# Web Services Security Kerberos Token Profile Version 1.1.1

## Committee Specification Draft 01

## 23 March 2011

**Specification URIs:**

**This Version:**

http://docs.oasis-open.org/wss-m/wss/v1.1.1/csd01/wss-KerberosTokenProfile-v1.1.1-csd01.doc (Authoritative)

http://docs.oasis-open.org/wss-m/wss/v1.1.1/csd01/wss-KerberosTokenProfile-v1.1.1-csd01.pdf

http://docs.oasis-open.org/wss-m/wss/v1.1.1/csd01/wss-KerberosTokenProfile-v1.1.1-csd01.html

**Previous Version:**

http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-errata-os-KerberosTokenProfile.doc

http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-errata-os-KerberosTokenProfile.pdf

http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-errata-os-KerberosTokenProfile.html

**Latest Version:**

http://docs.oasis-open.org/wss-m/wss/v1.1.1/wss-KerberosTokenProfile-v1.1.1.doc (Authoritative)

http://docs.oasis-open.org/wss-m/wss/v1.1.1/wss-KerberosTokenProfile-v1.1.1.pdf

http://docs.oasis-open.org/wss-m/wss/v1.1.1/wss-KerberosTokenProfile-v1.1.1.html

**Technical Committee:**

OASIS Web Services Security Maintenance (WSS-M) TC

**Chair(s):**

David Turner, Microsoft

**Editor(s):**

Ronald Monzillo, Sun

Chris Kaler, Microsoft

Anthony Nadalin, IBM

Phillip Hallam-Baker, VeriSign

Carlo Milono, Tibco

**Related work:**

This specification is one part of a multi-part Work Product.  The other parts include:

Web Services Security: SOAP Message Security Version 1.1.1

Web Services Security Rights Expression Language (REL) 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

Schemas: http://docs.oasis-open.org/wss-m/wss/v1.1.1/csd01/xsd/

This specification supersedes:

- Web Services Security Kerberos Token Profile 1.1.  01 November 2006. OASIS Standard incorporating Approved Errata.
- Web Services Security Kerberos Token Profile 1.1. 01 November 2006. OASIS Approved Errata.

**Abstract:**

This document describes how to use Kerberos [Kerb] tickets (specifically the AP-REQ packet) with the Web Services Security: SOAP Message Security 1.1.1.

**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-Kerberos-Token-Profile-V1.1.1]**

*Web Services Security Kerberos Token Profile Version 1.1.1*. 23 March 2011. OASIS Committee Specification Draft 01. http://docs.oasis-open.org/wss-m/wss/v1.1.1/csd01/wss-KerberosTokenProfile-v1.1.1-csd01.doc.

# Notices

Copyright © OASIS Open 2011. 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/who/trademark.php for above guidance.

# Table of Contents

# 1 Introduction

This specification describes the use of Kerberos [**RFC1510**] tokens with respect to the WSS: SOAP Message Security specification [WSS].

Specifically, this document defines how to encode Kerberos tickets and attach them to SOAP messages. As well, it specifies how to add signatures and encryption to the SOAP message, in accordance with WSS: SOAP Message Security, which uses and references the Kerberos tokens.

For interoperability concerns, and for some security concerns, the specification is limited to using the `AP-REQ` packet (service ticket and authenticator) defined by Kerberos as the Kerberos token. This allows a service to authenticate the ticket and interoperate with existing Kerberos implementations.

It should be noted that how the `AP-REQ` is obtained is out of scope of this specification as are scenarios involving other ticket types and user-to-user interactions.

Note that Sections 2.1, 2.2, all of 3, and indicated parts of 6 are normative. All other sections are non-normative.

# 2 Notations and Terminology

14

15 This section specifies the notations, namespaces, and terminology used in this specification.

## 2.1 Notational Conventions

16

17 The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD
18 NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described
19 in RFC2119 [2119].

20

21 Namespace URIs (of the general form "some-URI") represent some application-dependent or context-
22 dependent URI as defined in RFC2396 [URI].

23

24 This specification is designed to work with the general SOAP [S11, S12] message structure and message
25 processing model, and should be applicable to any version of SOAP. The current SOAP 1.2 namespace
26 URI is used herein to provide detailed examples, but there is no intention to limit the applicability of this
27 specification to a single version of SOAP.

## 2.2 Namespaces

28

29 The XML namespace [XML-ns] URIs that MUST be used by implementations of this specification are as
30 follows (note that different elements in this specification are from different namespaces):

31

```
32  http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-
33  1.0.xsd
34  http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
35  1.0.xsd
36  http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd
```

37 Note that this specification does not introduce new schema elements.

38 The following namespaces are used in this document:

| Prefix | Namespace |
|---|---|
| S11 | http://schemas.xmlsoap.org/soap/envelope/ |
| S12 | http://www.w3.org/2003/05/soap-envelope |
| 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 |

| | |
|---|---|
| ds | http://www.w3.org/2000/09/xmldsig# |
| xenc | http://www.w3.org/2001/04/xmlenc# |

39

40  The URLs provided for the wsse and wsu namespaces can be used to obtain the schema files. URI
41  fragments defined in this specification are relative to the following base URI unless otherwise specified:

42  http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1

## 2.3  Terminology

44  Readers are presumed to be familiar with the terms in the Internet Security Glossary [ISG].

45

46  This specification employs the terminology defined in the WSS: SOAP Message Security Core
47  Specification [WSS].

48

49  The following (non-normative) table defines additional acronyms and abbreviations for this document.

| Term | Definition |
|---|---|
| SHA | Secure Hash Algorithm |
| SOAP | Simple Object Access Protocol |
| URI | Uniform Resource Identifier |
| XML | Extensible Markup Language |

50

# 51 **3 Usage**

52 This section describes the profile (specific mechanisms and procedures) for the Kerberos binding of
53 WSS: SOAP Message Security.

54 **Identification:** `http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-`
55 `1.1`

## 56 **3.1 Processing Model**

57 The processing model for WSS: SOAP Message Security with Kerberos tokens is no different from that of
58 WSS: SOAP Message Security with other token formats as described in WSS: SOAP Message Security.

## 59 **3.2 Attaching Security Tokens**

60 Kerberos tokens are attached to SOAP messages using WSS: SOAP Message Security by using the

61 `<wsse:BinarySecurityToken>` described in WSS: SOAP Message Security.  When using this

62 element, the `@ValueType` attribute MUST be specified.  This specification defines six values for this

63 attribute as defined in the table below:

| URI | Description |
|-----|-------------|
| `http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#Kerberosv5_AP_REQ` | Kerberos v5 AP-REQ as defined in the Kerberos specification [Kerb]. This `ValueType` is used when the ticket is an AP Request. |
| `http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#GSS_Kerberosv5_AP_REQ` | A GSS-API Kerberos V5 mechanism token containing an KRB_AP_REQ message as defined in RFC-1964 [1964], Sec. 1.1 and its successor RFC-4121 [4121], Sec. 4.1. This `ValueType` is used when the ticket is an AP Request (ST + Authenticator). |
| `http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#Kerberosv5_AP_REQ1510` | Kerberos v5 AP-REQ as defined in RFC1510. This `ValueType` is used when the ticket is an AP Request per RFC1510. |
| `http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#GSS_Kerberosv5_AP_REQ1510` | A GSS-API Kerberos V5 mechanism token containing an KRB_AP_REQ message as defined in RFC-1964, Sec. 1.1 and its successor RFC-4121, Sec. 4.1. This `ValueType` is used when the ticket is an AP Request (ST + Authenticator) per RFC1510. |

| | |
|---|---|
| `http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#Kerberosv5_AP_REQ4120` | Kerberos v5 AP-REQ as defined in RFC4120. This `ValueType` is used when the ticket is an AP Request per RFC4120 |
| `http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#GSS_Kerberosv5_AP_REQ4120` | A GSS-API Kerberos V5 mechanism token containing an KRB_AP_REQ message as defined in RFC-1964, Sec. 1.1 and its successor RFC-4121, Sec. 4.1. This `ValueType` is used when the ticket is an AP Request (ST + Authenticator) per RFC4120. |

64  It should be noted that the URIs in the table above also serve as the official URIs identifying the Kerberos
65  tokens defined in this specification.

66

67  All token types defined in this section use the type 0x8003 defined in RFC1964 for the checksum field of
68  the authenticator inside the AP_REQ.

69

70  The octet sequence of either the GSS-API framed KRB_AP_REQ token or an unwrapped AP_REQ is
71  encoded using the indicated encoding (e.g. base 64) and the result is placed inside of the
72  `<wsse:BinarySecurityToken>` element.

73  The following example illustrates a SOAP message with a Kerberos token.

```
74  <S11:Envelope xmlns:S11="..." xmlns:wsu="...">
75      <S11:Header>
76          <wsse:Security xmlns:wsse="...">
77              <wsse:BinarySecurityToken EncodingType="http://docs.oasis-
78  open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary"
79  ValueType="http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-
80  1.1#Kerberosv5_AP_REQ" wsu:Id="MyToken">boIBxDCCAcCgAwIBBaEDAgEOogcD...
81              </wsse:BinarySecurityToken>
82              ...
83          </wsse:Security>
84      </S11:Header>
85      <S11:Body>
86          ...
87      </S11:Body>
88  </S11:Envelope>
```

89

## 3.3 Identifying and Referencing Kerberos Tokens

91  A Kerberos Token is referenced by means of the `<wsse:SecurityTokenReference>` element. This
92  mechanism, defined in WSS: SOAP Message Security, provides different referencing mechanisms. The
93  following list identifies the supported and unsupported mechanisms:

94  The `wsu:Id` MAY be specified on the `<wsse:BinarySecurityToken>` element allowing the token to
95  be directly referenced.

96  A `<wsse:KeyIdentifier>` element MAY be used which specifies the identifier for the Kerberos ticket.
97  This value is computed as the SHA1 of the pre-encoded octets that were used to form the contents of the

98  <wsse:BinarySecurityToken> element.  The <wsse:KeyIdentifier> element contains the
99  encoded form the of the KeyIdentifier which is defined as  the base64 encoding of the SHA1 result.

100  Key Name references MUST NOT be used.

101  When a Kerberos Token is referenced using <wsse:SecurityTokenReference> the
102  @wsse11:TokenType attribute SHOULD be specified. If the @wsse11:TokenType is specified its value
103  MUST be the URI that identifies the Kerberos token type as defined for a corresponding
104  BinarySecurityToken/@ValueType attribute.  The Reference/@ValueType attribute is not
105  required. If specified, its value MUST be equivalent to that of the @wsse11:TokenType attribute..

106  The <wsse:SecurityTokenReference> element from which the reference is made contains the
107  <wsse:KeyIdentifier> element. The <wsse:KeyIdentifier> element MUST have a ValueType
108  attribute on the <wsse:KeyIdentifier> element with the value #Kerberosv5APREQSHA1  and its
109  contents MUST be the SHA1 of GSS-API framed KRB_AP_REQ token or unwrapped AP-REQ, as
110  appropriate, encoded as per the <wsse:KeyIdentifier> element's EncodingType  attribute.

111

| Reference Identifier | ValueType URI | Description |
|---|---|---|
| Kerberos v5 AP-REQ | http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#Kerberosv5APREQSHA1 | SHA1 of the v5 AP-REQ octets, either GSS-API framed KRB_AP_REQ token or just the Kerberos AP-REQ. |

112

113  The following example illustrates using ID references to a Kerberos token:

114

```
<S11:Envelope xmlns:S11="..." xmlns:wsse="..." xmlns:wsu="...">
    <S11:Header>
        <wsse:Security>
            <wsse:BinarySecurityToken EncodingType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary"
ValueType="http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-
1.1#Kerberosv5_AP_REQ" wsu:Id="MyToken">
                boIBxDCCAcCgAwIBBaEDAgEOoigcD...
            </wsse:BinarySecurityToken>
            ...
            <wsse:SecurityTokenReference TokenType="http://docs.oasis-
open.org/wss/oasis-wss-kerberos-token-profile-1.1#Kerberosv5_AP_REQ">
                <wsse:Reference URI="#MyToken"
ValueType="http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-
1.1#Kerberosv5_AP_REQ">
                </wsse:Reference>
            </wsse:SecurityTokenReference>
            ...
        </wsse:Security>
    </S11:Header>
    <S11:Body>
        ...
    </S11:Body>
</S11:Envelope>
```

140

141 The AP-REQ packet is included in the initial message to the service, but need not be attached to
142 subsequent messages exchanged between the involved parties.  Consequently, the `KeyIdentifier`
143 reference mechanism SHOULD be used on subsequent exchanges as illustrated in the example below:

144

```
145     <S11:Envelope xmlns:S11="..." xmlns:wsse="..." xmlns:wsu="...">
146         <S11:Header>
147             <wsse:Security>
148                 ...
149                     <wsse:SecurityTokenReference
150     wsse11:TokenType=http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-
151     profile-1.1#Kerberosv5_AP_REQ>
152                         <wsse:KeyIdentifier ValueType="http://docs.oasis-
153     open.org/wss/oasis-wss-kerberos-token-profile-1.1#Kerberosv5APREQSHA1">
154                             GbsDt+WmD9XlnUUWbY/nhBveW8I=
155                         </wsse:KeyIdentifier>
156                     </wsse:SecurityTokenReference>
157                 ...
158             </wsse:Security>
159         </S11:Header>
160         <S11:Body>
161             ...
162         </S11:Body>
163     </S11:Envelope>
```

164

## 3.4 Authentication

166 When a Kerberos ticket is referenced as a signature key, the signature algorithm [DSIG] MUST be a
167 hashed message authentication code.

168

169 When a Kerberos ticket is referenced as an encryption key, the encryption algorithm MUST be a
170 symmetric encryption algorithm.

171

172 The value of the signature or encryption key is constructed from the value of the Kerberos sub-key when
173 it is present in the authenticator or a session key from the ticket if the sub-key is absent, either by using
174 the Kerberos sub-key or session key directly or using a key derived from that key using a mechanism
175 agreed to by the communicating parties.

## 3.5 Encryption

177 When a Kerberos ticket is referenced as an encryption key, the encryption algorithm MUST be a
178 symmetric encryption algorithm.

179

180 The value of the signature or encryption key is constructed from the value of the Kerberos sub-key when
181 it is present in the authenticator or a session key from the ticket if the sub-key is absent, either by using
182 the Kerberos sub-key or session key directly or using a key derived from that key using a mechanism
183 agreed to by the communicating parties..

## 3.6 Principal Name

185 Kerberos principal name definition and mapping of non-Kerberos names to Kerberos V principal names
186 are out of scope of this document.

## 3.7 Error Codes

When using Kerberos tokens, it is RECOMMENDED to use the error codes defined in the WSS: SOAP Message Security specification.  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  Threat Model and Countermeasures

The use of Kerberos assertion tokens with WSS: SOAP Message Security introduces no new message-level threats beyond those identified for Kerberos itself or by WSS: SOAP Message Security with other types of security tokens.

One potential threat is that of key re-use.  The mechanisms described in WSS: SOAP Message Security can be used to prevent replay of the message; however, it is possible that for some service scopes, there are host security concerns of key hijacking within a Kerberos infrastructure.  The use of the AP-REQ and its associated authenticator and sequencer mitigate this threat.

Message alteration and eavesdropping can be addressed by using the integrity and confidentiality mechanisms described in WSS: SOAP Message Security.  Replay attacks can be addressed by using message timestamps and caching, as well as other application-specific tracking mechanisms.  For Kerberos tokens ownership is verified by use of keys, so man-in-the-middle attacks are generally mitigated.

It is strongly recommended that GSS wrapped AP-REQ be used or that unwrapped AP-REQ be combined with `timestamp` be used to prevent replay attack.

It is strongly recommended that all relevant and immutable message data be signed to prevent replay attacks.

It should be noted that transport-level security MAY be used to protect the message and the security token in cases where neither a GSS-API framed KRB_AP_REQ token or an unwrapped AP-REQ combined with timestamp and signature are being used.

The last numbered section in the specification must be the Conformance section. Conformance Statements/Clauses go here.

# 5 References

The following are normative references

**[2119]**        S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels," RFC 2119, Harvard University, March 1997

**[Kerb]**        J. Kohl and C. Neuman, "The Kerberos Network Authentication Service (V5)," RFC 1510, September 1993, http://www.ietf.org/rfc/rfc1510.txt .

**[KEYWORDS]**    S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels," RFC 2119, Harvard University, March 1997

**[S11]**         W3C Note, "SOAP: Simple Object Access Protocol 1.1," 08 May 2000.

**[S12]**         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 3986, MIT/LCS, Day Software, Adobe Systems, January 2005.

**[WSS]**        A. Nadalin et al., Web Services Security: SOAP Message Security 1.1.1 http://docs.oasis-open.org/wss-m/wss/v1.1.1/csd01/wss-SOAPMessageSecurity-v1.1.1-csd01.pdf.

**[1964]**        J. Linn , The Kerberos Version 5 GSS-API Mechanism, RFC 1964, June 1996.

**[4121]**        L, Zhu, K. Jaganathan, S. Hartman, The Kerberos Version 5 Generic Security Service Application Program Interface (GSS-API) Mechanism: Version 2, RFC 4121, July 2005.

The following are non-normative references

**[ISG]**         Informational RFC 2828, "Internet Security Glossary," May 2000.

**[XML-ns]**     W3C Recommendation, "Namespaces in XML," 14 January 1999.

**[DSIG]**       D. Eastlake, J. R., D. Solo, M. Bartel, J. Boyer , B. Fox , E. Simon. *XML-Signature Syntax and Processing*, W3C Recommendation, 12 February 2002. http://www.w3.org/TR/xmldsig-core/.

# # Conformance

The last numbered section in the specification must be the Conformance section. Conformance
Statements/Clauses go here.

# A. Acknowledgements

249

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

252 **Participants:**
253 **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) |

254

255 **Previous Contributors:**

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

| | | |
|---|---|---|
| Dale | Moberg | Cyclone Commerce |
| Rich | Salz | Datapower |
| Sam | Wei | EMC |
| Dana S. | Kaufman | Forum Systems |
| Toshihiro | Nishimura | Fujitsu |
| Kefeng | Chen | GeoTrust |
| Irving | Reid | Hewlett-Packard |
| Kojiro | Nakayama | Hitachi |
| 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 |
| Don | Flinn | Individual |
| Kate | Cherry | Lockheed Martin |
| Paul | Cotton | Microsoft |
| Vijay | Gajjala | Microsoft |
| Martin | Gudgin | Microsoft |
| Chris | Kaler | Microsoft |
| Frederick | Hirsch | Nokia |
| Abbie | Barbir | Nortel |
| Prateek | Mishra | Oracle |
| Vamsi | Motukuru | Oracle |
| Ramana | Turlapi | Oracle |
| Ben | Hammond | RSA Security |
| Rob | Philpott | RSA Security |
| Blake | Dournaee | Sarvega |
| Sundeep | Peechu | Sarvega |
| Coumara | Radja | Sarvega |
| Pete | Wenzel | SeeBeyond |
| Manveen | Kaur | Sun Microsystems |
| Ronald | Monzillo | Sun Microsystems |
| Jan | Alexander | Systinet |
| Symon | Chang | TIBCO Software |
| John | Weiland | US Navy |

| | | |
|---|---|---|
| Hans | Granqvist | VeriSign |
| Phillip | Hallam-Baker | VeriSign |
| Hemma | Prafullchandra | VeriSign |
| Peter | Dapkus | BEA |
| Guillermo | Lao | ContentGuard |
| TJ | Pannu | ContentGuard |
| Xin | Wang | ContentGuard |
| Shawn | Sharp | Cyclone Commerce |
| Ganesh | Vaideeswaran | Documentum |
| Tim | Moses | Entrust |
| Carolina | Canales-Valenzuela | Ericsson |
| Tom | Rutt | Fujitsu |
| Yutaka | Kudo | Hitachi |
| Jason | Rouault | HP |
| Bob | Blakley | IBM |
| Joel | Farrell | IBM |
| Satoshi | Hada | IBM |
| Hiroshi | Maruyama | IBM |
| David | Melgar | IBM |
| Kent | Tamura | IBM |
| Wayne | Vicknair | IBM |
| Phil | Griffin | Individual |
| Mark | Hayes | Individual |
| John | Hughes | Individual |
| Peter | Rostin | Individual |
| Davanum | Srinivas | Individual |
| Bob | Morgan | Individual/Internet2 |
| Bob | Atkinson | Microsoft |
| Keith | Ballinger | Microsoft |
| Allen | Brown | Microsoft |
| Giovanni | Della-Libera | Microsoft |
| Alan | Geller | Microsoft |
| Johannes | Klein | Microsoft |

257

## 258 B. Revision History

259

| 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; Changed the Acknowledgements from Participants to reflect them as Current Contributors and Previous Contributors |
| WD03 | 16-March-2011 | David Turner | Corrected and updated links |

260

261