



1

2

Web Services Security Kerberos Token Profile 1.1

3

4

OASIS Committee Specification, 14 November 2005

5

6

OASIS identifier:

7

wss-v1.1-spec-cs-Kerberos-token-profile

8

Location:

9

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

10

11

Technical Committee:

12

Web Service Security (WSS)

13

Chairs:

14

Kelvin Lawrence, IBM

15

Chris Kaler, Microsoft

16

Editors:

17

Anthony Nadalin, IBM

18

Chris Kaler, Microsoft

19

Ronald Monzillo, Sun

20

Phillip Hallam-Baker, Verisign

21

Abstract:

22

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

23

24

Status:

25

Committee members should send comments on this specification to the wss@lists.oasis-open.org list. Others should subscribe to and send comments to the wss-comment@lists.oasis-open.org list. To subscribe, visit <http://lists.oasis-open.org/ob/adm.pl>.

26

27

28

29

30

For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing

31
32

terms, please refer to the Intellectual Property Rights section of the Security Services TC web page (<http://www.oasis-pen.org/who/intellectualproperty.shtml>).

33

Notices

34 OASIS takes no position regarding the validity or scope of any intellectual property or other rights
35 that might be claimed to pertain to the implementation or use of the technology described in this
36 document or the extent to which any license under such rights might or might not be available;
37 neither does it represent that it has made any effort to identify any such rights. Information on

38 OASIS's procedures with respect to rights in OASIS specifications can be found at the OASIS
39 website. Copies of claims of rights made available for publication and any assurances of licenses
40 to be made available, or the result of an attempt made to obtain a general license or permission
41 for the use of such proprietary rights by implementors or users of this specification, can be
42 obtained from the OASIS Executive Director. OASIS invites any interested party to bring to its
43 attention any copyrights, patents or patent applications, or other proprietary rights which may
44 cover technology that may be required to implement this specification. Please address the
45 information to the OASIS Executive Director.

46

47 Copyright (C) OASIS Open 2005. All Rights Reserved.

48

49 This document and translations of it may be copied and furnished to others, and derivative works
50 that comment on or otherwise explain it or assist in its implementation may be prepared, copied,
51 published and distributed, in whole or in part, without restriction of any kind, provided that the
52 above copyright notice and this paragraph are included on all such copies and derivative works.
53 However, this document itself may not be modified in any way, such as by removing the copyright
54 notice or references to OASIS, except as needed for the purpose of developing OASIS
55 specifications, in which case the procedures for copyrights defined in the OASIS Intellectual
56 Property Rights document must be followed, or as required to translate it into languages other
57 than English.

58

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

61

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

67

68 OASIS has been notified of intellectual property rights claimed in regard to some or all of the
69 contents of this specification. For more information consult the online list of claimed rights.

70

71 This section is non-normative.

| | | |
|----|---|----|
| 72 | Table of Contents | |
| 73 | 1 Introduction | 6 |
| 74 | 2 Notations and Terminology | 7 |
| 75 | 2.1 Notational Conventions | 7 |
| 76 | 2.2 Namespaces | 7 |
| 77 | 2.3 Terminology | 8 |
| 78 | 3 Usage | 9 |
| 79 | 3.1 Processing Model | 9 |
| 80 | 3.2 Attaching Security Tokens | 9 |
| 81 | 3.3 Identifying and Referencing Kerberos Tokens | 11 |
| 82 | 3.4 Authentication | 13 |
| 83 | 3.5 Encryption | 13 |
| 84 | 3.6 Principal Name | 13 |
| 85 | 3.7 Error Codes | 13 |
| 86 | 4 Threat Model and Countermeasures | 14 |
| 87 | 5 References | 15 |
| 88 | Appendix A. Acknowledgments | 16 |
| 89 | Appendix B. Revision History | 19 |
| 90 | | |

91 **1 Introduction**

92 This specification describes the use of Kerberos [Kerb] tokens with respect to the WSS: SOAP
93 Message Security specification [WSS].

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

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

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

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

106 2 Notations and Terminology

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

108 2.1 Notational Conventions

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

112

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

115

116 This specification is designed to work with the general SOAP [S11, S12] message structure and
117 message processing model, and should be applicable to any version of SOAP. The current SOAP
118 1.2 namespace URI is used herein to provide detailed examples, but there is no intention to limit
119 the applicability of this specification to a single version of SOAP.

120 2.2 Namespaces

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

123

```
124 http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-  
125 secext-1.0.xsd  
126 http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-  
127 utility-1.0.xsd  
128 http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd
```

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

130 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/xmlsig# |
| xenc | http://www.w3.org/2001/04/xmlenc# |

131

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

135 <http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1>

136 2.3 Terminology

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

138

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

141

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

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

144

145 3 Usage

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

148 **Identification:** [http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-](http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1)
149 [profile-1.1](http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1)

150 3.1 Processing Model

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

154 3.2 Attaching Security Tokens

155 Kerberos tokens are attached to SOAP messages using WSS: SOAP Message Security by using
156 the <wsse:BinarySecurityToken> described in WSS: SOAP Message Security. When using
157 this element, the @ValueType attribute MUST be specified. This specification defines six
158 values for this 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. 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 <code>ValueType</code> is used when the ticket is an AP Request (ST + Authenticator) per RFC1510. |
| <code>http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#Kerberosv5_AP_REQ4120</code> | Kerberos v5 AP-REQ as defined in RFC4120. This <code>ValueType</code> is used when the ticket is an AP Request per RFC4120 |
| <code>http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#GSS_Kerberosv5_AP_REQ4120</code> | 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 <code>ValueType</code> is used when the ticket is an AP Request (ST + Authenticator) per RFC4120. |

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

161

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

164

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

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

```

169 <S11:Envelope xmlns:S11="..." xmlns:wsu="...">
170   <S11:Header>
171     <wsse:Security xmlns:wsse="...">
172       <wsse:BinarySecurityToken EncodingType="http://docs.
173         oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-
174         security-1.0#Base64Binary" ValueType=" http://docs.oasis-
175         open.org/wss/oasis-wss-kerberos-token-profile-1.1#Kerb
176         erosv5_AP_REQ" wsu:Id="MyToken">boIBxDCCAcCgAwIBBaEDAgEOogcD...
177       </wsse:BinarySecurityToken>
178       ...
179     </wsse:Security>
180   </S11:Header>
181   <S11:Body>
182     ...
183   </S11:Body>
184 </S11:Envelope>

```

185

186 3.3 Identifying and Referencing Kerberos Tokens

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

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

193 A `<wsse:KeyIdentifier>` element MAY be used which specifies the identifier for the
194 Kerberos ticket. This value is computed as the SHA1 of the pre-encoded octets that were used to
195 form the contents of the `<wsse:BinarySecurityToken>` element. The
196 `<wsse:KeyIdentifier>` element contains the encoded form the of the `KeyIdentifier`
197 which is defined as the base64 encoding of the SHA1 result.

198 Key Name references MUST NOT be used.

199 When a Kerberos Token is referenced using `<wsse:SecurityTokenReference>` the
200 `@wsse11:TokenType` attribute SHOULD be specified. If the `@wsse11:TokenType` is specified
201 its value MUST be the URI that identifies the Kerberos token type as defined for a corresponding
202 `BinarySecurityToken/@ValueType` attribute. The `Reference/@ValueType` attribute is
203 not required. If specified, its value MUST be equivalent to that of the `@wsse11:TokenType`
204 attribute..

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

211

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

212

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

214

```
215 <S11:Envelope xmlns:S11="..." xmlns:wsse="..." xmlns:wsu="...">  
216 <S11:Header>
```

```

217     <wsse:Security>
218         <wsse:BinarySecurityToken EncodingType="http://docs.
219 oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-
220 1.0#Base64Binary" ValueType="http://docs.oasis-open.org/wss/oasis-wss-
221 kerberos-token-profile-1.1#Kerberosv5_AP_REQ" wsu:Id="MyToken">
222             boIBxDCCAcCgAwIBBaEDAgEOgcD...
223         </wsse:BinarySecurityToken>
224         ...
225         <wsse:SecurityTokenReference>
226             <wsse:Reference URI="#MyToken"
227 ValueType="http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-
228 profile-1.1#Kerberosv5_AP_REQ">
229             </wsse:Reference>
230         </wsse:SecurityTokenReference>
231         ...
232     </wsse:Security>
233 </S11:Header>
234 <S11:Body>
235     ...
236 </S11:Body>
237 </S11:Envelope>
238

```

239

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

244

```

245 <S11:Envelope xmlns:S11="..." xmlns:wsse="..." xmlns:wsu="...">
246     <S11:Header>
247         <wsse:Security>
248             ...
249             <wsse:SecurityTokenReference>
250 wss11:TokenType="http://docs.oasis-open.org/wss/oasis-wss-kerberos-
251 token-profile-1.1#Kerberosv5_AP_REQ"
252             <wsse:KeyIdentifier ValueType="http://docs.oasis-
253 open.org/wss/oasis-wss-kerberos-token-profile-1.1#Kerb
254 erosv5APREQSHA1">GbsDt+WmD9XlnUUWbY/nhBveW8I=
255             </wsse:KeyIdentifier>
256             </wsse:SecurityTokenReference>
257             ...
258         </wsse:Security>
259     </S11:Header>
260     <S11:Body>
261         ...
262     </S11:Body>
263 </S11:Envelope>
264

```

265 **3.4 Authentication**

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

268

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

271

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

276 **3.5 Encryption**

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

279

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

284 **3.6 Principal Name**

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

287 **3.7 Error Codes**

288 When using Kerberos tokens, it is RECOMMENDED to use the error codes defined in the WSS:
289 SOAP Message Security specification. However, implementations MAY use custom errors,
290 defined in private namespaces if they desire. Care should be taken not to introduce security
291 vulnerabilities in the errors returned.

292

4 Threat Model and Countermeasures

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

296

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

301

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

307

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

310

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

313

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

317

5 References

318 The following are normative references

- 319 **[2119]** S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels,"
320 RFC 2119, Harvard University, March 1997
- 321 **[Kerb]** J. Kohl and C. Neuman, "The Kerberos Network Authentication Service
322 (V5)," RFC 1510, September 1993, <http://www.ietf.org/rfc/rfc1510.txt> .
- 323 **[KEYWORDS]** S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels,"
324 RFC 2119, Harvard University, March 1997
- 325 **[S11]** W3C Note, "SOAP: Simple Object Access Protocol 1.1," 08 May 2000.
- 326 **[S12]** W3C Recommendation, "SOAP Version 1.2 Part 1: Messaging
327 Framework", 23 June 2003.
- 328 **[URI]** T. Berners-Lee, R. Fielding, L. Masinter, "Uniform Resource Identifiers
329 (URI): Generic Syntax," RFC 3986, MIT/LCS, Day Software, Adobe
330 Systems, January 2005.
- 331 **[WSS]** A. Nadalin et al., Web Services Security: SOAP Message Security 1.1
332 (WS-Security 2004), OASIS Standard, [http://docs.oasis-](http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.1.pdf)
333 [open.org/wss/2004/01/oasis-200401-wss-soap-message-security-](http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.1.pdf)
334 [1.1.pdf](http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.1.pdf).
- 335 **[1964]** J. Linn , The Kerberos Version 5 GSS-API Mechanism, RFC 1964, June
336 1996.
- 337 **[4121]** L, Zhu, K. Jaganathan, S. Hartman, The Kerberos Version 5 Generic
338 Security Service Application Program Interface (GSS-API) Mechanism:
339 Version 2, RFC 4121, July 2005.

340 The following are non-normative references

- 341 **[ISG]** Informational RFC 2828, "Internet Security Glossary," May 2000.
- 342 **[XML-ns]** W3C Recommendation, "Namespaces in XML," 14 January 1999.
- 343 **[DSIG]** D. Eastlake, J. R., D. Solo, M. Bartel, J. Boyer , B. Fox , E. Simon. *XML-*
344 *Signature Syntax and Processing*, W3C Recommendation, 12 February
345 2002. <http://www.w3.org/TR/xmlsig-core/>.

Appendix A. Acknowledgments

Current 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 |
| Sundeeep | 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 |

348

Previous Contributors:

| | | |
|-----------|--------------------|----------------------|
| 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 |
| 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 |
| Senthil | Sengodan | Nokia |
| Lloyd | Burch | Novell |
| Ed | Reed | Novell |
| Charles | Knouse | Oblix |
| Vipin | Samar | Oracle |
| Jerry | Schwarz | Oracle |
| Eric | Gravengaard | Reactivity |
| Andrew | Nash | Reactivity |
| Stuart | King | Reed Elsevier |
| Martijn | de Boer | SAP |
| Jonathan | Tourzan | Sony |
| Yassir | Elley | Sun |
| Michael | Nguyen | The IDA of Singapore |
| Don | Adams | TIBCO |
| Morten | Jorgensen | Vordel |

349

Appendix B. Revision History

350

| Rev | Date | By Whom | What |
|-----|------|---------|------|
|-----|------|---------|------|