



# SAML V2.0 Attribute Sharing Profile for X.509 Authentication-Based Systems

## Committee Draft 04

28 August 2007

### Specification URIs:

#### This Version:

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-x509-authn-attrib-profile-cd-04.html>

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-x509-authn-attrib-profile-cd-04.odt>

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-x509-authn-attrib-profile-cd-04.pdf>

#### Previous Version:

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-x509-authn-attrib-profile-cd-03.html>

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-x509-authn-attrib-profile-cd-03.odt>

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-x509-authn-attrib-profile-cd-03.pdf>

#### Latest Version:

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-x509-authn-attrib-profile-cd.html>

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-x509-authn-attrib-profile-cd.odt>

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-x509-authn-attrib-profile-cd.pdf>

#### Latest Approved Version:

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-x509-authn-attrib-profile-cd-04.html>

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-x509-authn-attrib-profile-cd-04.odt>

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-x509-authn-attrib-profile-cd-04.pdf>

### Technical Committee:

OASIS Security Services TC

### Chair(s):

Hal Lockhart, BEA Systems, Inc.

Brian Campbell, Ping Identity Corporation

### Editor(s):

Eve Maler, Sun Microsystems

Rob Philpott, EMC

Tom Scavo, National Center for Supercomputing Applications (NCSA)

Ari Kermaier, Oracle

### Contributor(s):

Scott Cantor, Internet2

Paul Madsen, NTT Corporation

36 **Related Work:**  
37 This specification is an alternative to the *SAML V2.0 Deployment Profiles for X.509 Subjects*  
38 [SAMLX509].

39 **Declared XML Namespace(s):**  
40 N/A

41 **Abstract:**  
42 This deployment profile specifies the use of SAML V2.0 attribute queries and assertions to  
43 support distributed authorization in support of X.509-based authentication.

44 **Status:**  
45 This document was last revised or approved by the SSTC on the above date. The level of  
46 approval is also listed above. Check the current location noted above for possible later revisions  
47 of this document. This document is updated periodically on no particular schedule.  
48 TC members should send comments on this specification to the TC's email list. Others should  
49 send comments to the TC by using the "Send A Comment" button on the TC's web page at  
50 <http://www.oasis-open.org/committees/security>.  
51 For information on whether any patents have been disclosed that may be essential to  
52 implementing this specification, and any offers of patent licensing terms, please refer to the IPR  
53 section of the TC web page (<http://www.oasis-open.org/committees/security/ipr.php>).  
54 The non-normative errata page for this specification is located at [http://www.oasis-](http://www.oasis-open.org/committees/security)  
55 [open.org/committees/security](http://www.oasis-open.org/committees/security).

# Notices

56

57 Copyright © OASIS Open 2007. All Rights Reserved.

58 All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual  
59 Property Rights Policy (the "OASIS IPR Policy"). The full Policy may be found at the OASIS website.

60 This document and translations of it may be copied and furnished to others, and derivative works that  
61 comment on or otherwise explain it or assist in its implementation may be prepared, copied, published,  
62 and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice  
63 and this section are included on all such copies and derivative works. However, this document itself may  
64 not be modified in any way, including by removing the copyright notice or references to OASIS, except as  
65 needed for the purpose of developing any document or deliverable produced by an OASIS Technical  
66 Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be  
67 followed) or as required to translate it into languages other than English.

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

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

75 OASIS requests that any OASIS Party or any other party that believes it has patent claims that would  
76 necessarily be infringed by implementations of this OASIS Committee Specification or OASIS Standard, to  
77 notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such  
78 patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced  
79 this specification.

80 OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any  
81 patent claims that would necessarily be infringed by implementations of this specification by a patent  
82 holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR  
83 Mode of the OASIS Technical Committee that produced this specification. OASIS may include such  
84 claims on its website, but disclaims any obligation to do so.

85 OASIS takes no position regarding the validity or scope of any intellectual property or other rights that  
86 might be claimed to pertain to the implementation or use of the technology described in this document or  
87 the extent to which any license under such rights might or might not be available; neither does it represent  
88 that it has made any effort to identify any such rights. Information on OASIS' procedures with respect to  
89 rights in any document or deliverable produced by an OASIS Technical Committee can be found on the  
90 OASIS website. Copies of claims of rights made available for publication and any assurances of licenses  
91 to be made available, or the result of an attempt made to obtain a general license or permission for the  
92 use of such proprietary rights by implementers or users of this OASIS Committee Specification or OASIS  
93 Standard, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any  
94 information or list of intellectual property rights will at any time be complete, or that any claims in such list  
95 are, in fact, Essential Claims.

96 The name "OASIS" is a trademark of OASIS, the owner and developer of this specification, and should be  
97 used only to refer to the organization and its official outputs. OASIS welcomes reference to, and  
98 implementation and use of, specifications, while reserving the right to enforce its marks against  
99 misleading uses. Please see <http://www.oasis-open.org/who/trademark.php> for above guidance.

# 100 **Table of Contents**

101	1 Introduction.....	5
102	1.1 Notation.....	5
103	1.2 Terminology.....	5
104	1.3 Outline.....	6
105	1.4 Normative References.....	6
106	1.5 Non-Normative References.....	6
107	2 Use Cases.....	8
108	2.1.1 Overview.....	8
109	2.1.2 Sequence.....	8
110	3 Basic Mode.....	10
111	3.1 Required Information.....	10
112	3.2 <samlp:AttributeQuery> Issued by Service Provider.....	10
113	3.2.1 <samlp:AttributeQuery> Usage.....	10
114	3.3 <samlp:Response> Issued by Identity Provider.....	10
115	3.3.1 <samlp:Response> Usage.....	11
116	3.4 Use of Metadata.....	11
117	4 Encrypted Mode.....	12
118	4.1 Required Information.....	12
119	4.2 <samlp:AttributeQuery> Issued by Service Provider.....	12
120	4.2.1 <samlp:AttributeQuery> Usage.....	12
121	4.2.2 Use of Encryption.....	12
122	4.2.3 Use of Digital Signatures.....	13
123	4.3 <samlp:Response> Issued by Identity Provider.....	13
124	4.3.1 <samlp:Response> Usage.....	13
125	4.3.2 Use of Encryption.....	14
126	4.3.3 Use of Digital Signatures.....	14
127	4.4 Use of Metadata.....	14
128	5 Security and Privacy Considerations.....	15
129	5.1 Background.....	15
130	5.2 General Security Requirements.....	15
131	5.3 User Privacy.....	15
132	6 Implementation Conformance.....	16
133	7 Implementation Guidance (Informative).....	17
134	7.1 Identity Provider Policy .....	17
135	7.2 Caching of Attributes .....	17
136		

# 1 Introduction

137

138 The *SAML V2.0 Attribute Sharing Profile for X.509 Authentication-Based Systems* describes the use of the  
139 SAML V2.0 Assertion Query and Request Protocol [SAMLCore] in conjunction with the SAML V2.0 SOAP  
140 Binding [SAMLBind] to retrieve the attributes of a principal who has authenticated using an X.509  
141 certificate.

142 There are two modes of operation specified in this deployment profile: Basic Mode (section 3) and  
143 Encrypted Mode (section 4). The Basic Mode deployment profile extends the SAML V2.0 Assertion  
144 Query/Request Profile [SAMLProf]. The Encrypted Mode deployment profile specifies the use of  
145 encryption to protect the privacy of the principal.

## 1.1 Notation

146

147 This specification uses normative text to describe the use of SAML attribute queries and assertions.

148 The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD  
149 NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this specification are to be interpreted as  
150 described in [RFC 2119].

151 ...they MUST only be used where it is actually required for interoperation or to limit behavior  
152 which has potential for causing harm (e.g., limiting retransmissions)...

153 These keywords are thus capitalized when used to unambiguously specify requirements over protocol and  
154 application features and behavior that affect the interoperability and security of implementations. When  
155 these words are not capitalized, they are meant in their natural-language sense.

156 Listings of XML schemas appear like this.

157

158 Example code listings appear like this.

159 Conventional XML namespace prefixes are used throughout the listings in this specification to stand for  
160 their respective namespaces as follows, whether or not a namespace declaration is present in the  
161 example:

<i>Prefix</i>	<i>XML Namespace</i>	<i>Comments</i>
saml:	urn:oasis:names:tc:SAML:2.0:assertion	This is the SAML V2.0 assertion namespace [SAMLCore].
samlp:	urn:oasis:names:tc:SAML:2.0:protocol	This is the SAML V2.0 protocol namespace [SAMLCore].
md:	urn:oasis:names:tc:SAML:2.0:metadata	This is the SAML V2.0 metadata namespace [SAMLMeta].
query:	urn:oasis:names:tc:SAML:metadata:ext:query	This is the SAML metadata extension query requester namespace [SAMLMeta-Ext].
ds:	<a href="http://www.w3.org/2000/09/xmldsig#">http://www.w3.org/2000/09/xmldsig#</a>	This is the XML Signature namespace [XMLSig].
xenc:	<a href="http://www.w3.org/2001/04/xmlenc#">http://www.w3.org/2001/04/xmlenc#</a>	This is the XML Encryption namespace [XMLEnc].

162 This specification uses the following typographical conventions in text: <UnqualifiedElement>,  
163 <ns:QualifiedElement>, Attribute, **Datatype**, OtherKeyword.

## 1.2 Terminology

164

165 The term *identity provider* as used in this specification refers to an ordinary SAML attribute authority  
166 [SAMLGloss]. The term *service provider* refers to a SAML attribute requester. However, as used in this

167 specification, a service provider is not a typical SAML service provider since it performs X.509  
168 authentication in lieu of consuming a SAML authentication assertion.

169 The term *X.509 identity certificate* as used in this specification refers to an X.509 end entity certificate  
170 [RFC3280] or a certificate based on an X.509 end entity certificate (such as an X.509 proxy certificate  
171 [RFC3280]).

## 172 1.3 Outline

173 The next section describes a typical use case scenario that motivates the Basic Mode deployment profile.  
174 Then sections 3 and 4 specify Basic Mode and Encrypted Mode, respectively. Security and privacy issues  
175 are discussed in section 5, while section 6 specifies requirements that all conforming implementations  
176 must follow. Finally, in section 7, some guidance for implementers is given.

## 177 1.4 Normative References

- 178 **[FIPS 140-2]**            *Security Requirements for Cryptographic Modules*, May 2001. See  
179 <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>.
- 180 **[RFC 2119]**            S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. IETF  
181 RFC 2119, March 1997. See <http://www.ietf.org/rfc/rfc2119.txt>.
- 182 **[RFC2246]**            T. Dierks and C. Allen. *The TLS Protocol Version 1.0*. IETF RFC 2246, January  
183 1999. See <http://www.ietf.org/rfc/rfc2246.txt>
- 184 **[RFC3280]**            R. Housley et al. *Internet X.509 Public Key Infrastructure: Certificate and  
185 Certificate Revocation List (CRL) Profile*. IETF RFC 3280, April 2002. See  
186 <http://www.ietf.org/rfc/rfc3280.txt>
- 187 **[SAMLBind]**            S. Cantor et al. *Bindings for the OASIS Security Assertion Markup Language  
188 (SAML) V2.0*. OASIS Standard, March 2005. See [http://docs.oasis-  
189 open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf).
- 190 **[SAMLCore]**            S. Cantor et al. *Assertions and Protocols for the OASIS Security Assertion  
191 Markup Language (SAML) V2.0*. OASIS Standard, March 2005. See  
192 <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>.
- 193 **[SAMLProf]**            S. Cantor et al. *Profiles for the OASIS Security Assertion Markup Language  
194 (SAML) V2.0*. OASIS Standard, March 2005. See [http://docs.oasis-  
195 open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf).
- 196 **[SAMLMeta]**            S. Cantor et al. *Metadata for the OASIS Security Assertion Markup Language  
197 (SAML) V2.0*. OASIS Standard, March 2005. See [http://docs.oasis-  
198 open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf).
- 199 **[SAMLMeta-Ext]**        T. Scavo and S. Cantor. *Metadata Extension for SAML V2.0 and V1.x Query  
200 Requesters*. OASIS Draft, September 2006. See [http://docs.oasis-  
201 open.org/security/saml/SpecDrafts-Post2.0/ssstc-saml-metadata-ext-query-cd-  
202 02.pdf](http://docs.oasis-open.org/security/saml/SpecDrafts-Post2.0/ssstc-saml-metadata-ext-query-cd-02.pdf)
- 203 **[SSL3]**                A. Frier et al. *The SSL Protocol Version 3.0*, IETF Internet-Draft, November 1996.  
204 See <http://wp.netscape.com/eng/ssl3/draft302.txt>
- 205 **[XMLEnc]**            D. Eastlake et al. *XML Encryption Syntax and Processing*. World Wide Web  
206 Consortium. See <http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/>.
- 207 **[XMLSig]**            D. Eastlake et al. *XML-Signature Syntax and Processing*, World Wide Web  
208 Consortium, February 2002. <http://www.w3.org/TR/xmlsig-core/>.

## 209 1.5 Non-Normative References

- 210 **[RFC3820]**            S. Tuecke et al. *Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate  
211 Profile*. IETF RFC 3820, June 2004. See <http://www.ietf.org/rfc/rfc3820.txt>

212 **[SAMLGloss]** J. Hodges et al. *Glossary for the OASIS Security Assertion Markup Language*  
213 *(SAML) V2.0*. OASIS Standard, March 2005. See <http://docs.oasis->  
214 [open.org/security/saml/v2.0/saml-glossary-2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-glossary-2.0-os.pdf)

215 **[SAMLSecure]** F. Hirsch et al. *Security and Privacy Considerations for the OASIS Security*  
216 *Assertion Markup Language (SAML) V2.0*. OASIS Standard, March 2005. See  
217 <http://docs.oasis-open.org/security/saml/v2.0/saml-sec-consider-2.0-os.pdf>

218 **[SAMLX509]** T. Scavo. *SAML V2.0 Deployment Profiles for X.509 Subjects*. OASIS Committee  
219 Draft, August 2007. Document ID sstc-saml2-profiles-deploy-x509-cd-02.

## 220 2 Use Cases

221 The following non-normative material describes a typical use case that motivates the Basic Mode  
222 deployment profile described in section 3.

### 223 2.1.1 Overview

224 A principal attempts to access a secured resource maintained at a service provider. Principal  
225 authentication is accomplished by presenting a trusted X.509 identity certificate and by demonstrating  
226 proof of possession of the associated private key.

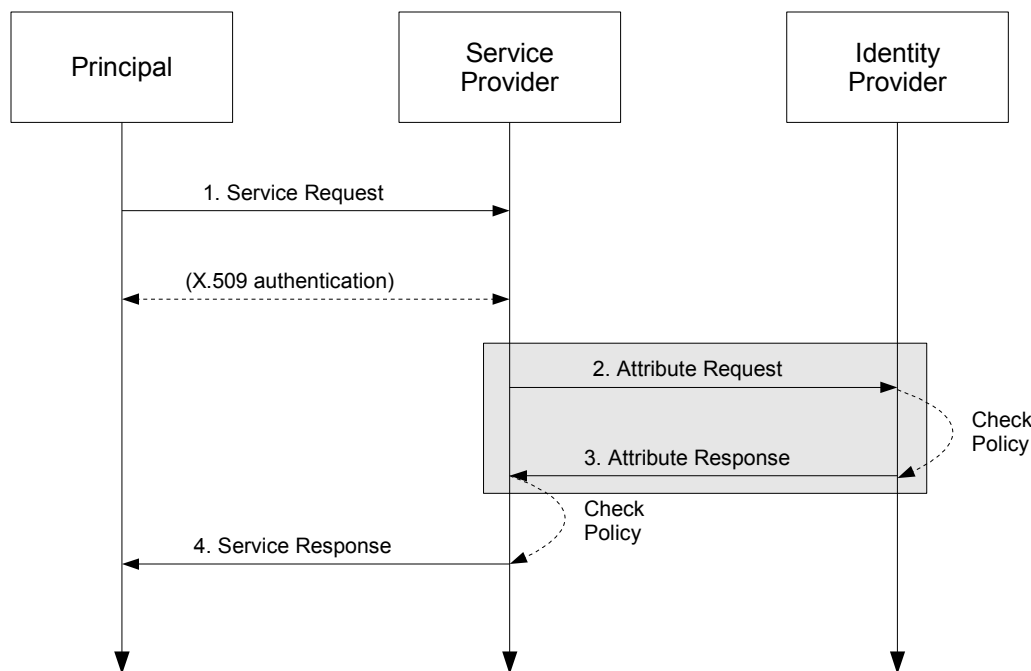
227 After the principal has been authenticated, the service provider requires additional information about the  
228 principal in order to determine whether to grant access to the resource. To obtain this information, the  
229 service provider uses the Subject Distinguished Name (Subject DN) field of the principal's X.509 identity  
230 certificate to query an identity provider for the required information about the principal. When the identity  
231 provider returns the relevant attributes, the service provider is able to make an informed authorization  
232 decision.

### 233 2.1.2 Sequence

234 The sequence of steps for the full use case is shown below.

235 **Note:** The steps constrained by this profile are highlighted with a gray box. The other  
236 steps are shown only for completeness; the profile does not constrain them.

237



238

#### 239 1. Service Request

240 In step 1, the principal requests a secured resource from a service provider who requires that the  
241 principal be authenticated. The principal authenticates to the service provider with an X.509 identity  
242 certificate. The details of this step are out of scope for this deployment profile.

#### 243 2. Attribute Request

244 In step 2, the service provider sends a SAML V2.0 `<samlp:AttributeQuery>` to the identity

245 provider using a SAML SOAP Binding. The Subject DN from the principal's X.509 identity certificate  
246 (presented in step 1 above) is used to construct the `<saml:Subject>` element. Thus, the  
247 `<saml:Subject>` element will contain a `<saml:NameID>` with the value of the Subject DN from the  
248 principal's X.509 identity certificate.

### 249 **3. Attribute Response**

250 In step 3, after verifying that the service provider is a valid requester, the identity provider issues a  
251 `<samlp:Response>` message containing appropriate attributes pertaining to the principal. The  
252 attributes returned to the service provider are subject to policy at the identity provider.

### 253 **4. Service Response**

254 In step 4, based on the attributes received from the identity provider in step 3, the service provider  
255 returns the requested resource or an error, subject to policy.

256 Of the sequence of steps described above, it is steps 2 and 3 that are profiled in sections 3 and 4 of this  
257 specification.

## 258 **3 Basic Mode**

259 In this mode, a service provider sends a SAML V2.0 `<samlp:AttributeQuery>` message directly to an  
260 identity provider. This message contains a name identifier assigned to a principal that authenticated to the  
261 service provider using an X.509 identity certificate.

262 If the identity provider receiving the request can:

- 263 • recognize the name identifier; and
- 264 • fulfill the request, subject to any applicable policies;

265 the identity provider responds with a successful `<samlp:Response>` containing the relevant attributes for  
266 the identified principal.

267 The `<samlp:AttributeQuery>`, `<samlp:Response>`, and `<saml:Assertion>` elements MAY be  
268 signed in this mode.

### 269 **3.1 Required Information**

270 **Identification:**

271 `urn:oasis:names:tc:SAML:2.0:profiles:query:attribute:X509-basic`

272 **Contact information:** [security-services-comment@lists.oasis-open.org](mailto:security-services-comment@lists.oasis-open.org)

273 **Description:** Given below.

274 **Updates:** N/A

275 **Extends:** Attribute Query/Request Profile (defined in [SAMLProf])

### 276 **3.2 `<samlp:AttributeQuery>` Issued by Service Provider**

277 To initiate the profile, the service provider uses the SAML SOAP Binding (see section 3.2 of [SAMLBind])  
278 to send a SAML V2.0 `<samlp:AttributeQuery>` message to an identity provider. The query MUST  
279 conform to the Assertion Query/Request Profile described in section 6 of [SAMLProf] except as specified  
280 below.

#### 281 **3.2.1 `<samlp:AttributeQuery>` Usage**

282 The `<samlp:AttributeQuery>` element MUST conform to the following rules:

- 283 • The `<saml:Subject>` element must contain a `<saml:NameID>` element whose value is the  
284 Subject DN from the principal's X.509 identity certificate.
- 285 • The `<saml:NameID>` element MUST have a `Format` attribute whose value is  
286 `urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName`, as defined in  
287 section 8.3.3 of [SAMLCore].

### 288 **3.3 `<samlp:Response>` Issued by Identity Provider**

289 The identity provider processes the `<samlp:AttributeQuery>` element and any enclosed  
290 `<saml:Attribute>` elements and returns a response to the service provider. The response MUST  
291 conform to the Assertion Query/Request Profile described in section 6 of [SAMLProf] except as specified  
292 below.

293 The service provider MUST process the `<samlp:Response>` message and any enclosed

294 <saml:Assertion> elements as described in section 6 of [SAMLProf].

### 295 **3.3.1 <samlp:Response> Usage**

296 If the request is successful, the <samlp:Response> element MUST conform to the following rules:

- 297     • Any <saml:Assertion> element(s) MUST satisfy the following conditions:
- 298         • The <saml:Assertion> element MUST contain at least one  
299             <saml:AttributeStatement> element that conveys the attributes of the principal to the  
300             service provider.
  - 301         • The <saml:Assertion> element MUST contain an <saml:AudienceRestriction>  
302             element that includes the service provider's unique identifier as an <saml:Audience>.
  - 303         • Other conditions (and other <saml:Audience> elements) MAY be included as requested by  
304             the service provider or at the discretion of the identity provider.

305 Otherwise, if the identity provider wishes to return an error, it MUST NOT include any assertions in the  
306 <samlp:Response> message.

### 307 **3.4 Use of Metadata**

308 The service provider and identity provider MAY use metadata in support of this deployment profile for  
309 locating endpoints, communicating key information, and so on. If SAML V2.0 metadata is used:

- 310     • The identity provider SHOULD use the <md:AttributeAuthorityDescriptor> element  
311         defined by the SAML metadata specification [SAMLMeta].
- 312     • The service provider SHOULD use the **query:AttributeQueryDescriptorType** complex type  
313         defined by the SAML metadata extension specification [SAMLMeta-Ext], or it MAY use the  
314         <md:SPSSODescriptor> element defined by the SAML metadata specification [SAMLMeta] if it  
315         also offers profile support consistent with that element.

316 Other role types defined in future specifications MAY be used in conjunction with this profile, subject to  
317 agreement by the parties.

## 318 4 Encrypted Mode

319 In this mode, as in Basic Mode, a service provider sends a SAML V2.0 `<samlp:AttributeQuery>`  
320 message directly to an identity provider. The Encrypted Mode request differs from that of Basic Mode in  
321 that the query message contains an encrypted name identifier assigned to a principal that authenticated to  
322 the service provider using an X.509 identity certificate.

323 If the identity provider receiving the request can:

- 324 • decrypt and recognize the name identifier; and
- 325 • fulfill the request subject to any applicable policies;

326 the identity provider responds with a successful `<samlp:Response>` containing the relevant attributes for  
327 the identified principal. The returned attributes MUST be encrypted as described below.

328 Each of the `<samlp:AttributeQuery>`, `<samlp:Response>`, and `<saml:Assertion>` elements  
329 MUST be signed in this mode.

### 330 4.1 Required Information

331 **Identification:**

332 `urn:oasis:names:tc:SAML:2.0:profiles:query:attribute:x509-encrypted`

333 **Contact information:** [security-services-comment@lists.oasis-open.org](mailto:security-services-comment@lists.oasis-open.org)

334 **Description:** Given below.

335 **Updates:** N/A

336 **Extends:** Basic Mode Attribute Sharing Profile (specified in section 3 of this document)

### 337 4.2 `<samlp:AttributeQuery>` Issued by Service Provider

338 In Encrypted Mode, the service provider sends a SAML V2.0 `<samlp:AttributeQuery>` message to  
339 an identity provider as described in section 3. In addition to the requirements of Basic Mode, this mode  
340 has the following requirements.

341 All requests MUST be made over either SSL 3.0 [SSL3] or TLS 1.0 [RFC2246] to maintain confidentiality  
342 and message integrity. In addition, the requester MAY use SSL/TLS client authentication.

#### 343 4.2.1 `<samlp:AttributeQuery>` Usage

344 In addition to the rules defined for Basic Mode in section 3.2.1, the `<samlp:AttributeQuery>` element  
345 MUST conform to the following rules:

- 346 • The `<saml:Subject>` element must contain an `<saml:EncryptedID>` element carrying the  
347 encrypted value of the `<saml:NameID>` element (using XML Encryption as specified in [XMLEnc]).  
348 See section 4.2.2 for details on the use of encryption.
- 349 • The `<samlp:AttributeQuery>` MUST contain a `<ds:Signature>` element carrying the  
350 signature of the service provider.

#### 351 4.2.2 Use of Encryption

352 The SAML V2.0 Assertions and Protocols specification [SAMLCore] defines the `<saml:EncryptedID>`  
353 element as a means of applying confidentiality to a name identifier.

354 In Encrypted Mode the service provider MUST use the `<saml:EncryptedID>` to carry the Subject DN of  
355 the principal in the `<samlp:AttributeQuery>`.

356 Exactly one of the following encryption procedures MUST be followed:

- 357 • The service provider generates a new symmetric key to encrypt the principal's name identifier  
358 containing the Subject DN. After performing the encryption, the service provider places the resulting  
359 ciphertext in the `<xenc:EncryptedData>` element. The symmetric key MUST be encrypted with  
360 the identity provider's public key and the resulting ciphertext placed in the `<xenc:EncryptedKey>`  
361 element.
- 362 • The service provider uses a previously established symmetric key to encrypt the principal's name  
363 identifier containing the Subject DN. After performing the encryption, the service provider places the  
364 resulting ciphertext in the `<xenc:EncryptedData>` element. In this case, the  
365 `<saml:EncryptedID>` element MUST NOT contain an `<xenc:EncryptedKey>` element.

366 A symmetric key transmitted in an `<xenc:EncryptedKey>` element MUST NOT be later reused by the  
367 service provider as a previously established symmetric key.

368 An encryption algorithm satisfying FIPS 140-2 Security Requirements [FIPS 140-2] SHALL be used for the  
369 encryption operation.

### 370 4.2.3 Use of Digital Signatures

371 The SAML V2.0 Assertions and Protocols specification [SAMLCore] describes how to use the  
372 `<ds:Signature>` element (defined in [XMLSig]) as a means of providing integrity and authenticity for a  
373 message.

374 In Encrypted Mode, a service provider MUST sign the `<samlp:AttributeQuery>` element containing  
375 the `<saml:EncryptedID>` element to allow the identity provider to authenticate the origin and verify the  
376 integrity of the request. A signing algorithm satisfying FIPS 140-2 Security Requirements [FIPS 140-2]  
377 SHALL be used for the digital signature operation.

## 378 4.3 `<samlp:Response>` Issued by Identity Provider

379 The identity provider processes the `<samlp:AttributeQuery>`, as defined in [SAMLCore] and  
380 section 6 of [SAMLProf], and returns a response to the service provider. In addition to the requirements of  
381 Basic Mode, this mode has the following requirements.

382 The responding identity provider MUST authenticate to the requester, both by signing the  
383 `<samlp:Response>` message and through TLS or SSL server authentication.

### 384 4.3.1 `<samlp:Response>` Usage

385 If the request is successful, the `<samlp:Response>` element MUST conform to the following rules:

- 386 • The `<samlp:Response>` element MUST contain a `<ds:Signature>` element carrying the  
387 signature of the identity provider.
- 388 • It MUST contain at least one `<saml:EncryptedAssertion>` element (but no  
389 `<saml:Assertion>` elements).
- 390 • The encrypted content of each `<saml:EncryptedAssertion>` element is a  
391 `<saml:Assertion>` element that MUST satisfy the following conditions, in addition to the rules of  
392 section 3.3.1:
  - 393 • The `<saml:Assertion>` element MUST contain a `<ds:Signature>` element carrying the  
394 signature of the identity provider.

395 Otherwise, if the identity provider wishes to return an error, it MUST NOT include any encrypted assertions

396 in the `<samlp:Response>` message.

### 397 **4.3.2 Use of Encryption**

398 The SAML V2.0 Assertions and Protocols specification [SAMLCore] defines the  
399 `<saml:EncryptedAssertion>` element as a mean of applying confidentiality to the contents of an  
400 assertion.

401 In Encrypted Mode the identity provider MUST use the `<saml:EncryptedAssertion>` element to  
402 carry the returned attribute values for the principal.

403 Exactly one of the following procedures MUST be followed:

- 404 • The identity provider generates a new symmetric key to encrypt the `<saml:Assertion>`. After  
405 performing the encryption, the identity provider places the resulting ciphertext in the  
406 `<xenc:EncryptedData>` element. The symmetric key MUST be encrypted with the service  
407 provider's public key and the resulting ciphertext placed in the `<xenc:EncryptedKey>` element.
- 408 • The identity provider uses the symmetric key used by the service provider to encrypt the name  
409 identifier. After encrypting the `<saml:Assertion>` using this key, the identity provider places the  
410 resulting ciphertext in the `<xenc:EncryptedData>` element. In this case, however, the  
411 `<saml:EncryptedAssertion>` element MUST NOT contain an `<xenc:EncryptedKey>`  
412 element.
- 413 • If the service provider did not include a symmetric key in the `<samlp:AttributeQuery>` for  
414 decryption of the `<saml:EncryptedID>`, the identity provider uses a previously established  
415 symmetric key to encrypt the `<saml:Assertion>`. If the identity provider reuses a key in this  
416 manner, the `<saml:EncryptedAssertion>` element MUST NOT contain an  
417 `<xenc:EncryptedKey>` element.

418 An encryption algorithm satisfying FIPS 140-2 Security Requirements [FIPS 140-2] SHALL be used for the  
419 encryption operation.

### 420 **4.3.3 Use of Digital Signatures**

421 The SAML V2.0 Assertions and Protocols specification [SAMLCore] defines how to use the  
422 `<ds:Signature>` element (defined in [XMLSig]) as a means of providing integrity and authenticity for a  
423 message.

424 In Encrypted Mode, the identity provider MUST sign both the `<samlp:Response>` element and the  
425 `<saml:Assertion>` element to ensure integrity. A signing algorithm satisfying the FIPS 140-2 Security  
426 Requirements [FIPS 140-2] SHALL be used for both digital signature operations.

### 427 **4.4 Use of Metadata**

428 As in Basic Mode, the service provider and identity provider MAY use metadata in support of this  
429 deployment profile. If SAML V2.0 metadata is used, in addition to the rules defined in section 3.4, there  
430 SHOULD be at least one `<md:KeyDescriptor>` element with attribute `use="encryption"` in both the  
431 service provider's and the identity provider's metadata.

## 432 **5 Security and Privacy Considerations**

433 The motivation for this deployment profile is to specify a secure means of obtaining SAML attributes in  
434 conjunction with X.509 authentication. As such, security considerations are highly important from the  
435 perspective of this deployment profile.

### 436 **5.1 Background**

437 The SAML Security and Privacy specification [SAMLSecure] provides general background material  
438 relevant to all SAML profiles. In addition, section 3.1.2 of the SAML Bindings specification [SAMLBind]  
439 provides general security guidelines regardless of binding. Sections 5 and 6 of the SAML Assertions and  
440 Protocols specification [SAMLCore] give general syntax and processing guidelines regarding XML  
441 Signature and XML Encryption, respectively. Finally, sections 6.3 and 6.4 of the SAML Profiles  
442 specification [SAMLProf] give specific security requirements governing queries.

### 443 **5.2 General Security Requirements**

444 SAML profiles often involve a system entity that relies on an earlier act of user authentication. For  
445 example, the SAML Web Browser SSO Profile [SAMLProf] relies on an authentication service that  
446 validates a credential (typically a username/password) for a user. The authentication service must be  
447 securely linked to an identity provider that issues SAML authentication assertions based on that user's act  
448 of authentication. Similarly, this deployment profile assumes that the system entity that performs the  
449 X.509 authentication is operating in a secure environment that includes the attribute requester.

450 In this deployment profile, an end user presents an X.509 certificate to authenticate at the service  
451 provider. The system entity that performs this authentication (i.e., validates the certificate and its trust  
452 chain) must be securely linked to the SAML attribute requester that subsequently initiates this deployment  
453 profile. The latter must have a secure means of obtaining the X.509 subject name from the user  
454 certificate and issuing a SAML V2.0 `<samlp:AttributeQuery>` for that subject to the appropriate  
455 asserting party. The mechanism by which these system entities are linked is out of scope for this  
456 deployment profile.

457 Local policy settings at the attribute authority will determine whether or not the asserting party is permitted  
458 to return attributes for the requested subject.

459 Since this deployment profile extends the SAML V2.0 Assertion Query/Request Profile (section 6 of  
460 [SAMLProf]), a Basic Mode requester SHOULD authenticate and ensure message integrity to the  
461 responder, and vice versa. In Encrypted Mode, a requester MUST authenticate and ensure message  
462 integrity to the responder, and vice versa.

463 Generally speaking, Basic Mode is applicable in point-to-point deployment scenarios where transport-level  
464 security suffices. Thus mutually authenticated SSL/TLS will be the norm. On the other hand, Encrypted  
465 Mode may apply in multi-hop scenarios that require end-to-end message-level security. In that case,  
466 SSL/TLS is not sufficient to guarantee authenticity and message integrity, and digital signatures are  
467 required. To ensure privacy, message-level encryption is also required.

### 468 **5.3 User Privacy**

469 The identity of the principal for which the assertion was issued SHOULD NOT be human readable (that is,  
470 stored in clear text) in log files, cache files or the cache repository (as applicable).

## 471 **6 Implementation Conformance**

472 An implementation of this specification shall be a conforming *Basic Mode X.509 Attribute*  
473 *Query/Requester* or a conforming *Encrypted Mode X.509 Attribute Query/Requester* (or both). An  
474 Encrypted Mode X.509 Attribute Query/Requester is a functional superset of a Basic Mode X.509 Attribute  
475 Query/Requester.

476 A Basic Mode X.509 Attribute Query/Requester MUST conform to the normative statements in section 3.  
477 An Encrypted Mode X.509 Attribute Query/Requester MUST conform to the normative statements in  
478 section 4, which includes references to normative portions of section 3.

## 479 **7 Implementation Guidance (Informative)**

480 The following non-normative guidance is provided for implementers.

### 481 **7.1 Identity Provider Policy**

482 Service providers may explicitly enumerate the required attributes in queries or may issue queries  
483 containing no `<saml:Attribute>` elements that essentially request all available attributes. Regardless  
484 of any attributes requested in the query (or in metadata, if used), it is the identity provider that determines  
485 the actual attributes to be returned to the service provider. Thus an identity provider should institute and  
486 enforce policy that strictly limits the attributes released to service providers.

### 487 **7.2 Caching of Attributes**

488 A capability to cache user attributes that are returned in assertions should be provided. Cache expiration  
489 settings should be configurable by administrators.

490 **A. Revision History**

491 TBA

<i>Document ID</i>	<i>Date</i>	<i>Committer</i>	<i>Comment</i>
Draft-01	22 Jun 2004		Initial draft
Draft-02	03 Feb 2005		
sstc-saml-x509-authn-based-attribute-protocol-profile-2.0-draft-03	25 Mar 2005	R. Randall	
sstc-saml-x509-authn-based-attribute-protocol-profile-2.0-draft-04	14 Apr 2005	R. Randall	
sstc-saml-x509-authn-based-attribute-protocol-profile-2.0-draft-05	02 May 2005	R. Randall	
sstc-saml-x509-authn-based-attribute-protocol-profile-2.0-draft-06	13 May 2005	R. Randall	
sstc-saml-x509-authn-based-attribute-protocol-profile-2.0-draft-07	23 May 2005	R. Randall	
sstc-saml-x509-authn-attrib-profile-cd-01	01 Jun 2005	E. Maler	Committee Draft
sstc-saml-x509-authn-attrib-profile-draft-08	14 Mar 2006	R. Philpott	
sstc-saml-x509-authn-attrib-profile-cd-02	28 Mar 2006	R. Philpott	Committee Draft
sstc-saml-x509-authn-attrib-profile-draft-09	26 Jun 2006	T. Scavo	
sstc-saml-x509-authn-attrib-profile-draft-10	05 Jul 2006	T. Scavo	
sstc-saml-x509-authn-attrib-profile-draft-11	13 Feb 2007	A. Kermaier	
sstc-saml-x509-authn-attrib-profile-draft-12	26 Mar 2007	T. Scavo	
sstc-saml-x509-authn-attrib-profile-draft-13	12 Apr 2007	A. Kermaier	
sstc-saml-x509-authn-attrib-profile-cd-03	07 Jun 2007	T. Scavo	Committee Draft
sstc-saml-x509-authn-attrib-profile-cd-04	28 Aug 2007	T. Scavo	Committee Draft

## 492 B. Acknowledgments

493 The editors would like to acknowledge the contributions of the OASIS Security Services Technical  
494 Committee, whose voting members at the time of publication were:

- 495 • George Fletcher, AOL
- 496 • Hal Lockhart, BEA Systems, Inc.
- 497 • Steve Anderson, BMC Software
- 498 • Jeff Bohren, BMC Software
- 499 • Carolina Canales-Valenzuela, Ericsson
- 500 • Greg Whitehead, Hewlett-Packard
- 501 • Eric Tiffany, IEEE Industry Standards and Technology Org (IEEE-ISTO)
- 502 • Conor Cahill, Intel Corporation
- 503 • Scott Cantor, Internet2
- 504 • Tom Scavo, National Center for Supercomputing Applications (NCSA)
- 505 • Peter Davis, Neustar, Inc.
- 506 • Jeff Hodges, Neustar, Inc.
- 507 • Frederick Hirsch, Nokia Corporation
- 508 • Abbie Barbir, Nortel Networks Limited
- 509 • Ari Kermaier, Oracle Corporation
- 510 • Eve Maler, Sun Microsystems
- 511 • Emily Xu, Sun Microsystems
- 512 • Sampo Kellomki, Symlabs, S.A.
- 513 • David Staggs, Veterans Health Administration

514 The editors would also like to acknowledge the contributions of the following individuals:

- 515 • Rick Randall, Booz Allen Hamilton
- 516 • Rebekah Metz, Booz Allen Hamilton
- 517 • Thomas Wisniewski, Entrust