971 The <t:OnBehalfOf> element MUST include a SAML 2.0 bearer assertion.

1972 **DelegateTO**

1973 The <t:DelegateTo> element MUST include a STR direct reference to X.509 certificate found in the SOAP security header.

1975 **Message Processing**

1976 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.

1978 The value of the <SubjectConfirmation>/<ds:KeyInfo> element in the SAML assertion is a  
1979 <ds:X.509Data> element with a <ds:X509Certificate> sub-element. The base-64 certificate value is taken  
1980 from the security header of the request message. The <SubjectConfirmation>/<NameID> element has  
1981 value equal to the SubjectDN of the X.509 certificate and has format attribute set to  
1982 urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName. The  
1983 <SubjectConfirmation>/<ConfirmationMethod> element is set to urn:oasis:names:tc:SAML:1.0:cm:holder-of-  
1984 key.

1985 If an error is detected, the STS MUST cease processing the message and report the fault with a value of  
1986 t:RequestFailed (other reasons for failure).

1987 **Example (Non-normative)**

1988 Here is an example request.

```
1989 <?xml version="1.0" encoding="utf-8" ?>
1990 <soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
1991 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
1992 xmlns:xsd="http://www.w3.org/2001/XMLSchema"
1993 xmlns:wssse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
1994 wssecurity-secext-1.0.xsd"
1995 xmlns:wst="http://docs.oasis-open.org/ws-sx/ws-trust/200512"
1996 >
1997
1998 <soap:Header>
1999 <wsse:Security soap:mustUnderstand="1">
2000 <wsse:BinarySecurityToken
2001 wsu:Id="binarytoken"
2002 ValueType="...#X509v3"
2003 EncodingType="...#Base64Binary">
2004 MIIEZzCCA9CgAwIBAgIQEmtJZc0...
2005 </wsse:BinarySecurityToken>
2006 </wsse:Security>
2007 </soap:Header>
2008 <soap:Body>
2009 <t:RequestSecurityToken>
2010 <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

```

2011 http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0
2012 </t:TokenType>
2013 <t:RequestType>
2014     http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue
2015 </t:RequestType>
2016 <wsp:AppliesTo>
2017 xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/03/addressing">
2018     <wsa:EndpointReference>
2019         <wsa:Address>http://www.example.org/</wsa:Address>
2020     </wsa:EndpointReference>
2021 </wsp:AppliesTo>
2022 <t:KeyType>
2023     http://docs.oasis-open.org/ws-sx/wstrust/200512/PublicKey
2024 </t:KeyType>
2025 <t:OnBehalfOf>
2026
2027         <saml:Assertion ID="_a75adf55-01d7-40cc-929f-
2028 dbd8372ebdfc"
2029             IssueInstant="2003-04-17T00:46:02Z"
2030             Version="2.0"
2031             Xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
2032                 <saml:Issuer>https://www.opensaml.org/IDP</Issuer>
2033                 <saml:Subject>
2034                     <saml:NameID
2035                         Format="urn:oasis:names:tc:SAML:1.1:nameid-
2036 format:emailAddress">
2037                         scott@example.org
2038                     </saml:NameID>
2039                 <saml:SubjectConfirmation
2040                     Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"/>
2041                 </saml:Subject>
2042                 <saml:Conditions NotBefore="2003-04-17T00:46:02Z"
2043                     NotOnOrAfter="2003-04-17T00:51:02Z">
2044                     </saml:Conditions>
2045                 </saml:Assertion>
2046             </t:OnBehalfOf>
2047             <t:DelegateTo>
2048                 <wsse:SecurityTokenReference wsu:Id="...">
2049                     <wsse:Reference URI="#binarytoken"/>
2050                 </wsse:SecurityTokenReference>
2051             </t:DelegateTo>
2052         </t:RequestSecurityToken>
2053 </soap:Body>
2054 </soap:Envelope>

```

2056

2057  
2058  
2059  
2060  
2061  
2062  
2063  
2064  
2065  
2066  
2067  
2068  
2069  
2070  
2071  
2072  
2073  
2074  
2075  
2076  
2077  
2078

**Policy**

Same as 3.5 but require WSS 1.1.

```
<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>  
      </sp:ProtectionToken>  
      <sp:SignBeforeEncrypting />  
      <sp:EncryptSignature />  
    </wsp:Policy>  
  </sp:SymmetricBinding>  
<sp:wss11 />  
</wsp:Policy>
```

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

2079  
2080  
2081  
2082  
2083  
2084  
2085  
2086  
2087  
2088  
2089  
2090

**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

2091 Assertion

2092 A SAML 2.0 Assertion MUST be returned; the assertion MUST contain a statement with  
2093 <saml:ConfirmationMethod> set to urn:oasis:names:tc:SAML:1.0:cm: holder-of-key. The value of the  
2094 <SubjectConfirmation>/<ds:KeyInfo> element in the SAML assertion MUST be a <ds:X.509Data>  
2095 element with a <ds:X509Certificate> sub-element. The base-64 certificate value is taken from the  
2096 BinarySecurityToken element in the request message. The <SubjectConfirmation>/<NameId> element  
2097 MUST have value equal to the SubjectDN of the X.509 certificate and has format attribute set to  
2098 urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName. The assertion MUST be signed and  
2099 include a <ds:Signature> element as part of an enveloped signature.

2100 **Message Processing**

2101 The requestor must check to see if all elements noted as mandatory are present in the response. It must  
2102 further verify that values for <t:TokenType> and <wsp:AppliesTo> are set as required above.

2103 Typically, requestors will not process the contents of the SAML assertion; instead, the assertion is used to  
2104 secure an exchange with a recipient. However, it is suggested that requestors check the value of the  
2105 <saml:ConfirmationMethod> and also ensure that the assertion contains an enveloped signature.

2106 **Example (Non-normative)**

2107 Here is an example response.

```
2108 <?xml version="1.0" encoding="utf-8" ?>
2109 <soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
2110 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance
2111 xmlns:wst="http://docs.oasis-open.org/ws-sx/ws-trust/200512"
2112 xmlns:xsd="http://www.w3.org/2001/XMLSchema">
2113   <soap:Header>
2114     </soap:Header>
2115   <soap:Body wsu:Id="body"
2116     xmlns:wsu="http://schemas.xmlsoap.org/ws/2003/06/utility">
2117     <t:RequestSecurityTokenResponse>
2118       <t:TokenType>
2119         http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0
2120       </t:TokenType>
2121       <wsp:AppliesTo>
2122     xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/03/addressing">
2123       <wsa:EndpointReference>
2124         <wsa:Address>http://www.example.org/</wsa:Address>
2125       </wsa:EndpointReference>
2126       <wsp:AppliesTo>
2127     <t:Lifetime>
2128       <wsu:Created>"2005-04-17T00:46:02Z"</wsu:Created>
2129       <wsu:Expires>"2005-04-17T00:51:02Z"</wsu:Expires>
2130     </t:Lifetime>
2131
2132     <t:RequestedSecurityToken>
2133       <saml:Assertion ID="_xw5adf55-01d7-40cc-ayp2-dbd8372ebdfc"
2134         IssueInstant="2005-04-17T00:46:02Z" Version="2.0"
2135         xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
```

```
2136 <saml:Issuer>https://www.example.org/STS</Issuer>
2137 <ds:Signature
2138 xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
2139 <ds:SignedInfo>
2140 <ds:CanonicalizationMethod
2141 Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
2142 <ds:SignatureMethod
2143 Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
2144 <ds:Reference
2145 URI="#_a75adf55-01d7-40cc-929f-dbd8372ebdfc">
2146 <ds:Transforms>
2147 <ds:Transform
2148 Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
2149 <ds:Transform
2150 Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
2151 <InclusiveNamespaces
2152 PrefixList="#default saml samlp ds xsd xsi"
2153 xmlns="http://www.w3.org/2001/10/xml-exc-c14n#" />
2154 </ds:Transform>
2155 </ds:Transforms>
2156 <ds:DigestMethod
2157 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
2158 <ds:DigestValue>Kclet6XcaOgOWXM4gty6/UNdviI=</ds:DigestValue>
2159 </ds:Reference>
2160 </ds:SignedInfo>
2161 <ds:SignatureValue>
2162 hq4zk+ZknjggCQgZm7ea8fI79gJEsRy3E8LHDpYXWQIgzpkJN9CMLG8ENR4Nrw+n
2163 7iyzixBvKXX8P53BTCT4VghPBWhFYSt9tHWu/AtJf0Th6qaAsNdeCyG86jmt3TD
2164 MWuL/cBUj2OtBZOQMF7jQ9YB7klIz3RqVL+wNmeWI4=</ds:SignatureValue>
2165 <ds:KeyInfo>
2166 <ds:X509Data>
2167 <ds:X509Certificate>
2168 MIICyjCCAjOgAwIBAgICAnUwDQYJKoZIhvcNAQEEBQAwgakkCzAJBgNVBAYTA1VT
2169 MRlWEAYDVQQIEWlXaXNjb25zaW4xEDAoBgNVBACjB01hZGlzb24xIDAeBgNVBAoT
2170 FlVuaXZlcnNpdHkgb2YgV2l2Y29uc2luMSswKQYDVQQLZyJlEaXZpc21vbiBvZiBJ
2171 bmZvcmlhdGlvbiBUZWNobm9sb2d5MSUwIwYDVQQDExxIRVBLSSBTZXJ2ZXIgc0Eg
2172 LS0gMjAwMjA3MDFBMB4XDTAyMDcyNjA3Mjc1MVoXDTA2MDkwNDA3Mjc1MVoWgYsx
2173 CzAJBgNVBAYTA1VTMREwDwYDVQQQIEwhNaWNoaWdhbjESMBAGA1UEBxMJQW5uIEFy
2174 Ym9yMQ4wDAYDVQQKEwVvQ0FJRDECMBoga1UEAxMTc2hpYjEuaW50ZXJlZmVkaWVl
2175 dTEuMCUGCSqGSIB3DQEJARYYcm9vdEBzaGlMS5pbnRlcm5ldDIuZWZRMIGfMA0G
2176 CSqGSIB3DQEBAQUAA4GNADCBiQKBgQDZSAb2sxvvhAXnXVIVTx8vuRay+x50z7GJj
2177 IHRYQgIv6IqaGG04eTcyVMhoeke0b45QgvBIAOAPSZB113R6+KYiE7x4XAWIrcP+
2178 c2MZVeXeTgV3Yz+USLg2Y1on+Jh4HxwkPFmZBctyXiUr6DxF8rvoP9W7O27rhRjE
2179 pmqOIftGTWQIDAQABox0wGzAMBgNVHRMBAf8EAjAAMAsGA1UdDwQEAwIFoDANBgkq
```

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



```

2180 hkiG9w0BAQQFAA0BgQBfDqEW+OI3jqBQHIBzhujN/PizdN7s/z4D5d3pptWDJf2n
2181 qgi7lFV6MDkhmTvTqBtjmNk3No7v/dnP6Hr7wHxvCCRwubnmIfz6QZAv2FU78pLX
2182 8I3bsbmRAUg4UP9hH6ABVq4KQKMknxulxQxLhpRlylGPdiowMNTTrEG8cCx3w/w==
2183 </ds:X509Certificate>
2184 </ds:X509Data>
2185 </ds:KeyInfo>
2186 </ds:signature>
2187 </ds:Signature>
2188     <saml:Subject>
2189         <saml:NameID
2190             Format="urn:oasis:names:tc:SAML:1.1:nameid-
2191 format:emailAddress">
2192             joes@example.org
2193         </saml:NameID>
2194         <saml:SubjectConfirmation
2195             Method="urn:oasis:names:tc:SAML:2.0:cm:holder-of-
2196 key">
2197
2198             <saml:NameId Format="urn:oasis:names:tc:SAML:1.1:nameid-
2199 format:X509SubjectName"
2200                 C=US, S=WA, L=Woodinville, O=Contoso,
2201 CN=FinanceServer
2202             </saml:NameId>
2203             <ds:KeyInfo>
2204                 <ds:KeyValue>
2205                     <ds:X509Data><ds:X509Certificate>
2206 MIEZzCCA9CgAwIBAgIQEmtJZc0...
2207                     <ds:X509Certificate>
2208                         <ds:X509Data>
2209                     </ds:KeyValue>
2210                 </ds:KeyInfo>
2211             </saml:SubjectConfirmation>
2212             <saml:Conditions NotBefore="2005-04-17T00:46:02Z"
2213                 NotOnOrAfter="2005-04-17T00:51:02Z">
2214             </saml:Conditions>
2215             <saml:AttributeStatement>
2216                 <saml:Attribute
2217 NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
2218                 Name="Division"
2219                 <saml:AttributeValue
2220 xsi:type="xs:string">Development</AttributeValue>
2221                 </saml:Attribute>
2222             </saml:AttributeStatement>
2223         </saml:Assertion>
2224     </t:RequestedSecurityToken>
2225 </t:SecurityTokenResponse>
2226 </soap:Body>
2227 </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

## 2229 4. Client and Service Security Bindings

2230 Each scenario defined above will use one of the following security bindings for message exchanges  
2231 between the Client and Service.

### 2232 **4.1. Issued SAML 1.1 Token over Transport**

2233 This binding is used in Scenario 1.

2234 SAML HoK token issued to the Client by the STS is used to authenticate the Client. The Service's X509  
2235 certificate is used to authenticate the Service. Secure transport (HTTPS) is used to protect messages.

#### 2236 **Request Message**

#### 2237 **Example (Non-normative)**

2238 Here is an example request.

```
2239 <s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope"
2240   xmlns:a="http://schemas.xmlsoap.org/ws/2004/08/addressing"
2241   xmlns:d="http://www.w3.org/2000/09/xmldsig#"
2242   xmlns:e="http://www.w3.org/2001/04/xmlenc#"
2243   xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
2244   wssecurity-secext-1.0.xsd"
2245   xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
2246   xmlns:sc="http://docs.oasis-open.org/ws-sx/ws-secureconversation/200512"
2247   xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
2248   wssecurity-utility-1.0.xsd">
2249   <s:Header>
2250     <a:Action s:mustUnderstand="1" u:Id="_4">
2251       http://example.org/Ping
2252     </a:Action>
2253     <a:MessageID u:Id=" 5">
2254       urn:uuid:b6345ac8-dfc4-4174-a985-2f69cf4ac54e
2255     </a:MessageID>
2256     <a:ReplyTo u:Id="_6">
2257       <a:Address>
2258         http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous
2259       </a:Address>
2260     </a:ReplyTo>
2261     <a:To s:mustUnderstand="1" u:Id="_7">
2262       http://server.example.com/Ping/Scenario1
2263     </a:To>
2264     <o:Security s:mustUnderstand="1">
2265       <u:Timestamp u:Id="uuid-c3cdb38b-e4aa-4467-9d0e-dd30f081e08d-10">
2266         <u:Created>2005-10-24T15:51:46.791Z</u:Created>
2267         <u:Expires>2005-10-24T15:56:46.791Z</u:Expires>
2268       </u:Timestamp>
2269       <saml:Assertion MajorVersion="1" MinorVersion="1"
2270         AssertionID="uuid-78c746a2-3ec4-4cf8-a913-50d2f7334cf9-32"
2271         Issuer="Test STS"
2272         IssueInstant="2005-10-24T15:51:47.025Z">
2273         <saml:Conditions NotBefore="2005-10-24T15:46:47.025Z"
2274         NotOnOrAfter="2005-10-25T01:51:47.025Z"/>
```

```

2275     <saml:Advice/>
2276     <saml:AttributeStatement>
2277         <saml:Subject>
2278             <saml:SubjectConfirmation>
2279                 <saml:ConfirmationMethod>
2280                     urn:oasis:names:tc:SAML:1.0:cm:holder-of-key
2281                 </saml:ConfirmationMethod>
2282                 <d:KeyInfo>
2283                     <e:EncryptedKey>
2284                         <e:EncryptionMethod
2285 Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p"/>
2286                         <d:KeyInfo>
2287                             <o:SecurityTokenReference>
2288                                 <o:KeyIdentifier
2289                                     ValueType="http://docs.oasis-open.org/wss/oasis-wss-
2290 wssecurity-secext-1.1.xsd#ThumbprintSHA1">
2291                                     NQM0IBvuplAtETQvk+6gn8C13wE=
2292                                 </o:KeyIdentifier>
2293                             </o:SecurityTokenReference>
2294                         </d:KeyInfo>
2295                     <e:CipherData>
2296                         <e:CipherValue>
2297 cb7+JW2idPNSarK9quqCe9PQwmW2hoUghuyKRe+I9zOts6HaMcg73LqCWuK/jtdpvNl6GT/ZDYfca
2298 J7NlyMGxSiwi4DUlTOShqS60TYBIKgUKiA+zXN12koVsy7amcUhPMIT6/fohH+6MZDA4t6jomcyhl
2299 CiW8d9IAzSWFkfg2k=
2300                         </e:CipherValue>
2301                     </e:CipherData>
2302                 </e:EncryptedKey>
2303             </d:KeyInfo>
2304         </saml:SubjectConfirmation>
2305     </saml:Subject>
2306 </saml:AttributeStatement>
2307 <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
2308     <SignedInfo>
2309         <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-
2310 exc-cl4n#"/>
2311         <SignatureMethod
2312 Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
2313         <Reference URI="#uuid-78c746a2-3ec4-4cf8-a913-50d2f7334cf9-32">
2314             <Transforms>
2315                 <Transform
2316 Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
2317                 <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
2318 cl4n#"/>
2319             </Transforms>
2320             <DigestMethod
2321 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
2322             <DigestValue>WubDx7buehNvSvpCoGr/3tKmcyg</DigestValue>
2323         </Reference>
2324     </SignedInfo>
2325     <SignatureValue>
2326 Cag6FeoBeoHrRpv9h8Evx58rXp6G5vKOK4BgMnJiq/wUp2sQyOjeCVnij/g+gbIi+2ZGa75zhMykv
2327 +9O/jXhlytRNRNGFTWhEznsU0olkBoezJ/FHhDnyTVUeDHiTChf/kwP8COZ4atCDtaQUN3ZXLaxbp
2328 FBYewpoh+OABMTBlo=
2329     </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

```

2330     <KeyInfo>
2331       <o:SecurityTokenReference>
2332         <o:KeyIdentifier ValueType="http://docs.oasis-
2334 open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd#ThumbprintSHA1">
2335         NQM0IBvuplAtETQvk+6gn8C13wE=
2336       </o:KeyIdentifier>
2337     </o:SecurityTokenReference>
2338   </KeyInfo>
2339 </Signature>
2340 </saml:Assertion>
2341 <sc:DerivedKeyToken u:Id="_0">
2342   <o:SecurityTokenReference>
2343     <o:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/oasis-
2344 wss-saml-token-profile-1.0#SAMLAssertionID">
2345     uuid-78c746a2-3ec4-4cf8-a913-50d2f7334cf9-32
2346   </o:KeyIdentifier>
2347 </o:SecurityTokenReference>
2348   <sc:Offset>
2349     0
2350   </sc:Offset>
2351   <sc:Length>
2352     24
2353   </sc:Length>
2354   <sc:Nonce>
2355     flvBVmEJTyhdYLlf8qDxBg==
2356   </sc:Nonce>
2357 </sc:DerivedKeyToken>
2358 <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
2359   <SignedInfo>
2360     <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-
2361 exc-c14n#" />
2362     <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#hmac-
2363 sha1" />
2364     <Reference URI="#uuid-c3cdb38b-e4aa-4467-9d0e-dd30f081e08d-10">
2365       <Transforms>
2366         <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
2367 c14n#" />
2368       </Transforms>
2369       <DigestMethod
2370 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
2371       <DigestValue>Tj0yGTMhbgonlFR9JUsLZpZ2TQY=</DigestValue>
2372     </Reference>
2373   </SignedInfo>
2374   <SignatureValue>DYf5TKftfZSszjz7x8+srholZ3nU=</SignatureValue>
2375   <KeyInfo>
2376     <o:SecurityTokenReference>
2377       <o:Reference URI="#_0" />
2378     </o:SecurityTokenReference>
2379   </KeyInfo>
2380 </Signature>
2381 </o:Security>
2382 </s:Header>
2383 <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>

2384 </s:Body>  
2385 </s:Envelope>

2386 **Service Policy**

2387 [This is the service policy.](#)

```
2388  
2389 <wsp:Policy>  
2390   <sp:TransportBinding />  
2391   <sp:SamlToken sp:IncludeToken='http://docs.oasis-open.org/ws-sx/ws-  
2392 securitypolicy/200512/IncludeToken/Always' />  
2393   <wsp:Policy>  
2394     <sp:WssSamlV11Token11 />  
2395   </wsp:Policy>  
2396 </sp:SamlToken>  
2397 </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

2398 **Response Message**

2399 **Example (Non-normative)**

2400 Here is an example response.

```
2401 <s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope"  
2402 xmlns:a="http://schemas.xmlsoap.org/ws/2004/08/addressing"  
2403 xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-  
2404 wssecurity-secext-1.0.xsd"  
2405 xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-  
2406 wssecurity-utility-1.0.xsd">  
2407   <s:Header>  
2408     <a:Action s:mustUnderstand="1" u:Id="_4">  
2409       http://example.org/PingResponse  
2410     </a:Action>  
2411     <a:MessageID u:Id="_5">  
2412       urn:uuid:b6345ac8-dfc4-4174-a985-2f69cf4ac54e  
2413     </a:MessageID>  
2414     <a:RelatesTo u:Id="_6">  
2415       urn:uuid:b6345ac8-dfc4-4174-a985-2f69cf4ac54e  
2416     </a:RelatesTo>  
2417     <a:To s:mustUnderstand="1" u:Id="_7">  
2418       http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous  
2419     </a:To>  
2420     <o:Security s:mustUnderstand="1">  
2421       <u:Timestamp u:Id="uuid-c3cdb38b-e4aa-4467-9d0e-dd30f081e08d-10">  
2422         <u:Created>2005-10-24T15:51:46.791Z</u:Created>  
2423         <u:Expires>2005-10-24T15:56:46.791Z</u:Expires>  
2424       </u:Timestamp>  
2425     </o:Security>  
2426   </s:Header>  
2427   <s:Body>  
2428     <PingResponse xmlns="http://example.org/Ping">Ping</PingResponse>  
2429   </s:Body>  
2430 </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

2431 **4.2. Issued SAML 1.1 Token for Certificate, WSS 1.0**

2432 This binding is used in Scenarios 2, 3 and 4.

2433 SAML token issued to the Client by STS is used to authenticate the Client. Messages are signed then  
2434 encrypted using symmetric keys derived from the symmetric proof-of-possession key Sx associated with  
2435 the SAML token.

2436 **Service Policy**

2437 [This is the service policy.](#)

2438

```
2439 <wsp:Policy>  
2440   <sp:SymmetricBinding>  
2441     <wsp:Policy>  
2442       <sp:ProtectionToken>  
2443         <wsp:Policy>  
2444           <sp:SamlToken sp:IncludeToken='http://docs.oasis-open.org/ws-sx/ws-  
2445 securitypolicy/200512/IncludeToken/Always' >  
2446             <wsp:Policy>  
2447               <sp:WssSamlV11Token11 />  
2448             </wsp:Policy>  
2449           </sp:SamlToken>  
2450         </wsp:Policy>  
2451       </sp:ProtectionToken>  
2452     <sp:SignBeforeEncrypting />  
2453     <sp:EncryptSignature />  
2454   </wsp:Policy>  
2455 </sp:SymmetricBinding>  
2456 </wsp:Policy>
```

2457

2458 **Request Message**

2459 **Example (Non-normative)**

2460 Here is an example request.

```
2461 <s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope"  
2462   xmlns:a="http://schemas.xmlsoap.org/ws/2004/08/addressing"  
2463   xmlns:e="http://www.w3.org/2001/04/xmlenc#"  
2464   xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-  
2465 wssecurity-secext-1.0.xsd"  
2466   xmlns:sc="http://docs.oasis-open.org/ws-sx/ws-secureconversation/200512"  
2467   xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-  
2468 wssecurity-utility-1.0.xsd">  
2469   <s:Header>  
2470     <a:Action s:mustUnderstand="1" u:Id="_4">  
2471       http://example.org/Ping  
2472     </a:Action>
```

```

2473 <a:MessageID u:Id=" 5">
2474   urn:uuid:b6345ac8-dfc4-4174-a985-2f69cf4ac54e
2475 </a:MessageID>
2476 <a:ReplyTo u:Id="_6">
2477   <a:Address>
2478     http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous
2479   </a:Address>
2480 </a:ReplyTo>
2481 <a:To s:mustUnderstand="1" u:Id="_7">
2482   http://server.example.com/Ping/Scenario2-3-4
2483 </a:To>
2484 <o:Security s:mustUnderstand="1" >
2485   <u:Timestamp u:Id="uuid-c3cdb38b-e4aa-4467-9d0e-dd30f081e08d-10">
2486     <u:Created>2005-10-24T15:51:46.791Z</u:Created>
2487     <u:Expires>2005-10-24T15:56:46.791Z</u:Expires>
2488   </u:Timestamp>
2489   <e:EncryptedData Id="_3">
2490     <e:EncryptionMethod
2491 Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>
2492     <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
2493       <!-- encrypted Key K-->
2494       <e:EncryptedKey>
2495         <e:EncryptionMethod
2496 Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p"/>
2497         <KeyInfo>
2498           <o:SecurityTokenReference>
2499             <o:KeyIdentifier
2500               ValueType="http://docs.oasis-open.org/wss/oasis-wss-
2501 wssecurity-secext-1.1.xsd#ThumbprintSHA1">
2502               NQM0IBvuplAtETQvk+6gn8C13wE=
2503             </o:KeyIdentifier>
2504             </o:SecurityTokenReference>
2505           </KeyInfo>
2506           <e:CipherData>
2507             <e:CipherValue>
2508 cb7+JW2idPNSarK9quqCe9PQwmW2hoUghuyKRe+I9zOts6HaMcg73LqCWuK/jtdpvN16GT/ZDYfca
2509 J7NlyMGxSiwi4DULTOshqS60TYBIKqUKiA+zXN12koVsy7amcUhPMIT6/fohH+6MzDA4t6jomcyhl
2510 CiW8d9IAzSWFkfg2k=
2511             </e:CipherValue>
2512           </e:CipherData>
2513         </e:EncryptedKey>
2514       </KeyInfo>
2515       <e:CipherData>
2516         <e:CipherValue>
2517 RDold6F1/Oewj36sjiinWLKObqsMneMhkt0toCmH6YxyszC0/M+q3CMDfwmOd0AoEeudo0NpMyjki
2518 YG9KylkWoPeTfPL+K52j2J6enttCQ8=
2519         </e:CipherValue>
2520       </e:CipherData>
2521     </e:EncryptedData>
2522     <sc:DerivedKeyToken u:Id="_0">
2523       <o:SecurityTokenReference>
2524         <o:KeyIdentifier
2525           ValueType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-
2526 profile-1.0#SAMLAssertionID">
2527           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



```

2528     </o:KeyIdentifier>
2529     </o:SecurityTokenReference>
2530     <sc:Offset>0</sc:Offset>
2531     <sc:Length>24</sc:Length>
2532     <sc:Nonce>flvBVmEJTyhdyLLf8qDxBg==</sc:Nonce>
2533     </sc:DerivedKeyToken>
2534     <sc:DerivedKeyToken u:Id="_1">
2535     <o:SecurityTokenReference>
2536     <o:KeyIdentifier
2537     Value="http://docs.oasis-open.org/wss/oasis-wss-saml-token-
2538 profile-1.0#SAMLAssertionID">
2539     uuid-78c746a2-3ec4-4cf8-a913-50d2f7334cf9-32
2540     </o:KeyIdentifier>
2541     </o:SecurityTokenReference>
2542     <sc:Nonce>
2543     OJha4PKuTZbrdYoRG+wGdQ==
2544     </sc:Nonce>
2545     </sc:DerivedKeyToken>
2546     <e:ReferenceList>
2547     <e:DataReference URI="#_3"/>
2548     </e:ReferenceList>
2549     <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
2550     <SignedInfo>
2551     <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-
2552 exc-c14n#"/>
2553     <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#hmac-
2554 sha1"/>
2555     <Reference URI="#_2">
2556     <Transforms>
2557     <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
2558 c14n#"/>
2559     </Transforms>
2560     <DigestMethod
2561 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
2562     <DigestValue>vbmdUSQRkAxqvUZpmId04sVvJtc=</DigestValue>
2563     </Reference>
2564     <Reference URI="#_4">
2565     <Transforms>
2566     <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
2567 c14n#"/>
2568     </Transforms>
2569     <DigestMethod
2570 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
2571     <DigestValue>tHsRP4mIFpGxuenN8F228dLQFgY=</DigestValue>
2572     </Reference>
2573     <Reference URI="#_5">
2574     <Transforms>
2575     <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
2576 c14n#"/>
2577     </Transforms>
2578     <DigestMethod
2579 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
2580     <DigestValue>00W235qGMKd6vRj1AYnT/wzwNUU=</DigestValue>
2581     </Reference>
2582     <Reference URI="#_6">

```

```

2583         <Transforms>
2584             <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
2585 c14n#" />
2586         </Transforms>
2587         <DigestMethod
2588 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
2589             <DigestValue>yxG97lENThCdELIX9DBR6DeuEcc=</DigestValue>
2590         </Reference>
2591         <Reference URI="#_7">
2592             <Transforms>
2593                 <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
2594 c14n#" />
2595             </Transforms>
2596             <DigestMethod
2597 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
2598                 <DigestValue>JTKMjWSZwz8Eda+SELo67k1So7U=</DigestValue>
2599             </Reference>
2600             <Reference URI="#uuid-c3cdb38b-e4aa-4467-9d0e-dd30f081e08d-10">
2601                 <Transforms>
2602                     <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
2603 c14n#" />
2604                 </Transforms>
2605                 <DigestMethod
2606 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
2607                     <DigestValue>Tj0yGTMhbgonlFR9JUsLZpZ2TQY=</DigestValue>
2608                 </Reference>
2609             </SignedInfo>
2610             <SignatureValue>DYf5TKftfZSzjz7x8+srholZ3nU=</SignatureValue>
2611             <KeyInfo>
2612                 <o:SecurityTokenReference>
2613                     <o:Reference URI="#_0" />
2614                 </o:SecurityTokenReference>
2615             </KeyInfo>
2616         </Signature>
2617     </o:Security>
2618 </s:Header>
2619 <s:Body u:Id="_2">
2620     <e:EncryptedData Id="_3">
2621         <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-
2622 cbc" />
2623         <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
2624             <o:SecurityTokenReference>
2625                 <o:Reference URI="#_1" />
2626             </o:SecurityTokenReference>
2627         </KeyInfo>
2628         <e:CipherData>
2629             <e:CipherValue>
2630 RDolD6F1/Oewj36sjiinWLKObqsMneMhkt0toCmH6YxyszC0/M+q3CMDfwmOd0AoEeudo0NpMyjki
2631 YG9KylkWoPeTfPL+K52j2J6enttCQ8=
2632             </e:CipherValue>
2633         </e:CipherData>
2634     </e:EncryptedData>
2635 </s:Body>
2636 </s:Envelope>
2637

```

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

2638 **Response Message**

2639 **Example (Non-normative)**

2640 Here is an example response.

```
2641 <s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope"
2642   xmlns:a="http://schemas.xmlsoap.org/ws/2004/08/addressing"
2643   xmlns:e="http://www.w3.org/2001/04/xmlenc#"
2644   xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
2645   wssecurity-secext-1.0.xsd"
2646   xmlns:sc="http://docs.oasis-open.org/ws-sx/ws-secureconversation/200512"
2647   xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
2648   wssecurity-utility-1.0.xsd">
2649   <s:Header>
2650     <a:Action s:mustUnderstand="1" u:Id="_4">
2651       http://example.org/PingResponse
2652     </a:Action>
2653     <a:RelatesTo u:Id="_5">
2654       urn:uuid:b6345ac8-dfc4-4174-a985-2f69cf4ac54e
2655     </a:RelatesTo>
2656     <a:To s:mustUnderstand="1" u:Id="_6">
2657       http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous
2658     </a:To>
2659     <o:Security s:mustUnderstand="1">
2660       <u:Timestamp u:Id="uuid-ad2ee057-8538-4e26-9b32-fc2cbf309f65-21">
2661         <u:Created>2005-10-24T15:51:47.244Z</u:Created>
2662         <u:Expires>2005-10-24T15:56:47.244Z</u:Expires>
2663       </u:Timestamp>
2664       <sc:DerivedKeyToken u:Id="_0" >
2665         <o:SecurityTokenReference>
2666           <o:KeyIdentifier
2667             ValueType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-
2668             profile-1.0#SAMLAssertionID">
2669             uuid-78c746a2-3ec4-4cf8-a913-50d2f7334cf9-32
2670           </o:KeyIdentifier>
2671         </o:SecurityTokenReference>
2672         <sc:Offset>0</sc:Offset>
2673         <sc:Length>24</sc:Length>
2674         <sc:Nonce>NSL/hWMxr06TuqM9TWw62g==</sc:Nonce>
2675       </sc:DerivedKeyToken>
2676       <sc:DerivedKeyToken u:Id="_1">
2677         <o:SecurityTokenReference>
2678           <o:KeyIdentifier
2679             ValueType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-
2680             profile-1.0#SAMLAssertionID">
2681             uuid-78c746a2-3ec4-4cf8-a913-50d2f7334cf9-32
2682           </o:KeyIdentifier>
2683         </o:SecurityTokenReference>
2684         <sc:Nonce>j9ELMPom+TqmOSCwKWwkhQ==</sc:Nonce>
2685       </sc:DerivedKeyToken>
2686       <e:ReferenceList>
2687         <e:DataReference URI="#_3"/>
2688       </e:ReferenceList>
2689       <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
2690         <SignedInfo>
```

```

2691     <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-
2692 exc-c14n#"/>
2693     <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#hmac-
2694 sha1"/>
2695         <Reference URI="#_2">
2696             <Transforms>
2697                 <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
2698 c14n#"/>
2699             </Transforms>
2700             <DigestMethod
2701 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
2702                 <DigestValue>BahfbtbT6EJYYlsuGAN9Yu9AdJQ=</DigestValue>
2703             </Reference>
2704             <Reference URI="#_4">
2705                 <Transforms>
2706                     <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
2707 c14n#"/>
2708                 </Transforms>
2709                 <DigestMethod
2710 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
2711                     <DigestValue>aIgoXzibEYVtNdiea5ozAxp8bcc=</DigestValue>
2712                 </Reference>
2713                 <Reference URI="#_5">
2714                     <Transforms>
2715                         <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
2716 c14n#"/>
2717                     </Transforms>
2718                     <DigestMethod
2719 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
2720                         <DigestValue>/zXTjyyUnWZONNIrgOaB0s/qJ3E=</DigestValue>
2721                     </Reference>
2722                     <Reference URI="#_6">
2723                         <Transforms>
2724                             <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
2725 c14n#"/>
2726                         </Transforms>
2727                         <DigestMethod
2728 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
2729                             <DigestValue>6LS4X08vC/GMGay2vwmD8fL7J2U=</DigestValue>
2730                         </Reference>
2731                         <Reference URI="#uuid-ad2ee057-8538-4e26-9b32-fc2cbf309f65-21">
2732                             <Transforms>
2733                                 <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
2734 c14n#"/>
2735                             </Transforms>
2736                             <DigestMethod
2737 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
2738                                 <DigestValue>t407ttquWCqTsJGFTk7YWiodT/U=</DigestValue>
2739                             </Reference>
2740                         </SignedInfo>
2741                     <SignatureValue>JrFIQ92/JCCn4QhpTHLv7sADuz8=</SignatureValue>
2742                 </KeyInfo>
2743                 <o:SecurityTokenReference>
2744                     <o:Reference URI="#_0"/>
2745                 </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

```

2746     </KeyInfo>
2747   </Signature>
2748 </o:Security>
2749 </s:Header>
2750 <s:Body u:Id=" 2">
2751   <e:EncryptedData Id="_3" Type="http://www.w3.org/2001/04/xmlenc#Content">
2752     <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-
2753 cbc"/>
2754     <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
2755       <o:SecurityTokenReference >
2756         <o:Reference URI="#_1"/>
2757       </o:SecurityTokenReference>
2758     </KeyInfo>
2759     <e:CipherData>
2760       <e:CipherValue>
2761         NdMch9ybfaSJDIZGh...
2762       </e:CipherValue>
2763     </e:CipherData>
2764   </e:EncryptedData>
2765 </s:Body>
2766 </s:Envelope>

```

### 2767 **4.3. Issued SAML 1.1 Token for Certificate, WSS 1.1**

2768 This binding is used for Scenario 5.

2769 This mode requires WS-Security 1.1.

2770 SAML token issued to the Client by STS is used to authenticate the Client. Service's X509 certificate is  
 2771 used to authenticate the Service. Client sends Request to the Service signed using DKT1(K), then  
 2772 encrypted using a DKT2(K), K is ephemeral key protected for STS's Certificate, DKT1(K) and DKT2(K)  
 2773 represent keys derived from K per WS-SecureConversation. Signature corresponding to DKT1(K) is  
 2774 signed using a key DKT(Sx) derived from symmetric proof-of-possession key Sx associated with the  
 2775 SAML token issued to the client by STS. SAML token is included in the message.

#### 2776 **Service Policy**

2777 [This is the service policy.](#)

```

2778 <wsp:Policy>
2779   <sp:SymmetricBinding>
2780     <wsp:Policy>
2781       <sp:ProtectionToken>
2782         <wsp:Policy>
2783           <sp:SamlToken sp:IncludeToken='http://docs.oasis-open.org/ws-sx/ws-
2784 securitypolicy/200512/IncludeToken/Always' >
2785             <wsp:Policy>
2786               <sp:WssSamlV11Token11 />
2787             </wsp:Policy>
2788           </sp:SamlToken>
2789         </wsp:Policy>
2790       </sp:SymmetricBinding>

```

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

2791 </sp:ProtectionToken>  
2792 <sp:SignBeforeEncrypting />  
2793 <sp:EncryptSignature />  
2794 </wsp:Policy>  
2795 </sp:SymmetricBinding>  
2796 </wsp:Policy>

## 2797 Request Message

### 2798 Example (Non-normative)

2799 Here is an example request.

```
2800 <s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope"  
2801   xmlns:a="http://schemas.xmlsoap.org/ws/2004/08/addressing"  
2802   xmlns:e="http://www.w3.org/2001/04/xmlenc#"  
2803   xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-  
2804   wssecurity-secext-1.0.xsd"  
2805   xmlns:sc="http://docs.oasis-open.org/ws-sx/ws-secureconversation/200512"  
2806   xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-  
2807   wssecurity-utility-1.0.xsd"  
2808   >  
2809   <s:Header>  
2810     <a:Action s:mustUnderstand="1" u:Id="_5">  
2811       http://example.org/Ping  
2812     </a:Action>  
2813     <a:MessageID u:Id="_6">  
2814       urn:uuid:a859eb17-1855-4d4f-8f73-85e4cba3e423  
2815     </a:MessageID>  
2816     <a:ReplyTo u:Id="_7">  
2817       <a:Address>  
2818         http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous  
2819       </a:Address>  
2820     </a:ReplyTo>  
2821     <a:To s:mustUnderstand="1" u:Id="_8">  
2822       http://server.example.com/Scenarios5  
2823     </a:To>  
2824     <o:Security s:mustUnderstand="1">  
2825       <u:Timestamp u:Id="uuid-40f5bac7-f9af-4384-80db-cfab34263849-14">  
2826         <u:Created>2005-10-25T00:47:38.222Z</u:Created>  
2827         <u:Expires>2005-10-25T00:52:38.222Z</u:Expires>  
2828       </u:Timestamp>  
2829       <e:EncryptedKey Id="uuid-40f5bac7-f9af-4384-80db-cfab34263849-4">  
2830         <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-  
2831         oaep-mgf1p"/>  
2832       <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

```

2833     <o:SecurityTokenReference>
2834         <o:KeyIdentifier
2835             ValueType="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-
2836 secext-1.1.xsd#ThumbprintSHA1">
2837             NQM0IBvuplAtETQvk+6gn8C13wE=
2838         </o:KeyIdentifier>
2839     </o:SecurityTokenReference>
2840 </KeyInfo>
2841 <e:CipherData>
2842     <e:CipherValue>
2843         <!-- base64 encoded octets of encrypted key K -->
2844     </e:CipherValue>
2845 </e:CipherData>
2846 </e:EncryptedKey>
2847 <sc:DerivedKeyToken u:Id="_0" >
2848     <o:SecurityTokenReference>
2849         <o:Reference URI="#uuid-40f5bac7-f9af-4384-80db-cfab34263849-4"/>
2850     </o:SecurityTokenReference>
2851     <sc:Offset>0</sc:Offset>
2852     <sc:Length>24</sc:Length>
2853     <sc:Nonce>7hI6U160HavffYgpquHWuQ==</sc:Nonce>
2854 </sc:DerivedKeyToken>
2855 <sc:DerivedKeyToken u:Id="_2">
2856     <o:SecurityTokenReference>
2857         <o:Reference URI="#uuid-40f5bac7-f9af-4384-80db-cfab34263849-4"/>
2858     </o:SecurityTokenReference>
2859     <sc:Nonce>OEu+WEEUxPFRQK7SCFAnEQ==</sc:Nonce>
2860 </sc:DerivedKeyToken>
2861 <e:ReferenceList>
2862     <e:DataReference URI="#_4"/>
2863 </e:ReferenceList>
2864 <!-- encrypted SAML assertion -->
2865 <e:EncryptedData Id="_3"
2866 Type="http://www.w3.org/2001/04/xmlenc#Element">
2867     <e:EncryptionMethod
2868 Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>
2869     <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
2870         <!-- encrypted Key K-->
2871         <e:EncryptedKey>
2872             <e:EncryptionMethod
2873 Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p"/>
2874             <KeyInfo>
2875                 <o:SecurityTokenReference>
2876                     <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

```

2877     ValueType="http://docs.oasis-open.org/wss/oasis-wss-
2879     NQM0IBvuplAtETQvk+6gn8C13wE=
2880     </o:KeyIdentifier>
2881     </o:SecurityTokenReference>
2882     </KeyInfo>
2883     <e:CipherData>
2884     <e:CipherValue>
2885     cb7+JW2idPNSarK9quqCe9PQwmW2hoUghuyKRe+I9zOts6HaMcg73LqCWuK/jtdpvNl6GT/ZDYfCA
2886     J7NlyMGxSiwi4DU1TOShqS6OTYBIKqUKiA+zXN12koVsy7amcUhPMIT6/fohH+6MZDA4t6jomcyhl
2887     CiW8d9IAzSWFkfg2k=
2888     </e:CipherValue>
2889     </e:CipherData>
2890     </e:EncryptedKey>
2891     </KeyInfo>
2892     <e:CipherData>
2893     <e:CipherValue>
2894     <!-- base64 encoded octets from SAML assertion encrypted with the
2895     encrypted key K above -->
2896     <!-- SAML assertion element is identical as received in RSTR ,
2897     unencrypted form is omitted for brevity -->
2898     <!--.....-->
2899     </e:CipherValue>
2900     </e:CipherData>
2901     </e:EncryptedData>
2902
2903
2904     <sc:DerivedKeyToken u:Id="\_9">
2905     <o:SecurityTokenReference>
2906     <o:KeyIdentifier
2907     ValueType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-
2908     profile-1.0#SAMLAssertionID">
2909     uuid-0c947d47-f527-410a-a674-753a9d7d97f7-16
2910     </o:KeyIdentifier>
2911     </o:SecurityTokenReference>
2912     <sc:Offset>0</sc:Offset>
2913     <sc:Length>24</sc:Length>
2914     <sc:Nonce>pgnS/VDSzJn6SFz+Vy23JA==</sc:Nonce>
2915     </sc:DerivedKeyToken>
2916     <Signature Id="\_1" xmlns="http://www.w3.org/2000/09/xmldsig#">
2917     <SignedInfo>
2918     <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-
2919     exc-c14n#"/>
2920     <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#hmac-
2921     sha1"/>
2922     <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



```
2923         <Transforms>
2924             <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
2925 c14n#" />
2926         </Transforms>
2927         <DigestMethod
2928 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
2929             <DigestValue>eQdQVGRkVl1YfKJBw7vOYCOeLQw=</DigestValue>
2930         </Reference>
2931         <Reference URI="#_5">
2932             <Transforms>
2933                 <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
2934 c14n#" />
2935             </Transforms>
2936             <DigestMethod
2937 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
2938                 <DigestValue>xxyKpp5RZ2TebKca2IGOafIgcxk=</DigestValue>
2939             </Reference>
2940             <Reference URI="#_6">
2941                 <Transforms>
2942                     <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
2943 c14n#" />
2944                 </Transforms>
2945                 <DigestMethod
2946 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
2947                     <DigestValue>WyGDdyYbL/hQZJfE3Yx2aK3RkK8=</DigestValue>
2948                 </Reference>
2949                 <Reference URI="#_7">
2950                     <Transforms>
2951                         <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
2952 c14n#" />
2953                     </Transforms>
2954                     <DigestMethod
2955 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
2956                         <DigestValue>AEOH0t2KYR8mivgqUGDrgMtxgEQ=</DigestValue>
2957                     </Reference>
2958                     <Reference URI="#_8">
2959                         <Transforms>
2960                             <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
2961 c14n#" />
2962                         </Transforms>
2963                         <DigestMethod
2964 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
2965                             <DigestValue>y8n6Dxd3DbD6TR6d6H/oVWsV4yE=</DigestValue>
2966                         </Reference>
2967                         <Reference URI="#uuid-40f5bac7-f9af-4384-80db-cfab34263849-14">
2968                             <Transforms>
```

```

2969         <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
2970 c14n#" />
2971     </Transforms>
2972     <DigestMethod
2973 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
2974     <DigestValue>/Cc+bGkkeQ6jlVXZx8PGgmF6MjI=</DigestValue>
2975     </Reference>
2976 </SignedInfo>
2977 <SignatureValue>
2978     <!--base64 encoded signature value -->
2979 </SignatureValue>
2980 <KeyInfo>
2981     <o:SecurityTokenReference>
2982     <o:Reference URI="#_0" />
2983     </o:SecurityTokenReference>
2984 </KeyInfo>
2985 </Signature>
2986 <!-- signature over the primary signature above
2987 using the key derived from the proof-key associated with SAML
2988 assertion-->
2989 <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
2990 <SignedInfo>
2991     <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-
2992 exc-c14n#" />
2993     <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#hmac-
2994 sha1" />
2995     <Reference URI="#_1">
2996     <Transforms>
2997         <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
2998 c14n#" />
2999     </Transforms>
3000     <DigestMethod
3001 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
3002     <DigestValue>TMSmLlgeUn8cxyb60Ye5Q2nUuxY=</DigestValue>
3003     </Reference>
3004 </SignedInfo>
3005 <SignatureValue>Fh4NyOpAi+NqVFihBgHWyvzah9I=</SignatureValue>
3006 <KeyInfo>
3007     <o:SecurityTokenReference>
3008     <o:Reference URI="#_9" />
3009     </o:SecurityTokenReference>
3010 </KeyInfo>
3011 </Signature>
3012 </o:Security>
3013 </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

```

3014 <s:Body u:Id="_3">
3015   <e:EncryptedData Id="_4" Type="http://www.w3.org/2001/04/xmlenc#Content">
3016     <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-
3017 cbc"/>
3018     <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
3019       <o:SecurityTokenReference >
3020         <o:Reference URI="#_2"/>
3021       </o:SecurityTokenReference>
3022     </KeyInfo>
3023     <e:CipherData>
3024       <e:CipherValue>
3025         <!-- base64 encoded octets of encrypted body content-->
3026       </e:CipherValue>
3027     </e:CipherData>
3028   </e:EncryptedData>
3029 </s:Body>
3030 </s:Envelope>

```

### 3031 Response Message

#### 3032 *Example (Non-normative)*

3033 Here is an example response.

```

3034 <s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope"
3035   xmlns:a="http://schemas.xmlsoap.org/ws/2004/08/addressing"
3036   xmlns:e="http://www.w3.org/2001/04/xmlenc#"
3037   xmlns:k="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-
3038 1.1.xsd"
3039   xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
3040 wssecurity-secext-1.0.xsd"
3041   xmlns:sc="http://docs.oasis-open.org/ws-sx/ws-secureconversation/200512"
3042   xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
3043 wssecurity-utility-1.0.xsd">
3044   <s:Header>
3045     <a:Action s:mustUnderstand="1" u:Id="_6">
3046       http://example.org/PingResponse
3047     </a:Action>
3048     <a:RelatesTo u:Id="_7">
3049       urn:uuid:a859eb17-1855-4d4f-8f73-85e4cba3e423
3050     </a:RelatesTo>
3051     <a:To s:mustUnderstand="1" u:Id="_8">
3052       http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous
3053     </a:To>
3054     <o:Security s:mustUnderstand="1">
3055       <u:Timestamp u:Id="uuid-24adda3a-247a-4fec-b4f7-fb3827496cee-16">
3056         <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

```

3057     <u:Expires>2005-10-25T00:52:38.921Z</u:Expires>
3058   </u:Timestamp>
3059   <sc:DerivedKeyToken u:Id="_0" >
3060     <o:SecurityTokenReference>
3061       <o:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/oasis-
3062 wss-wssecurity-secext-
3063 1.1.xsd#EncryptedKeySHA1">pDJlrSJLzIqi+AcQLUB4GjUuRLs</o:KeyIdentifier>
3064     </o:SecurityTokenReference>
3065     <sc:Offset>0</sc:Offset>
3066     <sc:Length>24</sc:Length>
3067     <sc:Nonce>KFjy1Gb73BubLul0ZGgx+w==</sc:Nonce>
3068   </sc:DerivedKeyToken>
3069   <sc:DerivedKeyToken u:Id="_3">
3070     <o:SecurityTokenReference>
3071       <o:KeyIdentifier
3072         ValueType="http://docs.oasis-open.org/wss/oasis-wssecurity-
3073 secext-
3074 1.1.xsd#EncryptedKeySHA1">pDJlrSJLzIqi+AcQLUB4GjUuRLs</o:KeyIdentifier>
3075     </o:SecurityTokenReference>
3076     <sc:Nonce>omyh+Eg6XIa8q3V5IkHiXg==</sc:Nonce>
3077   </sc:DerivedKeyToken>
3078   <e:ReferenceList>
3079     <e:DataReference URI="#_5"/>
3080   </e:ReferenceList>
3081   <k:SignatureConfirmation u:Id="_1"
3082 Value="EyKUHUuffPUPE/ZjaFrMJJ5KLKY="/>
3083   <k:SignatureConfirmation u:Id="_2"
3084 Value="Fh4NyOpAi+NqVFiHBgHWyvzah9I="/>
3085   <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
3086     <SignedInfo>
3087       <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-
3088 exc-c14n#" />
3089       <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#hmac-
3090 sha1" />
3091       <Reference URI="#_4">
3092         <Transforms>
3093           <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
3094 c14n#" />
3095         </Transforms>
3096         <DigestMethod
3097 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
3098         <DigestValue>y/oItF5TcTOFan7SavhZTTTv48M</DigestValue>
3099       </Reference>
3100       <Reference URI="#_6">
3101         <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

```
3102         <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
3103 c14n#" />
3104     </Transforms>
3105     <DigestMethod
3106 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
3107     <DigestValue>X4UIaLWnaAWTriw4UJ/SFDgm090=</DigestValue>
3108     </Reference>
3109     <Reference URI="#_7">
3110     <Transforms>
3111         <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
3112 c14n#" />
3113     </Transforms>
3114     <DigestMethod
3115 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
3116     <DigestValue>vqy8/D4CDCaI1nnd4w11Qjyp+qM=</DigestValue>
3117     </Reference>
3118     <Reference URI="#_8">
3119     <Transforms>
3120         <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
3121 c14n#" />
3122     </Transforms>
3123     <DigestMethod
3124 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
3125     <DigestValue>H11vLAr5g8pbZ6jfz+2WNYiNjiM=</DigestValue>
3126     </Reference>
3127     <Reference URI="#uuid-24adda3a-247a-4fec-b4f7-fb3827496cee-16">
3128     <Transforms>
3129         <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
3130 c14n#" />
3131     </Transforms>
3132     <DigestMethod
3133 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
3134     <DigestValue>dr0g6hycoc884i+BD8FYCJGbbbE=</DigestValue>
3135     </Reference>
3136     <Reference URI="#_1">
3137     <Transforms>
3138         <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
3139 c14n#" />
3140     </Transforms>
3141     <DigestMethod
3142 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
3143     <DigestValue>Rv3N7VNfAqpn0khr3F/qQZmE/l4=</DigestValue>
3144     </Reference>
3145     <Reference URI="#_2">
3146     <Transforms>
```

```

3147         <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
3148 c14n#" />
3149     </Transforms>
3150     <DigestMethod
3151 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
3152     <DigestValue>X2pxEnYPM8cMLrbhNqPgs8xk+a4=</DigestValue>
3153     </Reference>
3154 </SignedInfo>
3155 <SignatureValue>I2jQuDTWWQiNJy/ziyg8AFYO/z4=</SignatureValue>
3156 <KeyInfo>
3157     <o:SecurityTokenReference>
3158     <o:Reference URI="#_0" />
3159     </o:SecurityTokenReference>
3160 </KeyInfo>
3161 </Signature>
3162 </o:Security>
3163 </s:Header>
3164 <s:Body u:Id="_4">
3165     <e:EncryptedData Id="_5" Type="http://www.w3.org/2001/04/xmlenc#Content">
3166     <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-
3167 cbc" />
3168     <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
3169     <o:SecurityTokenReference>
3170     <o:Reference URI="#_3" />
3171     </o:SecurityTokenReference>
3172 </KeyInfo>
3173 <e:CipherData>
3174 <e:CipherValue>
3175     <!--base64 encoded octets of encrypted body content-->
3176 </e:CipherValue>
3177 </e:CipherData>
3178 </e:EncryptedData>
3179 </s:Body>
3180 </s:Envelope>

```

#### 3181 4.4. SecureConversation

3182 This binding is used for Scenario 6.

3183 Secure session key Sz is established following Secure Conversation. RequestSecurityToken and  
3184 RequestSecurityTokenResponse are protected following IssuedTokenForCertificate binding described  
3185 above. Application messages are protected using symmetric keys derived from Sz following Secure  
3186 Conversation.

3187

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

3188 [Service Policy](#)

3189 [This is the service policy.](#)

3190

```
3191 <wsp:Policy>
3192   <sp:SymmetricBinding>
3193     <wsp:Policy>
3194       <sp:ProtectionToken>
3195         <wsp:Policy>
3196           <sp:SecurityContextToken sp:IncludeToken='http://docs.oasis-
3197 open.org/ws-sx/ws-securitypolicy/200512/IncludeToken/Always' />
3198         </wsp:Policy>
3199       </sp:ProtectionToken>
3200     </wsp:Policy>
3201   </sp:SymmetricBinding>
3202 </wsp:Policy>
```

3203 [Request Message](#)

Frederick Hirsch 7/21/06 6:17 PM

Deleted: ¶

3204 **Example (Non-normative)**

3205 Here is an example request.

```
3206 <s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope"
3207   xmlns:a="http://schemas.xmlsoap.org/ws/2004/08/addressing"
3208   xmlns:e="http://www.w3.org/2001/04/xmlenc#"
3209   xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
3210 wssecurity-secext-1.0.xsd"
3211   xmlns:sc="http://docs.oasis-open.org/ws-sx/ws-secureconversation/200512"
3212   xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
3213 wssecurity-utility-1.0.xsd"
3214 >
3215   <s:Header>
3216     <a:Action s:mustUnderstand="1" u:Id="_2">
3217       http://example.org/Ping
3218     </a:Action>
3219     <a:MessageID u:Id="_3">
3220       urn:uuid:94e6ed8b-7084-48e1-bba7-85c4ea50c512
3221     </a:MessageID>
3222     <a:ReplyTo u:Id="_4">
3223       <a:Address>
3224         http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous
3225       </a:Address>
3226     </a:ReplyTo>
3227     <a:To s:mustUnderstand="1" u:Id="_5">
3228       http://server.example.com/Scenarios6
3229     </a:To>
```

```

3230 <o:Security s:mustUnderstand="1">
3231 <u:Timestamp u:Id="uuid-5df39133-c58e-4b83-9b86-e20bf5efe563-17">
3232 <u:Created>2005-11-02T23:38:05.175Z</u:Created>
3233 <u:Expires>2005-11-02T23:43:05.175Z</u:Expires>
3234 </u:Timestamp>
3235 <sc:SecurityContextToken u:Id="uuid-8930d45e-14b0-42f5-b415-
3236 6b4ee115b943-7">
3237 <sc:Identifier>
3238 urn:uuid:8e6a3a95-fd1b-4c24-96d4-28e875025ff7
3239 </sc:Identifier>
3240 </sc:SecurityContextToken>
3241 <!-- START: Key derived from SCT-Key used for signing. -->
3242 <sc:DerivedKeyToken u:Id="uuid-5df39133-c58e-4b83-9b86-e20bf5efe563-12">
3243 <o:SecurityTokenReference>
3244 <o:Reference URI="#uuid-8930d45e-14b0-42f5-b415-6b4ee115b943-7" />
3245 </o:SecurityTokenReference>
3246 <sc:Offset>0</sc:Offset>
3247 <sc:Length>24</sc:Length>
3248 <sc:Nonce>lCO/qhHek2+0qiFPEwdeLw==</sc:Nonce>
3249 </sc:DerivedKeyToken>
3250 <!-- END: Key derived from SCT-Key used for signing. -->
3251 <!-- START: Key derived from SCT-Key used for encryption. -->
3252 <sc:DerivedKeyToken u:Id="uuid-5df39133-c58e-4b83-9b86-e20bf5efe563-13">
3253 <o:SecurityTokenReference>
3254 <o:Reference URI="#uuid-8930d45e-14b0-42f5-b415-6b4ee115b943-7" />
3255 </o:SecurityTokenReference>
3256 <sc:Nonce>rMICQZ+A6CWAjF3/j6XauA==</sc:Nonce>
3257 </sc:DerivedKeyToken>
3258 <!-- END: Key derived from SCT-Key used for encryption. -->
3259 <e:ReferenceList xmlns:e="http://www.w3.org/2001/04/xmlenc#">
3260 <e:DataReference URI="#_1" />
3261 </e:ReferenceList>
3262 <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
3263 <SignedInfo>
3264 <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
3265 <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#hmac-sha1" />
3266 <Reference URI="#_0">
3267 <Transforms>
3268 <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
3269 </Transforms>
3270 <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
3271 <DigestValue>zXrQhCxRjuPxmhQB2iSzCDNp/fg</DigestValue>
3272 </Reference>
3273 <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



```
3274     <Transforms>
3275     <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
3276     </Transforms>
3277     <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
3278     <DigestValue>zXrQhCxRjuPxmhQB2iSzCDNp/fg=</DigestValue>
3279 </Reference>
3280 <Reference URI="#_2">
3281     <Transforms>
3282     <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
3283     </Transforms>
3284     <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
3285     <DigestValue>NQGQB5EcC5nODzdIHfvhYeqqxOE=</DigestValue>
3286 </Reference>
3287 <Reference URI="#_3">
3288     <Transforms>
3289     <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
3290     </Transforms>
3291     <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
3292     <DigestValue>IBNjyw72JuzKU0plbF2eEWm0rHk=</DigestValue>
3293 </Reference>
3294 <Reference URI="#_4">
3295     <Transforms>
3296     <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
3297     </Transforms>
3298     <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
3299     <DigestValue>IBNjyw72JuzKU0plbF2eEWm0rHk=</DigestValue>
3300 </Reference>
3301 <Reference URI="#_5">
3302     <Transforms>
3303     <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
3304     </Transforms>
3305     <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
3306     <DigestValue>IBNjyw72JuzKU0plbF2eEWm0rHk=</DigestValue>
3307 </Reference>
3308 <Reference URI="#uuid-ff348436-ba42-41ea-bec2-2f1138f29623-17">
3309     <Transforms>
3310     <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
3311     </Transforms>
3312     <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
3313     <DigestValue>jX1/gPMBRWBKgq7WNAjdFkIFPxI=</DigestValue>
3314 </Reference>
3315 </SignedInfo>
3316 <SignatureValue>j6nmdxEi4kTks81DqdxSPpZDiTw=</SignatureValue>
3317 <KeyInfo>
```

```

3318     <o:SecurityTokenReference>
3319     <o:Reference URI="#uuid-ff348436-ba42-41ea-bec2-2f1138f29623-12">
3320     </o:Reference>
3321     </o:SecurityTokenReference>
3322 </KeyInfo>
3323 </Signature>
3324 </o:Security>
3325 </s:Header>
3326 <s:Body u:Id="_0">
3327     <e:EncryptedData Id="_1" Type="http://www.w3.org/2001/04/xmlenc#Content">
3328 <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>
3329     <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
3330     <o:SecurityTokenReference >
3331     <o:Reference URI="#uuid-5df39133-c58e-4b83-9b86-e20bf5efe563-13" />
3332     </o:SecurityTokenReference>
3333     </KeyInfo>
3334     <e:CipherData>
3335     <e:CipherValue>...20X2ZX01grMOPbUMXYmeXXY</e:CipherValue>
3336     </e:CipherData>
3337     </e:EncryptedData>
3338 </s:Body>
3339 </s:Envelope>

```

#### 3340 Response Message

```

3341 <s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope"
3342   xmlns:a="http://schemas.xmlsoap.org/ws/2004/08/addressing"
3343   xmlns:e="http://www.w3.org/2001/04/xmlenc#"
3344   xmlns:k="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-
3345   1.1.xsd"
3346   xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
3347   wssecurity-secext-1.0.xsd"
3348   xmlns:sc="http://docs.oasis-open.org/ws-sx/ws-secureconversation/200512"
3349   xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
3350   wssecurity-utility-1.0.xsd">
3351 <s:Header>
3352   <a:Action s:mustUnderstand="1" u:Id="_2">
3353     http://example.org/Ping
3354   </a:Action>
3355   <a:RelatesTo u:Id="_1">
3356     urn:uuid:94e6ed8b-7084-48e1-bba7-85c4ea50c512
3357   </a:RelatesTo>
3358   <a:To s:mustUnderstand="1" u:Id="_3">
3359     http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous
3360   </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

```

3361 <o:Security s:mustUnderstand="1">
3362 <u:Timestamp u:Id="uuid-8930d45e-14b0-42f5-b415-6b4ee115b943-16">
3363 <u:Created>2005-11-02T23:38:05.253Z</u:Created>
3364 <u:Expires>2005-11-02T23:43:05.253Z</u:Expires>
3365 </u:Timestamp>
3366 <!-- START: Derived key SCT-Key1 used for signing. -->
3367 <sc:DerivedKeyToken u:Id="uuid-8930d45e-14b0-42f5-b415-6b4ee115b943-10">
3368 <o:SecurityTokenReference>
3369 <o:Reference URI="urn:uuid:8e6a3a95-fd1b-4c24-96d4-28e875025ff7"
3370 ValueType="http://docs.oasis-open.org/ws-sx/ws-secureconversation/200512/sct"
3371 />
3372 </o:SecurityTokenReference>
3373 <sc:Offset>0</sc:Offset>
3374 <sc:Length>24</sc:Length>
3375 <sc:Nonce>ZakR9dMZmd4Lba7qLOY56w==</sc:Nonce>
3376 </sc:DerivedKeyToken>
3377 <!-- END: Derived key SCT-Key1 used for signing. -->
3378 <!-- START: Derived key SCT-Key2 used for encryption. -->
3379 <sc:DerivedKeyToken u:Id="uuid-8930d45e-14b0-42f5-b415-6b4ee115b943-11">
3380 <o:SecurityTokenReference>
3381 <o:Reference URI="urn:uuid:8e6a3a95-fd1b-4c24-96d4-28e875025ff7"
3382 ValueType="http://docs.oasis-open.org/ws-sx/ws-secureconversation/200512/sct"
3383 />
3384 </o:SecurityTokenReference>
3385 <sc:Nonce>t+R+jHxI8T642/HLd0EHIA==</sc:Nonce>
3386 </sc:DerivedKeyToken>
3387 <!-- END: Derived key SCT-Key2 used for encryption. -->
3388 <e:ReferenceList>
3389 <e:DataReference URI="#_4" />
3390 </e:ReferenceList>
3391
3392 <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
3393 <SignedInfo>
3394 <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
3395 </CanonicalizationMethod>
3396 <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#hmac-sha1">
3397 </SignatureMethod>
3398 <Reference URI="#_0">
3399 <Transforms>
3400 <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
3401 </Transform>
3402 </Transforms>
3403 <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
3404 </DigestMethod>

```

```
3405     <DigestValue>3gVmAaye1xmL7Y+rC2iGKxAsT6w=</DigestValue>
3406 </Reference>
3407 <Reference URI="#_1">
3408   <Transforms>
3409     <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
3410     </Transform>
3411   </Transforms>
3412   <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
3413   </DigestMethod>
3414   <DigestValue>nHUD4Ojy3RPL1M7NFEkaF1SgRsI=</DigestValue>
3415 </Reference>
3416 <Reference URI="#_2">
3417   <Transforms>
3418     <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
3419     </Transform>
3420   </Transforms>
3421   <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
3422   </DigestMethod>
3423   <DigestValue>Y7ZFX24xNjoNfJMnX1YvgPNdQd0=</DigestValue>
3424 </Reference>
3425 <Reference URI="#_3">
3426   <Transforms>
3427     <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
3428     </Transform>
3429   </Transforms>
3430   <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
3431   </DigestMethod>
3432   <DigestValue>QgsDL8L8Nn0rI2wj44V5Wn6a7Vg=</DigestValue>
3433 </Reference>
3434 <Reference URI="#_7">
3435   <Transforms>
3436     <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
3437     </Transform>
3438   </Transforms>
3439   <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
3440   </DigestMethod>
3441   <DigestValue>QgsDL8L8Nn0rI2wj44V5Wn6a7Vg=</DigestValue>
3442 </Reference>
3443 <Reference URI="#uuid-f96d9fdb-f7d3-4e14-95b8-503a8e163d45-16">
3444   <Transforms>
3445     <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
3446     </Transform>
3447   </Transforms>
3448   <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

```

3449         </DigestMethod>
3450         <DigestValue>fUOV9sL3vcJtyC7agjaIvYG/bbw=</DigestValue>
3451     </Reference>
3452 </SignedInfo>
3453 <SignatureValue>DNxG4BukpgO8NJ6Rr7RXyZ15unM=</SignatureValue>
3454 <KeyInfo>
3455     <o:SecurityTokenReference>
3456         <o:Reference URI="#uuid-f96d9fdb-f7d3-4e14-95b8-503a8e163d45-10">
3457             </o:Reference>
3458         </o:SecurityTokenReference>
3459     </KeyInfo>
3460 </Signature>
3461 </o:Security>
3462 </s:Header>
3463 <s:Body u:Id="_7" >
3464     <e:EncryptedData Id="_3" Type="http://www.w3.org/2001/04/xmlenc#Content">
3465 <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>
3466     <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
3467         <o:SecurityTokenReference>
3468             <o:Reference URI="#uuid-8930d45e-14b0-42f5-b415-6b4ee115b943-11"/>
3469         </o:SecurityTokenReference>
3470     </KeyInfo>
3471     <e:CipherData>
3472 <e:CipherValue>gRGx8V7NPorFrFQ2TnzdUPT7h6nZuFERLwt7G1N8Npi01B0Uju7N27U5Fwqqw1
3473 zsIzQyJxKtmwTop6ghczvGh8jleW25N0JK4Ef7qCPhiTIwof/8abZuvJI+ckw+4HEe</e:CipherV
3474 alue>
3475 </e:CipherData>
3476 </e:EncryptedData>
3477 </s:Body>
3478 </s:Envelope>

```

#### 3480 **Example (Non-normative)**

3481 Here is an example response.

#### 3482 **4.5. Issued SAML 2.0 Token**

3483 This binding is used in Scenario 7.

3484 SAML token issued to the Client by STS is used to authenticate the Client. Messages are signed then  
3485 encrypted using symmetric keys derived from the symmetric proof-of-possession key Sx associated with  
3486 the SAML token.

3487

3488 **Service Policy**

3489 [This is the service policy, now with SAML 2.0 and WSS 1.1 SAML Token Profile](#)

3490

```
3491 <wsp:Policy>
3492   <sp:SymmetricBinding>
3493     <wsp:Policy>
3494       <sp:ProtectionToken>
3495         <wsp:Policy>
3496           <sp:SamlToken sp:IncludeToken='http://docs.oasis-open.org/ws-sx/ws-
3497 securitypolicy/200512/IncludeToken/Always' >
3498             <wsp:Policy>
3499               <sp:WssSamlV20Token11 />
3500             </wsp:Policy>
3501           </sp:SamlToken>
3502         </wsp:Policy>
3503       </sp:ProtectionToken>
3504     <sp:SignBeforeEncrypting />
3505     <sp:EncryptSignature />
3506   </wsp:Policy>
3507 </sp:SymmetricBinding>
3508 </wsp:Policy>
```

3509 **Request Message**

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

3510 **Example (Non-normative)**

3511 Here is an example request.

3512 **Response Message**

3513 **Example (Non-normative)**

3514 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

## 3516 5.1. STS

```
3517 <?xml version="1.0" encoding="utf-8"?>
3518 <wsdl:definitions name="SecurityTokenService"
3519   targetNamespace="http://tempuri.org/"
3520   xmlns:tns="http://tempuri.org/"
3521   xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
3522   xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/"
3523   xmlns:t="http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust">
3524   <wsdl:import namespace="http://docs.oasis-open.org/ws-sx/ws-
3525     trust/200512/ws-trust"
3526     location="http://www.oasis-open.org/apps/org/workgroup/ws-
3527     sx/download.php/16291/oasis-wssx-ws-trust-1.0.wsdl"/>
3528   <wsdl:binding name="SecurityTokenService" type="t:SecurityTokenService">
3529     <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
3530     <wsdl:operation name="ProcessRequestSecurityToken">
3531       <soap12:operation soapAction="http://docs.oasis-open.org/ws-sx/ws-
3532       trust/200512/ws-trust/RST/Issue" style="document"/>
3533       <wsdl:input>
3534         <soap12:body use="literal"/>
3535       </wsdl:input>
3536       <wsdl:output>
3537         <soap12:body use="literal"/>
3538       </wsdl:output>
3539     </wsdl:operation>
3540   </wsdl:binding>
3541   <wsdl:binding name="SecurityTokenService1" type="t:SecurityTokenService">
3542     <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
3543     <wsdl:operation name="ProcessRequestSecurityToken">
3544       <soap12:operation soapAction="http://docs.oasis-open.org/ws-sx/ws-
3545       trust/200512/ws-trust/RST/Issue" style="document"/>
3546       <wsdl:input>
3547         <soap12:body use="literal"/>
3548       </wsdl:input>
3549       <wsdl:output>
3550         <soap12:body use="literal"/>
3551       </wsdl:output>
3552     </wsdl:operation>
3553   </wsdl:binding>
3554   <wsdl:service name="SecurityTokenService">
3555     <wsdl:port name="SecurityTokenService_port"
3556     binding="tns:SecurityTokenService">
```

```
3557     <soap12:address location="http://example.org/Sts/MutualCertificate11"/>
3558   </wsdl:port>
3559   <wsdl:port name="SecurityTokenService1_port"
3560 binding="tns:SecurityTokenService1">
3561     <soap12:address location="http://example.org/Sts/MutualCertificate10"/>
3562   </wsdl:port>
3563 </wsdl:service>
3564 </wsdl:definitions>
```

## 5.2. Service

```
3565 <?xml version="1.0" encoding="utf-8"?>
3566 <wsdl:definitions name="PingService"
3567   targetNamespace="http://tempuri.org/"
3568   xmlns:tns="http://tempuri.org/"
3569   xmlns:i0="http://example.org/Ping"
3570   xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
3571   xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/"
3572 >
3573   <wsdl:import namespace="http://example.org/Ping"
3574 location="service_portType.wsdl"/>
3575   <wsdl:types/>
3576   <wsdl:binding name="IPingService" type="i0:IPingService">
3577     <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
3578     <wsdl:operation name="Ping">
3579       <soap12:operation soapAction="http://example.org/Ping"
3580 style="document"/>
3581       <wsdl:input name="PingRequest">
3582         <soap12:body use="literal"/>
3583       </wsdl:input>
3584       <wsdl:output name="PingResponse">
3585         <soap12:body use="literal"/>
3586       </wsdl:output>
3587     </wsdl:operation>
3588   </wsdl:binding>
3589   <wsdl:service name="PingService">
3590     <wsdl:port name="IPingService_port" binding="tns:IPingService">
3591       <soap12:address location="http://example.org/PingService"/>
3592     </wsdl:port>
3593   </wsdl:service>
3594 </wsdl:definitions>
```

3596

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



3597 6. References

- 3598 **6.1. Normative**  
3599 **[RFC2119]** S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*,  
3600 <http://www.ietf.org/rfc/rfc2119.txt>, IETF RFC 2119, March 1997.

3601  
3602

## 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

3603

## 8. Revision History

Frederick Hirsch 7/21/06 4:21 PM

Formatted: Bullets and Numbering

3604

Rev	Date	By Whom	What
00	2006-04-25	Marc Goodner	First merge of previous interop scenarios contributed to SX TC from <a href="#">Marc Goodner</a> and <a href="#">Prateek Mishra</a> .
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
<u>04</u>	<u>2006-07-18</u>	<u>Marc Goodner</u>	<u>Correction from Jan Alexander comments to TC list.</u>

3605