



SAML V2.0 Deployment Profiles for X.509 Subjects

Committee Draft 02

28 August 2007

Specification URIs:

This Version:

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml2-profiles-deploy-x509-cd-02.html>

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml2-profiles-deploy-x509-cd-02.odt>

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml2-profiles-deploy-x509-cd-02.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>

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-02.html>

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml2-profiles-deploy-x509-cd-02.odt>

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml2-profiles-deploy-x509-cd-02.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)

Related Work:

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

Declared XML Namespace(s):

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

35 **Abstract:**

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

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
45 should send comments to the TC by using the "Send A Comment" button on the TC's
46 web page at <http://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. 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
followed) or as required to translate it into languages other than English.

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

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

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

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

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

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

Table of Contents

62		
63	1 Introduction.....	6
64	1.1 Terminology.....	6
65	1.2 Outline.....	7
66	1.3 Normative References.....	7
67	1.4 Non-Normative References.....	8
68	2 X.509 SAML Subject Profile.....	9
69	2.1 Required Information.....	9
70	2.2 Profile Description.....	9
71	2.3 <saml:Subject> Usage.....	9
72	2.3.1 <saml:NameID> Usage.....	9
73	2.3.2 <saml:EncryptedID> Usage.....	9
74	2.4 Example.....	10
75	3 SAML Attribute Query Deployment Profile for X.509 Subjects.....	11
76	3.1 Profile Overview (non-normative).....	11
77	3.2 Required Information.....	12
78	3.3 Profile Description.....	13
79	3.3.1 <samlp:AttributeQuery> Issued by Service Provider.....	13
80	3.3.2 <samlp:Response> Issued by Identity Provider.....	13
81	3.4 Use of SAML Request-Response Protocol.....	14
82	3.4.1 <samlp:AttributeQuery> Usage.....	14
83	3.4.2 <samlp:Response> Usage.....	14
84	3.5 Example.....	15
85	3.6 Use of Encryption.....	16
86	3.7 Use of Digital Signatures.....	17
87	3.8 Use of Metadata.....	17
88	3.8.1 Identity Provider Metadata.....	17
89	3.8.2 Service Provider Metadata.....	18
90	3.9 Security and Privacy Considerations.....	19
91	3.9.1 Background.....	19
92	3.9.2 General Security Requirements.....	19
93	3.9.3 User Privacy.....	19
94	3.10 Implementation Guidelines (non-normative).....	20
95	3.10.1 Discovery.....	20
96	3.10.2 Name Mapping.....	20
97	3.10.3 Canonicalization.....	20
98	3.10.4 Identity Provider Policy	20

99	3.10.5 Caching of Attributes	21
100	4 SAML Attribute Self-Query Deployment Profile for X.509 Subjects.....	22
101	4.1 Profile Overview (non-normative).....	22
102	4.2 Required Information.....	23
103	4.3 Profile Description.....	24
104	4.3.1 <samlp:AttributeQuery> Issued by Principal.....	24
105	4.3.2 <samlp:Response> Issued by Identity Provider.....	24
106	4.4 Use of SAML Request-Response Protocol.....	24
107	4.4.1 <samlp:AttributeQuery> Usage.....	24
108	4.4.2 <samlp:Response> Usage.....	24
109	4.4.3 Processing Rules.....	25
110	4.5 Example.....	25
111	4.6 Use of Metadata.....	27
112	4.6.1 Identity Provider Metadata.....	27
113	4.7 Security and Privacy Considerations.....	28
114	4.8 Implementation Guidelines (non-normative).....	28
115	4.8.1 Discovery.....	28
116	5 Implementation Conformance.....	30
117	6 Acknowledgments.....	31
118	7 Revision History.....	32
119		

1 Introduction

120

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

1.1 Terminology

122

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

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

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

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

127 Listings of XML schemas appear like this.

128

129 Example code listings appear like this.

130 Conventional XML namespace prefixes are used throughout the listings in this specification to stand for
131 their respective namespaces as follows, whether or not a namespace declaration is present in the
132 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].

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

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

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

134 1.2 Outline

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

140 1.3 Normative References

- 141 **[FIPS 140-2]** Security Requirements for Cryptographic Modules, May 2001. See
142 <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>
- 142 **[RFC 2119]** S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. IETF
143 RFC 2119, March 1997. See <http://www.ietf.org/rfc/rfc2119.txt>
- 143 **[RFC2246]** T. Dierks and C. Allen. *The TLS Protocol Version 1.0*. IETF RFC 2246, January
144 1999. See <http://www.ietf.org/rfc/rfc2246.txt>
- 144 **[RFC2253]** M Wahl et al. *Lightweight Directory Access Protocol (v3): UTF-8 String
145 Representation of Distinguished Names*. IETF RFC 2253, December 1997. See
146 <http://www.ietf.org/rfc/rfc2253.txt>
- 145 **[RFC3280]** R. Housley et al. *Internet X.509 Public Key Infrastructure: Certificate and
146 Certificate Revocation List (CRL) Profile*. IETF RFC 3280, April 2002. See
147 <http://www.ietf.org/rfc/rfc3280.txt>
- 146 **[SAMLBind]** S. Cantor et al. *Bindings for the OASIS Security Assertion Markup Language
147 (SAML) V2.0*. OASIS Standard, March 2005. See [http://docs.oasis-
148 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)
- 147 **[SAMLCore]** S. Cantor et al. *Assertions and Protocols for the OASIS Security Assertion
148 Markup Language (SAML) V2.0*. OASIS Standard, March 2005. See
149 <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>
- 148 **[SAMLMeta]** S. Cantor et al. *Metadata for the OASIS Security Assertion Markup Language
149 (SAML) V2.0*. OASIS Standard, March 2005. See [http://docs.oasis-
150 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)
- 149 **[SAMLMeta-Ext]** T. Scavo and S. Cantor. *Metadata Extension for SAML V2.0 and V1.x Query
150 Requesters*. OASIS Draft, September 2006. Document ID sstc-saml-metadata-
151 ext-query-cd-02. See [http://docs.oasis-open.org/security/saml/SpecDrafts-
152 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)
- 150 **[SAMLProf]** S. Cantor et al. *Profiles for the OASIS Security Assertion Markup Language*

151		(SAML) V2.0. OASIS Standard, March 2005. See http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf
152		
152	[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/
153		
154		
153	[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
154		
154	[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
155		
155	[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/
156		
156	[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
157		
157	[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-xmldsig-core-20020212/
158		
158	[XMLSig-XSD]	<i>Schema for XML Signatures</i> . World Wide Web Consortium Recommendation, February 2002. See http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/xmldsig-core-schema.xsd
159		

159 1.4 Non-Normative References

160	[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
161		
162		
161	[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
162		
162	[SAMLASP]	R. Randall et al. <i>SAML V2.0 Attribute Sharing Profile for X.509 Authentication-Based Systems</i> . OASIS Committee Draft, August 2007. Document ID sstc-saml-x509-authn-attrib-profile-cd-04.
163		
164		
165	[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
166		
166	[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
167		
168		

2 X.509 SAML Subject Profile

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

2.1 Required Information

Identification:

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

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

Description: Given below.

Updates: N/A

Extends: N/A

2.2 Profile Description

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

2.3 `<saml:Subject>` Usage

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

2.3.1 `<saml:NameID>` Usage

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

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

2.3.2 `<saml:EncryptedID>` Usage

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

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

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

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

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

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

191 2.4 Example

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

```
193 <!-- unencrypted X.509 SAML Subject -->  
194 <saml:Subject>  
195   <saml:NameID  
196     Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">  
197     C=US, O=NCSA-TEST, OU=User, CN=trscavo@uiuc.edu  
198   </saml:NameID>  
199 </saml:Subject>
```

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

```
201 <!-- encrypted X.509 SAML Subject -->  
202 <saml:Subject>  
203   <saml:EncryptedID  
204     xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">  
205     <xenc:EncryptedData  
206       Type="http://www.w3.org/2001/04/xmlenc#Element">  
207       ...  
208     </xenc:EncryptedData>  
209     <xenc:EncryptedKey  
210       Recipient="https://idp.example.org/saml">  
211       ...  
212     </xenc:EncryptedKey>  
213   </saml:EncryptedID>  
214 </saml:Subject>
```

215 3 SAML Attribute Query Deployment Profile for X.509 216 Subjects

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

217 3.1 Profile Overview (non-normative)

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

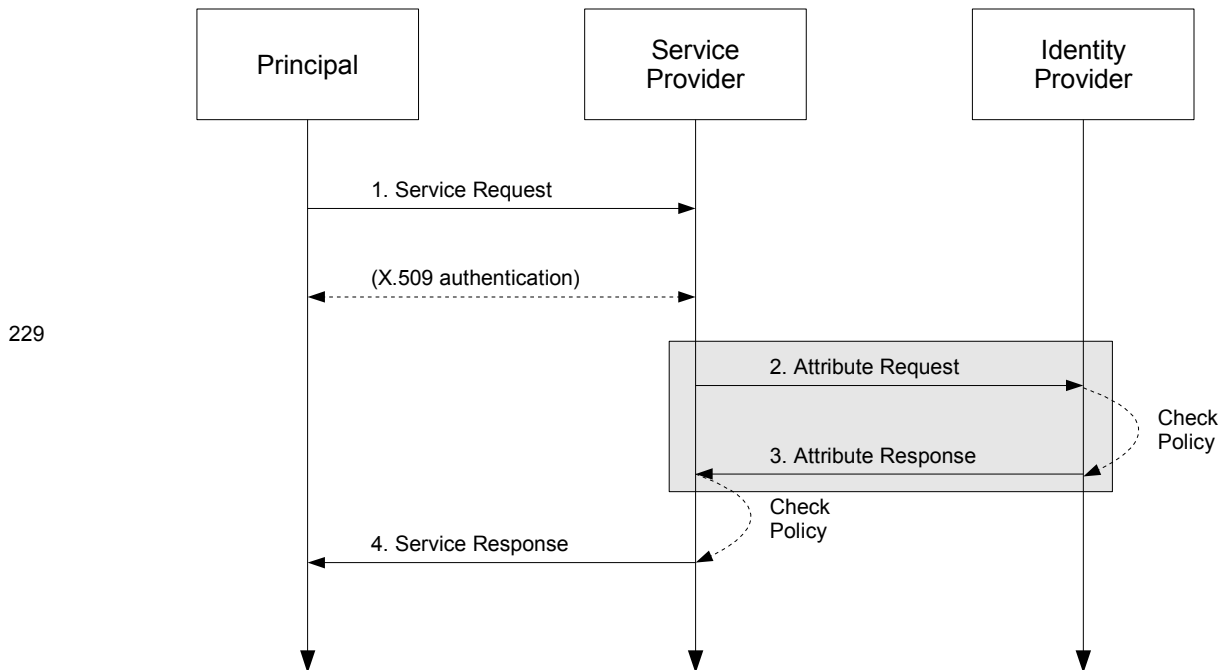
219 After the principal has been authenticated, the service provider requires additional information about the
220 principal in order to determine whether to grant access to the resource. To obtain this information, the
221 service provider uses the Subject Distinguished Name (DN) field (and perhaps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

220 This use case is based upon the following assumptions:

- 221 • A principal possesses an X.509 identity credential.
- 222 • The principal wields a client that requests a service from a service provider.
- 223 • The client can access the principal's X.509 identity credential.
- 224 • The principal has an account with a SAML identity provider.
- 225 • The service provider knows the principal's preferred identity provider and is able to query that
226 identity provider for attributes.
- 226 • The identity provider is able to map an X.509 SAML Subject (as defined in section 2 of this
227 document) to one and only one principal in its security domain. In particular, the identity provider is
228 able to map the X.509 SAML Subject that represents this principal.

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

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



229

230 **1. Service Request**

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

232 **2. Attribute Request**

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

234 **3. Attribute Response**

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

236 **4. Service Response**

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

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

239 **3.2 Required Information**

240 **Identification:**

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

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

242 **Description:** Given below.

243 **Updates:** N/A

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

245 **3.3 Profile Description**

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

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

- 248 • recognize the name identifier; and
- 249 • fulfill the request subject to any applicable policies;

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

251 **3.3.1 `<samlp:AttributeQuery>` Issued by Service Provider**

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

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

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

255 **3.3.2 `<samlp:Response>` Issued by Identity Provider**

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

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

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

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

260 3.4 Use of SAML Request-Response Protocol

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

262 3.4.1 `<samlp:AttributeQuery>` Usage

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

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

267 3.4.2 `<samlp:Response>` Usage

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

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

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

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

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

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

279 See section 3.6 for additional rules regarding encryption.

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

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

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

284 3.5 Example

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

```
286 <samlp:AttributeQuery
287   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
288   xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
289   ID="aaf23196-1773-2113-474a-fe114412ab72"
290   Version="2.0"
291   IssueInstant="2006-07-17T22:26:40Z">
292   <saml:Issuer>https://sp.example.org/saml</saml:Issuer>
293   <saml:Subject>
294     <saml:NameID
295       Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
296       C=US, O=NCSA-TEST, OU=User, CN=trscavo@uiuc.edu
297     </saml:NameID>
298   </saml:Subject>
299   <saml:Attribute
300     xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
301     x500:Encoding="LDAP"
302     NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
303     Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
304     FriendlyName="eduPersonPrincipalName">
305   </saml:Attribute>
306   <saml:Attribute
307     xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
308     x500:Encoding="LDAP"
309     NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
310     Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.1"
311     FriendlyName="eduPersonAffiliation">
312   </saml:Attribute>
313 </samlp:AttributeQuery>
```

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

```
311 <samlp:Response
312   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
313   xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
314   InResponseTo="aaf23196-1773-2113-474a-fe114412ab72"
315   ID="b07b804c-7c29-ea16-7300-4f3d6f7928ac"
316   Version="2.0"
317   IssueInstant="2006-07-17T22:26:41Z">
318   <saml:Issuer>https://idp.example.org/saml</saml:Issuer>
319   <samlp:Status>
320     <samlp:StatusCode
321       Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
322   </samlp:Status>
323   <saml:Assertion
324     xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
325     xmlns:xs="http://www.w3.org/2001/XMLSchema"
326     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
327     xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
328     ID="a144e8f3-adad-594a-9649-924517abe933">
```

```

329     Version="2.0"
330     IssueInstant="2006-07-17T22:26:41Z">
331     <saml:Issuer>https://idp.example.org/saml</saml:Issuer>
332     <saml:Subject>
333         <saml:NameID
334             Format="urn:oasis:names:tc:SAML:1.1:nameid-
335 format:X509SubjectName">
336             C=US, O=NCSA-TEST, OU=User, CN=trscavo@uiuc.edu
337         </saml:NameID>
338     </saml:Subject>
339     <!-- assertion lifetime constrained by principal's X.509 cert -->
340     <saml:Conditions
341         NotBefore="2006-07-17T22:21:41Z"
342         NotOnOrAfter="2006-07-17T22:51:41Z">
343         <saml:AudienceRestriction>
344             <saml:Audience>https://sp.example.org/saml</saml:Audience>
345         </saml:AudienceRestriction>
346     </saml:Conditions>
347     <saml:AttributeStatement>
348         <saml:Attribute
349             xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
350             x500:Encoding="LDAP"
351             NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
352             Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
353             FriendlyName="eduPersonPrincipalName">
354             <saml:AttributeValue xsi:type="xs:string">
355                 trscavo@uiuc.edu
356             </saml:AttributeValue>
357         </saml:Attribute>
358         <saml:Attribute
359             xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
360             x500:Encoding="LDAP"
361             NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
362             Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.1"
363             FriendlyName="eduPersonAffiliation">
364             <saml:AttributeValue xsi:type="xs:string">
365                 member
366             </saml:AttributeValue>
367             <saml:AttributeValue xsi:type="xs:string">
368                 staff
369             </saml:AttributeValue>
370         </saml:Attribute>
371     </saml:AttributeStatement>
372     </saml:Assertion>
373 </saml:Response>

```

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

370 3.6 Use of Encryption

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

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

373 3.7 Use of Digital Signatures

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

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

376 3.8 Use of Metadata

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

378 3.8.1 Identity Provider Metadata

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

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

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

```
384 <xs:attribute  
385 name="supportsX509Query" type="boolean" use="optional"/>
```

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

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

389 An example of identity provider metadata follows:

```
390 <!-- An Identity Provider supporting this deployment profile -->  
391 <md:EntityDescriptor  
392 xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"  
393 entityID="https://idp.example.org/saml">  
394  
395 <md:AttributeAuthorityDescriptor  
396 protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">  
397
```

```

398     <md:AttributeService
399         x509qry:supportsX509Query="true"
400         xmlns:x509qry="urn:oasis:names:tc:SAML:metadata:X509:query"
401         Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
402         Location="https://idp.example.org:8443/saml-idp/AA"/>
403
404     <md:NameIDFormat>
405         urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName
406     </md:NameIDFormat>
407
408     <!-- see [MACEAttr] -->
409     <md:AttributeProfile>
410         urn:mace:dir:profiles:attribute:samlv2
411     </md:AttributeProfile>
412
413 </md:AttributeAuthorityDescriptor>
414
415 </md:EntityDescriptor>

```

416 3.8.2 Service Provider Metadata

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

- 419 • The containing `<md:EntityDescriptor>` element **MUST** have an `entityID` attribute whose
420 value is the same unique identifier used as the `<saml:Issuer>` element in attribute queries
421 issued by the service provider.
- 422 • The type of the `<md:RoleDescriptor>` element **MUST** be derived from type
423 **query:AttributeQueryDescriptorType** [SAMLMeta-Ext].
- 424 • The `<md:RoleDescriptor>` element **MUST** include an `<md:NameIDFormat>` element with
425 value "urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName".
- 426 • One or more `<md:RequestedAttribute>` elements **MAY** be included in the
427 `<md:AttributeConsumingService>` element.

428 An example of service provider metadata follows:

```

429 <!-- A Service Provider supporting this profile -->
430 <md:EntityDescriptor
431     xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
432     entityID="https://sp.example.org/saml">
433
434     <md:RoleDescriptor
435         xmlns:query="urn:oasis:names:tc:SAML:metadata:ext:query"
436         xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
437         xsi:type="query:AttributeQueryDescriptorType"
438         protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
439
440         <md:NameIDFormat>
441             urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName
442         </md:NameIDFormat>
443
444         <md:AttributeConsumingService isDefault="true" index="0">
445             <md:ServiceName xml:lang="en">
446                 Grid Service Provider
447             </md:ServiceName>
448             <md:RequestedAttribute
449                 NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
450                 Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
451                 FriendlyName="eduPersonPrincipalName">
452             </md:RequestedAttribute>
453             <md:RequestedAttribute
454                 NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
455                 Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.1"

```

```
456         FriendlyName="eduPersonAffiliation">
457         </md:RequestedAttribute>
458         </md:AttributeConsumingService>
459
460     </md:RoleDescriptor>
461
462 </md:EntityDescriptor>
```

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

466 **3.9 Security and Privacy Considerations**

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

469 **3.9.1 Background**

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

475 **3.9.2 General Security Requirements**

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

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

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

491 **3.9.3 User Privacy**

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

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

498 **3.10 Implementation Guidelines (non-normative)**

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

500 **3.10.1 Discovery**

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

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

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

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

518 **3.10.2 Name Mapping**

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

524 **3.10.3 Canonicalization**

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

532 **3.10.4 Identity Provider Policy**

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

538 **3.10.5 Caching of Attributes**

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

541 4 SAML Attribute Self-Query Deployment Profile for 542 X.509 Subjects

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

547 4.1 Profile Overview (non-normative)

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

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

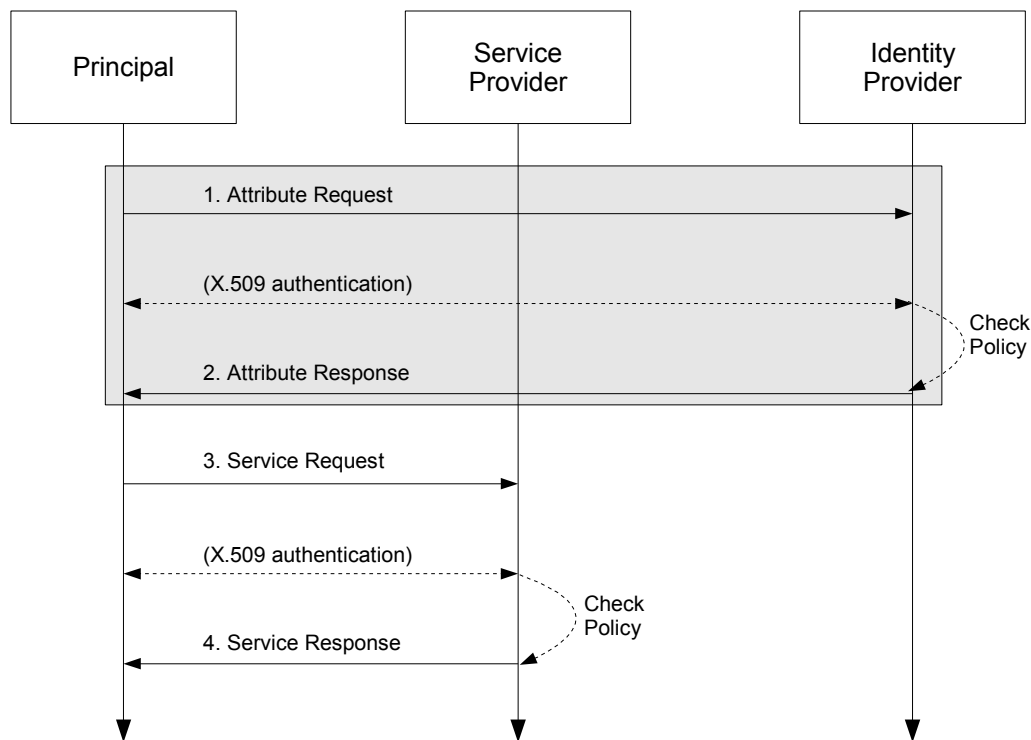
558 This use case is based on the following assumptions:

- 559 • A principal possesses an X.509 credential.
- 560 • The principal wields a client that can both query an identity provider for attributes and request a
561 service from a service provider.
- 562 • The client can access the principal's X.509 credential.
- 563 • The principal has an account with a SAML identity provider.
- 564 • The client knows the principal's preferred identity provider and the attribute requirements of the
565 target service provider.
- 566 • The identity provider is able to map an X.509 SAML Subject (as defined in section 2 of this
567 document) to one and only one principal in its security domain. In particular, the identity provider is
568 able to map the X.509 SAML Subject that represents this principal.

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

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

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



574

575 **1. Attribute Request**

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

581 **2. Attribute Response**

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

585 **3. Service Request**

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

590 **4. Service Response**

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

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

595 **4.2 Required Information**

596 **Identification:**

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

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

599 **Description:** Given below.

600 **Updates:** N/A

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

602 **4.3 Profile Description**

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

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

- 608 • recognize the name identifier; and
- 609 • determine that the requester is the principal; and
- 610 • fulfill the request subject to any applicable policies;

611 the identity provider responds with a successful `<samlp:Response>` containing the relevant attributes for
612 the principal. To determine that the requester is the principal, the identity provider **MUST** authenticate the
613 principal.

614 **4.3.1 `<samlp:AttributeQuery>` Issued by Principal**

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

621 **4.3.2 `<samlp:Response>` Issued by Identity Provider**

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

623 **4.4 Use of SAML Request-Response Protocol**

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

628 **4.4.1 `<samlp:AttributeQuery>` Usage**

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

631 **4.4.2 `<samlp:Response>` Usage**

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

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

- 635 whose Method attribute has value "urn:oasis:names:tc:SAML:2.0:cm:holder-of-key".
- 636 • A <saml:SubjectConfirmationData> element MUST be present and it MUST contain a
 - 637 <ds:KeyInfo> element that refers to the principal's X.509 identity certificate.
 - 638 • On the <saml:Conditions> element, the value of the NotBefore attribute (resp., the
 - 639 NotOnOrAfter attribute) MUST be greater than or equal to (resp., less than or equal to) the
 - 640 NotBefore field (resp., the NotOnOrAfter field) of the certificate.
 - 641 • The <saml:Assertion> element MUST be signed.
 - 642 • The <saml:Assertion> element MAY include a <saml:AuthnStatement> element.

643 4.4.3 Processing Rules

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

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

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

653 4.5 Example

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

```
655 <samlp:AttributeQuery
656   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
657   xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
658   ID="aaf23196-1773-2113-474a-fe114412ab72"
659   Version="2.0"
660   IssueInstant="2006-07-17T20:31:40Z">
661   <saml:Issuer
662     Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
663     C=US, O=NCSA-TEST, OU=User, CN=trscavo@uiuc.edu
664   </saml:Issuer>
665   <saml:Subject>
666     <saml:NameID
667       Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
668       C=US, O=NCSA-TEST, OU=User, CN=trscavo@uiuc.edu
669     </saml:NameID>
670   </saml:Subject>
671   <saml:Attribute
672     NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
673     Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
674     FriendlyName="eduPersonPrincipalName">
675   </saml:Attribute>
676   <saml:Attribute
677     NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
678     Name="urn:oid:2.5.4.42"
679     FriendlyName="givenName">
680   </saml:Attribute>
681   <saml:Attribute
682     NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
683     Name="urn:oid:2.5.4.4"
684     FriendlyName="sn">
685   </saml:Attribute>
686   <saml:Attribute
```



```

752 <saml:AttributeStatement>
753   <saml:Attribute
754     xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
755     x500:Encoding="LDAP"
756     NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
757     Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
758     FriendlyName="eduPersonPrincipalName">
759     <saml:AttributeValue xsi:type="xs:string">
760       trscavo@uiuc.edu
761     </saml:AttributeValue>
762   </saml:Attribute>
763   <saml:Attribute
764     xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
765     x500:Encoding="LDAP"
766     NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
767     Name="urn:oid:2.5.4.42"
768     FriendlyName="givenName">
769     <saml:AttributeValue xsi:type="xs:string">
770       Tom
771     </saml:AttributeValue>
772   </saml:Attribute>
773   <saml:Attribute
774     xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
775     x500:Encoding="LDAP"
776     NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
777     Name="urn:oid:2.5.4.4"
778     FriendlyName="sn">
779     <saml:AttributeValue xsi:type="xs:string">
780       Scavo
781     </saml:AttributeValue>
782   </saml:Attribute>
783   <saml:Attribute
784     xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
785     x500:Encoding="LDAP"
786     NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
787     Name="urn:oid:1.3.6.1.4.1.1466.115.121.1.26"
788     FriendlyName="mail">
789     <saml:AttributeValue xsi:type="xs:string">
790       trscavo@gmail.com
791     </saml:AttributeValue>
792   </saml:Attribute>
793 </saml:AttributeStatement>
794 </saml:Assertion>

```

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

797 4.6 Use of Metadata

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

802 4.6.1 Identity Provider Metadata

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

```
807 <xs:attribute
```

808 name="supportsX509SelfQuery" type="boolean" use="optional"/>

809 As before, use of this attribute is OPTIONAL.

810 An example of identity provider metadata follows:

```
811 <!-- An Identity Provider supporting both deployment profiles -->
812 <md:EntityDescriptor
813   xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
814   entityID="https://idp.example.org/saml">
815
816   <md:AttributeAuthorityDescriptor
817     protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
818
819     <md:AttributeService
820       x509qry:supportsX509Query="true"
821       x509qry:supportsX509SelfQuery="true"
822       xmlns:x509qry="urn:oasis:names:tc:SAML:metadata:X509:query"
823       Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
824       Location="https://idp.example.org:8443/saml-idp/AA"/>
825
826     <md:NameIDFormat>
827       urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName
828     </md:NameIDFormat>
829
830     <!-- see [MACEAttr] -->
831     <md:AttributeProfile>
832       urn:mace:dir:profiles:attribute:samlv2
833     </md:AttributeProfile>
834
835   </md:AttributeAuthorityDescriptor>
836
837 </md:EntityDescriptor>
```

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

840 4.7 Security and Privacy Considerations

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

847 4.8 Implementation Guidelines (non-normative)

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

850 4.8.1 Discovery

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

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

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

860 **5 Implementation Conformance**

861 An implementation of this specification shall be a conforming *Extended Mode X.509 Attribute*
862 *Query/Requester* or a conforming *Extended Mode X.509 Attribute Self-Query/Requester* (or both). An
863 Extended Mode X.509 Attribute Self-Query/Requester is a functional superset of an Extended Mode X.509
864 Attribute Query/Requester.

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

868 **6 Acknowledgments**

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

- 871 • George Fletcher, AOL
- 872 • Hal Lockhart, BEA Systems, Inc.
- 873 • Steve Anderson, BMC Software
- 874 • Christopher Laskowski, Booz Allen Hamilton
- 875 • Rob Philpott, EMC Corporation
- 876 • Carolina Canales-Valenzuela, Ericsson
- 877 • Ashish Patel, France Telecom
- 878 • Greg Whitehead, Hewlett-Packard
- 879 • Heather Hinton, IBM
- 880 • Anthony Nadalin, IBM
- 881 • Eric Tiffany, IEEE Industry Standards and Technology Org (IEEE-ISTO)
- 882 • Scott Cantor, Internet2
- 883 • Bob Morgan, Internet2
- 884 • Tom Scavo, National Center for Supercomputing Applications (NCSA)
- 885 • Jeff Hodges, Neustar, Inc.
- 886 • Frederick Hirsch, Nokia Corporation
- 887 • Abbie Barbir, Nortel Networks Limited
- 888 • Paul Madsen, NTT Corporation
- 889 • Ari Kermaier, Oracle Corporation
- 890 • Prateek Mishra, Oracle Corporation
- 891 • Brian Campbell, Ping Identity Corporation
- 892 • Eve Maler, Sun Microsystems
- 893 • Emily Xu, Sun Microsystems
- 894 • David Staggs, Veterans Health Administration

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

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

7 Revision History

<i>Document ID</i>	<i>Date</i>	<i>Committer</i>	<i>Comment</i>
sstc-saml2-profiles-deploy-x509-draft-01	18 Dec 2006	T. Scavo	Initial draft.
sstc-saml2-profiles-deploy-x509-draft-02	26 Mar 2007	T. Scavo	
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

•