Web Services Security
X509 Certificate Token Profile

Working Draft 03, 30 January 2003

Document identifier:

WSS-X509-03

Location:

TBD

Editors:

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

Contributors:

TBD – Revise this list to include WSS TC contributors

Bob Atkinson, Microsoft
Giovanni Della-Libera, Microsoft
Satoshi Hada, IBM
Phillip Hallam-Baker, VeriSign
Maryann Hondo, IBM
Chris Kaler, Microsoft
Johannes Klein, Microsoft
Brian LaMacchia, Microsoft
Paul Leach, Microsoft
John Manferdelli, Microsoft
Hiroshi Maruyama, IBM
Anthony Nadalin, IBM
Nataraj Nagaratnam, IBM
Hemma Prafullchandra, VeriSign
John Shewchuk, Microsoft
Dan Simon, Microsoft
Kent Tamura, IBM
Hervey Wilson, Microsoft

Abstract:

This document describes how to use X509 Certificates with the WS-Security 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 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 X509 certificates with respect to the WS-Security specification.

Note that Section 1 is 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.

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

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

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

2.2 Namespaces

The XML namespace 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://schemas.xmlsoap.org/ws/2002/xx/secext
        http://schemas.xmlsoap.org/ws/2002/xx/utility
```

The following namespaces are used in this document:

Prefix	Namespace
S	http://www.w3.org/2001/12/soap-envelope
ds	http://www.w3.org/2000/09/xmldsig#
xenc	http://www.w3.org/2001/04/xmlenc#
wsse	http://schemas.xmlsoap.org/ws/2002/xx/secext
wsu	http://schemas.xmlsoap.org/ws/2002/xx/utility

2.3 Terminology

This specification employs the terminology defined in the WS-Security Core Specification.

Defined below are the basic definitions for additional terminology used in this specification.

[TBS]

3 Usage

This section describes the profile (specific mechanisms and procedures) for the X509 binding of WS-Security.

Identification: urn:oasis:names:tc:WSS:1.0:profiles:WSS-X509-token

Contact information: TBD

Description: Given below.

Updates: None.

3.1 Processing Model

The processing model for WS-Security with X509 certificates is no different from that of WS-Security with other token formats as described in WS-Security.

3.2 Attaching Security Tokens

The WS-Security specification indicates that X.509 certificates MAY be described inside of a `<ds:KeyInfo>` element, however, it is RECOMMENDED that they be specified using a `<wsse:BinarySecurityToken>`. If, however, an implementation needs to use `<ds:KeyInfo>`, it SHOULD place the `<ds:KeyInfo>` element as a child of the `<wsse:Security>` header rather than embedded within the signature. This allows receivers to have a single processing model.

The following value space is defined for the ValueType attribute of the `<wsse:BinarySecurityToken>` element.

QName	Description
wsse:X509v3	X.509 v3 certificate

The following example illustrates a SOAP message with an X509 Certificate.

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

            <wsse:BinarySecurityToken
             xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/04/secext"
             Id="myToken"
             ValueType="wsse:X509v3"
             EncodingType="wsse:Base64Binary">
             MIIEZzCCA9CgAwIBAgIQEmtJZc0...
          </wsse:BinarySecurityToken>

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

```
</S:Envelope>

```

3.3 Identifying and Referencing Certificates

An attached X.509 certificate is referenced by means of the wsse:SecurityTokenReference element. The wsu:Id attribute of the wsse:SecurityTokenReference element has the value of the wsu:Id attribute specified in the wsse:BinarySecurityToken.

```
Example TBS
```

3.4 Authentication

When an X.509 certificate is used to specify a signature key, the signature algorithm MUST be a digital signature algorithm.

The value of the signature key is the value of the public key specified in the certificate.

3.5 Encryption

When an X.509 certificate is used to specify an encryption key, the encryption algorithm MUST be a public key encryption algorithm.

The value of the encryption key is the value of the public key specified in the certificate.

3.6 Error Codes

When using X509 Certificates, it is RECOMMENDED to use the error codes defined in the WS-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.

3.7 Threat Model and Countermeasures

The use of X509 certificates with WS-Security introduces no new threats beyond those identified for WS-Security with other types of security tokens.

Message alteration and eavesdropping can be addressed by using the integrity and confidentiality mechanisms described in WS-Security. Replay attacks can be addressed by using message timestamps and caching, as well as other application-specific tracking mechanisms. For X.509 certificates 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.

4 Acknowledgements

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

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.

5 References

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

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

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

[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.

[WS-Security] TBS – point to the OASIS draft

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

[XML Signature] W3C Recommendation, "XML Signature Syntax and Processing," 12 February 2002.

[X509] S. Santesson, et al,"Internet X.509 Public Key Infrastructure Qualified Certificates Profile," http://www.itu.int/rec/recommendation.asp?type=items&lang=e&parent=T-REC-X.509-200003-I

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

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.