

1 | OASIS WEB SERVICES SECURE EXCHANGE TC

2  
3 a. Name of the TC

4  
5 OASIS Web Services Secure Exchange (WS-SX) Technical  
6 Committee

7  
8 b. Statement of Purpose

9  
10 The purpose of the Web Services Secure Exchange (WS-SX)  
11 Technical Committee (TC) is to define extensions to OASIS Web  
12 Services Security [1] to enable trusted SOAP message exchanges  
13 involving multiple message exchanges and to define security policies  
14 that govern the formats and tokens of such messages. This work will  
15 be carried out through continued refinement of the Web Services  
16 SecureConversation, SecurityPolicy and Trust specifications [2-4]  
17 submitted to the TC as referenced in this charter.

18  
19 c. Scope of Work

20  
21 The TC will accept as input the February 2005 Version 1.2 of the  
22 WS-SecureConversation [2] and the February 2005 Version 1.2 of  
23 the WS-Trust [3] as published by Actional Corporation, BEA  
24 Systems, Inc., Computer Associates International, Inc., IBM, Layer 7  
25 Technologies, Microsoft Corporation, Oblix Inc., OpenNetwork  
26 Technologies Inc., Ping Identity Corporation, Reactivity Inc., RSA  
27 Security Inc., and VeriSign Inc and the July 2005 Version 1.1 WS-  
28 SecurityPolicy [4] specifications (the Input Documents) as published  
29 by IBM, Microsoft, RSA Security and VeriSign.

30  
31 Other contributions and changes to the input documents will be  
32 accepted for consideration without any prejudice or restrictions and  
33 evaluated based on technical merit in so far as they conform to this  
34 charter. OASIS members with extensive experience and knowledge  
35 in these areas are particularly invited to participate.

36  
37 In order to support general secure Web Service messaging,  
38 additional facilities are needed beyond what is provided in OASIS  
39 Web Services Security [1]. The OASIS Web Services Security  
40 specification describes a base mechanism for securing SOAP

41 messages but does not deal with trust brokering, multi-message  
42 exchanges, and policies describing how to secure message  
43 exchanges with a Web service. The following sub-sections describe  
44 the charter of the WS-SX TC with respect to these areas.  
45 The scope of the TC's work is to continue further refinement and  
46 finalization of the Input Documents to produce as output modular  
47 specifications that standardize the concepts, WSDL documents and  
48 XML Schema renderings of the areas described below.

#### 49 50 Trusted Brokering of SOAP message exchanges

51  
52 OASIS Web Services Security [1] defines the basic mechanism for  
53 providing secure SOAP messaging. It describes how to use security  
54 tokens to obtain message integrity, confidentiality and authentication  
55 of the message sender. In order to establish the authenticity of any  
56 message sender, the recipient needs to "trust" the asserted  
57 credentials of the sender. The WS-SX TC will add additional  
58 primitives to enable the establishing and brokering of these trust  
59 relationships between parties in a SOAP message exchange as  
60 defined by the policy expressions associated with the SOAP  
61 endpoints.

62  
63 The scope of this work is to develop extensions to OASIS Web  
64 Services Security [1] that facilitate "trusted" SOAP message  
65 exchanges. This will be done by enabling the web services to  
66 participate in the establishment and brokering of trust relationships  
67 by means of an exchange and issuance of the relevant security  
68 tokens. In addition, some token and message validation may require  
69 the definition of specialized SOAP messages and header blocks.

70  
71 This work will focus on:

- 72 1. Describing a protocol for brokering trust on behalf of a requestor  
73 by obtaining designated security tokens containing required claims  
74 from the trusted authorities.
- 75 2. Describing a framework for interactions with trusted authorities  
76 known as security token services. This includes describing the  
77 request/response elements for interactions with a security token  
78 service. This base framework for requesting and returning of security  
79 tokens should be usable for a variety of purposes related to security  
80 token services. Web service trust bindings define how this

81 framework is used for specific usage patterns. This specification  
82 defines Web service trust bindings for issuance, renewal, cancellation  
83 and validation of security tokens.

84 3. Declaring specific Web service bindings to a security token  
85 service for security token issuance including, but not limited to the  
86 following cases:

87 a. Actions and elements for requesting a security token (or  
88 tokens).

89 b. Actions and elements for responding with a security token (or  
90 tokens).

91 c. Specifying the scope of each requested and returned security  
92 token using WS-Policy [5] <wsp:AppliesTo> (eg.  
93 wsa:endpointReference).

Frederick Hirsch 12/6/05 2:12 PM  
Formatted: Font:Times New Roman, 16  
pt

94 d. Specifying mechanisms for issuing, computing or utilizing  
95 existing keys as proof keys associated with the issued token.

Frederick Hirsch 12/6/05 2:12 PM  
Formatted: Font:Times New Roman, 16  
pt

96 e. Support for requesting and returning bearer tokens

97 f. Requesting or returning multiple security tokens.

Frederick Hirsch 12/6/05 2:12 PM  
Formatted: Font:Times New Roman

98 g. Transferring security tokens as part of application messages as  
99 well as part of the SOAP body of a separate response message

100 h. Requesting a security token (or tokens) on behalf of another  
101 entity (or entities).

102 i. Requesting a security token (or tokens) that may be forwardable  
103 or delegatable.

104 j. Specifying characteristics of the requested type of keys.

105 k. Enabling additional negotiation and challenge mechanisms  
106 (e.g. SASL, SPNEGO) initiated by either client or server.

Frederick Hirsch 12/6/05 2:12 PM  
Formatted: Font:Times New Roman, 16  
pt

Frederick Hirsch 12/6/05 2:12 PM  
Formatted: Font:Times New Roman, 16  
pt

108 4. Declaring specific Web service bindings of the security token  
109 service framework for security token renewal. Renewal is the process  
110 by which a previously issued token with expiration is presented at a  
111 security token service and the same token is returned with new  
112 expiration characteristics. Such a renewal binding should be defined  
113 for (but not be limited to) the following:

114 a. Actions and elements for requesting the renewal of a single  
115 token.

116 b. Actions and elements for responding with a renewed token (or  
117 tokens).

Frederick Hirsch 12/6/05 2:13 PM  
Formatted: Font:Times New Roman, 16  
pt

118 c. Allowing for direct or indirect references to the security tokens  
119 being renewed.

Frederick Hirsch 12/6/05 2:13 PM  
Formatted: Font:Times New Roman

120 5. Declaring specific Web service trust bindings of the security token  
121 service framework for cancellation. When a previously issued token  
122 is no longer needed, the cancel binding can be used to cancel the  
123 token,  
124 terminating its use. Such cancel binding should define (but not be  
125 limited to) the following cases:  
126 a. Actions and elements for requesting the cancellation of a single  
127 token.  
128 b. Actions and elements for responding with the cancellation  
129 result.  
130 c. Allowing for direct or indirect references to the security tokens  
131 being cancelled.

132 6. Declaring specific Web service trust bindings of the security token  
133 service framework for token validation. Validation binding is used to  
134 evaluate a security token (or OASIS Web Services Security [1]  
135 compliant message) and the result is returned as a status, token or  
136 both. Such a validation binding should be defined for (but not be  
137 limited to) the following:  
138 a. Actions and elements for requesting the validation of a token  
139 (or message).  
140 b. Actions and elements for responding about the validity of a  
141 token (or tokens).  
142 c. Allowing for direct or indirect references to the security tokens  
143 being validated.

144 7. Generalizing the mechanism for a security token service to allow  
145 for multi-leg exchanges. Such exchange should allow for, but not be  
146 limited to "challenges", tunnelling of legacy binary protocols, and  
147 tunnelling of  
148 hardware-based legacy protocols. Specifically, the following models  
149 of challenge and exchanges should be defined by this specification:  
150 a. Signature challenge that requires the other party to sign  
151 specified information.  
152 b. Binary exchanges involving the usage of binary data from  
153 existing non-Web Services protocols.  
154 c. Exchanges involving request and passing of a key exchange  
155 token

156  
157 Shared security contexts  
158  
159 OASIS Web Services Security [1] describes using security

160 credentials to implement message integrity, confidentiality and  
161 authentication. In cases where multiple messages need to be  
162 exchanged securely, typically a shared security context is established  
163 between the communicating parties and used for the life time of the  
164 message exchange. This TC will also address adding extensions to  
165 Web Services Security [1] and define the appropriate secure SOAP  
166 message exchanges (see above) to permit the definition of shared  
167 security contexts.

168  
169 This work will encompass:

- 170 1. Defining mechanisms for establishing a shared security context in  
171 the following cases:
  - 172 a. When one of the communicating parties creates the context and  
173 propagates it to other parties.
  - 174 b. When the shared context is achieved through a sequence of  
175 negotiations.
  - 176 c. When the shared context is brokered through a third party  
177 security token service.
- 178 2. Defining specific Web service bindings for security context  
179 establishment by utilizing the Web service trust binding elements for  
180 requesting and responding with security context tokens.
- 181 3. Defining specific Web service bindings for renewal of the security  
182 context token.
- 183 4. Defining specific Web service bindings for cancellation of the  
184 security context token.
- 185 5. Defining specific Web service bindings for amendment of the  
186 claims associated with a security context.
- 187 6. Since a shared security context may contain or imply a shared  
188 key, this specification must contain descriptions of common elements  
189 for key derivation models, where such a scheme is desirable for  
190 improving the security characteristics of the keys being used.
- 191 7. Defining a token profile for use of security context tokens with  
192 OASIS Web Services Security [1].
- 193 8. Defining a token profile for use of derived key tokens with OASIS  
194 Web Services Security [1].

195  
196 Security policies

197  
198 OASIS Web Services Security [1], WS-SecureConversation [2] and  
199 WS-Trust [3] define open-ended wire formats. WS-Policy [5]

200 defines a framework for allowing web services to express their  
201 constraints and requirements as policy assertions. WS-SecurityPolicy  
202 [4] uses the facilities of WS-Policy [5] to express the conditions and  
203 restrictions on the wire formats defined by OASIS Web Services  
204 Security [1], WS-SecureConversation [2] and WS-Trust [3] to a  
205 specific set of typed message interchanges. That is to say WS-  
206 SecurityPolicy "strongly types" the supported security messages.  
207 This type of policy enablement allows the supported message  
208 exchanges to be analyzed from a security perspective to indicate  
209 which security protocols an end point supports.

210

211 This work will specifically define the following:

212 1. Mechanism for specifying what parts of the message must be  
213 secured, called protection assertions

214 a. Such protection assertions must be able to specify integrity  
215 requirements at both the element and header/body level in a security  
216 policy binding (defined below) neutral manner.

217 b. Such protection assertions must be able to specify  
218 confidentiality requirements at both the element and header/body  
219 level in a security policy binding (defined below) neutral manner.

220 c. Such mechanisms must not require the use of XPath 1.0 [21]  
221 but may provide it as an option.

222 2. Mechanism for specifying pre-conditions of security, called  
223 conditional assertions

224 a. Such conditional assertions must be able to specify the required  
225 elements in the message

226 3. General mechanism for specifying tokens to use in protecting the  
227 message or binding claims to the message, called token assertions

228 a. Such token assertions should facilitate the specification of at  
229 least the following token types defined by OASIS SOAP Message  
230 Security, WS-Trust and WS-SecureConversation: Username token,  
231 X509 token, Kerberos token, SPNego Context Token, Security  
232 Context Token, Secure Conversation Token, SAML token, REL  
233 token, HTTPS token as well as any opaque token issued by a  
234 security token service.

235 b. Such token assertions should specify conditions for inclusion in  
236 the message such as whether the token should be included in every  
237 message explicitly, whether the token should be always excluded  
238 from the message and a reference included in the message, whether  
239 the token should be included once in a message exchange and

240 external reference should be used subsequently.

241 c. Such token assertions should support specification of derived  
242 keys.

243 4. An abstraction for describing some of the common security usage  
244 patterns called security policy bindings.

245 a. Such an abstraction should contain a description of the required  
246 and optional elements of such a security policy binding, including  
247 minimal token requirements, necessary key transfer mechanism,  
248 structure and contents of elements in wsse:security header, and  
249 correlation mechanisms.

250 b. Such a binding framework should also include properties for  
251 describing algorithm suite to be used, whether a timestamp should be  
252 included, signature/encryption ordering in the message, whether  
253 signatures are encrypted, and whether the signing token should also  
254 be covered by the signature.

255 c. Specific security policy binding assertions for the patterns  
256 where transport is used, where a symmetric key token is used for  
257 message security or where an asymmetric key token pair is used for  
258 message security.

259 5. A mechanism for specifying additional token types that provide  
260 additional claims, called supporting token assertions. Such a  
261 mechanism should support the following cases:

262 a. When additional tokens are used to sign additional parts of the  
263 message

264 b. When additional tokens are signed by the primary signature  
265 token

266 c. When additional tokens sign the primary signature

267 d. When additional tokens sign the primary signature and are  
268 signed by the primary signature token

269 6. A mechanism for specifying token referencing and token issuance  
270 called WSS assertions and Trust assertions that meet the referencing  
271 mechanisms and properties defined in OASIS Web Services  
272 Security 1.0 (and associated token profiles) [1], OASIS Web  
273 Services Security 1.1 (and associated token profiles) [6], in WS-Trust  
274 [3] and WS-SecureConversation [2]. Such a mechanism should  
275 include:

276 a. Properties for indicating the Web Services Security 1.0 [1] defined  
277 reference mechanism to use

278 b. Properties for indicating the Web Services Security 1.1 [6]  
279 defined reference mechanism to use including thumbprint reference

- 280 and encryptedkey reference
- 281 c. Signature confirmation requirement
- 282 d. Properties for indicating the type of challenges required (as
- 283 defined in WS-Trust [3])
- 284 e. Properties for indication the type of entropy mechanism
- 285 required in a negotiation sequence (as defined in WS-Trust [3])

286

## 287 General Notes on Scope

288

289 The output specifications will uphold the basic principles of other  
290 Web services specifications of independence and composition and be  
291 composable with the other specifications in the Web services  
292 architecture, such as the specifications listed in the References  
293 section, numbers 1, 5-12 and 18-20. The TC will also take into  
294 consideration the following specifications/works listed in the  
295 References section, numbers 13, 14, 15 and 16.

296 If any of the above specifications is outside of a standardization  
297 process at the time this TC moves to ratify its deliverables, or is not  
298 far enough along in the standardization process, any normative  
299 references to it in the TC output will be expressed in an abstract  
300 manner, and the incarnation will be left at that time as an exercise in  
301 interoperability.

302 While composition with other specifications is a goal of the TC, it is  
303 also a goal to leave the specifics of how that composition is achieved  
304 outside the scope of this TC.

305 Each of the protocol elements will use implementation and language  
306 neutral XML formats defined in XML Schema [17].

307

## 308 Out of Scope

309

310 The following is a non-exhaustive list. It is provided only for the sake  
311 of clarity. If some function, mechanism or feature is not mentioned  
312 here, and it is not mentioned in the Scope of Work section either,  
313 then it will be deemed to be out of scope.

314 The TC will not define a mapping of the functions and elements  
315 described in the specifications to any programming language, to any  
316 particular messaging middleware, nor to specific network transports.

317

318 The following items are specifically out of scope of the work of the  
319 TC:



- 320 1. Definition and management of trust policy expressions (that is,  
321 statements about who is trusted to make what claims about an entity);  
322 these are different from the in-scope "trust assertions" referred to in  
323 the Scope  
324 of Work section above  
325 2. Token revocation notifications and revocation management (e.g.  
326 via CRLs)  
327 3. Schemas for specific tokens issued, renewed, cancelled or  
328 validated as part of the trust process.  
329 4. The establishment of trust between two or more business parties  
330 5. Definition of new key derivation algorithms  
331 6. Providing a general purpose boxcaring model  
332 7. Definition of APIs

333 8. Definition of additional negotiation and challenge protocol  
334 mechanisms.  
335 9. Developing the roadmaps [15], [16] or other specifications  
336 mentioned in those roadmaps, beyond the material listed explicitly  
337 as within the scope of this charter.  
338

Frederick Hirsch 12/6/05 2:15 PM  
Formatted: Font:Times New Roman, 16 pt

Frederick Hirsch 12/6/05 2:15 PM  
Formatted: Font:Times New Roman

339 The TC will not attempt to define concepts or renderings for  
340 functions that are of wider applicability including but not limited to:

- 341 -- Addressing
- 342 -- Policy language frameworks
- 343 -- Routing
- 344 -- Reliable message exchange
- 345 -- Transactions and compensation

346 Where required these functions are achieved by composition with  
347 other Web services specifications.

348  
349 The TC will not attempt to define functionality duplicating that of  
350 any normatively referenced specification in the input WS-  
351 SecureConversation [2], WS-Trust [3] or WS-SecurityPolicy [4]  
352 specifications.If the referenced specification is outside of a  
353 standardization process at the time this TC moves to ratify its  
354 deliverables, or is not far along enough in the standardization  
355 process, any normative references to it in the TC output will be  
356 expressed in an abstract manner, and the incarnation will be left at  
357 that time as an exercise in interoperability.  
358

359 d. Deliverables

360

361 The TC has the following set of deliverables:

362 \* A revised Web Services SecureConversation specification and  
363 associated Schema. A Committee Specification is scheduled for  
364 completion within 18 months of the first TC meeting.

365 \* A revised Web Services Trust specification with associated  
366 Schema and WSDL. A Committee Specification is scheduled for  
367 completion within 18 months of the first TC meeting.

368 \* A revised Web Services SecurityPolicy specification and  
369 associated Schema. A Committee Specification is scheduled for  
370 completion within 18 months of the first TC meeting.

371

372 These specifications will reflect refinements, corrections or material  
373 technological improvements with respect to the input documents and  
374 in accordance with this charter.

375 Ratification of the above specifications as OASIS standards,  
376 including a brief period to address any errata will mark the end of the  
377 TC's lifecycle.

378

379 e. Anticipated Audience

380

381 The anticipated audience for this work includes:

382 \* Vendors offering web services products

383 \* Other specification authors that need security for Web services

384 \* Software architects and programmers, who design, write or  
385 integrate applications for Web services

386 \* End users implementing Web services-based solutions that  
387 require an interoperable, composable solution for trusted SOAP  
388 message exchanges, security policies and shared security contexts.

389 \* Vendors making gateway and router class products (both  
390 hardware and software)

391

392 f. Language

393

394 TC business will be conducted in English.

395

396 g. IPR Policy

397

398 This TC will operate under the "RF (Royalty Free) on RAND

399 Terms" IPR mode as defined in the OASIS Intellectual Property  
400 Rights (IPR) Policy, effective 15 April 2005.  
401