



SAML_V2.0 Deployment Profiles for X.509 Subjects

Committee Draft **024**

~~07-May~~ **28 August 2007**

Specification URIs:

[sstc-saml2-x509-profiles-deploy-cd-01](http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml2-profiles-deploy-cd-01)

This Version:

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml2-profiles-deploy-x509-cd-024.html>

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml2-profiles-deploy-x509-cd-024.odt>

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml2-profiles-deploy-x509-cd-024.pdf>

Previous Version:

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml2-profiles-deploy-x509-cd-01.html>

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml2-profiles-deploy-x509-cd-01.odt>

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml2-profiles-deploy-x509-cd-01.pdf> N/A

Latest Version:

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml2-profiles-deploy-x509.html>

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml2-profiles-deploy-x509.odt>

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml2-profiles-deploy-x509.pdf>

Latest Approved Version:

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml2-profiles-deploy-x509-cd-024.html>

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml2-profiles-deploy-x509-cd-024.odt>

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml2-profiles-deploy-x509-cd-024.pdf>

Technical Committee:

OASIS Security Services TC

Chair(s):

Hal Lockhart, BEA Systems, Inc.

Brian Campbell, Ping Identity Corporation

Editor(s):

Tom Scavo, National Center for Supercomputing Applications (NCSA)

37 **Related Work:**

38 This specification is an alternative to the *SAML V2.0 Attribute Sharing Profile for X.509*
39 *Authentication-Based Systems* [SAMLASP].

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

41 urn:oasis:names:tc:SAML:metadata:X509:query

42 **Abstract:**

43 This related set of SAML V2.0 deployment profiles specifies how a principal who has been issued
44 an X.509 identity certificate is represented as a SAML Subject, how an assertion regarding such a
45 principal is produced and consumed, and finally how two entities exchange attributes about such
46 a principal.

47 **Status:**

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

51 TC members should send comments on this specification to the TC's email list. Others
52 should send comments to the TC by using the "Send A Comment" button on the TC's
53 web page at <http://www.oasis-open.org/committees/security>.

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

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

Notices

59

60 Copyright © OASIS Open 2007. All Rights Reserved.

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

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

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

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

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

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

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

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

Table of Contents

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
133
134
135
136
137
138
139

1 Introduction.....	6
1.1 Terminology.....	6
1.2 Outline.....	7
1.3 Normative References.....	7
1.4 Non-Normative References.....	8
2 X.509 SAML Subject Profile.....	9
2.1 Required Information.....	9
2.2 Profile Description.....	9
2.3 <saml:Subject> Usage.....	9
2.3.1 <saml:NameID> Usage.....	9
2.3.2 <saml:EncryptedID> Usage.....	9
2.4 Example.....	10
3 SAML Attribute Query Deployment Profile for X.509 Subjects.....	11
3.1 Profile Overview (non-normative).....	11
3.2 Required Information.....	12
3.3 Profile Description.....	13
3.3.1 <samlp:AttributeQuery> Issued by Service Provider.....	13
3.3.2 <samlp:Response> Issued by Identity Provider.....	13
3.4 Use of SAML Request-Response Protocol.....	14
3.4.1 <samlp:AttributeQuery> Usage.....	14
3.4.2 <samlp:Response> Usage.....	14
3.5 Example.....	15
3.6 Use of Encryption.....	16
3.7 Use of Digital Signatures.....	17
3.8 Use of Metadata.....	17
3.8.1 Identity Provider Metadata.....	17
3.8.2 Service Provider Metadata.....	18
3.9 Security and Privacy Considerations.....	19
3.9.1 Background.....	19
3.9.2 General Security Requirements.....	19
3.9.3 User Privacy.....	19
3.10 Implementation Guidelines (non-normative).....	20
3.10.1 Discovery.....	20
3.10.2 Name Mapping.....	20
3.10.3 Canonicalization.....	20
3.10.4 Identity Provider Policy	20

140	3.10.5 Caching of Attributes	21
141	4 SAML Attribute Self-Query Deployment Profile for X.509 Subjects.....	22
142	4.1 Profile Overview (non-normative).....	22
143	4.2 Required Information.....	23
144	4.3 Profile Description.....	24
145	4.3.1 <samlp:AttributeQuery> Issued by Principal.....	24
146	4.3.2 <samlp:Response> Issued by Identity Provider.....	24
147	4.4 Use of SAML Request-Response Protocol.....	24
148	4.4.1 <samlp:AttributeQuery> Usage.....	24
149	4.4.2 <samlp:Response> Usage.....	24
150	4.4.3 Processing Rules.....	25
151	4.5 Example.....	25
152	4.6 Use of Metadata.....	27
153	4.6.1 Identity Provider Metadata.....	27
154	4.7 Security and Privacy Considerations.....	28
155	4.8 Implementation Guidelines (non-normative).....	28
156	4.8.1 Discovery.....	28
157	5 Implementation Conformance.....	30
158	6 Acknowledgments.....	31
159	7 Revision History.....	32
160		

1 Introduction

161

162 This related set of *SAML V2.0 Deployment Profiles for X.509 Subjects* describes how a principal who has
163 been issued an X.509 identity certificate is represented as a SAML Subject, how an assertion regarding
164 such a principal is produced and consumed, and finally how two entities exchange attributes about such a
165 principal.

1.1 Terminology

166

167 This specification uses normative text to describe the use of SAML assertions and attribute queries for
168 X.509 subjects.

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

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

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

177 Listings of XML schemas appear like this.

178 Example code listings appear like this.

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

Prefix	XML Namespace	Comments
saml:	urn:oasis:names:tc:SAML:2.0:assertion	This is the SAML V2.0 assertion namespace [SAMLCore]. This is the default namespace used throughout this document.
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 query extension namespace [SAMLMeta-Ext].
x509qry:	urn:oasis:names:tc:SAML:metadata:X509:query	This is the SAML X.509 query namespace defined by this document and its accompanying schema [X509Query-XSD].
ds:	http://www.w3.org/2000/09/xmldsig#	This is the W3C XML Signature namespace, defined in the XML-Signature Syntax and Processing specification and schema [XMLSig-XSD].
xenc:	http://www.w3.org/2001/04/xmlenc#	This is the W3C XML Encryption namespace, defined in the XML Encryption Syntax and Processing specification [XMLEnc] and schema [XMLEnc-XSD].
xs:	http://www.w3.org/2001/XMLSchema	This is the XML Schema namespace [Schema1].

Prefix	XML Namespace	Comments
xsi:	http://www.w3.org/2001/XMLSchema-instance	This is the XML Schema namespace for schema-related markup that appears in XML instances [Schema1].

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

185 The term *identity provider* as used in this specification refers to a typical SAML attribute authority
186 [SAMLGloss]. The term *service provider* refers to a SAML attribute requester. However, as used in this
187 specification, a service provider is not a typical SAML service provider since it performs X.509
188 authentication in lieu of consuming a SAML authentication assertion.

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

192 1.2 Outline

193 Section 2 describes how a principal who has been issued an X.509 identity certificate is represented as a
194 SAML Subject. Section 3 describes in detail how a service provider and identity provider exchange
195 attributes about a principal who has been issued an X.509 identity certificate. ~~Finally, s~~Section 4 describes
196 the special case where the requester is the subject of the query, that is, where the principal self-queries
197 for attributes. ~~Finally, section 5 specifies requirements that all conforming implementations must follow.~~

198 1.3 Normative References

- 199 **[FIPS 140-2]** Security Requirements for Cryptographic Modules, May 2001. See
200 <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>
- 201 **[RFC 2119]** S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. IETF
202 RFC 2119, March 1997. See <http://www.ietf.org/rfc/rfc2119.txt>
- 203 **[RFC2246]** T. Dierks and C. Allen. *The TLS Protocol Version 1.0*. IETF RFC 2246, January
204 1999. See <http://www.ietf.org/rfc/rfc2246.txt>
- 205 **[RFC2253]** M Wahl et al. *Lightweight Directory Access Protocol (v3): UTF-8 String*
206 *Representation of Distinguished Names*. IETF RFC 2253, December 1997. See
207 <http://www.ietf.org/rfc/rfc2253.txt>
- 208 **[RFC3280]** R. Housley et al. *Internet X.509 Public Key Infrastructure: Certificate and*
209 *Certificate Revocation List (CRL) Profile*. IETF RFC 3280, April 2002. See
210 <http://www.ietf.org/rfc/rfc3280.txt>
- 211 **[SAMLBind]** S. Cantor et al. *Bindings for the OASIS Security Assertion Markup Language*
212 *(SAML) V2.0*. OASIS Standard, March 2005. See [http://docs.oasis-](http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf)
213 [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)
- 214 **[SAMLCore]** S. Cantor et al. *Assertions and Protocols for the OASIS Security Assertion*
215 *Markup Language (SAML) V2.0*. OASIS Standard, March 2005. See
216 <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>
- 217 **[SAMLMeta]** S. Cantor et al. *Metadata for the OASIS Security Assertion Markup Language*
218 *(SAML) V2.0*. OASIS Standard, March 2005. See [http://docs.oasis-](http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf)
219 [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)
- 220 **[SAMLMeta-Ext]** T. Scavo and S. Cantor. *Metadata Extension for SAML V2.0 and V1.x Query*
221 *Requesters*. OASIS Draft, September 2006. Document ID sstc-saml-metadata-
222 *ext-query-cd-02*. See [http://docs.oasis-open.org/security/saml/SpecDrafts-](http://docs.oasis-open.org/security/saml/SpecDrafts-Post2.0/sstc-saml-metadata-ext-query-cd-02.pdf)
223 [Post2.0/sstc-saml-metadata-ext-query-cd-02.pdf](http://docs.oasis-open.org/security/saml/SpecDrafts-Post2.0/sstc-saml-metadata-ext-query-cd-02.pdf)
- 224 **[SAMLProf]** S. Cantor et al. *Profiles for the OASIS Security Assertion Markup Language*

225		(SAML) V2.0. OASIS Standard, March 2005. See http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf
226		
227	[Schema1]	H. S. Thompson et al. <i>XML Schema Part 1: Structures</i> . World Wide Web Consortium Recommendation, May 2001. See http://www.w3.org/TR/2001/REC-xmlschema-1-20010502/
228		
229		
230	[SSL3]	A. Freier et al. <i>The SSL Protocol Version 3.0</i> , IETF Internet-Draft, November 1996. See http://wp.netscape.com/eng/ssl3/draft302.txt
231		
232	[X509Query-XSD]	<i>Schema for SAML V2.0 Deployment Profiles for X.509 Subjects</i> . OASIS, December 2006. Document ID sstc-saml-metadata-x509-query.xsd. See http://www.oasis-open.org/committees/documents.php?wg_abbrev=security
233		
234		
235	[XMLEnc]	D. Eastlake et al. <i>XML Encryption Syntax and Processing</i> . World Wide Web Consortium Recommendation, December 2002. See http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/
236		
237		
238	[XMLEnc-XSD]	<i>XML Encryption Schema</i> . World Wide Web Consortium Recommendation, December 2002. See http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/xenc-schema.xsd
239		
240		
241	[XMLSig]	D. Eastlake et al. <i>XML-Signature Syntax and Processing</i> . World Wide Web Consortium Recommendation, February 2002. See http://www.w3.org/TR/2002/REC-xmlsig-core-20020212/
242		
243		
244	[XMLSig-XSD]	<i>Schema for XML Signatures</i> . World Wide Web Consortium Recommendation, February 2002. See http://www.w3.org/TR/2002/REC-xmlsig-core-20020212/xmlsig-core-schema.xsd
245		
246		

247 1.4 Non-Normative References

248	[MACEAttrib]	S. Cantor et al. <i>MACE-Dir SAML Attribute Profiles</i> . Internet2 MACE, April 2006. See http://middleware.internet2.edu/dir/docs/internet2-mace-dir-saml-attributes-200604.pdf
249		
250		
251	[RFC3820]	S. Tuecke et al. <i>Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile</i> . IETF RFC 3820, June 2004. See http://www.ietf.org/rfc/rfc3820.txt
252		
253	[SAMLASP]	R. Randall et al. <i>SAML V2.0 Attribute Sharing Profile for X.509 Authentication-Based Systems</i> . OASIS Committee Draft, April August 2007. Document ID sstc-saml-x509-authn-attrib-profile-cd-04.
254		
255		
256	[SAMLGloss]	J. Hodges et al. <i>Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0</i> . OASIS Standard, March 2005. See http://docs.oasis-open.org/security/saml/v2.0/saml-glossary-2.0-os.pdf
257		
258		
259	[SAMLSecure]	F. Hirsch et al. <i>Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0</i> . OASIS Standard, March 2005. See http://docs.oasis-open.org/security/saml/v2.0/saml-sec-consider-2.0-os.pdf
260		
261		

262 **2 X.509 SAML Subject Profile**

263 The X.509 SAML Subject Profile describes how a principal who has been issued an X.509 identity
264 certificate is represented as a SAML V2.0 Subject.

265 **2.1 Required Information**

266 **Identification:**

267 urn:oasis:names:tc:SAML:2.0:profiles:query:attribute:X509-subject

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

269 **Description:** Given below.

270 **Updates:** N/A

271 **Extends:** N/A

272 **2.2 Profile Description**

273 This deployment profile specifies a SAML V2.0 `<saml:Subject>` element that represents a principal
274 who has been issued an X.509 identity certificate. An entity that produces a `<saml:Subject>` element
275 according to this deployment profile MUST have previously determined that the principal does in fact
276 possess the corresponding private key.

277 **2.3 `<saml:Subject>` Usage**

278 The `<saml:Subject>` element MUST contain exactly one of `<saml:NameID>` or
279 `<saml:EncryptedID>`. The `<saml:Subject>` element MAY contain one or more
280 `<saml:SubjectConfirmation>` elements that are out of scope for this deployment profile.

281 **2.3.1 `<saml:NameID>` Usage**

282 If the `<saml:Subject>` element contains a `<saml:NameID>` element, the following requirements MUST
283 be satisfied:

- 284 • The value of the `<saml:NameID>` element is the Subject Distinguished Name (DN) from the
285 principal's X.509 identity certificate.
- 286 • The `<saml:NameID>` element MUST have a `Format` attribute whose value is
287 `urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName`. Thus the DN value
288 of the `<saml:NameID>` element MUST satisfy the rules of section 8.3.3 of [SAMLCore]. Moreover,
289 for the purposes of this deployment profile, the DN value MUST conform to RFC 2253 [RFC2253].
- 290 • As specified in [SAMLCore], the `NameQualifier` attribute of the `<saml:NameID>` element
291 SHOULD be omitted.

292 **2.3.2 `<saml:EncryptedID>` Usage**

293 If the `<saml:Subject>` element contains a `<saml:EncryptedID>` element, the content of the
294 enclosed `<xenc:EncryptedData>` element MUST be an encrypted `<saml:NameID>` element that
295 satisfies the requirements of the previous section.

296 To encrypt the `<saml:NameID>` element, exactly one of the following procedures MUST be followed:

- 297 • The producer generates a new symmetric key to encrypt the `<saml:NameID>` element. After

298 performing the encryption, the producer places the resulting ciphertext in the
299 <xenc:EncryptedData> element. The symmetric key MUST be encrypted with the consumer's
300 public key and the resulting ciphertext MUST be placed in the <xenc:EncryptedKey> element.

- 301 • The producer uses a symmetric key previously established with the consumer to encrypt the
302 <saml:NameID> element. After performing the encryption, the producer places the resulting
303 ciphertext in the <xenc:EncryptedData> element. In this case, however, the
304 <saml:EncryptedID> element MUST NOT contain an <xenc:EncryptedKey> element.

305 A symmetric key transmitted in an <xenc:EncryptedKey> element MUST NOT be later reused by the
306 producer as a previously established symmetric key.

307 2.4 Example

308 An example of an unencrypted X.509 SAML Subject:

```
309 <!-- unencrypted X.509 SAML Subject -->  
310 <saml:Subject>  
311   <saml:NameID  
312     Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">  
313     C=US, O=NCSA-TEST, OU=User, CN=trscavo@uiuc.edu  
314   </saml:NameID>  
315 </saml:Subject>
```

316 An example of an encrypted X.509 SAML Subject:

```
317 <!-- encrypted X.509 SAML Subject -->  
318 <saml:Subject>  
319   <saml:EncryptedID  
320     xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">  
321     <xenc:EncryptedData  
322       Type="http://www.w3.org/2001/04/xmlenc#Element">  
323       ...  
324     </xenc:EncryptedData>  
325     <xenc:EncryptedKey  
326       Recipient="https://idp.example.org/saml">  
327       ...  
328     </xenc:EncryptedKey>  
329   </saml:EncryptedID>  
330 </saml:Subject>
```

331 **3 SAML Attribute Query Deployment Profile for X.509** 332 **Subjects**

332 The *SAML Attribute Query Deployment Profile for X.509 Subjects* specifies how a service provider and an
333 identity provider exchange attributes about a principal who has been issued an X.509 identity certificate.
334 As such, the profile relies on the X.509 SAML Subject Profile specified in section 2 of this document. Note
335 that the deployment profile specified in section 4 is an extension of this profile.

333 **3.1 Profile Overview (non-normative)**

334 Consider the use case where a principal attempts to access a secured resource at a service provider.
335 Principal authentication at the service provider is accomplished by presenting a trusted X.509 identity
336 certificate and by demonstrating proof of possession of the associated private key.

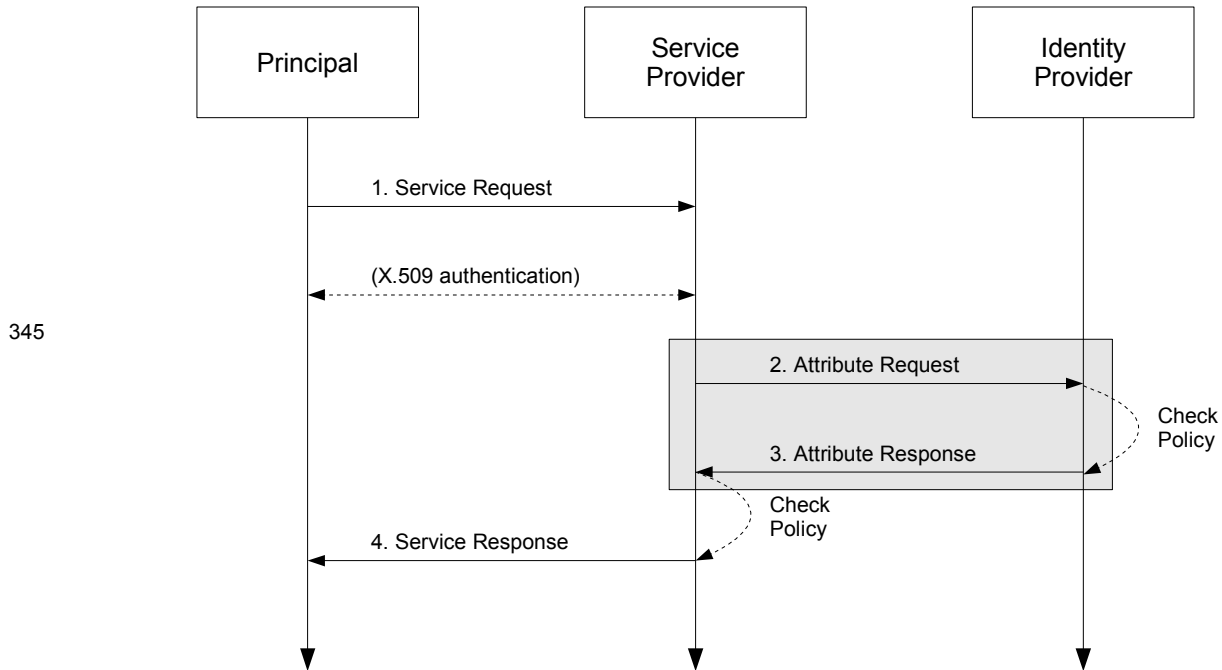
335 After the principal has been authenticated, the service provider requires additional information about the
336 principal in order to determine whether to grant access to the resource. To obtain this information, the
337 service provider uses the Subject Distinguished Name (DN) field (and perhaps other information) from the
338 principal's X.509 identity certificate to query an identity provider for attributes about the principal. Using the
339 attributes received from the identity provider, the service provider is able to make an informed access
340 control decision.

336 This use case is based upon the following assumptions:

- 337 • A principal possesses an X.509 identity credential.
- 338 • The principal wields a client that requests a service from a service provider.
- 339 • The client can access the principal's X.509 identity credential.
- 340 • The principal has an account with a SAML identity provider.
- 341 • The service provider knows the principal's preferred identity provider and is able to query that
342 identity provider for attributes.
- 342 • The identity provider is able to map an X.509 SAML Subject (as defined in section 2 of this
343 document) to one and only one principal in its security domain. In particular, the identity provider is
344 able to map the X.509 SAML Subject that represents this principal.

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

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



345

346 **1. Service Request**

347 In step 1, the principal requests a secured resource from a service provider who requires that the
 348 principal be authenticated. The principal authenticates to the service provider with an X.509 identity
 349 certificate.

350 **2. Attribute Request**

351 In step 2, the service provider sends a SAML V2.0 `<samlp:AttributeQuery>` message to the
 352 identity provider using a SAML SOAP Binding. The Subject DN from the principal's X.509 identity
 353 certificate (presented in step 1) is used to construct the `<saml:Subject>` element.

354 **3. Attribute Response**

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

358 **4. Service Response**

359 In step 4, based on the attributes received from the identity provider, the service provider returns the
 360 requested resource or an error, subject to policy.

361 Of the sequence of steps described above, it is steps 2 and 3 that are profiled in sections 3.3 and 3.4 of
 362 this deployment profile.

363 **3.2 Required Information**

364 **Identification:**

365 urn:oasis:names:tc:SAML:2.0:profiles:query:attribute:X509

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

366 **Description:** Given below.

367 **Updates:** N/A

368 **Extends:** Assertion Query/Request Profile [SAMLProf]

369 **3.3 Profile Description**

370 This deployment profile describes the use of the SAML V2.0 Assertion Query and Request Protocol
371 [SAMLCore] in conjunction with the SAML V2.0 SOAP Binding [SAMLBind] to retrieve the attributes of a
372 principal who has authenticated using an X.509 identity certificate. The attribute exchange MUST conform
373 to the Assertion Query/Request Profile given in section 6 of [SAMLProf] unless otherwise specified below.

371 As outlined in section 3.1, a service provider sends a SAML V2.0 `<samlp:AttributeQuery>` message
372 directly to an identity provider. This message contains a name identifier that identifies a principal who has
373 authenticated to the service provider using an X.509 identity certificate. If the identity provider receiving the
374 request can:

- 372 • recognize the name identifier; and
- 373 • fulfill the request subject to any applicable policies;

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

375 **3.3.1 `<samlp:AttributeQuery>` Issued by Service Provider**

376 To initiate the profile, the service provider uses a synchronous binding such as the SAML SOAP Binding
377 [SAMLBind] to send a SAML V2.0 `<samlp:AttributeQuery>` message to an Attribute Service
378 endpoint at the identity provider. SAML metadata (section 3.8) MAY be used to determine the endpoint
379 locations and bindings supported by the identity provider.

377 The service provider uses information obtained from the principal's X.509 identity certificate to construct
378 the query. As required by the X.509 SAML Subject Profile (section 2), the service provider MUST have
379 previously determined that the principal does in fact possess the corresponding private key. The details of
380 this step are out of scope for this deployment profile.

378 The service provider MUST authenticate itself to the identity provider. SSL 3.0 [SSL3] or TLS 1.0
379 [RFC2246] with client authentication MAY be used for this purpose and to provide integrity protection and
380 confidentiality. Also, the `<samlp:AttributeQuery>` element MAY be signed.

379 **3.3.2 `<samlp:Response>` Issued by Identity Provider**

380 The identity provider MUST process the request as outlined in [SAMLCore]. After processing the message
381 or upon encountering an error, the identity provider MUST return a `<samlp:Response>` message
382 containing an appropriate status code to the service provider to complete the SAML protocol exchange. If
383 the identity provider is successful in locating one or more attributes for this principal, they will be included
384 in the response.

381 The identity provider MUST be able to map the referenced X.509 Subject to one and only one principal in
382 its security domain. If the identity provider is not able to map the `<saml:Subject>` element to a local
383 principal, it MUST return an error.

382 The identity provider processes the `<samlp:AttributeQuery>` element and any enclosed
383 `<saml:Attribute>` elements before returning an assertion containing a
384 `<saml:AttributeStatement>` to the requester. If no `<saml:Attribute>` elements are included in
385 the query, the identity provider returns all attributes for this principal, subject to policy. SAML metadata
386 (section 3.8) MAY be used to determine the attribute requirements of the service provider. If the identity
387 provider is unable to resolve attributes for this principal (for any reason), it MUST return an error.

383 The identity provider MUST authenticate itself to the service provider. Also, either the
384 `<samlp:Response>` element or the `<saml:Assertion>` element (or both) MAY be signed.

384 3.4 Use of SAML Request-Response Protocol

385 As required by the Assertion Query/Request Profile [SAMLProf], the `<samlp:AttributeQuery>`
386 element MUST contain a `<saml:Issuer>` element.

386 3.4.1 `<samlp:AttributeQuery>` Usage

387 The request MUST contain a `<samlp:AttributeQuery>` element that conforms to the following rules:

- 388 • The `<saml:Subject>` element MUST conform to the X.509 SAML Subject Profile defined in
389 section 2 of this document.
- 389 • The `<saml:Subject>` element MUST NOT contain a `<saml:SubjectConfirmation>`
390 element.
- 390 • The `<samlp:AttributeQuery>` element MAY include one or more `<saml:Attribute>`
391 elements.

391 3.4.2 `<samlp:Response>` Usage

392 If the request is successful, the `<samlp:Response>` element MUST conform to the following rules. Any
393 assertion(s) included in the response may be encrypted or unencrypted. See section 2 of the SAML V2.0
394 Assertions and Protocols specification [SAMLCore] for general requirements regarding SAML assertions.

393 For each `<saml:Assertion>` element the following conditions MUST be satisfied:

- 394 • The `<saml:Subject>` element (which strongly matches the subject of the query [SAMLCore])
395 SHOULD NOT contain a `<saml:SubjectConfirmation>` element.
- 395 • The `<saml:Assertion>` element MUST contain a `<saml:Conditions>` element with
396 `NotBefore` and `NotOnOrAfter` attributes.
- 396 • The `<saml:Assertion>` element SHOULD contain a `<saml:Audience>` element whose value
397 is identical to the value of the `<saml:Issuer>` element in the request.
- 397 • Other conditions (including other `<saml:Audience>` elements) MAY be included as required by
398 the service provider or at the discretion of the identity provider.
- 398 • The `<saml:Assertion>` element MUST contain at least one `<saml:AttributeStatement>`
399 element and SHOULD contain *only* `<saml:AttributeStatement>` elements.

399 For each `<saml:EncryptedAssertion>` element, the content of the enclosed
400 `<xenc:EncryptedData>` element MUST be an encrypted `<saml:Assertion>` element that satisfies
401 the above requirements.

400 To encrypt the `<saml:Assertion>` element, exactly one of the following procedures MUST be followed:

- 401 • The identity provider generates a new symmetric key to encrypt the `<saml:Assertion>` element.
402 After performing the encryption, the identity provider places the resulting ciphertext in the
403 `<xenc:EncryptedData>` element. The symmetric key MUST be encrypted with the service
404 provider's public key and the resulting ciphertext placed in the `<xenc:EncryptedKey>` element.
- 402 • The identity provider uses a symmetric key previously established with the service provider to
403 encrypt the `<saml:Assertion>` element. After encrypting the `<saml:Assertion>` element
404 using this key, the identity provider places the resulting ciphertext in the `<xenc:EncryptedData>`
405 element. In this case, however, the `<saml:EncryptedAssertion>` element MUST NOT contain
406 an `<xenc:EncryptedKey>` element.

403 See section 3.6 for additional rules regarding encryption.

404 If the request is unsuccessful and the identity provider wishes to return an error, the `<samlp:Response>`

405 element MUST NOT contain a <saml:Assertion> element. Possible error responses include the
406 following:

- 406 • The identity provider MAY return one of the status codes
407 urn:oasis:names:tc:SAML:2.0:status:UnknownAttrProfile or
408 urn:oasis:names:tc:SAML:2.0:status:InvalidAttrNameOrValue as suggested in
409 section 3.3.2.3 of [SAMLCore].
- 410 • If the identity provider does not recognize the <saml:NameID> element or otherwise is unable to
411 map the <saml:NameID> element to a local principal name, it MAY return the following status
412 code:
413 urn:oasis:names:tc:SAML:2.0:status:UnknownPrincipal

414 3.5 Example

415 For example, the requester issues the following attribute query:

```
416 <samlp:AttributeQuery
417   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
418   xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
419   ID="aaf23196-1773-2113-474a-fe114412ab72"
420   Version="2.0"
421   IssueInstant="2006-07-17T22:26:40Z">
422   <saml:Issuer>https://sp.example.org/saml</saml:Issuer>
423   <saml:Subject>
424     <saml:NameID
425       Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
426       C=US, O=NCSA-TEST, OU=User, CN=trscavo@uiuc.edu
427     </saml:NameID>
428   </saml:Subject>
429   <saml:Attribute
430     xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
431     x500:Encoding="LDAP"
432     NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
433     Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
434     FriendlyName="eduPersonPrincipalName">
435   </saml:Attribute>
436   <saml:Attribute
437     xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
438     x500:Encoding="LDAP"
439     NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
440     Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.1"
441     FriendlyName="eduPersonAffiliation">
442   </saml:Attribute>
443 </samlp:AttributeQuery>
```

444 After processing the request, the identity provider issues the following response:

```
445 <samlp:Response
446   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
447   xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
448   InResponseTo="aaf23196-1773-2113-474a-fe114412ab72"
449   ID="b07b804c-7c29-ea16-7300-4f3d6f7928ac"
450   Version="2.0"
451   IssueInstant="2006-07-17T22:26:41Z">
452   <saml:Issuer>https://idp.example.org/saml</saml:Issuer>
453   <samlp:Status>
454     <samlp:StatusCode
455       Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
456   </samlp:Status>
457   <saml:Assertion
458     xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
459     xmlns:xs="http://www.w3.org/2001/XMLSchema"
460     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
461     xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
462     ID="a144e8f3-adad-594a-9649-924517abe933">
```

```

463     Version="2.0"
464     IssueInstant="2006-07-17T22:26:41Z">
465     <saml:Issuer>https://idp.example.org/saml</saml:Issuer>
466     <saml:Subject>
467         <saml:NameID
468             Format="urn:oasis:names:tc:SAML:1.1:nameid-
469 format:X509SubjectName">
469             C=US, O=NCSA-TEST, OU=User, CN=trscavo@uiuc.edu
470         </saml:NameID>
471     </saml:Subject>
472     <!-- assertion lifetime constrained by principal's X.509 cert -->
473     <saml:Conditions
474         NotBefore="2006-07-17T22:21:41Z"
475         NotOnOrAfter="2006-07-17T22:51:41Z">
476         <saml:AudienceRestriction>
477             <saml:Audience>https://sp.example.org/saml</saml:Audience>
478         </saml:AudienceRestriction>
479     </saml:Conditions>
480     <saml:AttributeStatement>
481         <saml:Attribute
482             xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
483             x500:Encoding="LDAP"
484             NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
485             Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
485             FriendlyName="eduPersonPrincipalName">
486             <saml:AttributeValue xsi:type="xs:string">
486                 trscavo@uiuc.edu
487             </saml:AttributeValue>
488         </saml:Attribute>
489         <saml:Attribute
490             xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
491             x500:Encoding="LDAP"
492             NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
493             Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.1"
493             FriendlyName="eduPersonAffiliation">
494             <saml:AttributeValue xsi:type="xs:string">
494                 member
495             </saml:AttributeValue>
496             <saml:AttributeValue xsi:type="xs:string">
497                 staff
498             </saml:AttributeValue>
499         </saml:Attribute>
500     </saml:AttributeStatement>
501 </saml:Assertion>
502 </samlp:Response>

```

503 The attributes in the above example (eduPersonAffiliation and eduPersonPrincipalName)
504 conform to the MACE-Dir Attribute Profile for SAML 2.0 [MACEAttrib] and are for illustration purposes
505 only.

506 3.6 Use of Encryption

507 If the service provider encrypts the <saml:NameID> element in the query, the identity provider SHOULD
508 encrypt any resulting assertions. Moreover, if the service provider uses a previously established symmetric
509 key, the identity provider SHOULD use the same symmetric key to encrypt the assertion. In the case
510 where the service provider generates a new symmetric key, the identity provider MUST treat this key as a
511 previously established key, that is, the identity provider SHOULD use the same symmetric key to encrypt
512 the assertion and MUST NOT encrypt this key into the <xenc:EncryptedKey> element.

513 An encryption algorithm satisfying FIPS 140-2 Security Requirements [FIPS 140-2] SHALL be used for all
514 encryption operations.

515 3.7 Use of Digital Signatures

516 If the service provider encrypts the `<saml:NameID>` element in the query, the
517 `<samlp:AttributeQuery>` element MUST be signed *after* the encryption operation takes place. If the
518 identity provider encrypts a `<saml:Assertion>` element in the response, the `<saml:Assertion>`
519 element MUST be signed *before* the encryption operation takes place. Whether or not an assertion is
520 encrypted, the `<saml:Response>` element MAY be signed.

521 A signing algorithm satisfying FIPS 140-2 Security Requirements [FIPS 140-2] SHALL be used for all
522 digital signature operations on encrypted elements or elements with encrypted content.

523 3.8 Use of Metadata

524 The identity provider and the service provider MAY use metadata for locating endpoints, communicating
525 key information, and so forth. The use of SAML V2.0 metadata [SAMLMeta], which is RECOMMENDED,
526 is profiled in sections 3.8.1 and 3.8.2 below.

527 3.8.1 Identity Provider Metadata

528 An identity provider that uses SAML V2.0 metadata MUST include an
529 `<md:AttributeAuthorityDescriptor>` element that satisfies the following rules:

- 529 • The containing `<md:EntityDescriptor>` element MUST have an `entityID` attribute whose
530 value is the same unique identifier given as the `<saml:Issuer>` element in assertions issued by
531 the identity provider.
- 530 • The `<md:AttributeAuthorityDescriptor>` element MUST include an
531 `<md:NameIDFormat>` element with value `"urn:oasis:names:tc:SAML:1.1:nameid-`
532 `format:X509SubjectName"`.
- 531 • One or more `<saml:Attribute>` elements MAY be included in the
532 `<md:AttributeAuthorityDescriptor>` element. Since a service provider may choose not to
533 query the identity provider based on the attributes in this list, this list SHOULD be comprehensive or
534 otherwise omitted.

532 To distinguish between this deployment profile and other uses of `X509SubjectName`, an identity provider
533 requires the means to explicitly call out its support of this deployment profile. An XML attribute has been
534 specified for this purpose [X509Query-XSD]:

```
533 <xs:attribute  
534   name="supportsX509Query" type="boolean" use="optional"/>
```

535 Use of this attribute is OPTIONAL. An identity provider that chooses to use this attribute, however, MUST
536 do so as follows:

- 536 • The `<md:AttributeAuthorityDescriptor>` element MUST include at least one
537 `<md:AttributeService>` element having attribute `supportsX509Query` set to `"true"`.
- 537 • At least one `<md:AttributeService>` element having attribute `supportsX509Query` set to
538 `"true"` MUST have its `Binding` attribute set to
539 `"urn:oasis:names:tc:SAML:2.0:bindings:SOAP"`.

538 An example of identity provider metadata follows:

```
539 <!-- An Identity Provider supporting this deployment profile -->  
540 <md:EntityDescriptor  
541   xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"  
542   entityID="https://idp.example.org/saml">  
543  
544   <md:AttributeAuthorityDescriptor  
545     protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">  
546
```

```

547     <md:AttributeService
548         x509qry:supportsX509Query="true"
549         xmlns:x509qry="urn:oasis:names:tc:SAML:metadata:X509:query"
550         Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
551         Location="https://idp.example.org:8443/saml-idp/AA"/>
552
553     <md:NameIDFormat>
554         urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName
555     </md:NameIDFormat>
556
557     <!-- see [MACEAttr] -->
558     <md:AttributeProfile>
559         urn:mace:dir:profiles:attribute:samlv2
560     </md:AttributeProfile>
561
562 </md:AttributeAuthorityDescriptor>
563
564 </md:EntityDescriptor>

```

565 3.8.2 Service Provider Metadata

566 A service provider that uses SAML V2.0 metadata **MUST** include an `<md:RoleDescriptor>` element
567 that satisfies the following rules:

- 568 • The containing `<md:EntityDescriptor>` element **MUST** have an `entityID` attribute whose
569 value is the same unique identifier used as the `<saml:Issuer>` element in attribute queries
570 issued by the service provider.
- 571 • The type of the `<md:RoleDescriptor>` element **MUST** be derived from type
572 **query:AttributeQueryDescriptorType** [SAMLMeta-Ext].
- 573 • The `<md:RoleDescriptor>` element **MUST** include an `<md:NameIDFormat>` element with
574 value "urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName".
- 575 • One or more `<md:RequestedAttribute>` elements **MAY** be included in the
576 `<md:AttributeConsumingService>` element.

577 An example of service provider metadata follows:

```

578 <!-- A Service Provider supporting this profile -->
579 <md:EntityDescriptor
580     xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
581     entityID="https://sp.example.org/saml">
582
583     <md:RoleDescriptor
584         xmlns:query="urn:oasis:names:tc:SAML:metadata:ext:query"
585         xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
586         xsi:type="query:AttributeQueryDescriptorType"
587         protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
588
589         <md:NameIDFormat>
590             urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName
591         </md:NameIDFormat>
592
593         <md:AttributeConsumingService isDefault="true" index="0">
594             <md:ServiceName xml:lang="en">
595                 Grid Service Provider
596             </md:ServiceName>
597             <md:RequestedAttribute
598                 NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
599                 Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
600                 FriendlyName="eduPersonPrincipalName">
601             </md:RequestedAttribute>
602             <md:RequestedAttribute
603                 NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
604                 Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.1"

```

```
605         FriendlyName="eduPersonAffiliation">
606         </md:RequestedAttribute>
607         </md:AttributeConsumingService>
608
609     </md:RoleDescriptor>
610
611 </md:EntityDescriptor>
```

612 The attributes in the above example (`eduPersonAffiliation` and `eduPersonPrincipalName`)
613 conform to the MACE-Dir Attribute Profile for SAML 2.0 [MACEAttrib] and are for illustration purposes
614 only.

615 **3.9 Security and Privacy Considerations**

616 The motivation for this deployment profile is to specify a secure means of obtaining SAML attributes in
617 conjunction with X.509 authentication.

618 **3.9.1 Background**

619 The SAML Security and Privacy specification [SAMLSecure] provides general background material
620 relevant to all SAML bindings and profiles. Section 6.1 of [SAMLSecure], in particular, considers the
621 security requirements of the SAML SOAP Binding, and is therefore pertinent to this deployment profile. In
622 addition, section 3.1.2 of the SAML Bindings specification [SAMLBind] provides further security guidelines
623 regarding SAML bindings.

624 **3.9.2 General Security Requirements**

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

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

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

628 **3.9.3 User Privacy**

629 Since a DN persists for the life of the certificate, a service provider may query for attributes at any time.
630 To prevent service providers from querying for attributes after the certificate has expired, an identity
631 provider SHOULD check the lifetime of the referenced certificate before issuing an assertion regarding an
632 X.509 Subject. If the certificate has expired, an error should be returned.

630 As a further privacy measure, the principal may use a short-lived X.509 identity certificate. For example,
631 an X.509 proxy certificate [RFC3820]) may be used.

631 **3.10 Implementation Guidelines (non-normative)**

632 The following non-normative guidelines are provided for the convenience of implementers.

633 **3.10.1 Discovery**

634 The service provider must determine the principal's preferred identity provider. This is called *identity*
635 *provider discovery*.

636 Some possible approaches to identity provider discovery in the context of this deployment profile are
637 discussed briefly below:

- 638 • The identity provider's unique identifier may be preconfigured at the service provider. This is useful,
639 for instance, if there is only one identity provider per deployment.
- 640 • The subject DN of the principal's X.509 identity certificate may include a reference to the identity
641 provider. New deployments are discouraged from decorating long-lived DNs in this manner,
642 however, since this practice may lessen interoperability with existing PKIs. For short-lived X.509
643 identity certificates, this practice may be satisfactory.
- 644 • The issuer DN or the issuer alternative name may provide clues about the principal's preferred
645 identity provider. This technique may not be practical, however, since SAML authorities do not
646 typically issue X.509 credentials.
- 647 • A reference to the identity provider may be inserted into a non-critical X.509 extension [RFC3280] at
648 the time the credential is issued. For long-term credentials, this practice may not be feasible, but
649 for short-term credentials, this technique may be satisfactory.

650 This deployment profile does not specify a particular method of identity provider discovery.

641 **3.10.2 Name Mapping**

642 An identity provider that consumes a `<saml:Subject>` element produced according to this deployment
643 profile must be able to map the referenced X.509 Subject to one and only one principal in its security
644 domain. If the identity provider issued the X.509 credential in the first place, or otherwise has access to
645 the principal's X.509 identity certificate, this should be straightforward. Otherwise a persistent certificate
646 registration process to facilitate the mapping of X.509 Subjects to principals may be used.

643 **3.10.3 Canonicalization**

644 According to this deployment profile, the format of the DNs used to construct the `<saml:Subject>`
645 element is dictated by [SAMLCore]. Since the latter allows some flexibility in the precise format of a DN
646 (by virtue of its dependence on [RFC2253]), it may be necessary for an identity provider to canonicalize
647 the DN during the course of mapping it to a local principal name. Note that the details of the
648 canonicalization process are of concern only to the identity provider. As long as the service provider
649 provides a DN whose canonicalization is recognized by the identity provider, the correct mapping will
650 occur.

645 **3.10.4 Identity Provider Policy**

646 Service providers may explicitly enumerate the required attributes in queries or may issue so-called
647 "empty queries" that essentially request all available attributes. Regardless of the attribute requirements
648 called out in the query (or in metadata, if used for this purpose), it is the identity provider that determines
649 the actual attributes returned to the service provider. Thus a responsible identity provider will initiate and
650 enforce policy that strictly limits the attributes released to service providers.

647 **3.10.5 Caching of Attributes**

648 A service provider will most likely provide a capability to cache user attributes returned in assertions. If so,
649 cache expiration settings should be configurable by administrators.

649 4 SAML Attribute Self-Query Deployment Profile for 650 X.509 Subjects

650 The *SAML Attribute Self-Query Deployment Profile for X.509 Subjects* specifies how a principal who has
651 been issued an X.509 identity certificate self-queries an identity provider for attributes. The profile extends
652 the SAML Attribute Query Deployment Profile for X.509 Subjects specified in section 3 of this document.
653 Where the two profiles conflict, this deployment profile takes precedence.

651 4.1 Profile Overview (non-normative)

652 In this scenario, a principal self-queries an identity provider for attributes. The principal uses the Subject
653 Distinguished Name (DN) field (and perhaps other information) from its X.509 identity certificate to
654 formulate the query. Principal authentication is accomplished by presenting a trusted X.509 identity
655 certificate (the same certificate used to construct the query) and by demonstrating proof of possession of
656 the associated private key. After the principal has been authenticated, the identity provider binds the
657 principal's public key to an assertion, which is issued directly to the principal.

653 The principal subsequently requests a secured resource at the service provider. The principal presents
654 the previously obtained assertion to the service provider and demonstrates proof of possession of the
655 corresponding private key. Using the attributes in the assertion, the service provider is able to make an
656 informed access control decision.

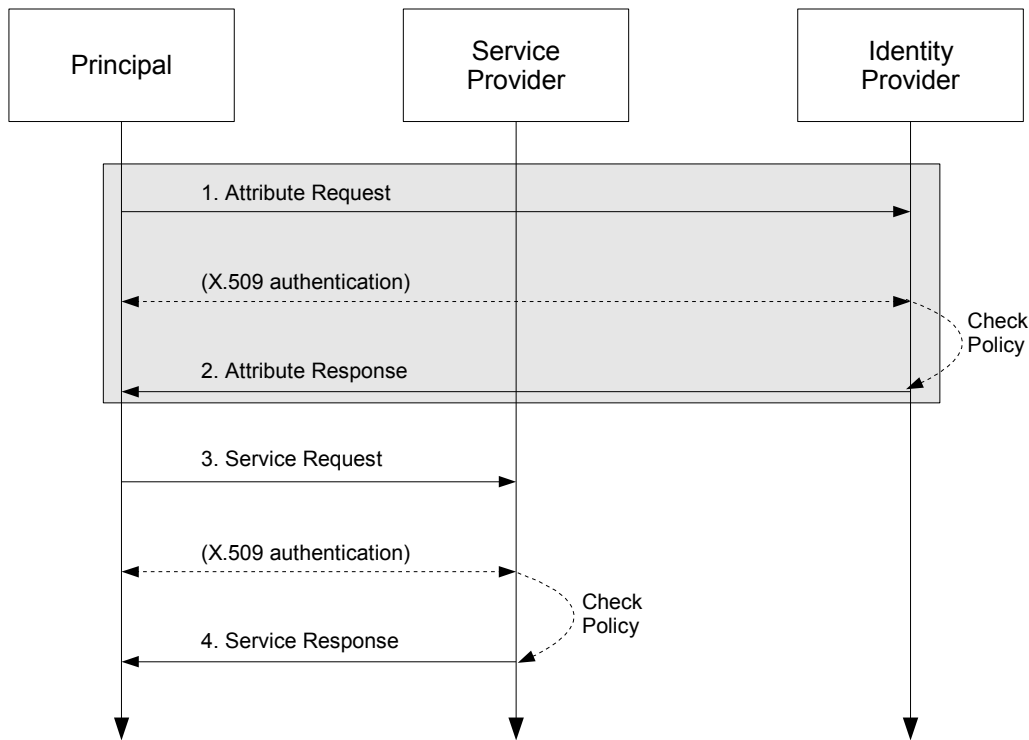
654 This use case is based on the following assumptions:

- 655 • A principal possesses an X.509 credential.
- 656 • The principal wields a client that can both query an identity provider for attributes and request a
657 service from a service provider.
- 657 • The client can access the principal's X.509 credential.
- 658 • The principal has an account with a SAML identity provider.
- 659 • The client knows the principal's preferred identity provider and the attribute requirements of the
660 target service provider.
- 660 • The identity provider is able to map an X.509 SAML Subject (as defined in section 2 of this
661 document) to one and only one principal in its security domain. In particular, the identity provider is
662 able to map the X.509 SAML Subject that represents this principal.

661 Note that in the case of a self-query, the client possesses significantly more functionality than the client
662 alluded to in section 3.1.

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

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



664

665 **1. Attribute Request**

666 In step 1, the principal sends a SAML V2.0 `<samlp:AttributeQuery>` message to the identity
 667 provider using a SAML SOAP Binding. The Subject DN from the principal's X.509 identity certificate is
 668 used to construct the `<saml:Subject>` element of the query. The identity provider requires that the
 669 principal be authenticated. The principal authenticates to the identity provider using the same X.509
 670 credential used to construct the query.

667 **2. Attribute Response**

668 In step 2, after verifying that the principal is a valid requester, the identity provider issues a
 669 `<samlp:Response>` message containing appropriate attributes. The attributes returned to the
 670 principal are subject to policy at the identity provider.

669 **3. Service Request**

670 In step 3, the principal requests a secured resource at the service provider. The principal presents the
 671 assertion obtained at step 2 to the service provider. The service provider requires that the principal be
 672 authenticated. The principal authenticates to the service provider using the same X.509 credential
 673 used to authenticate to the identity provider at step 1.

671 **4. Service Response**

672 In step 4, based on the attributes in the pushed assertion, the service provider returns the requested
 673 resource or an error, subject to policy.

673 Of the sequence of steps described above, it is steps 1 and 2 that are profiled in sections 4.3 and 4.4 of
 674 this deployment profile.

674 **4.2 Required Information**

675 **Identification:**

676 `urn:oasis:names:tc:SAML:2.0:profiles:query:attribute:X509-self`

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

677 **Description:** Given below.

678 **Updates:** N/A

679 **Extends:** SAML Attribute Query Deployment Profile for X.509 Subjects (section 3)

680 **4.3 Profile Description**

681 This deployment profile extends the SAML Attribute Query Deployment Profile for X.509 Subjects
682 described in section 3.3.

682 As outlined in section 4.1, a principal sends a SAML V2.0 `<samlp:AttributeQuery>` message directly
683 to an identity provider. The principal authenticates to the identity provider using an X.509 identity
684 certificate. If the identity provider receiving the request can:

- 683 • recognize the name identifier; and
- 684 • determine that the requester is the principal; and
- 685 • fulfill the request subject to any applicable policies;

686 the identity provider responds with a successful `<samlp:Response>` containing the relevant attributes for
687 the principal. To determine that the requester is the principal, the identity provider MUST authenticate the
688 principal.

687 **4.3.1 `<samlp:AttributeQuery>` Issued by Principal**

688 To initiate the profile, the principal uses a synchronous binding such as the SAML SOAP Binding
689 [SAMLBind] to send a SAML V2.0 `<samlp:AttributeQuery>` message as described in section 3.3.
690 The principal uses information obtained from its X.509 identity certificate to construct the query. The
691 principal MUST authenticate itself to the identity provider using the same X.509 credential used to
692 construct the query. SSL 3.0 [SSL3] or TLS 1.0 [RFC2246] with client authentication MAY be used for this
693 purpose and to provide integrity protection and confidentiality.

689 **4.3.2 `<samlp:Response>` Issued by Identity Provider**

690 The identity provider MUST process the request as outlined in section 3.3.

691 **4.4 Use of SAML Request-Response Protocol**

692 As required by the Assertion Query/Request Profile [SAMLProf], the `<samlp:AttributeQuery>`
693 element MUST contain a `<saml:Issuer>` element. Since the requester is the principal, the
694 `<saml:Issuer>` element MUST be identical to the `<saml:NameID>` element, that is, both MUST satisfy
695 the rules of the X.509 SAML Subject Profile (section 2).

693 **4.4.1 `<samlp:AttributeQuery>` Usage**

694 The request MUST contain a `<samlp:AttributeQuery>` element that conforms to the rules of
695 section 3.4.1.

695 **4.4.2 `<samlp:Response>` Usage**

696 If the request is successful, the `<samlp:Response>` element MUST conform to the rules of section 3.4.2
697 except as noted below:

- 697 • The `<saml:Subject>` element MUST contain a `<saml:SubjectConfirmation>` element

698 whose Method attribute has value "urn:oasis:names:tc:SAML:2.0:cm:holder-of-key".

- 699 • A <saml:SubjectConfirmationData> element MUST be present and it MUST contain a
700 <ds:KeyInfo> element that refers to the principal's X.509 identity certificate.
- 700 • On the <saml:Conditions> element, the value of the NotBefore attribute (resp., the
701 NotOnOrAfter attribute) MUST be greater than or equal to (resp., less than or equal to) the
702 NotBefore field (resp., the NotOnOrAfter field) of the certificate.
- 701 • The <saml:Assertion> element MUST be signed.
- 702 • The <saml:Assertion> element MAY include a <saml:AuthnStatement> element.

703 4.4.3 Processing Rules

704 In addition to the assertion processing rules outlined in [SAMLCore], the service provider MUST verify the
705 following:

- 705 • The <saml:SubjectConfirmationData> element MUST be present and it MUST contain a
706 <ds:KeyInfo> element that refers to the principal's X.509 identity certificate.
- 706 • The value of the NotBefore attribute (resp., the NotOnOrAfter attribute) MUST be greater than
707 or equal to (resp., less than or equal to) the NotBefore field (resp., the NotOnOrAfter field) of
708 the certificate.

707 The certificate referred to in the above processing rules MUST be the same certificate used to construct
708 the <saml:Subject> of the query.

708 4.5 Example

709 For example, the principal issues the following attribute query:

```
710 <samlp:AttributeQuery
711   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
712   xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
713   ID="aaf23196-1773-2113-474a-fe114412ab72"
714   Version="2.0"
715   IssueInstant="2006-07-17T20:31:40Z">
716   <saml:Issuer
717     Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
718     C=US, O=NCSA-TEST, OU=User, CN=trscavo@uiuc.edu
719   </saml:Issuer>
720   <saml:Subject>
721     <saml:NameID
722       Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
723       C=US, O=NCSA-TEST, OU=User, CN=trscavo@uiuc.edu
724     </saml:NameID>
725   </saml:Subject>
726   <saml:Attribute
727     NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
728     Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
729     FriendlyName="eduPersonPrincipalName">
730   </saml:Attribute>
731   <saml:Attribute
732     NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
733     Name="urn:oid:2.5.4.42"
734     FriendlyName="givenName">
735   </saml:Attribute>
736   <saml:Attribute
737     NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
738     Name="urn:oid:2.5.4.4"
739     FriendlyName="sn">
740   </saml:Attribute>
741   <saml:Attribute
```

```

742     NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
743     Name="urn:oid:1.3.6.1.4.1.1466.115.121.1.26"
744     FriendlyName="mail">
745   </saml:Attribute>
746 </samlp:AttributeQuery>

```

747 After processing the request, the identity provider issues a response containing an assertion such as the
 748 one listed below. Note that the assertion was obtained by a principal who authenticated to an identity
 749 provider via TLS [RFC2246] client authentication, as indicated in the <saml:AuthnStatement>
 750 element.

```

748 <!-- SAML Assertion for an X.509 Subject -->
749 <saml:Assertion
750   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
751   xmlns:xs="http://www.w3.org/2001/XMLSchema"
752   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
753   xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
754   ID="_33776a319493ad607b7ab3e689482e45"
755   Version="2.0"
756   IssueInstant="2006-07-17T20:31:41Z">
757   <saml:Issuer>https://idp.example.org/saml</saml:Issuer>
758   <ds:Signature>...</ds:Signature>
759   <saml:Subject>
760     <saml:NameID
761       Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
762       C=US, O=NCSA-TEST, OU=User, CN=trscavo@uiuc.edu
763     </saml:NameID>
764     <saml:SubjectConfirmation
765       Method="urn:oasis:names:tc:SAML:2.0:cm:holder-of-key">
766       <saml:SubjectConfirmationData
767         <ds:KeyInfo>
768           <ds:X509Data>
769             <!-- principal's X.509 cert -->
770             <ds:X509Certificate>
771 MIIcDiCCAXACCQDE+9eiWrm62jANBgkqhkiG9w0BAQQFADBFMQswCQYDVQOGEwJV
772 UzESMBAGA1UEChMJTkNTQS1URVNUMQ0wCwYDVQOLEwRvc2VYMRMwEQYDVQOQDEwPT
773 UC1TZXJ2aWNlMB4XDTA2MDcxNzIwMjE0MVoXDTA2MDcxODIwMjE0MVoVszELMAkG
774 A1UEBhmCVVMxEjAQBgNVBAoTCU5DU0EtVEVTVDENMASGA1UECXMVXN1cjEzMBCG
775 A1UEAwwQdHJzY2F2b0B1aXVjLmVkdTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkC
776 gYEAyv9QMe4lRl3XbWPcflbCjGK9gty6zBJmp+tsaJINM0VaBaZ3t+tSXknelYife
777 nCc2O3yaX76aq53QMxy+5wkQYe8Rzdw28Nv3a73wffjXJXoUhGkvERcscs9EfIWCc
778 g2bH0g8uSh+Fbv3lHih4lBJ5MCS2buJfsR7dlr/xsadU2RcCAWEAATANBgkqhkiG
779 9w0BAQQFAAOCAQEAadyIcMTob7TVkelFJ7+I1j0LO24UlKvbLzd2OPvcFTcV6fVHx
780 Ejk0QxaZXJhreZ6+rIdiMXrEz1RdJESNMxtDW8++sVp6avoB5EX1y3ez+CEAIL4g
781 cJvKZUR4dMryWshWIBHKFFul+r7urUgvWI12KbMeE9KP+kiiiiTskLcKgfzngw1J
782 selmHhTcTcRcdocn5yO2+d3dog52vS0tVFDbsBuvDixO2hv679JR6Hlqjtk4GExp
783 E9iVI0wdPE038uQIJJTXlhsMMLvUGVh/c0ReJbn92Vj4dI/yy6PtY/8ncYLYNkjg
784 oVN0J/ymOktn9lTlFyTiuY4OuJsZR01+zWLy9g==
785           </ds:X509Certificate>
786         </ds:X509Data>
787       </ds:KeyInfo>
788     </saml:SubjectConfirmationData>
789   </saml:SubjectConfirmation>
790 </saml:Subject>
791 <!-- assertion lifetime constrained by principal's X.509 cert -->
792 <saml:Conditions
793   NotBefore="2006-07-17T20:31:41Z"
794   NotOnOrAfter="2006-07-18T20:21:41Z">
795 </saml:Conditions>
796 <saml:AuthnStatement
797   AuthnInstant="2006-07-17T20:31:41Z">
798   <saml:AuthnContext>
799     <saml:AuthnContextClassRef>
800       urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient
801     </saml:AuthnContextClassRef>
802   </saml:AuthnContext>
803 </saml:AuthnStatement>

```

```

804 <saml:AttributeStatement>
805   <saml:Attribute
806     xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
807     x500:Encoding="LDAP"
808     NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
809     Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
809     FriendlyName="eduPersonPrincipalName">
810     <saml:AttributeValue xsi:type="xs:string">
810       trscavo@uiuc.edu
811     </saml:AttributeValue>
812   </saml:Attribute>
813   <saml:Attribute
814     xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
815     x500:Encoding="LDAP"
816     NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
817     Name="urn:oid:2.5.4.42"
817     FriendlyName="givenName">
818     <saml:AttributeValue xsi:type="xs:string">
818       Tom
819     </saml:AttributeValue>
820   </saml:Attribute>
821   <saml:Attribute
822     xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
823     x500:Encoding="LDAP"
824     NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
825     Name="urn:oid:2.5.4.4"
825     FriendlyName="sn">
826     <saml:AttributeValue xsi:type="xs:string">
826       Scavo
827     </saml:AttributeValue>
828   </saml:Attribute>
829   <saml:Attribute
830     xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
831     x500:Encoding="LDAP"
832     NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
833     Name="urn:oid:1.3.6.1.4.1.1466.115.121.1.26"
833     FriendlyName="mail">
834     <saml:AttributeValue xsi:type="xs:string">
834       trscavo@gmail.com
835     </saml:AttributeValue>
836   </saml:Attribute>
837 </saml:AttributeStatement>
838 </saml:Assertion>

```

839 The attributes in the above example (eduPersonPrincipalName, givenName, sn, and mail) conform
840 to the MACE-Dir Attribute Profile for SAML 2.0 [MACEAttrib] and are for illustration purposes only.

840 4.6 Use of Metadata

841 As outlined in section 3.8, the use of SAML V2.0 metadata [SAMLMeta] is RECOMMENDED, but since a
842 principal is not expected to publish metadata about itself, only the use of identity provider metadata is
843 profiled below. Note, however, that the principal may wield a client that relies on service provider metadata
844 (see, e.g., section 4.8.1), in which case the rules in section 3.8.2 apply as well.

842 4.6.1 Identity Provider Metadata

843 An identity provider that uses SAML V2.0 metadata MUST include an
844 <md:AttributeAuthorityDescriptor> element that satisfies the rules given in section 3.8.1, except
845 that in this case the identity provider uses XML attribute supportsX509SelfQuery instead of
846 supportsX509Query [X509Query-XSD]:

```
844 <xsi:attribute
```

845 `name="supportsX509SelfQuery" type="boolean" use="optional"/>`

846 As before, use of this attribute is OPTIONAL.

847 An example of identity provider metadata follows:

```
848 <!-- An Identity Provider supporting both deployment profiles -->
849 <md:EntityDescriptor
850   xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
851   entityID="https://idp.example.org/saml">
852
853   <md:AttributeAuthorityDescriptor
854     protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
855
856     <md:AttributeService
857       x509qry:supportsX509Query="true"
858       x509qry:supportsX509SelfQuery="true"
859       xmlns:x509qry="urn:oasis:names:tc:SAML:metadata:X509:query"
860       Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
861       Location="https://idp.example.org:8443/saml-idp/AA"/>
862
863     <md:NameIDFormat>
864       urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName
865     </md:NameIDFormat>
866
867     <!-- see [MACEAttr] -->
868     <md:AttributeProfile>
869       urn:mace:dir:profiles:attribute:samlv2
870     </md:AttributeProfile>
871
872   </md:AttributeAuthorityDescriptor>
873
874 </md:EntityDescriptor>
```

875 Note that this identity provider supports both X.509 attribute query deployment profiles at the same
876 endpoint location.

876 4.7 Security and Privacy Considerations

877 Except for section 3.9.2, the security and privacy considerations outlined in section 3.9 apply equally as
878 well in the case of self-query. As a further privacy measure, a principal may limit the self-query to non-
879 identity attributes (such as givenName) and push the resulting assertion to the service provider who
880 subsequently queries the identity provider for additional attributes (according to the deployment profile in
881 section 3). In this way, a service provider receives only those attributes that are actually required for
882 access.

878 4.8 Implementation Guidelines (non-normative)

879 In addition to the guidelines outlined in section 3.10, the following non-normative guidelines are provided
880 for the convenience of implementers.

880 4.8.1 Discovery

881 In the SAML Attribute Query Deployment Profile for X.509 Subjects (section 3), we encounter the problem
882 of identity provider discovery (section 3.10.1). In the case where the principal self-queries for attributes, we
883 encounter a different problem, which we call *service provider discovery*. In both cases, we assume the
884 client knows the principal's preferred identity provider, so identity provider discovery is a non-issue in the
885 case of self-queries, but in that case the client is faced with a self-query for unknown attributes.

882 If the client had access to the published metadata of potential service providers, and that metadata
883 included the attribute requirements of the service providers, the client would be able to formulate specific
884 attribute queries targeted for specific service providers.

883 | This deployment profile does not specify a particular method of service provider discovery.

884 | **5 Implementation Conformance**

885 | An implementation of this specification shall be a conforming *Extended Mode X.509 Attribute*
886 | *Query/Requester* or a conforming *Extended Mode X.509 Attribute Self-Query/Requester* (or both). An
887 | *Extended Mode X.509 Attribute Self-Query/Requester* is a functional superset of an *Extended Mode X.509*
888 | *Attribute Query/Requester*.

889 | An *Extended Mode X.509 Attribute Query/Requester* MUST conform to the normative statements in
890 | section 3. An *Extended Mode X.509 Attribute Self-Query/Requester* MUST conform to the normative
891 | statements in section 4, which includes references to normative portions of section 3.

892 **6 Acknowledgments**

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

- 894 • George Fletcher, AOL
- 895 • Hal Lockhart, BEA Systems, Inc.
- 896 • Steve Anderson, BMC Software
- 897 • Christopher Laskowski, Booz Allen Hamilton
- 898 • Rob Philpott, EMC Corporation
- 899 • Carolina Canales-Valenzuela, Ericsson
- 900 • Ashish Patel, France Telecom
- 901 • Greg Whitehead, Hewlett-Packard
- 902 • Heather Hinton, IBM
- 903 • Anthony Nadalin, IBM
- 904 • Eric Tiffany, IEEE Industry Standards and Technology Org (IEEE-ISTO)
- 905 • Scott Cantor, Internet2
- 906 • Bob Morgan, Internet2
- 907 • Tom Scavo, National Center for Supercomputing Applications (NCSA)
- 908 • Jeff Hodges, Neustar, Inc.
- 909 • Frederick Hirsch, Nokia Corporation
- 910 • Abbie Barbir, Nortel Networks Limited
- 911 • Paul Madsen, NTT Corporation
- 912 • Ari Kermaier, Oracle Corporation
- 913 • Prateek Mishra, Oracle Corporation
- 914 • Brian Campbell, Ping Identity Corporation
- 915 • Eve Maler, Sun Microsystems
- 916 • Emily Xu, Sun Microsystems
- 917 • David Staggs, Veterans Health Administration

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

- 919 • Von Welch, National Center for Supercomputing Applications (NCSA)

920

7 Revision History

<i>Document ID</i>	<i>Date</i>	<i>Committer</i>	<i>Comment</i>
D sstc-saml2-profiles-deploy-x509-draft-01	18 Dec 2006	T. Scavo	Initial draft.
D sstc-saml2-profiles-deploy-x509-draft-02	26 Mar 2007	T. Scavo	
CD sstc-saml2-profiles-deploy-x509-cd-01	07 May 2007	T. Scavo	Committee Draft
sstc-saml2-profiles-deploy-x509-cd-02	28 Aug 2007	T. Scavo	Committee Draft

921

•