Web Services Security
XCBF Token Profile

Working Draft 1.0, Monday, 25 November 2002

Document identifier:

{draft}-{*WS-Security*}-{*XCBF Binding*}-{*1.0*} (Word) (PDF)

Location:

http://www.oasis-open.org/committees/wss

Editors:

Phillip H. Griffin, Griffin Consulting <phil.griffin@asn-1.com>
Monica J. Martin, Drake Certivo <mmartin@certivo.net>

Contributors:

TEXT TO BE REVISED TO INCLUDE ADDITIONAL CONTRIBUTORS AS NECESSARY

Phillip H. Griffin, Griffin Consulting
Monica J. Martin, Drake Certivo

Abstract:

This document describes how to use XML Common Biometric Format (XCBF) with the Web Services Security (WSS) specification. Biometric technology can be used for identification and authentication. Biometrics are the measurable physical characteristics or personal behavioral traits that can be used to recognize the identity of an individual, or to verify a claimed identity.

XCBF defines a common XML markup representation of the patron formats specified in NIST Common Biometric Exchange File Format [11]. These XML values are based on the ASN.1 schema and cryptographic message types defined in the X9.84 Biometrics Information Management and Security standard [9]. These values may contain X.509 certificates [4] and other digitally signed or encrypted information. XBCF values may be represented as XML markup or in a compact binary format.

Status:

This is a working draft submitted for consideration by the OASIS Web Services Security (WSS) technical committee. Please send comments to the editors.

If you are on the wss@lists.oasis-open.org list for committee members, send comments there. If you are not on that list, subscribe to the wss-comment@lists.oasis-open.org list and send comments there. To subscribe, send an email message to wss-comment-request@lists.oasis-open.org with the word "subscribe" as the body of the message.

For patent disclosure information that may be essential to the implementation of this specification, and any offers of licensing terms, refer to the Intellectual Property Rights

section of the OASIS Security Services Technical Committee (SSTC) web page at http://www.oasis-open.org/who/intellectualproperty.shtml.

Table of Contents

1 Introduction

This document describes the use of XML Common Biometric Format (XCBF) [1] cryptographic messages within the WS-Security specification. XCBF messages are validated against an ASN.1 schema [5]. This schema definition language is used to define X.509 certificates and CRLs, and the cryptographic messages used to secure electronic mail in RFC3369 [15] and X9.96 XML Cryptographic Message Syntax [10]. In an instance of communication, XCBF messages may be represented in a compact binary format or as well-formed XML markup.

A common XCBF security token is defined to convey and manage biometric information used for authentication and identification. Each binary representation of an XCBF message has an XML markup representation. Both representations share the same schema. This characteristic allows XML markup to be used in resource rich environments, but transferred or stored in a compressed binary format in resource poor environments, e.g. smart cards, wireless and remote devices, and high volume transaction systems.

XCBF messages may include digitally signed or encrypted information. The binary format used to represent XCBF messages relies on the canonical Distinguished Encoding Rules (DER) [6] used to encode X.509 certificates. The XML markup format used in this Standard is the canonical variant of the XML Encoding Rules (XER) [7].

Section 1 is non-normative.

2 Terminology

The key words *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 [12].

Namespace URIs (of the general form "some-URI") represent some application-dependent or context-dependent URI as defined in RFC2396 [13].

This specification design is intended to work with any version the general SOAP [3] message structure and processing model, though the SOAP 1.2 namespace URI is used in examples.

Commonly used security terms are defined in the Internet Security Glossary [14].

The namespaces used in this document are shown in the following table.

Prefix	Namespace
S	http://www.w3.org/2001/12/soap-envelope
wsse	http://schemas.xmlsoap.org/ws/2002/xx/secext

Note that the namespaces for XML Digital Signature and XML Encryption are not used. Instead the cryptographic processing used in XCBF security tokens are founded on simple cryptographic techniques commonly used for the protection of binary data. The same techniques are applied to both XML markup and binary token content. These techniques are based on standards that define their message schemas using ASN.1, such as the RSA Security PKCS #7 Cryptographic Message Syntax Standard (CMS) [17] and the IETF SMIME standard used for secure electronic mail, RFC 3369.

3 Acronyms and Abbreviations

Term	Definition
ASN.1	Abstract Syntax Notation One
CBEFF	Common Biometric Exchange File Format
CMS	Cryptographic Message Syntax
CRL	Certificate Revocation List
DER	Distinguished Encoding Rules
PKCS	Public Key Cryptography System
SOAP	Simple Object access Protocol
URI	Uniform Resource Identifier
XCBF	XML Common Biometric Format
XCMS	XML Cryptographic Message Syntax
XER	XML Encoding Rules
XML	Extensible Markup Language

4 Usage

A value of **<BiometricSyntaxSets>** is a series of **<BiometricSyntax>** values, each containing a collection of biometric information defined in one of four possible formats. These four choice alternatives have the following meanings:

<biometricObjects>	unprotected biometric values
<integrityObjects>	digitally signed biometric values
<privacyObjects>	encrypted biometric values
<privacyAndIntegrityObjects>	digitally signed and encrypted biometric values

All of the message objects in XCBF are values of **<BiometricSyntaxSets>**. XCBF messages may contain any combination of signed, encrypted or unprotected sets of biometric information.

4.1 Processing Model

The processing model for WS-Security with XCBF objects is no different from that of other token formats described in WS-Security. XCBF objects can be represented for transfer in two formats, a compact binary encoding and XML 1.0 markup. These two formats represent the same abstract values and both rely on the ASN.1 schema defined in XCBF and X9.84.

When these objects are represented in binary, they rely on the same ASN.1 schema definition language and Distinguished Encoding Rules used by X.509 certificates. When represented as XML markup, they are formatted using the XML Encoding Rules and do not use any attributes or namespace information.

Like X.509 certificates, XCBF biometric objects may contain digitally signed information. Some XCBF objects may contain digitally signed X.509 certificates and CRLs. XCBF objects may contain encrypted or signed and encrypted information. The biometric, signature and encryption processing of XCBF objects is not a direct part of the WS-Security processing model.

4.2 Attaching Security Tokens

XCBF message values must be specified using a **<wsse:XCBFSecurityToken>**. Token attributes are used to indicate characteristics of the token content to the processing WS-Security application.

The following value spaces are defined for `@ValueType`:

QName	Description
wsse:XCBFv1	XCBF v1 security token

The attributes are:

Attribute	Value	Description
Id	Any application specified string	Application defined
ValueType	XCBFv1	This token contains an XCBF version one value of type BiometricSyntaxSets
EncodingType	XER DER	XML Encoding Rules value Distinguished Encoding Rules value

Examples are provided in upcoming sections.

4.2.1 XML XCBF Security Token - BiometricObjects

The following example illustrates a SOAP message with an XCBF security token encoded using the XML Encoding Rules (XER). The token content is a simple, unprotected biometric object.

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

      <wsse:XCBFSecurityToken

         xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/04/secext"
         Id="XCBF-biometric-object"
         ValueType="wsse:XCBFv1"
         EncodingType="wsee:XER">

         <BiometricSyntaxSets>
            <BiometricSyntax>
               <biometricObjects>
                  <BiometricObject>
                     <biometricHeader>
                        <version> 0 </version>
                        <recordType> <id> 4 </id> </recordType>
                        <dataType> <processed/> </dataType>
                        <purpose> <audit/> </purpose>
                        <quality> -1 </quality>
                        <validityPeriod>
                           <notBefore> 1980.10.4 </notBefore>
                           <notAfter>2003.10.3.23.59.59</notAfter>
                        </validityPeriod>
                        <format>
                           <formatOwner>
                              <oid> 2.23.42.9.10.4.2 </oid>
                           </formatOwner>
                        </format>
                     </biometricHeader>
                     <biometricData>
                        0A0B0C0D0E0F1A1B1C1D1E1F2A2B2C2D2E2F
                     </biometricData>
                  </BiometricObject>
               </biometricObjects>
            </BiometricSyntax>
         </BiometricSyntaxSets>

      </wsse:XCBFSecurityToken>

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

In this example the XCBFSecurityToken contains a **<BiometricSyntaxSets>** value which contains a single biometric object. The biometric object is neither signed nor encrypted, and the **<biometricHeader>** information appears in the clear. The **<biometricData>** is an opaque string of hexadecimal characters and may be cryptographically enhanced according to the

security requirements of a biometric service provider or XCBF application. Such requirements are outside the scope of WS-Security.

4.2.2 Binary XCBF Security Token - BiometricSyntaxSets

The following example illustrates a SOAP message with an XCBF security token encoded using the DER Encoding Rules (DER), then Base64 armored [16].

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

      <wsse:XCBFSecurityToken
         xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/04/secext"
         Id="biometric-objects"
         ValueType="wsse:XCBFv1"
         EncodingType="wsee:DER">

            MIIEZzMJMzCCA9CzPHGzAwIBA ...

      </wsse:XCBFSecurityToken>

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

In this example the XCBFSecurityToken contains a **<BiometricSyntaxSets>** value which contains one or more biometric objects. The biometric objects may be signed nor encrypted, and the binary token content has been obscured by Base64 armoring.

4.2.3 XML XCBF Security Token - EncryptedData

The following example illustrates a SOAP message with an XCBF security token encoded using the XML Encoding Rules (XER). This message contains an XCBF privacy object.

The **<namedKey>** choice alternative of the privacy block is used. This choice alternative pairs a cryptographic key identifier **<keyName>** with an XML markup representation of a value of CMS **<EncryptedData>**.

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

      <wsse:XCBFSecurityToken
         xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/04/secext"
         Id="biometric-privacy-objects"
         ValueType="wsse:XCBFv1"
         EncodingType="wsee:XER">
         <BiometricSyntaxSets>
            <BiometricSyntax>
```

```
               <privacyObjects>
                  <privacyBlock>
                     <namedKey>
                        <keyName>6AE173BF5A973D1E</keyName>
                        <encryptedData>
                           <version>84</version>
                           <encryptedContentInfo>
                              <contentType>
                                 1.2.840.113549.1.7.6

                              <contentEncryptionAlgorithm>
                                 <algorithm>
                                    1.2.840.113549.3.7
                                 </algorithm>
                                 <parameters>
                                    <IV>7EA13D6E143CB5C9</IV>
                                 </parameters>
                              </contentEncryptionAlgorithm>
                              <encryptedContent>
                                 C99FA8CEA043B88D7A4981C32836A0D0444
                                 F24112F04B24710498D82996183196809FA
                                 BC659700F9ACE6CEA6B06033282486BB1E9
                                       ...
                                 B511FCF485E06F85A58B310746507330CF3
                                 5EED489BFDD89F7020BD59C8AD15D403DE2
                                 571EBF80C780448F5B71144FFEBE4B5726B
                              </encryptedContent>
                           </encryptedContentInfo>
                        </encryptedData>
                     </namedKey>
                  </privacyBlock>
               </privacyObjects>
            </BiometricSyntax>
         </BiometricSyntaxSets>

      </wsse:XCBFSecurityToken>

    </wsse:Security>
  </S:Header>

  <S:Body>
     ...
  </S:Body>
```

In this example the XCBFSecurityToken contains a **<BiometricSyntaxSets>** value which contains encrypted biometric information. None of the optional **<biometricHeader>** information appears in the clear. The **<encryptedData>** is an opaque string of hexadecimal characters that result from the encryption of a series of one or more biometric objects using the shared secret key identified by the **<keyName>** element.

The cryptographic processing requirements are defined in the XCBF standard. This processing of encrypted XML markup is identical to that used when a **<BiometricSyntaxSets>** value is encoded in binary. The same cryptographic processing requirements used in XCBF are used in other security standards, including X9.73 Cryptographic Message Syntax [8], X9.84, X9.96 XCMS, and RFC 3369. The details of this cryptographic processing are outside the scope of WS-Security.

4.3 Error Codes

Implementations may use custom error codes defined in private namespaces if needed. But it is recommended that they use the error handling codes defined in the WS-Security specification for signature, decryption, encoding and token header errors. When using custom error codes, implementations should be careful not to introduce security vulnerabilities that may assist an attacker in the error codes returned.

At this time, the error codes defined in WS-Security core largely support XCBF. However, they do not appear to support hash, MAC or HMAC. Therefore, XCBF recommends the error codes be generalized to support specified hash, MAC and HMAC (for example with more general references to “cryptographic algorithm”). In lieu of that change, XCBF recommends definition of a XCBF namespace for any specific error codes such as:

xbcf:UnsupportedAlgorithm - An unsupported cryptographic algorithm was used.

4.4 Threat Model

The use of XCBF messages in an XCBF security token introduces no new threats beyond those already identified for other types of WS-Security tokens. Message alteration and eavesdropping are addressed directly in the XCBF message that forms the token content by using the integrity and privacy mechanisms described in XCBF. Replay attacks can be addressed by using message timestamps and caching, as well as other application-specific tracking mechanisms. For XCBF messages ownership is verified by use of keys and man-in-the-middle attacks are generally mitigated.

It is strongly recommended that XCBF token content be protected by use of one of the integrity object choice alternatives defined in XCBF. While it is possible that transport-level security could be used to protect the overall message and the XCBF security token, great care must be taken to protect biometric information. It is strongly recommended that XCBF token content be protected by use of one of the privacy object choice alternatives defined in XCBF.

5 References

5.1 Normative

[1] XCBF 2002 (draft) XML Common Biometric Format, Organization for the Advancement of Structured Information Standards (OASIS), http://www.oasis-open.org/.

[2] W3C Extensible Markup Language (XML) 1.0 (Second Edition), W3C Recommendation, Copyright © [6 October 2000] World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/2000/REC-xml-20001006/.

[3] W3C SOAP 1.1:2000, Simple Object Access Protocol (Note), W3C Recommendation, Copyright © 2000 World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University, http://www.w3.org/TR/SOAP/.

[4] ISO/IEC 9594-8: Information technology (2000) | ITU-T Recommendation X.509 (2001), Open Systems Interconnection -- The Directory: Authentication framework.

[5] ISO/IEC 8824 [Part 1-4]:2001 | ITU-T Recommendation X.680-Series (2002), Information Technology - Abstract Syntax Notation One (ASN.1), http://www.itu.int/ITU-T/studygroups/com17/languages/.

[6] ISO/IEC 8825-1:2001 | ITU-T Recommendation X.690 (2002), Information Technology - ASN.1 Encoding Rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER), http://www.itu.int/ITU-T/studygroups/com17/languages/.

[7] ISO/IEC 8825-4:2001 | X.693 ITU-T Recommendation X.693 (2002) |, Information Technology - ASN.1 Encoding Rules: XML Encoding Rules (XER). http://www.itu.int/ITU-T/studygroups/com17/languages/.

[8] ANS X9.73:2002 Cryptographic Message Syntax (CMS) For The Financial Services Industry**.**

[9] ANS X9.84:2002 Biometrics Information Management and Security For The Financial Services Industry**.**

[10] ANS X9.96:2002 (draft) XML Cryptographic Message Syntax (XCMS).

[11] CBEFF Common Biometric Exchange File Format, NISTIR-6529, January 3, 2001.

[12] S. Bradner, Key words for use in RFCs to Indicate Requirement Levels, http://www.ietf.org/rfc/rfc2119.txt, IETF RFC 2119, March 1997.

[13] T. Berners-Lee, Uniform Resource Identifiers (URI): General Syntax, http://www.ietf.org/rfc/rfc2396.txt, IETF RFC 2396, August 1998.

[14] R. Shirley, Internet Security Glossary, http://www.ietf.org/rfc/rfc2828.txt, IETF RFC 2828, May 2000.

[15] R. Housley, Cryptographic Message Syntax (CMS), http://www.ietf.org/rfc/rfc3369.txt, IETF RFC 3369, August 2002.

[16] N. Freed and N. Borenstein, Multipurpose Internet Mail Extensions (MIME) Part 1: Format of Internet Message Bodies, http://www.ietf.org/rfc/rfc2045.txt, IETF RFC 2045, November 1996.

[17] RSA Security PKCS #7 - Cryptographic Message Syntax Standard, http://www.rsasecurity.com/rsalabs/pkcs/pkcs-7/index.html, Public-Key Cryptography Sstandards, November 1, 1993.

374

Appendix A. Acknowledgments

The following individuals were members of the committee during the development of this specification:

- TBD

Appendix B. Revision History

Rev	Date	By Whom	What
Wd-0.9	2002-11-16	Monica Martin	Initial version
Wd-1.0	2002-11-25	Phil Griffin	Updated; added references, text, examples; spell check, links, other.

Appendix C. 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.