Web Services Security
Kerberos Token Profile 1.0

Working Draft 05, 15 April 2004

Document identifier:

{*WSS: SOAP Message Security* }-{Kerboer Token Profile }-{*1.0*} (Word) (PDF)

Location:

http://docs.oasis-open.org/wss/2004/04/oasis-xxxxxx-wss-kerberos-token-profile-1.0

Editors:

Anthony	Nadalin	IBM
Phil	Griffin	Individual
Chris	Kaler	Microsoft
Phillip	Hallam-Baker	VeriSign
Ronald	Monzillo	Sun

Contributors:

Gene	Thurston	AmberPoint
Frank	Siebenlist	Argonne National Lab
Merlin	Hughes	Baltimore Technologies
Irving	Reid	Baltimore Technologies
Peter	Dapkus	BEA
Hal	Lockhart	BEA
Symon	Chang	CommerceOne
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
Steve	Anderson	OpenNetwork (Sec)
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
John	Weiland	US Navy
Phillip	Hallam-Baker	VeriSign
Mark	Hays	Verisign
Hemma	Prafullchandra	VeriSign

Abstract:

This document describes how to use Kerberos [Kerb] tickets with the Web Services Security: SOAP Message Security specification [WSS].

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 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.

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).

Table of Contents

1 Introduction

This specification describes the use of Kerberos [Kerb] tokens with respect to the Web Services Security: 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, which uses and references the Kerberos tokens.

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

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

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 RFC2119 [2119].

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

This specification is designed to work with the general SOAP [S11, S12] 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 XML namespace [XML-ns] URIs that MUST be used by implementations of this specification are as follows (note that different elements in this specification are from different namespaces):

```
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
secext-1.0.xsd
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
utility-1.0.xsd
```

Note that this specification does not introduce new schema elements.

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/2004/01oasis-200401-wss-wssecurity-secext-1.0.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#

2.3 Terminology

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

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

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
UCS	Universal Character Set
UTF8	UCS Transformation Format, 8-bit form
XML	Extensible Markup Language

3 Usage

This section describes the profile (specific mechanisms and procedures) for the Kerberos binding of WSS.

Identification: http://docs.oasis-open.org/wss/2004/04/oasis-xxxxxx-wss-kerberos-token-profile-1.0

3.1 Processing Model

The processing model for WSS with Kerberos tokens is no different from that of WSS with other token formats as described in WSS.

3.2 Attaching Security Tokens

Kerberos tokens are attached to SOAP messages using WSS by using the `<wsse:BinarySecurityToken>` described in WSS. When using this element, the @ValueType attribute MUST be specified. This specification defines two values for this token as defined in the table below (note that the URIs are relative to the URI for this document as identified on the cover page of this specification):

URI	Description
#Kerberosv5TGT	Kerberos v5 ticket as defined in the Kerberos specification. This ValueType is used when the ticket is a ticket granting ticket (TGT).
#Kerberosv5ST	Kerberos v5 ticket as defined in the Kerberos specification. This ValueType is used when the ticket is a service ticket (ST).

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

The octet sequence of the Kerberos ticket is encoded using the indicated algorithm (e.g. base 64) and the result is placed inside of the `<wsse:BinarySecurityToken>` element.

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

```
<S11:Envelope xmlns:S11="...">
    <S11:Header>
        <wsse:Security xmlns:wsse="...">
            <wsse:BinarySecurityToken
            xmlns:wsse="... "
                wsu:Id="myToken"
                ValueType="...#Kerberosv5ST"
                EncodingType="...#Base64Binary">
                MIIEZzCCA9CgAwIBAgIQEmtJZc0...
            </wsse:BinarySecurityToken>
            ...
        </wsse:Security>
    </S11:Header>
    <S11:Body>
        ...
    </S11:Body>
```

```
</S11:Envelope>

```

3.3 Identifying and Referencing Kerberos Tokens

An attached Kerberos Token is referenced by means of the `<wsse:SecurityTokenReference>` element. This mechanism, defined in WSS provides different referencing mechanisms. The following list identifies the supported and unsupported mechanisms:

- The *wsu:Id* MAY be specified on the `<wsse:BinarySecurityToken>` element allowing the token to be directly referenced.
- A `<wsse:KeyIdentifier>` element MAY be used which specifies the identifier for the Kerberos ticket. This value is computed as the SHA1 of the pre-encoded octets that use used in the `<wsse:BinarySecurityToken>` element. The `<wsse:KeyIdentifier>` element contains the encoded form the of the KeyIdentifier (e.g. the base64 encoding of the SHA1 result).
- Key Name references MAY NOT be used.

When a Kerberos Token is referenced using `<wsse:SecurityTokenReference>` the *@ValueType* attribute is not required. If specified, one of the URIs listed above as Kerberos token types MUST be specified.

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

```
<S11:Envelope xmlns:S11="...">
    <S11:Header>
        <wsse:Security xmlns:wsse="...">
            <wsse:BinarySecurityToken
            xmlns:wsse="... "
                wsu:Id="myToken"
                ValueType="...#Kerberosv5ST"
                EncodingType="...#Base64Binary">
                MIIEZzCCA9CgAwIBAgIQEmtJZc0...
            </wsse:BinarySecurityToken>
            ...
               <wsse:SecurityTokenReference>
                   <wsse:Reference URI="#myToken"/>
               </wsse:SecurityTokenReference>
            ...
        </wsse:Security>
    </S11:Header>
    <S11:Body>
        ...
    </S11:Body>
</S11:Envelope>

```

The following example illustrates using key identifier references to a Kerberos token:

```
<S11:Envelope xmlns:S11="...">
    <S11:Header>
        <wsse:Security xmlns:wsse="...">
            <wsse:BinarySecurityToken
            xmlns:wsse="... "
                wsu:Id="myToken"
                ValueType="...#Kerberosv5ST"
                EncodingType="...#Base64Binary">
                MIIEZzCCA9CgAwIBAgIQEmtJZc0...
            </wsse:BinarySecurityToken>
            ...
               <wsse:SecurityTokenReference
                                     ValueType="...#Kerberosv5ST>
                   <wsse:KeyIdentifier>
                       EZzCCA9CgAwIB...
                   <wsse:KeyIdentifier>
               </wsse:SecurityTokenReference>
            ...
        </wsse:Security>
    </S11:Header>
    <S11:Body>
        ...
    </S11:Body>
</S11:Envelope>

```

3.4 Authentication

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

The value of the signature key is the value of the Kerberos session key or a key derived from this session key using a mechanism agreed to by the communicating parties.

3.5 Encryption

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

The value of the encryption key is the value of the Kerberos session key or a key derived from this session key using a mechanism agreed to by the communicating parties.

3.6 Error Codes

When using Kerberos tokens, it is RECOMMENDED to use the error codes defined in the WSS 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 introduces no new threats beyond those identified for Kerberos or WSS with other types of security tokens.

Message alteration and eavesdropping can be addressed by using the integrity and confidentiality mechanisms described in WSS. 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, 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.

5 Acknowledgements

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

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

6 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, http://www.ietf.org/rfc/rfc2119.txt

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

[S12] W3C Recomendation**, “**http://www.w3.org/TR/2003/REC-soap12-part1-20030624/”, 24 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

[WSS] OASIS Standard,”Web Services Security: SOAP Message Security”, http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.

[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.

[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/.

The following are non-normative references

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

Appendix A: 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	Jan-04	Revise based on comments, switch to new URLs and formats and recent decisions in TC
05	15-Apr-04	Bring in-line with other profiles documents and WSS

Appendix B: Notices

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's procedures with respect to rights in OASIS specifications can be found at 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 implementors or users of this specification, can be obtained from the OASIS Executive Director.

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

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 RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.