



# Web Services Security Kerberos Token Profile 1.1

## OASIS Public Review Draft – 28 June 2005

**OASIS identifier:**

{product-productVersion-artifactType-stage-descriptiveName-revision.form  
(Word) (PDF) (HTML)}

**Location:**

<http://docs.oasis-open.org/wss/2005/xx/wss-v1.1-spec-pr-KerberosTokenProfile-01>

**Technical Committee:**

Web Service Security (WSS)

**Chairs:**

Kelvin Lawrence, IBM  
Chris Kaler, Microsoft

**Editors:**

Anthony Nadalin, IBM  
Chris Kaler, Microsoft  
Ronald Monzillo, Sun  
Phillip Hallam-Baker, Verisign

**Abstract:**

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

**Status:**

This is an interim draft. Please send comments to the editors.

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

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 Security Services TC web page (<http://www.oasis-open.org/who/intellectualproperty.shtml>).

---

## Notices

37 OASIS takes no position regarding the validity or scope of any intellectual property or other rights  
38 that might be claimed to pertain to the implementation or use of the technology described in this  
39 document or the extent to which any license under such rights might or might not be available;  
40 neither does it represent that it has made any effort to identify any such rights. Information on  
41 OASIS's procedures with respect to rights in OASIS specifications can be found at the OASIS  
42 website. Copies of claims of rights made available for publication and any assurances of licenses  
43 to be made available, or the result of an attempt made to obtain a general license or permission  
44 for the use of such proprietary rights by implementors or users of this specification, can be  
45 obtained from the OASIS Executive Director.

46 OASIS invites any interested party to bring to its attention any copyrights, patents or patent  
47 applications, or other proprietary rights which may cover technology that may be required to  
48 implement this specification. Please address the information to the OASIS Executive Director.

49 Copyright © The Organization for the Advancement of Structured Information Standards [OASIS]  
50 2002-2005. All Rights Reserved.

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

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

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	Table of Contents	
68	1 Introduction .....	4
69	2 Notations and Terminology .....	5
70	2.1 Notational Conventions .....	5
71	2.2 Namespaces .....	5
72	2.3 Terminology .....	6
73	3 Usage .....	7
74	3.1 Processing Model .....	7
75	3.2 Attaching Security Tokens .....	7
76	3.3 Identifying and Referencing Kerberos Tokens .....	8
77	3.4 Authentication .....	9
78	3.5 Encryption .....	10
79	3.6 Principal Name .....	10
80	3.7 Error Codes .....	10
81	4 Threat Model and Countermeasures .....	11
82	5 References .....	12
83	Appendix A. Acknowledgments .....	13
84	Appendix B. Revision History .....	16
85		

---

86 **1 Introduction**

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

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

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

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

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

---

## 101 2 Notations and Terminology

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

### 103 2.1 Notational Conventions

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

107

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

110

111 This specification is designed to work with the general SOAP [S11, S12] message structure and  
112 message processing model, and should be applicable to any version of SOAP. The current SOAP  
113 1.2 namespace URI is used herein to provide detailed examples, but there is no intention to limit  
114 the applicability of this specification to a single version of SOAP.

### 115 2.2 Namespaces

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

118

```
119 http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-  
120 secext-1.0.xsd  
121 http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-  
122 utility-1.0.xsd  
123 http://docs.oasis-open.org/wss/2005/xx/oasis-2005xx-wss-wssecurity-  
124 secext-1.1.xsd
```

125

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

127 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	<a href="http://docs.oasis-open.org/wss/2005/xx/oasis-2005xx-wss-wssecurity-seceext-1.1.xsd">http://docs.oasis-open.org/wss/2005/xx/oasis-2005xx-wss-wssecurity-seceext-1.1.xsd</a>
wsu	<a href="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd</a>
ds	<a href="http://www.w3.org/2000/09/xmlsig#">http://www.w3.org/2000/09/xmlsig#</a>
xenc	<a href="http://www.w3.org/2001/04/xmlenc#">http://www.w3.org/2001/04/xmlenc#</a>

128

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

132 <http://docs.oasis-open.org/wss/2005/xx/oasis-2005xx-wss-kerberos-token-profile-1.1>

### 133 2.3 Terminology

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

135

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

138

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

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

141

---

## 142 3 Usage

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

145 **Identification:** <http://docs.oasis-open.org/wss/2005/xx/oasis-2005xx-wss-kerberos-token-profile-1.1>  
146

### 147 3.1 Processing Model

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

### 151 3.2 Attaching Security Tokens

152 Kerberos tokens are attached to SOAP messages using WSS: SOAP Message Security by using  
153 the `<wsse:BinarySecurityToken>` described in WSS: SOAP Message Security. When using  
154 this element, the `@ValueType` attribute **MUST** be specified. This specification defines two values  
155 for this token as defined in the table below:

URI	Description
<a href="http://docs.oasis-open.org/wss/2005/xx/oasis-2005xx-wss-kerberos-token-profile-1.1#Kerberosv5_AP_REQ">http://docs.oasis-open.org/wss/2005/xx/oasis-2005xx-wss-kerberos-token-profile-1.1#Kerberosv5_AP_REQ</a>	Kerberos v5 AP-REQ as defined in the Kerberos specification. This ValueType is used when the ticket is an AP Request.
<a href="http://docs.oasis-open.org/wss/2005/xx/oasis-2005xx-wss-kerberos-token-profile-1.1#GSS_Kerberosv5_AP_REQ">http://docs.oasis-open.org/wss/2005/xx/oasis-2005xx-wss-kerberos-token-profile-1.1#GSS_Kerberosv5_AP_REQ</a>	A GSS wrapped Kerberos v5 AP-REQ as defined in the GSSAPI specification. This ValueType is used when the ticket is an AP Request (ST + Authenticator).

156 It should be noted that the URIs in the table above also serves as the official URIs  
157 identifying the Kerberos token defined in this specification.

158

159 Both token types defined in this section use the type 0x8003 defined in RFC1964 for the  
160 checksum field of the authenticator inside the AP\_REQ.

161

162 The octet sequence of the either the GSS wrapped Kerberos ticket or the Kerberos  
163 ticket (e.g. AP-REQ) is encoded using the indicated algorithm (e.g. base 64) and the  
164 result is placed inside of the `<wsse:BinarySecurityToken>` element.

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

```
166 <S11:Envelope xmlns:S11="...">  
167 <S11:Header>
```

168  
169  
170  
171  
172  
173  
174  
175  
176  
177  
178  
179  
180  
181  
182

```
<wsse:Security xmlns:wsse="...">
  <wsse:BinarySecurityToken
    xmlns:wsse="..."
    wsu:Id="myToken"
    ValueType="...#Kerberosv5_AP_REQ"
    EncodingType="...#Base64Binary">
    MIEZzCCA9CgAwIBAgIQEmtJZc0...
  </wsse:BinarySecurityToken>
  ...
</wsse:Security>
</S11:Header>
<S11:Body>
  ...
</S11:Body>
</S11:Envelope>
```

183

### 184 3.3 Identifying and Referencing Kerberos Tokens

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

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

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

196 Key Name references MUST NOT be used.

197 When a Kerberos Token is referenced using `<wsse:SecurityTokenReference>` the  
198 `@ValueType` attribute is not required. If specified, the URI listed above as Kerberos token type  
199 MUST be specified.

200 The `<wsse:SecurityTokenReference>` element from which the reference is made contains  
201 the `<wsse:KeyIdentifier>` element. The `<wsse:KeyIdentifier>` element MUST have a  
202 `ValueType` attribute with the value `#Kerberosv5APREQSHA1` and its contents MUST be the  
203 SHA1 of GSS wrapped or unwrapped AP-REQ, encoded as per the `<wsse:KeyIdentifier>`  
204 element's `EncodingType` attribute.

205

Reference Identifier	ValueType URI	Description
Kerberos v5 AP-REQ	#Kerberosv5APREQSHA1	SHA1 of the v5 AP-REQ octets, either GSS wrapped Kerberos AP-REQ or just the Kerberos AP-REQ.

206



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

208

```
209 <S11:Envelope xmlns:S11="...">
210   <S11:Header>
211     <wsse:Security xmlns:wsse="...">
212       <wsse:BinarySecurityToken
213         xmlns:wsse="..."
214         wsu:Id="myToken"
215         ValueType="...#Kerberosv5_AP_REQ"
216         EncodingType="...#Base64Binary">
217         MIEZzCCA9CgAwIBAgIQEmtJZc0...
218       </wsse:BinarySecurityToken>
219       ...
220       <wsse:SecurityTokenReference>
221         <wsse:Reference URI="#myToken" />
222       </wsse:SecurityTokenReference>
223       ...
224     </wsse:Security>
225   </S11:Header>
226   <S11:Body>
227     ...
228   </S11:Body>
229 </S11:Envelope>
230
```

231

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

236

```
237 <S11:Envelope xmlns:S11="...">
238   <S11:Header>
239     <wsse:Security xmlns:wsse="...">
240       ...
241       <wsse:SecurityTokenReference
242 <wsse:KeyIdentifier    ValueType="...#Kerberosv5APREQSHA1">
243         EZzCCA9CgAwIB...
244         <wsse:KeyIdentifier>
245         </wsse:KeyIdentifier>
246       </wsse:SecurityTokenReference>
247       ...
248     </wsse:Security>
249   </S11:Header>
250   <S11:Body>
251     ...
252   </S11:Body>
253 </S11:Envelope>
254
```

### 254 3.4 Authentication

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

257

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

260

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

### 265 **3.5 Encryption**

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

268

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

### 273 **3.6 Principal Name**

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

### 276 **3.7 Error Codes**

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

281

---

## 4 Threat Model and Countermeasures

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

285

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

290

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

296

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

299

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

302

303 It should be noted that transport-level security MAY be used to protect the message and the  
304 security token if either a wrapped AP-REQ or that unwrapped AP-REQ be combined with  
305 timestamp and signature are not being used.

---

## 5 References

306

307 The following are normative references

308       **[2119]**       S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels,"  
309                    [RFC 2119](#), Harvard University, March 1997

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

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

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

315       **[S12]**        W3C Recommendation, "SOAP Version 1.2 Part 1: Messaging  
316                    Framework", 23 June 2003.

317       **[URI]**        T. Berners-Lee, R. Fielding, L. Masinter, "Uniform Resource Identifiers  
318                    (URI): Generic Syntax," RFC 3986, MIT/LCS, Day Software, Adobe  
319                    Systems, January 2005.

320 The following are non-normative references

321       **[ISG]**        Informational RFC 2828, "[Internet Security Glossary](#)," May 2000.

322       **[WSS]**        A. Nadalin et al., Web Services Security: SOAP Message Security 1.0  
323                    (WS-Security 2004), OASIS Standard 200401, March 2004,  
324                    [http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-](http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf)  
325                    [message-security-1.0.pdf](http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf).

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

327       **[DSIG]**        D. Eastlake, J. R., D. Solo, M. Bartel, J. Boyer , B. Fox , E. Simon. *XML-*  
328                    *Signature Syntax and Processing*, W3C Recommendation, 12 February  
329                    2002. <http://www.w3.org/TR/xmlsig-core/>.

---

330 **Appendix A. Acknowledgments**

331 This specification was developed as a result of joint work of many individuals from the WSS TC.

332 The input specifications for this document were developed as a result of joint work with many  
333 individuals and teams, including: Keith Ballinger, Microsoft, Bob Blakley, IBM, Allen Brown,  
334 Microsoft, Joel Farrell, IBM, Mark Hayes, VeriSign, Kelvin Lawrence, IBM, Scott Konersmann,  
335 Microsoft, David Melgar, IBM, Dan Simon, Microsoft, Wayne Vicknair, IBM.

336

Gene	Thurston	AmberPoint
Frank	Siebenlist	Argonne National Lab
Merlin	Hughes	Baltimore Technologies
Irving	Reid	Baltimore Technologies
Peter	Dapkus	BEA
Hal	Lockhart	BEA
Steve	Anderson	BMC (Sec)
Thomas	DeMartini	ContentGuard
Guillermo	Lao	ContentGuard
TJ	Pannu	ContentGuard
Shawn	Sharp	Cyclone Commerce
Ganesh	Vaideeswaran	Documentum
Sam	Wei	Documentum
John	Hughes	Entegrity
Tim	Moses	Entrust
Toshihiro	Nishimura	Fujitsu
Tom	Rutt	Fujitsu
Yutaka	Kudo	Hitachi
Jason	Rouault	HP
Bob	Blakley	IBM
Joel	Farrell	IBM
Satoshi	Hada	IBM
Maryann	Hondo	IBM
Hiroshi	Maruyama	IBM

David	Melgar	IBM
Anthony	Nadalin	IBM
Nataraj	Nagaratnam	IBM
Wayne	Vicknair	IBM
Kelvin	Lawrence	IBM (co-Chair)
Don	Flinn	Individual
Bob	Morgan	Individual
Bob	Atkinson	Microsoft
Keith	Ballinger	Microsoft
Allen	Brown	Microsoft
Paul	Cotton	Microsoft
Giovanni	Della-Libera	Microsoft
Vijay	Gajjala	Microsoft
Johannes	Klein	Microsoft
Scott	Konermann	Microsoft
Chris	Kurt	Microsoft
Brian	LaMacchia	Microsoft
Paul	Leach	Microsoft
John	Manferdell	Microsoft
John	Shewchuk	Microsoft
Dan	Simon	Microsoft
Hervey	Wilson	Microsoft
Chris	Kaler	Microsoft (co-Chair)
Prateek	Mishra	Netegrity
Frederick	Hirsch	Nokia
Senthil	Sengodan	Nokia
Lloyd	Burch	Novell
Ed	Reed	Novell
Charles	Knouse	Oblix
Vipin	Samar	Oracle
Jerry	Schwarz	Oracle

Eric	Gravengaard	Reactivity
Stuart	King	Reed Elsevier
Andrew	Nash	RSA Security
Rob	Philpott	RSA Security
Peter	Rostin	RSA Security
Martijn	de Boer	SAP
Pete	Wenzel	SeeBeyond
Jonathan	Tourzan	Sony
Yassir	Elley	Sun Microsystems
Jeff	Hodges	Sun Microsystems
Ronald	Monzillo	Sun Microsystems
Jan	Alexander	Systinet
Michael	Nguyen	The IDA of Singapore
Don	Adams	TIBCO
Symon	Chang	TIBCO
John	Weiland	US Navy
Phillip	Hallam-Baker	VeriSign
Mark	Hays	Verisign
Hemma	Prafullchandra	VeriSign

337

---

## Appendix B. Revision History

Rev	Date	What
01	18-Sep-02	Initial draft based on input documents and editorial review
03	30-Jan-03	Changes in title
04	20-Jan-04	Revise based on comments, switch to new URLs and formats and recent decisions in TC
05	27-Jul-04	Revise based on comments and recent decisions in TC
06	16-May-05	Revise based on comments and recent decisions in TC. Issues 381, 382, 383, 384, 385, 386, 387
07	17-May-05	Formatting Issues
08	14-June-05	Issues 396