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

Committee Specification Draft 02 / Public Review Draft 01

18 May 2011

Specification URIs:

This version:

http://docs.oasis-open.org/wss-m/wss/v1.1.1/csprd01/wss-rel-token-profile-v1.1.1-csprd01.doc (Authoritative)
http://docs.oasis-open.org/wss-m/wss/v1.1.1/csprd01/wss-rel-token-profile-v1.1.1-csprd01.html
http://docs.oasis-open.org/wss-m/wss/v1.1.1/csprd01/wss-rel-token-profile-v1.1.1-csprd01.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, Microsoft

Editors:

Ronald Monzillo, Sun
Chris Kaler, Microsoft
Anthony Nadalin, IBM
Phillip Hallam-Baker, Verisign
Carlo Milono, Tibco
Thomas DeMartini, ContentGuard, Inc.

Additional Work Product artifacts:

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

- XML schemas: wss/v1.1.1/csprd01/xsd/
- Web Services Security: SOAP Message Security Version 1.1.1
- Web Services Security Kerberos Token Profile Version 1.1.1
- Web Services Security SOAP Messages with Attachments (SwA) Profile Version 1.1.1
- Web Services Security Username Token Profile Version 1.1.1
- Web Services Security X.509 Certificate Token Profile Version 1.1.1

- Web Services Security SAML Token Profile Version 1.1.1

Related work:

This specification supersedes:

- Web Services Security Rights Expression Language (REL) Token Profile 1.1, OASIS Standard, 1 February 2006

Abstract:

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

Status:

This document was last revised or approved by the OASIS Web Services Security Maintenance (WSS-M) TC 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).

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).

Citation Format:

[WSS-REL-Token-Profile-V-1.1.1]

Web Services Security Rights Expression Language (REL) Token Profile Version 1.1.1. 18 May 2011. OASIS Committee Specification Draft 02 / Public Review Draft 01. http://docs.oasis-open.org/wss-m/wss/v1.1.1/csprd01/wss-rel-token-profile-v1.1.1-csprd01.html.

Notices

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/who/trademark.php for above guidance.

Table of Contents

1 Introduction (Informative)

The Web Services Security: SOAP Message Security [WS-Security] specification proposes a standard set of SOAP extensions that can be used when building secure Web services to implement message level integrity and confidentiality. This specification describes the use of ISO/IEC 21000-5 Rights Expressions 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	http://www.w3.org/2003/05/soap-envelope
ds	http://www.w3.org/2000/09/xmldsig#
xenc	http://www.w3.org/2001/04/xmlenc#
wsse	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd
wsse11	http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd
wsu	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd
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

3 Usage (Normative)

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

3.1 Token Types

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

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

3.2 Processing Model

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

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

3.3 Attaching Security Tokens

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

```
<S:Envelope xmlns:S="...">
    <S:Header>
        <wsse:Security xmlns:wsse="...">
            <r:license xmlns:r="...">
                ...
            </r:license>
            ...
        </wsse:Security>
    </S:Header>
    <S:Body>
        ...
    </S:Body>
</S:Envelope>
```

3.4 Identifying and Referencing Security Tokens

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

```
<r:license xmlns:r="..." xmlns:wsu="..."
  licenseId="urn:foo:SecurityToken:ef375268"
  wsu:Id="SecurityToken-ef375268">
  ...
</r:license>
```

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

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

WS-Security specifies that tokens are referenced using the <wsse:SecurityTokenReference> element.

Implementations compliant with this profile SHOULD set the /wsse:SecurityTokenReference/wsse:Reference/@ValueType attribute to http://docs.oasis-open.org/wss/oasis-wss-rel-token-profile-1.0.pdf#license when using wsse:SecurityTokenReference to refer to a license by licenseId. This is OPTIONAL when referring to a license by location.

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

<table>
<tr><td rowspan="2">By Location</td><td>Local</td><td></td><td><pre>
<wsse:SecurityTokenReference>
  <wsse:Reference
    URI="#SecurityToken-ef375268"
  />
</wsse:SecurityTokenReference>
</pre></td><td></td></tr>
<tr><td>Remote</td><td></td><td><pre>
<wsse:SecurityTokenReference>
  <wsse:Reference
    URI="http://www.foo.com/ef375268.xml"
  />
</wsse:SecurityTokenReference>
</pre></td><td></td></tr>
<tr><td colspan="2">By licenseId</td><td></td><td><pre>
<wsse:SecurityTokenReference>
  <wsse:Reference
    URI="urn:foo:SecurityToken:ef375268"
    ValueType="http://docs.oasis-
open.org/wss/oasis-wss-rel-token-profile-
1.0.pdf#license"
  />
</wsse:SecurityTokenReference>
</pre></td><td></td></tr>
</table>

Table 2. <wsse:SecurityTokenReference>

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

```
<S:Envelope xmlns:S="..." xmlns:ds="...">
  <S:Header>
    <wsse:Security xmlns:wsse="...">
      <r:license xmlns:r="..." licenseId="urn:foo:SecurityToken:ef375268"
xmlns:wsu="..." wsu:Id="SecurityToken-ef375268">
        ...
      </r:license>
      ...
      <ds:Signature>
        <ds:SignedInfo>
          ...
        </ds:SignedInfo>
        <ds:SignatureValue>...</ds:SignatureValue>
        <ds:KeyInfo>
          <wsse:SecurityTokenReference>
            <wsse:Reference
              URI="#SecurityToken-ef375268"
            />
          </wsse:SecurityTokenReference>
        </ds:KeyInfo>
      </ds:Signature>
    </wsse:Security>
  </S:Header>
  <S:Body>
    ...
```



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

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

```
<S:Envelope xmlns:S="..." xmlns:wsu="..." >
  <S:Header>
    <wsse:Security xmlns:wsse="...">
      <r:license xmlns:r="..." wsu:Id="SecurityToken-ef375268">
        ...
      </r:license>
      ...
      <wsse:SecurityTokenReference wsu:Id="Str1">
        <wsse:Reference
          URI="#SecurityToken-ef375268"
        />
      </wsse:SecurityTokenReference>
      ...
      <ds:Signature>
        <ds:SignedInfo>
          ...
          <ds:Reference URI="#Str1">
            <ds:Transforms>
              <ds:Transform
                Algorithm="http://schemas.xmlsoap.org/2003/06/STR-Transform">
                <ds:CanonicalizationMethod
                  Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315"/>
              </ds:Transform>
            </ds:Transforms>
            <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>
```

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

```
<S:Envelope xmlns:S="..." xmlns:ds="...">
  <S:Header>
    <wsse:Security xmlns:wsse="...">
      <r:license xmlns:r="..." xmlns:wsu="..." wsu:Id="SecurityToken-
ef375268">
        ...
      </r:license>
      ...
      <ds:Signature>
        <ds:SignedInfo>
          ...
          <ds:Reference URI="#SecurityToken-ef375268">
```



```
            <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>
```

3.5 Authentication

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

The following table enumerates the mandatory principals to be supported by claim confirmation and summarizes their associated processing models. It should be noted that this table is not all-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.

Table 3. Processing Rules for Claim Confirmation

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

3.5.1 <r:keyHolder> Principal

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

Sender

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

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

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

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

Receiver

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

Example

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

```
<S:Envelope xmlns:S="...">

  <S:Header>
    <wsse:Security xmlns:wsse="...">

      <r:license xmlns:r="..." licenseId="urn:foo:SecurityToken:ef375268">
        <r:grant>
          <r:keyHolder>
            <r:info>
              <ds:KeyValue>...</ds:KeyValue>
            </r:info>
          </r:keyHolder>
          <r:possessProperty/>
          <sx:commonName xmlns:sx="...">John Doe</sx:commonName>
        </r:grant>
        <r:issuer>
          <ds:Signature>...</ds:Signature>
        </r:issuer>
      </r:license>

      <ds:Signature>
        <ds:SignedInfo>
          ...
          <ds:Reference URI="#MsgBody">
            <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>
          <wsse:SecurityTokenReference>
            <wsse:Reference
              URI="urn:foo:SecurityToken:ef375268"
              ValueType="http://docs.oasis-open.org/wss/oasis-wss-rel-token-
profile-1.0.pdf#license"
            />
          </wsse:SecurityTokenReference>
        </ds:KeyInfo>
      </ds:Signature>

```



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

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

</S:Envelope>
```

3.6 Confidentiality

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

The following table enumerates the mandatory principals to be supported for confidentiality and summarizes their associated processing models. It should be noted that this table is not all-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.

Table 4. Processing Rules for Confidentiality

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

3.6.1 <r:keyHolder> Principal

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

Sender

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

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

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

Receiver

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

Example

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

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

```
<S:Envelope xmlns:S="..." xmlns:ds="...">
  <S:Header>
   <wsse:Security xmlns:wsse="...">
      <r:license xmlns:r="..." licenseId="urn:foo:SecurityToken:ef375268">
          <r:grant>
            <r:keyHolder>
                 <r:info>
                   <ds:KeyValue>...</ds:KeyValue>
                 </r:info>
            </r:keyHolder>
            <r:possessProperty/>
            <sx:commonName xmlns:sx="...”>SOME COMPANY</sx:commonName>
          </r:grant>
          <r:issuer>
                <ds:Signature>...</ds:Signature>
          </r:issuer>
      </r:license>
      <xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
        <xenc:EncryptionMethod
            Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
        <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
          <wsse:SecurityTokenReference>
                <wsse:Reference URI="urn:foo:SecurityToken:ef375268"/>
          </wsse:SecurityTokenReference>
        </KeyInfo>
        <xenc:CipherData>
          <xenc:CipherValue>dNYS...fQ=</xenc:CipherValue>
        </xenc:CipherData>
        <xenc:ReferenceList>
          <xenc:DataReference URI="#enc"/>
        </xenc:ReferenceList>
      </xenc:EncryptedKey>
   </wsse:Security>
  </S:Header>
   <S:Body wsu:Id="body"
        xmlns:wsu="http://schemas.xmlsoap.org/ws/2003/06/utility">
      <xenc:EncryptedData Id="enc"
           Type="http://www.w3.org/2001/04/xmlenc#Content"
           xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
         <xenc:EncryptionMethod
```



```
            Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc"/>
          <xenc:CipherData>
              <xenc:CipherValue>d2s...GQ=</xenc:CipherValue>
          </xenc:CipherData>
       </xenc:EncryptedData>
    </S:Body>
</S:Envelope>
```

3.7 Error Codes

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

4 Types of Licenses (Informative)

4.1 Attribute Licenses

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.

The following is an example client attribute license.

```
      <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>
```

The following is an example service attribute license.

```
      <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>
```

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

4.2 Sender Authorization

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

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

```
<r:license xmlns:r="..." licenseId="urn:foo:SecurityToken:ef375268">
       <r:grant>
         <r:keyHolder>
            <r:info>
              <ds:KeyValue>FDFEWEFF…</ds:KeyValue>
            </r:info>
         </r:keyHolder>
         <sx:rightUri definition='...'/>
         <x:someResource/>
         <x:someCondition/>
        </r:grant>
        <r:issuer>
           <ds:Signature>...</ds:Signature>
        </r:issuer>
</r:license>
```

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

4.3 Issuer Authorization

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

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

```
<r:license xmlns:r="..." licenseId="urn:foo:SecurityToken:ef375268">
       <r:grant>
          <r:forAll varName='K'/>
          <r:forAll varName='P'/>
         <r:keyHolder>
            <r:info>
              <ds:KeyValue>FDFEWEFF…</ds:KeyValue>
            </r:info>
         </r:keyHolder>
         <r:issue/>
         <r:grant>
           <r:keyHolder varRef='K'/>
           <r:possessProperty/>
           <r:propertyAbstract varRef='P'/>
         </r:grant>
        </r:grant>
        <r:issuer>
           <ds:Signature>...</ds:Signature>
        </r:issuer>
</r:license>
```

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

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



```
              <r:info>
                <ds:KeyValue>FDFEWEFF…</ds:KeyValue>
              </r:info>
           </r:keyHolder>
           <r:issue/>
           <r:grant>
             <r:keyHolder varRef='K'/>
             <sx:rightUri definition='...'/>
             <r:resource varRef='R'/>
           </r:grant>
         </r:grant>
         <r:issuer>
            <ds:Signature>...</ds:Signature>
         </r:issuer>
</r:license>
```

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

```
<r:license xmlns:r="..." licenseId="urn:foo:SecurityToken:ef375268">
   <r:grant>
      <r:forAll varName='I'/>
      <r:keyHolder>
         <r:info>
            <ds:KeyValue>FDFEWEFF…</ds:KeyValue>
         </r:info>
      </r:keyHolder>
      <r:issue/>
      <r:grant>
         <r:forAll varName='K'/>
         <r:forAll varName='P'/>
         <r:keyHolder varRef='I'/>
         <r:issue/>
         <r:grant>
           <r:keyHolder varRef='K'/>
           <r:possessProperty/>
           <r:propertyAbstract varRef='P'/>
         </r:grant>
      </r:grant>
   </r:grant>
   <r:issuer>
      <ds:Signature>...</ds:Signature>
   </r:issuer>
</r:license>
```


5 Threat Model and Countermeasures (Informative)

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

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

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

5.1 Eavesdropping

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

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

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

5.2 Replay

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

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

5.3 Message Insertion

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

5.4 Message Deletion

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

5.5 Message Modification

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

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

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

5.6 Man-in-the-Middle

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

6 References

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

[REL] ISO/IEC 21000-5:2004, "Information technology -- Multimedia framework (MPEG-21) -- Part 5: Rights Expression Language," http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=36095&ICS1=35&ICS2=40&ICS3=

[SOAP] D. Box, D Ehnebuske, G. Kakivaya, A. Layman, N. Mendelsohn, H. Frystyk Nielsen, S Thatte, D. Winer. Simple Object Access Protocol (SOAP) 1.1, W3C Note 08 May 2000, http://www.w3.org/TR/SOAP/

W3C Recommendation, "SOAP Version 1.2 Part 1: Messaging Framework", 23 June 2003

[URI] T. Berners-Lee, R. Fielding, L. Masinter, "Uniform Resource Identifiers (URI): Generic Syntax," RFC 2396, MIT/LCS, U.C. Irvine, Xerox Corporation, August 1998, http://www.ietf.org/rfc/rfc2396.txt

T. Berners-Lee, R. Fielding, L. Masinter, "Uniform Resource Identifiers (URI): Generic Syntax," RFC 3986, MIT/LCS, Day Software, Adobe Systems, January 2005, http://www.ietf.org/rfc/rfc3986.txt.

[WS-Security] Nadalin et al., “Web Services Security: SOAP Message Security 1.1 http://docs.oasis-open.org/wss-m/wss/v1.1.1/csd01/wss-SOAPMessageSecurity-v1.1.1-csd01.pdf

OASIS Standard, "Web Services Security: Soap Message Security 1.1 (WS-Security 2004)," November 2005, http://docs.oasis-open.org/wss/ oasis-wss-soap-message-security-1.1.pdf

[XML-ns] T. Bray, D. Hollander, A. Layman. Namespaces in XML. W3C Recommendation. January 1999, http://www.w3.org/TR/1999/REC-xml-names-19990114

[XML Signature] D. Eastlake, J. R., D. Solo, M. Bartel, J. Boyer , B. Fox , E. Simon. XML-Signature Syntax and Processing, W3C Recommendation, 12 February 2002.

7 Conformance

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

A. Acknowledgements

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

Participants:

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)

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
Sundeep	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

636
637

B. Revision History

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 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.