



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

Committee Specification 01

27 March 2008

Specification URIs:

This Version:

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-x509-authn-attrib-profile-cs-01.html>

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-x509-authn-attrib-profile-cs-01.odt>

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-x509-authn-attrib-profile-cs-01.pdf>

Previous Version:

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-x509-authn-attrib-profile-cd-05.html>

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-x509-authn-attrib-profile-cd-05.odt>

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-x509-authn-attrib-profile-cd-05.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>

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

Related Work:

This specification is an alternative to the *SAML V2.0 Deployment Profiles for X.509 Subjects* [SAMLX509].

35 **Declared XML Namespace(s):**

36 N/A

37 **Abstract:**

38 This deployment profile specifies the use of SAML V2.0 attribute queries and assertions to
39 support distributed authorization in support of X.509-based authentication.

40 **Status:**

41 This document was last revised or approved by the SSTC on the above date. The level of
42 approval is also listed above. Check the current location noted above for possible later revisions
43 of this document. This document is updated periodically on no particular schedule.

44 TC members should send comments on this specification to the TC's email list. Others should
45 send comments to the TC by using the "Send A Comment" button on the TC's web page at [http://](http://www.oasis-open.org/committees/security)
46 www.oasis-open.org/committees/security.

47 For information on whether any patents have been disclosed that may be essential to
48 implementing this specification, and any offers of patent licensing terms, please refer to the IPR
49 section of the TC web page (<http://www.oasis-open.org/committees/security/ipr.php>).

50 The non-normative errata page for this specification is located at [http://www.oasis-](http://www.oasis-open.org/committees/security)
51 [open.org/committees/security](http://www.oasis-open.org/committees/security).

Notices

52

53 Copyright © OASIS Open 2007-2008. All Rights Reserved.

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

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

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

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

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

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

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

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

96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132

Table of Contents

- 1 Introduction.....5
- 1.1 Notation.....5
- 1.2 Terminology.....5
- 1.3 Outline.....6
- 1.4 Normative References.....6
- 1.5 Non-Normative References.....6
- 2 Use Cases.....8
 - 2.1.1 Overview.....8
 - 2.1.2 Sequence.....8
- 3 Basic Mode.....10
 - 3.1 Required Information.....10
 - 3.2 <samlp:AttributeQuery> Issued by Service Provider.....10
 - 3.2.1 <samlp:AttributeQuery> Usage.....10
 - 3.3 <samlp:Response> Issued by Identity Provider.....10
 - 3.3.1 <samlp:Response> Usage.....11
 - 3.4 Use of Metadata.....11
- 4 Encrypted Mode.....12
 - 4.1 Required Information.....12
 - 4.2 <samlp:AttributeQuery> Issued by Service Provider.....12
 - 4.2.1 <samlp:AttributeQuery> Usage.....12
 - 4.2.2 Use of Encryption.....12
 - 4.2.3 Use of Digital Signatures.....13
 - 4.3 <samlp:Response> Issued by Identity Provider.....13
 - 4.3.1 <samlp:Response> Usage.....13
 - 4.3.2 Use of Encryption.....14
 - 4.3.3 Use of Digital Signatures.....14
 - 4.4 Use of Metadata.....14
- 5 Security and Privacy Considerations.....15
 - 5.1 Background.....15
 - 5.2 General Security Requirements.....15
 - 5.3 User Privacy.....15
- 6 Implementation Conformance.....16
- 7 Implementation Guidance (Informative).....17
 - 7.1 Identity Provider Policy17
 - 7.2 Caching of Attributes17

1 Introduction

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

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

1.1 Notation

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

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

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

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

Listings of XML schemas appear like this.

Example code listings appear like this.

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

Prefix	XML Namespace	Comments
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:	http://www.w3.org/2000/09/xmldsig#	This is the XML Signature namespace [XMLSig].
xenc:	http://www.w3.org/2001/04/xmlenc#	This is the XML Encryption namespace [XMLEnc].

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

1.2 Terminology

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

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

165 The term *X.509 identity certificate* as used in this specification refers to an X.509 end entity certificate
166 [RFC3280] or a certificate based on an X.509 end entity certificate (such as an X.509 proxy certificate
167 [RFC3820]).

168 **1.3 Outline**

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

173 **1.4 Normative References**

- 174 **[FIPS 140-2]** *Security Requirements for Cryptographic Modules*, May 2001. See
175 <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>.
- 176 **[RFC 2119]** S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. IETF
177 RFC 2119, March 1997. See <http://www.ietf.org/rfc/rfc2119.txt>.
- 178 **[RFC2246]** T. Dierks and C. Allen. *The TLS Protocol Version 1.0*. IETF RFC 2246, January
179 1999. See <http://www.ietf.org/rfc/rfc2246.txt>
- 180 **[RFC3280]** R. Housley et al. *Internet X.509 Public Key Infrastructure: Certificate and
181 Certificate Revocation List (CRL) Profile*. IETF RFC 3280, April 2002. See [http://
182 www.ietf.org/rfc/rfc3280.txt](http://www.ietf.org/rfc/rfc3280.txt)
- 183 **[SAMLBind]** S. Cantor et al. *Bindings for the OASIS Security Assertion Markup Language
184 (SAML) V2.0*. OASIS Standard, March 2005. See [http://docs.oasis-
185 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).
- 186 **[SAMLCore]** S. Cantor et al. *Assertions and Protocols for the OASIS Security Assertion
187 Markup Language (SAML) V2.0*. OASIS Standard, March 2005. See <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>.
- 188
- 189 **[SAMLProf]** S. Cantor et al. *Profiles for the OASIS Security Assertion Markup Language
190 (SAML) V2.0*. OASIS Standard, March 2005. See [http://docs.oasis-
191 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).
- 192 **[SAMLMeta]** S. Cantor et al. *Metadata for the OASIS Security Assertion Markup Language
193 (SAML) V2.0*. OASIS Standard, March 2005. See [http://docs.oasis-
194 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).
- 195 **[SAMLMeta-Ext]** T. Scavo and S. Cantor. *Metadata Extension for SAML V2.0 and V1.x Query
196 Requesters*. OASIS Standard, November 2007. See [http://docs.oasis-
197 open.org/security/saml/Post2.0/sstc-saml-metadata-ext-query-os.pdf](http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-ext-query-os.pdf)
- 198 **[SSL3]** A. Frier et al. *The SSL Protocol Version 3.0*, IETF Internet-Draft, November 1996.
199 See <http://wp.netscape.com/eng/ssl3/draft302.txt>
- 200 **[XMLEnc]** D. Eastlake et al. *XML Encryption Syntax and Processing*. World Wide Web
201 Consortium. See <http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/>.
- 202 **[XMLSig]** D. Eastlake et al. *XML-Signature Syntax and Processing*, World Wide Web
203 Consortium, February 2002. <http://www.w3.org/TR/xmlsig-core/>.

204 **1.5 Non-Normative References**

- 205 **[RFC3820]** S. Tuecke et al. *Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate
206 Profile*. IETF RFC 3820, June 2004. See <http://www.ietf.org/rfc/rfc3820.txt>
- 207 **[SAMLGloss]** J. Hodges et al. *Glossary for the OASIS Security Assertion Markup Language*

208 (SAML) V2.0. OASIS Standard, March 2005. See [http://docs.oasis-](http://docs.oasis-open.org/security/saml/v2.0/saml-glossary-2.0-os.pdf)
209 [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)
210 **[SAMLSecure]** F. Hirsch et al. *Security and Privacy Considerations for the OASIS Security*
211 *Assertion Markup Language (SAML) V2.0*. OASIS Standard, March 2005. See
212 <http://docs.oasis-open.org/security/saml/v2.0/saml-sec-consider-2.0-os.pdf>
213 **[SAMLX509]** T. Scavo. *SAML V2.0 Deployment Profiles for X.509 Subjects*. OASIS Committee
214 Draft, August 2007. Document ID sstc-saml2-profiles-deploy-x509-cd-02.

2 Use Cases

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

2.1.1 Overview

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

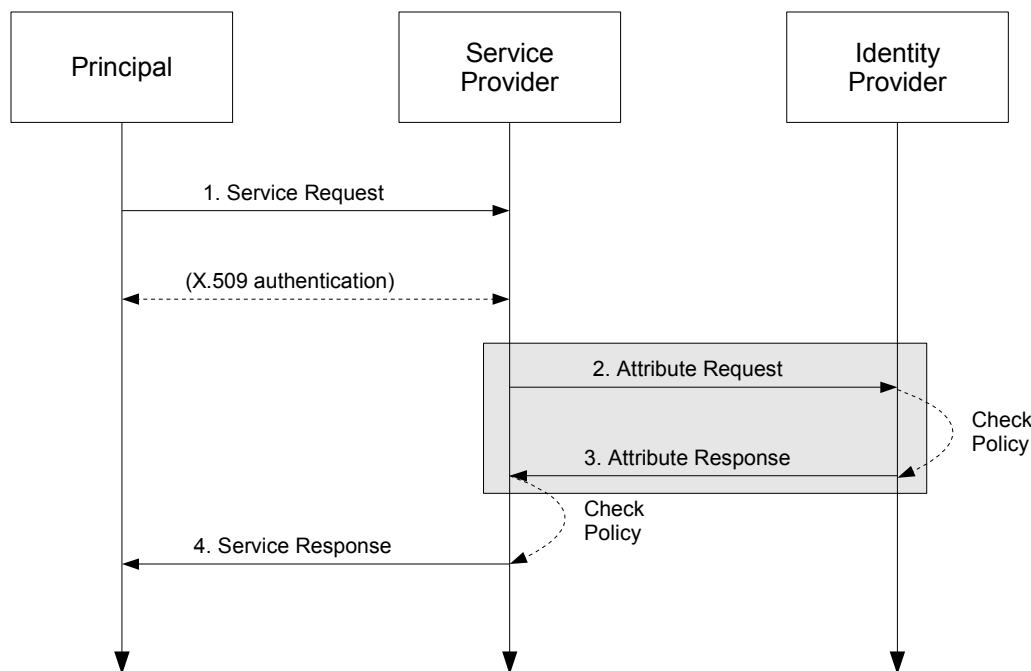
After the principal has been authenticated, the service provider requires additional information about the principal in order to determine whether to grant access to the resource. To obtain this information, the service provider uses the Subject Distinguished Name (Subject DN) field of the principal's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

2.1.2 Sequence

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

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

232



233

1. Service Request

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

2. Attribute Request

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

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

244 **3. Attribute Response**

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

248 **4. Service Response**

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

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

253 **3 Basic Mode**

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

257 If the identity provider receiving the request can:

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

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

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

264 **3.1 Required Information**

265 **Identification:**

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

267 **Contact information:** security-services-comment@lists.oasis-open.org

268 **Description:** Given below.

269 **Updates:** N/A

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

271 **3.2 `<samlp:AttributeQuery>` Issued by Service Provider**

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

276 **3.2.1 `<samlp:AttributeQuery>` Usage**

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

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

283 **3.3 `<samlp:Response>` Issued by Identity Provider**

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

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

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

290 **3.3.1 <samlp:Response> Usage**

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

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

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

302 **3.4 Use of Metadata**

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

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

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

313 4 Encrypted Mode

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

318 If the identity provider receiving the request can:

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

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

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

325 4.1 Required Information

326 **Identification:**

327 `urn:oasis:names:tc:SAML:2.0:profiles:query:attribute:X509-encrypted`

328 **Contact information:** security-services-comment@lists.oasis-open.org

329 **Description:** Given below.

330 **Updates:** N/A

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

332 4.2 `<samlp:AttributeQuery>` Issued by Service Provider

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

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

338 4.2.1 `<samlp:AttributeQuery>` Usage

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

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

346 4.2.2 Use of Encryption

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

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

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

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

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

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

365 4.2.3 Use of Digital Signatures

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

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

373 4.3 `<samlp:Response>` Issued by Identity Provider

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

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

379 4.3.1 `<samlp:Response>` Usage

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

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

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

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

392 **4.3.2 Use of Encryption**

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

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

398 Exactly one of the following procedures **MUST** be followed:

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

413 An encryption algorithm satisfying FIPS 140-2 Security Requirements [FIPS 140-2] **SHALL** be used for the
414 encryption operation.

415 **4.3.3 Use of Digital Signatures**

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

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

422 **4.4 Use of Metadata**

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

427 **5 Security and Privacy Considerations**

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

431 **5.1 Background**

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

438 **5.2 General Security Requirements**

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

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

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

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

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

463 **5.3 User Privacy**

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

466 **6 Implementation Conformance**

467 A client implementation of this specification shall be a conforming *Basic Mode X.509 Attribute Query*
468 *Requester* or a conforming *Encrypted Mode X.509 Attribute Query Requester* (or both). On the server
469 side, an implementation of this specification shall be a conforming *Basic Mode X.509 Attribute Query*
470 *Responder* or a conforming *Encrypted Mode X.509 Attribute Query Responder*, respectively.

471 A Basic Mode X.509 Attribute Query Requester or Responder MUST conform to the relevant normative
472 statements in section 3. An Encrypted Mode X.509 Attribute Query Requester or Responder MUST
473 conform to the relevant normative statements in section 4, which includes references to normative
474 portions of section 3.

475 **7 Implementation Guidance (Informative)**

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

477 **7.1 Identity Provider Policy**

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

483 **7.2 Caching of Attributes**

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

486 **A. Revision History**

487 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
sstc-saml-x509-authn-attrib-profile-draft-14	06 Mar 2008	T. Scavo	
sstc-saml-x509-authn-attrib-profile-cd-05	11 Mar 2008	T. Scavo	Committee Draft

488 **B. Acknowledgments**

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

- 491 • Hal Lockhart, BEA Systems, Inc.
- 492 • Rob Philpott, EMC Corporation
- 493 • Eric Tiffany, Liberty Alliance Project
- 494 • Scott Cantor, Internet2
- 495 • Bob Morgan, Internet2
- 496 • Tom Scavo, National Center for Supercomputing Applications (NCSA)
- 497 • Peter Davis, Neustar, Inc.
- 498 • Jeff Hodges, Neustar, Inc.
- 499 • Frederick Hirsch, Nokia Corporation
- 500 • Abbie Barbir, Nortel Networks Limited
- 501 • Paul Madsen, NTT Corporation
- 502 • Ari Kermaier, Oracle Corporation
- 503 • Prateek Mishra, Oracle Corporation
- 504 • Brian Campbell, Ping Identity Corporation
- 505 • Anil Saldhana, Red Hat
- 506 • Eve Maler, Sun Microsystems
- 507 • Emily Xu, Sun Microsystems
- 508 • Kent Spaulding, Tripod Technology Group, Inc.
- 509 • David Staggs, Veterans Health Administration

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

- 511 • Rick Randall, Booz Allen Hamilton
- 512 • Rebekah Metz, Booz Allen Hamilton
- 513 • Thomas Wisniewski, Entrust