



# Web Services Security Rights Expression Language (REL) Token Profile Version 1.1.1

## OASIS Standard

18 May 2012

### Specification URIs

#### This version:

<http://docs.oasis-open.org/wss-m/wss/v1.1.1/os/wss-rel-token-profile-v1.1.1-os.doc> (Authoritative)  
<http://docs.oasis-open.org/wss-m/wss/v1.1.1/os/wss-rel-token-profile-v1.1.1-os.html>  
<http://docs.oasis-open.org/wss-m/wss/v1.1.1/os/wss-rel-token-profile-v1.1.1-os.pdf>

#### Previous version:

<http://docs.oasis-open.org/wss-m/wss/v1.1.1/csd01/wss-rel-token-profile-v1.1.1-csd01.doc>  
(Authoritative)  
<http://docs.oasis-open.org/wss-m/wss/v1.1.1/csd01/wss-rel-token-profile-v1.1.1-csd01.html>  
<http://docs.oasis-open.org/wss-m/wss/v1.1.1/csd01/wss-rel-token-profile-v1.1.1-csd01.pdf>

#### Latest version:

<http://docs.oasis-open.org/wss-m/wss/v1.1.1/wss-rel-token-profile-v1.1.1.doc> (Authoritative)  
<http://docs.oasis-open.org/wss-m/wss/v1.1.1/wss-rel-token-profile-v1.1.1.html>  
<http://docs.oasis-open.org/wss-m/wss/v1.1.1/wss-rel-token-profile-v1.1.1.pdf>

#### Technical Committee:

OASIS Web Services Security Maintenance (WSS-M) TC

#### Chair:

David Turner ([david.turner@microsoft.com](mailto:david.turner@microsoft.com)), Microsoft

#### Editors:

Ronald Monzillo ([ronald.monzillo@sun.com](mailto:ronald.monzillo@sun.com)), Sun Microsystems  
Chris Kaler ([ckaler@microsoft.com](mailto:ckaler@microsoft.com)), Microsoft  
Anthony Nadalin ([droidsecure@us.ibm.com](mailto:droidsecure@us.ibm.com)), IBM  
Phillip Hallam-Baker ([pbaker@verisign.com](mailto:pbaker@verisign.com)), Verisign  
Carlo Milono ([cmilono@tibco.com](mailto:cmilono@tibco.com)), Tibco  
Thomas DeMartini ([Thomas.DeMartini@ContentGuard.com](mailto:Thomas.DeMartini@ContentGuard.com)), ContentGuard, Inc.

#### Additional artifacts:

This prose specification is one component of a multi-part Work Product which includes:

- *Web Services Security Kerberos Token Profile Version 1.1.1.* <http://docs.oasis-open.org/wss-m/wss/v1.1.1/os/wss-KerberosTokenProfile-v1.1.1-os.html>.
- *Web Services Security Rights Expression Language (REL) Token Profile Version 1.1.1.* <http://docs.oasis-open.org/wss-m/wss/v1.1.1/os/wss-rel-token-profile-v1.1.1-os.html>. (this document)
- *Web Services Security SAML Token Profile Version 1.1.1.* <http://docs.oasis-open.org/wss-m/wss/v1.1.1/os/wss-SAMLTOKENProfile-v1.1.1-os.html>.
- *Web Services Security: SOAP Message Security Version 1.1.1.* <http://docs.oasis-open.org/wss-m/wss/v1.1.1/os/wss-SOAPMessageSecurity-v1.1.1-os.html>.
- *Web Services Security SOAP Message with Attachments (SwA) Profile Version 1.1.1.* <http://docs.oasis-open.org/wss-m/wss/v1.1.1/os/wss-SwAProfile-v1.1.1-os.html>.

- *Web Services Security Username Token Profile Version 1.1.1*. <http://docs.oasis-open.org/wss-m/wss/v1.1.1/os/wss-UsernameTokenProfile-v1.1.1-os.html>.
- *Web Services Security X.509 Certificate Token Profile Version 1.1.1*. <http://docs.oasis-open.org/wss-m/wss/v1.1.1/os/wss-x509TokenProfile-v1.1.1-os.html>.
- XML schemas: <http://docs.oasis-open.org/wss-m/wss/v1.1.1/os/xsd/>

**Related work:**

This specification supersedes:

- *Web Services Security Rights Expression Language (REL) Token Profile 1.1*. 01 February 2006. OASIS Standard. <http://docs.oasis-open.org/wss/v1.1/oasis-wss-rel-token-profile-1.1.pdf>

**Abstract:**

This document describes how to use ISO/IEC 21000-5 Rights Expressions with the Web Services Security (WSS) specification.

This document integrates specific error corrections or editorial changes to the preceding specification, within the scope of the Web Services Security and this TC.

This document introduces a third digit in the numbering convention where the third digit represents a consolidation of error corrections, bug fixes or editorial formatting changes (e.g., 1.1.1); it does not add any new features beyond those of the base specifications (e.g., 1.1).

**Status:**

This document was last revised or approved by the membership of OASIS on the above date. The level of approval is also listed above. Check the “Latest version” location noted above for possible later revisions of this document.

Technical Committee members should send comments on this specification to the Technical Committee’s email list. Others should send comments to the Technical Committee by using the “Send A Comment” button on the Technical Committee’s web page at <http://www.oasis-open.org/committees/wss-m/>.

For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the Technical Committee web page (<http://www.oasis-open.org/committees/wss-m/ipr.php>).

**Citation format:**

When referencing this specification the following citation format should be used:

**[WSS-REL-Token-Profile-V1.1.1]**

*Web Services Security Rights Expression Language (REL) Token Profile Version 1.1.1*. 18 May 2012. OASIS Standard. <http://docs.oasis-open.org/wss-m/wss/v1.1.1/os/wss-rel-token-profile-v1.1.1-os.html>.

---

## Notices

Copyright © OASIS Open 2012. All Rights Reserved.

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full [Policy](#) may be found at the OASIS website.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Committee Specification or OASIS Standard, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification.

OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this specification by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification. OASIS may include such claims on its website, but disclaims any obligation to do so.

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this OASIS Committee Specification or OASIS Standard, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.

The name "OASIS" is a trademark of [OASIS](#), the owner and developer of this specification, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, specifications, while reserving the right to enforce its marks against misleading uses. Please see <http://www.oasis-open.org/policies-guidelines/trademark> for above guidance.

---

# Table of Contents

|       |  |    |
|-------|--|----|
| 1     | Introduction (Informative) .....                     | 5  |
| 2     | Notations and Terminology (Normative).....           | 6  |
| 2.1   | Notational Conventions.....                          | 6  |
| 2.2   | Namespaces.....                                      | 6  |
| 2.3   | Terminology .....                                    | 6  |
| 3     | Usage (Normative) .....                              | 7  |
| 3.1   | Token Types .....                                    | 7  |
| 3.2   | Processing Model .....                               | 7  |
| 3.3   | Attaching Security Tokens .....                      | 7  |
| 3.4   | Identifying and Referencing Security Tokens .....    | 7  |
| 3.5   | Authentication .....                                 | 10 |
| 3.5.1 | <r:keyHolder> Principal .....                        | 10 |
| 3.6   | Confidentiality .....                                | 12 |
| 3.6.1 | <r:keyHolder> Principal .....                        | 12 |
| 3.7   | Error Codes.....                                     | 14 |
| 4     | Types of Licenses (Informative) .....                | 15 |
| 4.1   | Attribute Licenses .....                             | 15 |
| 4.2   | Sender Authorization .....                           | 15 |
| 4.3   | Issuer Authorization .....                           | 16 |
| 5     | Threat Model and Countermeasures (Informative) ..... | 18 |
| 5.1   | Eavesdropping.....                                   | 18 |
| 5.2   | Replay.....  | 18 |
| 5.3   | Message Insertion .....                              | 18 |
| 5.4   | Message Deletion .....                               | 18 |
| 5.5   | Message Modification .....                           | 19 |
| 5.6   | Man-in-the-Middle .....                              | 19 |
| 6     | References .....                                     | 20 |
| 7     | Conformance .....                                    | 21 |
| A.    | Acknowledgements .....                               | 22 |
| B.    | Revision History.....                                | 26 |

---

# 1 Introduction (Informative)

2 The Web Services Security: SOAP Message Security [WS-Security] specification proposes a standard set  
3 of SOAP extensions that can be used when building secure Web services to implement message level  
4 integrity and confidentiality. This specification describes the use of ISO/IEC 21000-5 Rights Expressions  
5 with respect to the WS-Security specification.

---

## 2 Notations and Terminology (Normative)

### 2.1 Notational Conventions

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [KEYWORDS].

Namespace URIs (of the general form "some-URI") represent some application-dependent or context-dependent URI as defined in [URI].

This specification is designed to work with the general SOAP message structure and message processing model, and should be applicable to any version of SOAP. The current SOAP 1.2 namespace URI is used herein to provide detailed examples, but there is no intention to limit the applicability of this specification to a single version of SOAP.

### 2.2 Namespaces

The following namespaces are used in this document:

| Prefix | Namespace   |
|--------|---|
| S      | <a href="http://www.w3.org/2003/05/soap-envelope">http://www.w3.org/2003/05/soap-envelope</a>   |
| ds     | <a href="http://www.w3.org/2000/09/xmldsig#">http://www.w3.org/2000/09/xmldsig#</a>   |
| xenc   | <a href="http://www.w3.org/2001/04/xmlenc#">http://www.w3.org/2001/04/xmlenc#</a>   |
| wsse   | <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>   |
| wsse11 | <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>                                 |
| wsu    | <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> |
| r      | urn:mpeg:mpeg21:2003:01-REL-R-NS  |
| sx     | urn:mpeg:mpeg21:2003:01-REL-SX-NS   |

Table 1 Namespace Prefixes

### 2.3 Terminology

This specification employs the terminology defined in the Web Services Security: SOAP Message Security [WS-Security] Specification.

Defined below are the basic definitions for additional terminology used in this specification.

**License** – ISO/IEC 21000-5 Rights Expression

---

## 26 3 Usage (Normative)

27 This section describes the syntax and processing rules for the use of licenses with the Web  
28 Services Security: Soap Message Security specification [WS-Security].

### 29 3.1 Token Types

30 When a URI value is used to indicate a license according to this profile, its value MUST be  
31 <http://docs.oasis-open.org/wss/oasis-wss-rel-token-profile-1.0.pdf#license>.

32 Note: This URI is for both the ValueType and TokenType attributes. It is also for use by any elements or  
33 attributes that require a token type URI and are defined in another specification taking advantage of REL  
34 Tokens.

### 35 3.2 Processing Model

36 The processing model for WS-Security with licenses is no different from that of WS-Security with other  
37 token formats as described in Web Services Security: SOAP Message Security [WS-Security].

38 At the token level, a processor of licenses MUST conform to the required validation and processing rules  
39 defined in ISO/IEC 21000-5 [REL].

### 40 3.3 Attaching Security Tokens

41 Licenses are attached to SOAP messages using WS-Security by placing the license element  
42 inside the `<wsse:Security>` header. The following example illustrates a SOAP message  
43 with a license.

```
44 <S:Envelope xmlns:S="...">  
45   <S:Header>  
46     <wsse:Security xmlns:wsse="...">  
47       <r:license xmlns:r="...">  
48         ...  
49       </r:license>  
50       ...  
51     </wsse:Security>  
52   </S:Header>  
53   <S:Body>  
54     ...  
55   </S:Body>  
56 </S:Envelope>
```

### 57 3.4 Identifying and Referencing Security Tokens

58 The Web Services Security: SOAP Message Security [WS-Security] specification defines the *wsu:id*  
59 attribute as the common mechanism for identifying security tokens (the specification describes the  
60 reasons for this). Licenses have an additional identification mechanism available: their *licenseId* attribute,  
61 the value of which is a URI. The following example shows a license that uses both mechanisms:

```
62 <r:license xmlns:r="..." xmlns:wsu="...">  
63   licenseId="urn:foo:SecurityToken:ef375268"  
64   wsu:Id="SecurityToken-ef375268">  
65   ...  
66 </r:license>
```

67 Licenses can be referenced either according to their location or their *licenseId*. Location references are  
68 dependent on location and can be either local or remote. *LicenseId* references are not dependent on  
69 location.

70 Local location references are RECOMMENDED when they can be used. Remote location references are  
 71 OPTIONAL for cases where it is not feasible to transmit licenses with the SOAP message. licenseld  
 72 references are OPTIONAL for cases where location is unknown or cannot be indicated.

73 WS-Security specifies that tokens are referenced using the <wsse:SecurityTokenReference> element.  
 74 Implementations compliant with this profile SHOULD set the  
 75 /wsse:SecurityTokenReference/wsse:Reference/@ValueType attribute to http://docs.oasis-  
 76 open.org/wss/oasis-wss-rel-token-profile-1.0.pdf#license when using wsse:SecurityTokenReference to  
 77 refer to a license by licenseld. This is OPTIONAL when referring to a license by location.

78 The following table demonstrates the use of the <wsse:SecurityTokenReference> element to refer to  
 79 licenses.

|              |        |  |
|--------------|--------|--|
| By Location  | Local  | <pre>&lt;wsse:SecurityTokenReference&gt;   &lt;wsse:Reference     URI="#SecurityToken-ef375268"   /&gt; &lt;/wsse:SecurityTokenReference&gt;</pre>   |
|              | Remote | <pre>&lt;wsse:SecurityTokenReference&gt;   &lt;wsse:Reference     URI="http://www.foo.com/ef375268.xml"   /&gt; &lt;/wsse:SecurityTokenReference&gt;</pre>   |
| By licenseld |        | <pre>&lt;wsse:SecurityTokenReference&gt;   &lt;wsse:Reference     URI="urn:foo:SecurityToken:ef375268"     ValueType="http://docs.oasis- open.org/wss/oasis-wss-rel-token-profile- 1.0.pdf#license"   /&gt; &lt;/wsse:SecurityTokenReference&gt;</pre> |

80 *Table 2. <wsse:SecurityTokenReference>*

81 The following example demonstrates how a <wsse:SecurityTokenReference> can be used to indicate that  
 82 the message parts specified inside the <ds:SignedInfo> element were signed using a key from the license  
 83 referenced by licenseld in the <ds:KeyInfo> element.

```
84 <S:Envelope xmlns:S="..." xmlns:ds="...">
85   <S:Header>
86     <wsse:Security xmlns:wsse="...">
87       <r:license xmlns:r="..." licenseId="urn:foo:SecurityToken:ef375268"
88       xmlns:wsu="..." wsu:Id="SecurityToken-ef375268">
89         ...
90       </r:license>
91       ...
92     <ds:Signature>
93       <ds:SignedInfo>
94         ...
95       </ds:SignedInfo>
96       <ds:SignatureValue>...</ds:SignatureValue>
97       <ds:KeyInfo>
98         <wsse:SecurityTokenReference>
99           <wsse:Reference
100             URI="#SecurityToken-ef375268"
101           />
102         </wsse:SecurityTokenReference>
103       </ds:KeyInfo>
104     </ds:Signature>
105   </wsse:Security>
106 </S:Header>
107 <S:Body>
108   ...
```



```
109     </S:Body>
110 </S:Envelope>
```

111 The following example shows a signature over a local license using a location reference to that license.  
112 The example demonstrates how the integrity of an (unsigned) license can be preserved by signing it in  
113 the <wsse:Security> header.

```
114 <S:Envelope xmlns:S="..." xmlns:wsu="..." >
115   <S:Header>
116     <wsse:Security xmlns:wsse="...">
117       <r:license xmlns:r="..." wsu:Id="SecurityToken-ef375268">
118         ...
119       </r:license>
120       ...
121       <wsse:SecurityTokenReference wsu:Id="Str1">
122         <wsse:Reference
123           URI="#SecurityToken-ef375268"
124         />
125       </wsse:SecurityTokenReference>
126       ...
127       <ds:Signature>
128         <ds:SignedInfo>
129           ...
130           <ds:Reference URI="#Str1">
131             <ds:Transforms>
132               <ds:Transform
133                 Algorithm="http://schemas.xmlsoap.org/2003/06/STR-Transform">
134                 <ds:CanonicalizationMethod
135                   Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
136 20010315"/>
137                 </ds:Transform>
138               </ds:Transforms>
139               <ds:DigestMethod
140                 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
141               />
142               <ds:DigestValue>...</ds:DigestValue>
143             </ds:Reference>
144           </ds:SignedInfo>
145           <ds:SignatureValue>...</ds:SignatureValue>
146           <ds:KeyInfo>...</ds:KeyInfo>
147         </ds:Signature>
148       </wsse:Security>
149     </S:Header>
150     <S:Body>
151       ...
152     </S:Body>
153 </S:Envelope>
```

154 Note: since licenses allow the use of the wsu:Id attribute, it is usually not necessary to use the STR-  
155 Transform because the license can be referred to directly in the ds:SignedInfo as shown in the following  
156 example:

```
157 <S:Envelope xmlns:S="..." xmlns:ds="...">
158   <S:Header>
159     <wsse:Security xmlns:wsse="...">
160       <r:license xmlns:r="..." xmlns:wsu="..." wsu:Id="SecurityToken-
161 ef375268">
162         ...
163       </r:license>
164       ...
165       <ds:Signature>
166         <ds:SignedInfo>
167           ...
168           <ds:Reference URI="#SecurityToken-ef375268">
```

169  
170  
171  
172  
173  
174  
175  
176  
177  
178  
179  
180  
181  
182  
183

```
<ds:DigestMethod
  Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
/>
<ds:DigestValue>...</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>...</ds:SignatureValue>
<ds:KeyInfo>...</ds:KeyInfo>
</ds:Signature>
</wsse:Security>
</S:Header>
<S:Body>
...
</S:Body>
</S:Envelope>
```

### 184 3.5 Authentication

185 The Web Services Security: SOAP Message Security [WS-Security] specification does not dictate how  
186 claim confirmation must be performed. As well, the REL allows for multiple types of confirmation. This  
187 profile of WS-Security REQUIRES that message senders and receivers support claim confirmation for  
188 <r:keyHolder> principals. It is RECOMMENDED that an XML Signature be used to establish the  
189 relationship between the message sender and the claims. This is especially RECOMMENDED whenever  
190 the SOAP message exchange is conducted over an unprotected transport.

191 The following table enumerates the mandatory principals to be supported by claim confirmation and  
192 summarizes their associated processing models. It should be noted that this table is not all-  
193 encompassing, and it is envisioned that future specifications may expand this table over time.

| Principal     | RECOMMENDED Processing Rules  |
|---------------|---|
| <r:keyHolder> | The message sender adds (to the security header) an XML Signature that can be verified with the key information specified in the <r:keyHolder> of the referenced license. |

194 *Table 3. Processing Rules for Claim Confirmation*

195 Note that the high-level processing model described in the following sections does not differentiate  
196 between message author and message sender as would be necessary to guard against replay attacks.  
197 The high-level processing model also does not take into account requirements for authentication of  
198 receiver by sender or for message or token confidentiality. These concerns must be addressed by means  
199 other than those described in the high-level processing model. If confidentiality of the token in the  
200 message is important, then use the approach defined by [WS-Security] to encrypt the token.

#### 201 3.5.1 <r:keyHolder> Principal

202 The following sections describe the <r:keyHolder> method of establishing the correspondence between a  
203 SOAP message sender and the claims within a license.

#### 204 Sender

205 The message sender MUST include within the <wsse:Security> header element a <r:license> containing  
206 at least one <r:grant> to an <r:keyHolder> identifying the key to be used to confirm the claims. If the  
207 message sender includes an <r:license> containing more than one <r:grant> to an <r:keyHolder>, then all  
208 of those <r:keyHolder> elements MUST be equal.

209 In order for the receiver to perform claim confirmation, the sender MUST demonstrate knowledge of the  
210 confirmation key. The sender MAY accomplish this by using the confirmation key to sign content from

211 within the message and by including the resulting <ds:Signature> element in the <wsse:Security> header  
212 element. <ds:Signature> elements produced for this purpose MUST conform to the canonicalization and  
213 token inclusion rules defined in the core WS-Security specification and this profile specification.

214 Licenses that contain at least one <r:grant> to an <r:keyHolder> SHOULD contain an <r:issuer> with a  
215 <ds:Signature> element that identifies the license issuer to the relying party and protects the integrity of  
216 the confirmation key established by the license issuer.

## 217 Receiver

218 If the receiver determines that the sender has demonstrated knowledge of a confirmation key as specified  
219 in an <r:keyHolder>, then the claims (found in the licenses) pertaining to that <r:keyHolder> MAY be  
220 attributed to the sender. If one of these claims is an identity and if the conditions of that claim are  
221 satisfied, then any elements of the message whose integrity is protected by the confirmation key MAY be  
222 considered to have been authored by that identity.

## 223 Example

224 The following example illustrates how a license security token having an <r:keyHolder> principal can be  
225 used with a <ds:Signature> to establish that John Doe is requesting a stock report on FOO.

```
226 <S:Envelope xmlns:S="...">
227   <S:Header>
228     <wsse:Security xmlns:wsse="...">
229       <r:license xmlns:r="..." licenseId="urn:foo:SecurityToken:ef375268">
230         <r:grant>
231           <r:keyHolder>
232             <r:info>
233               <ds:KeyValue>...</ds:KeyValue>
234             </r:info>
235           </r:keyHolder>
236           <r:possessProperty/>
237           <sx:commonName xmlns:sx="...">John Doe</sx:commonName>
238         </r:grant>
239         <r:issuer>
240           <ds:Signature>...</ds:Signature>
241         </r:issuer>
242       </r:license>
243     <ds:Signature>
244       <ds:SignedInfo>
245         ...
246         <ds:Reference URI="#MsgBody">
247           <ds:DigestMethod
248             Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
249           />
250           <ds:DigestValue>...</ds:DigestValue>
251         </ds:Reference>
252       </ds:SignedInfo>
253       <ds:SignatureValue>...</ds:SignatureValue>
254       <ds:KeyInfo>
255         <wsse:SecurityTokenReference>
256           <wsse:Reference
257             URI="urn:foo:SecurityToken:ef375268"
258             ValueType="http://docs.oasis-open.org/wss/oasis-wss-rel-token-
259 profile-1.0.pdf#license"
260           />
261         </wsse:SecurityTokenReference>
262       </ds:KeyInfo>
263     </ds:Signature>
264   </S:Header>
265 </S:Envelope>
```

268  
269  
270  
271  
272  
273  
274  
275  
276  
277

```
</wsse:Security>
</S:Header>

<S:Body wsu:Id="MsgBody" xmlns:wsu="...">
  <ReportRequest>
    <TickerSymbol>FOO</TickerSymbol>
  </ReportRequest>
</S:Body>

</S:Envelope>
```

### 278 3.6 Confidentiality

279 This section details how licenses may be used to protect the confidentiality of a SOAP message within  
280 WS-Security. The Web Services Security: SOAP Message Security [WS-Security] specification does not  
281 dictate how confidentiality must be performed. As well, the REL allows for multiple types of confidentiality.  
282 This profile of WS-Security REQUIRES that message senders and receivers support confidentiality for  
283 <r:keyHolder> principals. It is RECOMMENDED that XML Encryption be used to ensure confidentiality.  
284 This is especially RECOMMENDED whenever the SOAP message exchange is conducted over an  
285 unprotected transport.

286 The following table enumerates the mandatory principals to be supported for confidentiality and  
287 summarizes their associated processing models. It should be noted that this table is not all-  
288 encompassing, and it is envisioned that future specifications may expand this table over time.

| Principal     | RECOMMENDED Processing Rules   |
|---------------|--|
| <r:keyHolder> | The message sender adds (to the security header) either 1) an <xenc:ReferenceList> that points to one or more <xenc:EncryptedData> elements that can be decrypted with a key which can be determined from information specified in the <r:keyHolder> of the referenced license or 2) an <xenc:EncryptedKey> that can be decrypted with a key determined from information specified in the <r:keyHolder> of the referenced license. |

289 *Table 4. Processing Rules for Confidentiality*

290 Note that this section deals only with Confidentiality. Details of authentication of the sender by the  
291 receiver must be addressed by means other than those described in this section (see the previous  
292 section).

#### 293 3.6.1 <r:keyHolder> Principal

294 The following sections describe the <r:keyHolder> method of establishing confidentiality using a license.

##### 295 Sender

296 The message sender MUST include within the <wsse:Security> header element a <r:license> containing  
297 at least one <r:grant> to an <r:keyHolder> identifying the key used to encrypt some data or key. If the  
298 message sender includes an <r:license> containing more than one <r:grant> to an <r:keyHolder>, then all  
299 of those <r:keyHolder> elements MUST be equal.

300 In order for the receiver to know when to decrypt the data or key, the sender MUST indicate the  
301 encryption in the message. The sender MAY accomplish this by placing an <xenc:EncryptedData> or

302 <xenc:EncryptedKey> in the appropriate place in the message and by including the resulting  
303 <xenc:ReferenceList> or <xenc:EncryptedKey> element in the <wsse:Security> header element.  
304 <xenc:ReferenceList> or <xenc:EncryptedKey> elements produced for this purpose MUST conform to the  
305 rules defined in the core WS-Security specification and this profile specification.

## 306 Receiver

307 If the receiver determines that he has knowledge of a decryption key as specified in an <r:keyHolder>,  
308 then he MAY decrypt the associated data or key. In the case of decrypting a key, he may then  
309 recursively decrypt any data or key that that key can decrypt.

## 310 Example

311 The following example illustrates how a license containing a <r:keyHolder> principal can be used with  
312 XML encryption schema elements to protect the confidentiality of a message using a separate encryption  
313 key given in the <xenc:EncryptedKey> in the security header.

314 In this example, the r:license element provides information about the recipient's RSA public key (i.e.,  
315 KeyValue in keyHolder) used to encrypt the symmetric key carried in the EncryptedKey element. The  
316 recipient uses this information to determine the correct private key to use in decrypting the symmetric key.  
317 The symmetric key is then used to decrypt the EncryptedData child of the Body element.

318

```
319 <S:Envelope xmlns:S="..." xmlns:ds="...">
320   <S:Header>
321     <wsse:Security xmlns:wsse="...">
322       <r:license xmlns:r="..." licenseId="urn:foo:SecurityToken:ef375268">
323         <r:grant>
324           <r:keyHolder>
325             <r:info>
326               <ds:KeyValue>...</ds:KeyValue>
327             </r:info>
328           </r:keyHolder>
329           <r:possessProperty/>
330           <sx:commonName xmlns:sx="...">SOME COMPANY</sx:commonName>
331         </r:grant>
332         <r:issuer>
333           <ds:Signature>...</ds:Signature>
334         </r:issuer>
335       </r:license>
336       <xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
337         <xenc:EncryptionMethod
338           Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
339         <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
340           <wsse:SecurityTokenReference>
341             <wsse:Reference URI="urn:foo:SecurityToken:ef375268"/>
342           </wsse:SecurityTokenReference>
343         </KeyInfo>
344         <xenc:CipherData>
345           <xenc:CipherValue>dNYS...fQ</xenc:CipherValue>
346         </xenc:CipherData>
347         <xenc:ReferenceList>
348           <xenc:DataReference URI="#enc"/>
349         </xenc:ReferenceList>
350       </xenc:EncryptedKey>
351     </wsse:Security>
352   </S:Header>
353   <S:Body wsu:Id="body"
354     xmlns:wsu="http://schemas.xmlsoap.org/ws/2003/06/utility">
355     <xenc:EncryptedData Id="enc"
356       Type="http://www.w3.org/2001/04/xmlenc#Content"
357       xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
358       <xenc:EncryptionMethod
```

```
359         Algorithm="http://www.w3.org/2001/04/xmlenc#tripleDES-cbc"/>
360     <xenc:CipherData>
361         <xenc:CipherValue>d2s...GQ=</xenc:CipherValue>
362     </xenc:CipherData>
363 </xenc:EncryptedData>
364 </S:Body>
365 </S:Envelope>
```

### 366 **3.7 Error Codes**

367 It is RECOMMENDED that the error codes defined in the Web Services Security: SOAP  
368 Message Security [WS-Security] specification are used. However, implementations MAY use  
369 custom errors, defined in private namespaces if they desire. Care should be taken not to  
370 introduce security vulnerabilities in the errors returned.

371

## 4 Types of Licenses (Informative)

372

### 4.1 Attribute Licenses

373

In addition to key information, licenses can carry information about attributes of those keys. Examples of such information on a client are e-mail address or common name. A service's key, on the other hand, might be associated with a DNS name and common name.

375

376

The following is an example client attribute license.

377

378

379

380

381

382

383

384

385

386

387

388

389

390

391

392

393

394

395

396

397

398

399

```
<r:license xmlns:r="..." xmlns:ds="..."
licenseId="urn:foo:SecurityToken:ef375268">
  <r:inventory>
    <r:keyHolder licensePartId="client">
      <r:info>
        <ds:KeyValue>FDFEWEFF...</ds:KeyValue>
      </r:info>
    </r:keyHolder>
  </r:inventory>
  <r:grant>
    <r:keyHolder licensePartIdRef="client"/>
    <r:possessProperty/>
    <sx:commonName>John Doe</sx:commonName>
  </r:grant>
  <r:grant>
    <r:keyHolder licensePartIdRef="client"/>
    <r:possessProperty/>
    <sx:emailName>jd@foo.com</sx:emailName>
  </r:grant>
  <r:issuer>
    <ds:Signature>...</ds:Signature>
  </r:issuer>
</r:license>
```

400

The following is an example service attribute license.

401

402

403

404

405

406

407

408

409

410

411

412

413

414

415

416

417

418

419

420

421

422

423

```
<r:license xmlns:r="..." xmlns:ds="..."
licenseId="urn:foo:SecurityToken:ef375268">
  <r:inventory>
    <r:keyHolder licensePartId="service">
      <r:info>
        <ds:KeyValue>FDFEWEFF...</ds:KeyValue>
      </r:info>
    </r:keyHolder>
  </r:inventory>
  <r:grant>
    <r:keyHolder licensePartIdRef="service"/>
    <r:possessProperty/>
    <sx:commonName>MyService Company</sx:commonName>
  </r:grant>
  <r:grant>
    <r:keyHolder licensePartIdRef="service"/>
    <r:possessProperty/>
    <sx:dnsName>www.myservice.com</sx:dnsName>
  </r:grant>
  <r:issuer>
    <ds:Signature>...</ds:Signature>
  </r:issuer>
</r:license>
```

424

Additional examples of and processing rules for the use of attribute licenses can be found in the above sections on Authentication and Confidentiality.

425

426

### 4.2 Sender Authorization

427

Licenses may be used by a sender as proof of authorization to perform a certain action on a particular resource. This WS-Security specification does not describe how authorization must be performed. In the

428

429 context of web services, a sender can send to a receiver an authorization license in the security header  
430 as proof of authorization to call the sender. Typically, this authorization license is signed by a trusted  
431 authority and conforms to the syntax pattern specified below.

```
432 <r:license xmlns:r="..." licenseId="urn:foo:SecurityToken:ef375268">  
433   <r:grant>  
434     <r:keyHolder>  
435       <r:info>  
436         <ds:KeyValue>FDFEWEFF...</ds:KeyValue>  
437       </r:info>  
438     </r:keyHolder>  
439     <sx:rightUri definition='...' />  
440     <x:someResource />  
441     <x:someCondition />  
442   </r:grant>  
443   <r:issuer>  
444     <ds:Signature>...</ds:Signature>  
445   </r:issuer>  
446 </r:license>
```

447 The above license contains an authorization grant authorizing the keyholder (sender's public key), the  
448 right to exercise the right identified in the <sx:rightUri> element. The resource in the license typically  
449 corresponds to the semantics of the URI given in the definition attribute of the <sx:rightUri> element. The  
450 entire license along with the <ds:Signature> element in the <r:issuer> certifies the fact that the principal  
451 (<keyholder>) is granted the authorization to exercise the right in the <sx:rightUri> element over the  
452 specified resource. The integrity of the license is usually protected with a digital signature contained  
453 within the <ds:Signature>.

### 454 4.3 Issuer Authorization

455 To enunciate that a particular issuer is allowed to issue particular types of licenses, one can use the kind  
456 of license described here. Issuer authorization licenses can accompany other licenses in the security  
457 header such as those used for authentication, sender authorization, or other issuer authorizations. These  
458 issuer authorization licenses might help complete the authorization proof that is required for authorizing or  
459 authenticating a particular sender.

460  
461 The following license is an example issuer authorization license for authorizing an issuer to issue a simple  
462 attribute license.

```
463 <r:license xmlns:r="..." licenseId="urn:foo:SecurityToken:ef375268">  
464   <r:grant>  
465     <r:forAll varName='K' />  
466     <r:forAll varName='P' />  
467     <r:keyHolder>  
468       <r:info>  
469         <ds:KeyValue>FDFEWEFF...</ds:KeyValue>  
470       </r:info>  
471     </r:keyHolder>  
472     <r:issue />  
473   </r:grant>  
474   <r:grant>  
475     <r:keyHolder varRef='K' />  
476     <r:possessProperty />  
477     <r:propertyAbstract varRef='P' />  
478   </r:grant>  
479   <r:issuer>  
480     <ds:Signature>...</ds:Signature>  
481   </r:issuer>  
482 </r:license>
```

483 The following license is an example issuer authorization license for authorizing an issuer to issue sender  
484 authorization licenses.

```
485 <r:license xmlns:r="..." licenseId="urn:foo:SecurityToken:ef375268">  
486   <r:grant>  
487     <r:forAll varName='K' />  
488     <r:forAll varName='R' />  
489     <r:keyHolder>
```



```

490     <r:info>
491         <ds:KeyValue>FDFEWEFF...</ds:KeyValue>
492     </r:info>
493 </r:keyHolder>
494 <r:issue/>
495 <r:grant>
496     <r:keyHolder varRef='K' />
497     <sx:rightUri definition='...'/>
498     <r:resource varRef='R' />
499 </r:grant>
500 </r:grant>
501 <r:issuer>
502     <ds:Signature>...</ds:Signature>
503 </r:issuer>
504 </r:license>

```

505 The following license is an example issuer authorization license for authorizing an issuer to issue (to other  
506 issuers) issuer authorization licenses allowing those other issuers to issue simple attribute licenses, such  
507 as those that can be used for authentication or confidentiality.

```

508 <r:license xmlns:r="..." licenseId="urn:foo:SecurityToken:ef375268">
509   <r:grant>
510     <r:forAll varName='I' />
511     <r:keyHolder>
512       <r:info>
513         <ds:KeyValue>FDFEWEFF...</ds:KeyValue>
514       </r:info>
515     </r:keyHolder>
516     <r:issue/>
517     <r:grant>
518       <r:forAll varName='K' />
519       <r:forAll varName='P' />
520       <r:keyHolder varRef='I' />
521       <r:issue/>
522       <r:grant>
523         <r:keyHolder varRef='K' />
524         <r:possessProperty/>
525         <r:propertyAbstract varRef='P' />
526       </r:grant>
527     </r:grant>
528   </r:grant>
529   <r:issuer>
530     <ds:Signature>...</ds:Signature>
531   </r:issuer>
532 </r:license>

```

533

---

## 534 **5 Threat Model and Countermeasures (Informative)**

535 This section addresses the potential threats that a SOAP message may encounter and the  
536 countermeasures that may be taken to thwart such threats. A SOAP message containing licenses may  
537 face threats in various contexts. This includes the cases where the message is in transit, being routed  
538 through a number of intermediaries, or during the period when the message is in storage.

539 The use of licenses with WS-Security introduces no new threats beyond those identified for the REL or  
540 WS-Security with other types of security tokens. Message alteration and eavesdropping can be  
541 addressed by using the integrity and confidentiality mechanisms described in WS-Security. Replay  
542 attacks can be addressed by using of message timestamps and caching, as well as other application-  
543 specific tracking mechanisms. For licenses, ownership is verified by the use of keys; man-in-the-middle  
544 attacks are generally mitigated. It is strongly RECOMMENDED that all relevant and immutable message  
545 data be signed. It should be noted that transport-level security MAY be used to protect the message and  
546 the security token. In order to trust licenses, they SHOULD be signed natively and/or using the  
547 mechanisms outlined in WS-Security. This allows readers of the licenses to be certain that the licenses  
548 have not been forged or altered in any way. It is strongly RECOMMENDED that the <r:license> elements  
549 be signed (either within the token, as part of the message, or both).

550 The following few sections elaborate on the afore-mentioned threats and suggest countermeasures.

### 551 **5.1 Eavesdropping**

552 Eavesdropping is a threat to the confidentiality of the message, and is common to all types of network  
553 protocols. The routing of SOAP messages through intermediaries increases the potential incidences of  
554 eavesdropping. Additional opportunities for eavesdropping exist when SOAP messages are persisted.

555 To provide maximum protection from eavesdropping, licenses, license references, and sensitive message  
556 content SHOULD be encrypted such that only the intended audiences can view their content. This  
557 removes threats of eavesdropping in transit, but does not remove risks associated with storage or poor  
558 handling by the receiver.

559 Transport-layer security MAY be used to protect the message from eavesdropping while in transport, but  
560 message content must be encrypted above the transport if it is to be protected from eavesdropping by  
561 intermediaries.

### 562 **5.2 Replay**

563 The reliance on authority protected (e.g. signed) licenses to <r:keyHolder> principals precludes all but the  
564 key holder from binding the licenses to a SOAP message. Although this mechanism effectively restricts  
565 message authorship to the holder of the confirmation key, it does not preclude the capture and  
566 resubmission of the message by other parties.

567 Replay attacks can be addressed by using message timestamps and caching, as well as other  
568 application-specific tracking mechanisms.

### 569 **5.3 Message Insertion**

570 This profile of WS-Security is not vulnerable to message insertion attacks. Higher-level protocols built on  
571 top of SOAP and WS-Security should avoid introducing message insertion threats and provide proper  
572 countermeasures for any they do introduce.

### 573 **5.4 Message Deletion**

574 This profile of WS-Security is not vulnerable to message deletion attacks other than denial of service.  
575 Higher-level protocols built on top of SOAP and WS-Security should avoid introducing message deletion  
576 threats and provide proper countermeasures for any they do introduce.

## 577 **5.5 Message Modification**

578 Message Modification poses a threat to the integrity of a message. The threat of message modification  
579 can be thwarted by signing the relevant and immutable content by the key holder. The receivers SHOULD  
580 only trust the integrity of those segments of the message that are signed by the key holder.

581 To ensure that message receivers can have confidence that received licenses have not been forged or  
582 altered since their issuance, licenses appearing in <wsse:Security> header elements SHOULD be  
583 integrity protected (e.g. signed) by their issuing authority. It is strongly RECOMMENDED that a message  
584 sender sign any <r:license> elements that it is confirming and that are not signed by their issuing  
585 authority.

586 Transport-layer security MAY be used to protect the message and contained licenses and/or license  
587 references from modification while in transport, but signatures are required to extend such protection  
588 through intermediaries.

## 589 **5.6 Man-in-the-Middle**

590 This profile of WS-Security is not vulnerable to man-in-the-middle attacks. Higher-level protocols built on  
591 top of SOAP and WS-Security should avoid introducing Man-in-the-Middle threats and provide proper  
592 countermeasures for any they do introduce.

593

---

## 594 6 References

- 595 **[KEYWORDS]** S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels," RFC  
596 2119, Harvard University, March 1997, <http://www.ietf.org/rfc/rfc2119.txt>
- 597 **[REL]** ISO/IEC 21000-5:2004, "Information technology -- Multimedia framework  
598 (MPEG-21) -- Part 5: Rights Expression Language,"  
599 [http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=36](http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=36095&ICS1=35&ICS2=40&ICS3=)  
600 [095&ICS1=35&ICS2=40&ICS3=](http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=36095&ICS1=35&ICS2=40&ICS3=)
- 601 **[SOAP]** D. Box, D Ehnebuske, G. Kakivaya, A. Layman, N. Mendelsohn, H. Frystyk  
602 Nielsen, S Thatte, D. Winer. Simple Object Access Protocol (SOAP) 1.1, W3C  
603 Note 08 May 2000, <http://www.w3.org/TR/SOAP/>  
604  
605 W3C Recommendation, "SOAP Version 1.2 Part 1: Messaging Framework", 23  
606 June 2003
- 607 **[URI]** T. Berners-Lee, R. Fielding, L. Masinter, "Uniform Resource Identifiers (URI):  
608 Generic Syntax," RFC 2396, MIT/LCS, U.C. Irvine, Xerox Corporation, August  
609 1998, <http://www.ietf.org/rfc/rfc2396.txt>  
610  
611 T. Berners-Lee, R. Fielding, L. Masinter, "Uniform Resource Identifiers (URI):  
612 Generic Syntax," RFC 3986, MIT/LCS, Day Software, Adobe Systems, January  
613 2005, <http://www.ietf.org/rfc/rfc3986.txt>.
- 614 **[WS-Security]** *Web Services Security: SOAP Message Security Version 1.1.1*. 18 May 2012.  
615 OASIS Standard. [http://docs.oasis-open.org/wss-m/wss/v1.1.1/os/wss-](http://docs.oasis-open.org/wss-m/wss/v1.1.1/os/wss-SOAPMessageSecurity-v1.1.1-os.html)  
616 [SOAPMessageSecurity-v1.1.1-os.html](http://docs.oasis-open.org/wss-m/wss/v1.1.1/os/wss-SOAPMessageSecurity-v1.1.1-os.html).  
617  
618 OASIS Standard, "Web Services Security: Soap Message Security 1.1 (WS-  
619 Security 2004)," November 2005, [http://docs.oasis-open.org/wss/ oasis-wss-](http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1.pdf)  
620 [soap-message-security-1.1.pdf](http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1.pdf)
- 621 **[XML-ns]** T. Bray, D. Hollander, A. Layman. Namespaces in XML. W3C Recommendation.  
622 January 1999, <http://www.w3.org/TR/1999/REC-xml-names-19990114>
- 623 **[XML Signature]** D. Eastlake, J. R., D. Solo, M. Bartel, J. Boyer , B. Fox , E. Simon. XML-  
624 Signature Syntax and Processing, W3C Recommendation, 12 February 2002.  
625

---

626 **7 Conformance**

627 An implementation conforms to this specification if it meets the requirements in Sections 2.1, 2.2 and 3.  
628

---

## 629 A. Acknowledgements

630 The following individuals have participated in the creation of this specification and are gratefully  
631 acknowledged:

632 **Participants:**

633 **Current Contributors:**

|          |          |                                |
|----------|----------|--------------------------------|
| Tom      | Rutt     | Fujitsu Limited                |
| Jacques  | Durand   | Fujitsu Limited                |
| Calvin   | Powers   | IBM                            |
| Kelvin   | Lawrence | IBM                            |
| Michael  | McIntosh | Individual                     |
| Thomas   | Hardjono | M.I.T.                         |
| David    | Turner   | Microsoft Corporation          |
| Anthony  | Nadalin  | Microsoft Corporation          |
| Monica   | Martin   | Microsoft Corporation          |
| Marc     | Goodner  | Microsoft Corporation          |
| Peter    | Davis    | Neustar                        |
| Hal      | Lockhart | Oracle Corporation             |
| Rich     | Levinson | Oracle Corporation             |
| Anil     | Saldhana | Red Hat                        |
| Martin   | Raepple  | SAP AG                         |
| Federico | Rossini  | Telecom Italia S.p.a.          |
| Carlo    | Milono   | TIBCO Software Inc.            |
| Don      | Adams    | TIBCO Software Inc.            |
| Jerry    | Smith    | US Department of Defense (DoD) |

634 **Previous Contributors:**

|           |            |                             |
|-----------|------------|-----------------------------|
| Michael   | Hu         | Actional                    |
| Maneesh   | Sahu       | Actional                    |
| Duane     | Nickull    | Adobe Systems               |
| Gene      | Thurston   | AmberPoint                  |
| Frank     | Siebenlist | Argonne National Laboratory |
| Peter     | Dapkus     | BEA                         |
| Hal       | Lockhart   | BEA Systems                 |
| Denis     | Pilipchuk  | BEA Systems                 |
| Corinna   | Witt       | BEA Systems                 |
| Steve     | Anderson   | BMC Software                |
| Rich      | Levinson   | Computer Associates         |
| Thomas    | DeMartini  | ContentGuard                |
| Guillermo | Lao        | ContentGuard                |
| TJ        | Pannu      | ContentGuard                |
| Xin       | Wang       | ContentGuard                |
| Merlin    | Hughes     | Cybertrust                  |

|           |                    |                                 |
|-----------|--------------------|---------------------------------|
| Dale      | Moberg             | Cyclone Commerce                |
| Shawn     | Sharp              | Cyclone Commerce                |
| Rich      | Salz               | Datapower                       |
| Ganesh    | Vaideeswaran       | Documentum                      |
| Sam       | Wei                | EMC                             |
| John      | Hughes             | Entegrity                       |
| Tim       | Moses              | Entrust                         |
| Carolina  | Canales-Valenzuela | Ericsson                        |
| Davanum   | Srinivas           | formerly of Computer Associates |
| Mark      | Hayes              | formerly of VeriSign            |
| Dana S.   | Kaufman            | Forum Systems                   |
| Toshihiro | Nishimura          | Fujitsu                         |
| Tom       | Rutt               | Fujitsu                         |
| Kefeng    | Chen               | GeoTrust                        |
| Irving    | Reid               | Hewlett-Packard                 |
| Kojiro    | Nakayama           | Hitachi                         |
| Yutaka    | Kudo               | Hitachi                         |
| Jason     | Rouault            | HP                              |
| Paula     | Austel             | IBM                             |
| Derek     | Fu                 | IBM                             |
| Maryann   | Hondo              | IBM                             |
| Kelvin    | Lawrence           | IBM                             |
| Michael   | McIntosh           | IBM                             |
| Anthony   | Nadalin            | IBM                             |
| Nataraj   | Nagaratnam         | IBM                             |
| Bruce     | Rich               | IBM                             |
| Ron       | Williams           | IBM                             |
| Bob       | Blakley            | IBM                             |
| Joel      | Farrell            | IBM                             |
| Satoshi   | Hada               | IBM                             |
| Hiroshi   | Maruyama           | IBM                             |
| David     | Melgar             | IBM                             |
| Kent      | Tamura             | IBM                             |
| Wayne     | Vicknair           | IBM                             |
| Don       | Flinn              | Individual                      |
| Phil      | Griffin            | Individual                      |
| Bob       | Morgan             | Individual/Internet2            |
| Kate      | Cherry             | Lockheed Martin                 |
| Paul      | Cotton             | Microsoft                       |
| Vijay     | Gajjala            | Microsoft                       |
| Martin    | Gudgin             | Microsoft                       |
| Chris     | Kaler              | Microsoft                       |

|           |              |                      |
|-----------|--------------|----------------------|
| Bob       | Atkinson     | Microsoft            |
| Keith     | Ballinger    | Microsoft            |
| Allen     | Brown        | Microsoft            |
| Giovanni  | Della-Libera | Microsoft            |
| Alan      | Geller       | Microsoft            |
| Johannes  | Klein        | Microsoft            |
| Scott     | Konersmann   | Microsoft            |
| Chris     | Kurt         | Microsoft            |
| Brian     | LaMacchia    | Microsoft            |
| Paul      | Leach        | Microsoft            |
| John      | Manferdelli  | Microsoft            |
| John      | Shewchuk     | Microsoft            |
| Dan       | Simon        | Microsoft            |
| Hervey    | Wilson       | Microsoft            |
| Jeff      | Hodges       | Neustar/Sun          |
| Frederick | Hirsch       | Nokia                |
| Senthil   | Sengodan     | Nokia                |
| Abbie     | Barbir       | Nortel               |
| Lloyd     | Burch        | Novell               |
| Ed        | Reed         | Novell               |
| Charles   | Knouse       | Oblix                |
| Vamsi     | Motukuru     | Oracle               |
| Vipin     | Samar        | Oracle               |
| Jerry     | Schwarz      | Oracle               |
| Prateek   | Mishra       | Principal Identity   |
| Eric      | Gravengaard  | Reactivity           |
| Stuart    | King         | Reed Elsevier        |
| Ben       | Hammond      | RSA Security         |
| Rob       | Philpott     | RSA Security         |
| Andrew    | Nash         | RSA Security         |
| Peter     | Rostin       | RSA Security         |
| Martijn   | de Boer      | SAP                  |
| Blake     | Dournaee     | Sarvega              |
| Sundeeep  | Peechu       | Sarvega              |
| Pete      | Wenzel       | SeeBeyond            |
| Jonathan  | Tourzan      | Sony                 |
| Yassir    | Elley        | Sun                  |
| Manveen   | Kaur         | Sun Microsystems     |
| Ronald    | Monzillo     | Sun Microsystems     |
| Jan       | Alexander    | Systinet             |
| Michael   | Nguyen       | The IDA of Singapore |
| Don       | Adams        | TIBCO                |



|         |                |                |
|---------|----------------|----------------|
| Symon   | Chang          | TIBCO Software |
| John    | Weiland        | US Navy        |
| Hans    | Granqvist      | VeriSign       |
| Phillip | Hallam-Baker   | VeriSign       |
| Hemma   | Prafullchandra | VeriSign       |
| Morten  | Jorgensen      | Vordel         |

635

636

637

## B. Revision History

638

| Revision    | Date            | Editor       | Changes Made  |
|-------------|-----------------|--------------|---|
| WD01        | 17-January-2011 | Carlo Milono | Corrected/added hyperlinks where missing; added Status section  |
| WD02        | 8-February-2011 | Carlo Milono | Added Related Work to reflect v1.1.1 of the specs; changed References for SOAP Message Security to reflect v1.1.1; Changed WD# to 2; Added Date; Moved Current Members to Previous and added new Current Members; saved document under wd02; entered the Revision History<br><br>Merged Old Current Contributors with Old Previous, created a New Current Contributors. |
| CSD01       | 2-May-2011      | TC Admin     | Generated from WD02   |
| CSD02-draft | 16-May-11       | David Turner | Added conformance statement and corrected a few formatting issues.  |

639