



# 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](mailto:phil.griffin@asn-1.com)>  
Monica J. Martin, Drake Certivo <[mmartin@certivo.net](mailto: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. XCBF 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](mailto: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](mailto: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](mailto: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

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

40

## 40 Table of Contents

41	1	Introduction .....	4
42	2	Terminology .....	4
43	3	Acronyms and Abbreviations .....	5
44	4	Usage.....	5
45	4.1	Processing Model.....	6
46	4.2	Attaching Security Tokens .....	6
47	4.2.1	XML XCBF Security Token - BiometricObjects .....	7
48	4.2.2	Binary XCBF Security Token - BiometricSyntaxSets .....	8
49	4.2.3	XML XCBF Security Token - EncryptedData.....	8
50	4.3	Error Codes .....	10
51	4.4	Threat Model .....	10
52	5	References.....	10
53	5.1	Normative .....	10
54		Appendix A. Acknowledgments .....	13
55		Appendix B. Revision History .....	14
56		Appendix C. Notices .....	15
57			
58			

---

## 58 1 Introduction

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

65

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

72

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

77

78 Section 1 is non-normative.

---

## 79 2 Terminology

80 The key words *must*, *must not*, *required*, *shall*, *shall not*, *should*, *should not*, *recommended*, *may*,  
81 and *optional* in this document are to be interpreted as described in RFC2119 [12].

82

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

85

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

88

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

90

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

92

Prefix	Namespace
S	<a href="http://www.w3.org/2001/12/soap-envelope">http://www.w3.org/2001/12/soap-envelope</a>
wsse	<a href="http://schemas.xmlsoap.org/ws/2002/xx/secext">http://schemas.xmlsoap.org/ws/2002/xx/secext</a>

93

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

---

## 101 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

---

## 102 4 Usage

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

106

107 <code>&lt;biometricObjects&gt;</code>	unprotected biometric values
108 <code>&lt;integrityObjects&gt;</code>	digitally signed biometric values
109 <code>&lt;privacyObjects&gt;</code>	encrypted biometric values
110 <code>&lt;privacyAndIntegrityObjects&gt;</code>	digitally signed and encrypted biometric values

111

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

## 114 4.1 Processing Model

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

119

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

124

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

## 129 4.2 Attaching Security Tokens

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

133

134 The following value spaces are defined for @ValueType:

QName	Description
wsse:XCBFv1	XCBF v1 security token

135

136 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

137

138 Examples are provided in upcoming sections.

## 139 4.2.1 XML XCBF Security Token - BiometricObjects

140 The following example illustrates a SOAP message with an XCBF security token encoded using  
141 the XML Encoding Rules (XER). The token content is a simple, unprotected biometric object.  
142

```
143 <S:Envelope xmlns:S="...">
144   <S:Header>
145     <wsse:Security xmlns:wsse="...">
146       <wsse:XCBFSecurityToken
147         xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/04/secext"
148         Id="XCBF-biometric-object"
149         ValueType="wsse:XCBFv1"
150         EncodingType="wsse:XER">
151         <BiometricSyntaxSets>
152           <BiometricSyntax>
153             <biometricObjects>
154               <BiometricObject>
155                 <biometricHeader>
156                   <version> 0 </version>
157                   <recordType> <id> 4 </id> </recordType>
158                   <dataType> <processed/> </dataType>
159                   <purpose> <audit/> </purpose>
160                   <quality> -1 </quality>
161                   <validityPeriod>
162                     <notBefore> 1980.10.4 </notBefore>
163                     <notAfter>2003.10.3.23.59.59</notAfter>
164                   </validityPeriod>
165                   <format>
166                     <formatOwner>
167                       <oid> 2.23.42.9.10.4.2 </oid>
168                     </formatOwner>
169                   </format>
170                 </biometricHeader>
171                 <biometricData>
172                   0A0B0C0D0E0F1A1B1C1D1E1F2A2B2C2D2E2F
173                 </biometricData>
174               </BiometricObject>
175             </biometricObjects>
176           </BiometricSyntax>
177         </BiometricSyntaxSets>
178       </wsse:XCBFSecurityToken>
179     </wsse:Security>
180   </S:Header>
181   <S:Body>
182     ...
183   </S:Body>
```

189  
190 In this example the XCBFSecurityToken contains a **<BiometricSyntaxSets>** value which  
191 contains a single biometric object. The biometric object is neither signed nor encrypted, and the  
192 **<biometricHeader>** information appears in the clear. The **<biometricData>** is an opaque  
193 string of hexadecimal characters and may be cryptographically enhanced according to the

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

## 196 4.2.2 Binary XCBF Security Token - BiometricSyntaxSets

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

199

```
200 <S:Envelope xmlns:S="...">
201   <S:Header>
202     <wsse:Security xmlns:wsse="...">
203
204       <wsse:XCBFSecurityToken
205         xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/04/secext"
206         Id="biometric-objects"
207         ValueType="wsse:XCBFv1"
208         EncodingType="wsse:DER">
209
210           MIIIEZzMJMzCCA9CzPHGzAwIBA ...
211
212       </wsse:XCBFSecurityToken>
213
214     </wsse:Security>
215   </S:Header>
216   <S:Body>
217     ...
218   </S:Body>
```

219

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

## 223 4.2.3 XML XCBF Security Token - EncryptedData

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

226

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

230

```
231 <S:Envelope xmlns:S="...">
232   <S:Header>
233     <wsse:Security xmlns:wsse="...">
234
235       <wsse:XCBFSecurityToken
236         xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/04/secext"
237         Id="biometric-privacy-objects"
238         ValueType="wsse:XCBFv1"
239         EncodingType="wsse:XER">
240         <BiometricSyntaxSets>
241           <BiometricSyntax>
```



242  
243  
244  
245  
246  
247  
248  
249  
250  
251  
252  
253  
254  
255  
256  
257  
258  
259  
260  
261  
262  
263  
264  
265  
266  
267  
268  
269  
270  
271  
272  
273  
274  
275  
276  
277  
278  
279  
280  
281  
282  
283  
284

```
<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>
</BiometricSyntaxSets>
</BiometricSyntaxSets>

</wsse:XCBFSecurityToken>

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

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

285

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

291

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

## 298 4.3 Error Codes

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

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

309       xbcf:UnsupportedAlgorithm - An unsupported cryptographic algorithm was used.

## 310 4.4 Threat Model

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

318

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

---

## 324 5 References

### 325 5.1 Normative

- 326 [1] XCBF 2002 (draft) XML Common Biometric Format, Organization for the  
327 Advancement of Structured Information Standards (OASIS),  
328 <http://www.oasis-open.org/>.
- 329 [2] W3C Extensible Markup Language (XML) 1.0 (Second Edition), W3C  
330 Recommendation, Copyright © [6 October 2000] World Wide Web  
331 Consortium, (Massachusetts Institute of Technology, Institut National de  
332 Recherche en Informatique et en Automatique, Keio University),  
333 <http://www.w3.org/TR/2000/REC-xml-20001006/>.
- 334 [3] W3C SOAP 1.1:2000, Simple Object Access Protocol (Note), W3C  
335 Recommendation, Copyright © 2000 World Wide Web Consortium,  
336 (Massachusetts Institute of Technology, Institut National de Recherche  
337 en Informatique et en Automatique, Keio University,  
338 <http://www.w3.org/TR/SOAP/>.

339 [4] ISO/IEC 9594-8: Information technology (2000) | ITU-T Recommendation  
340 X.509 (2001), Open Systems Interconnection -- The Directory:  
341 Authentication framework.

342 [5] ISO/IEC 8824 [Part 1-4]:2001 | ITU-T Recommendation X.680-Series  
343 (2002), Information Technology - Abstract Syntax Notation One (ASN.1),  
344 <http://www.itu.int/ITU-T/studygroups/com17/languages/>.

345 [6] ISO/IEC 8825-1:2001 | ITU-T Recommendation X.690 (2002),  
346 Information Technology - ASN.1 Encoding Rules: Specification of Basic  
347 Encoding Rules (BER), Canonical Encoding Rules (CER) and  
348 Distinguished Encoding Rules (DER), <http://www.itu.int/ITU-T/studygroups/com17/languages/>.

350 [7] ISO/IEC 8825-4:2001 | X.693 ITU-T Recommendation X.693 (2002) |,  
351 Information Technology - ASN.1 Encoding Rules: XML Encoding Rules  
352 (XER). <http://www.itu.int/ITU-T/studygroups/com17/languages/>.

353 [8] ANS X9.73:2002 Cryptographic Message Syntax (CMS) For The  
354 Financial Services Industry.

355 [9] ANS X9.84:2002 Biometrics Information Management and Security For  
356 The Financial Services Industry.

357 [10] ANS X9.96:2002 (draft) XML Cryptographic Message Syntax (XCMS).

358 [11] CBEFF Common Biometric Exchange File Format, NISTIR-6529,  
359 January 3, 2001.

360 [12] S. Bradner, Key words for use in RFCs to Indicate Requirement Levels,  
361 <http://www.ietf.org/rfc/rfc2119.txt>, IETF RFC 2119, March 1997.

362 [13] T. Berners-Lee, Uniform Resource Identifiers (URI): General Syntax,  
363 <http://www.ietf.org/rfc/rfc2396.txt>, IETF RFC 2396, August 1998.

364 [14] R. Shirley, Internet Security Glossary, <http://www.ietf.org/rfc/rfc2828.txt>,  
365 IETF RFC 2828, May 2000.

366 [15] R. Housley, Cryptographic Message Syntax (CMS),  
367 <http://www.ietf.org/rfc/rfc3369.txt>, IETF RFC 3369, August 2002.

368 [16] N. Freed and N. Borenstein, Multipurpose Internet Mail Extensions  
369 (MIME) Part 1: Format of Internet Message Bodies,  
370 <http://www.ietf.org/rfc/rfc2045.txt>, IETF RFC 2045, November 1996.

371 [17] RSA Security PKCS #7 - Cryptographic Message Syntax Standard,  
372 <http://www.rsasecurity.com/rsalabs/pkcs/pkcs-7/index.html>, Public-Key  
373 Cryptography Standards, November 1, 1993.



---

374 **Appendix A. Acknowledgments**

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

377

- 378 • 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.

380

---

## Appendix C. Notices

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

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

393 Copyright © The Organization for the Advancement of Structured Information Standards [OASIS]  
394 2002. All Rights Reserved.

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

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

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