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

Committee Specification 01

27 March 2008

Specification URIs:

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

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

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

Technical Committee:
> OASIS Security Services TC

Chair(s):
> Hal Lockhart, BEA Systems, Inc.
> Brian Campbell, Ping Identity Corporation

Editor(s):
> Eve Maler, Sun Microsystems
> Rob Philpott, EMC
> Tom Scavo, National Center for Supercomputing Applications (NCSA)
> Ari Kermaier, Oracle

Contributor(s):
> Scott Cantor, Internet2
> Paul Madsen, NTT Corporation

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

Declared XML Namespace(s):

N/A

Abstract:

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

Status:

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

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

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

The non-normative errata page for this specification is located at http://www.oasis-open.org/committees/security.

Notices

Table of Contents

1 Introduction

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

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

1.1 Notation

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

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

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

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

```
Listings of XML schemas appear like this.

Example code listings appear like this.
```

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

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

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

1.2 Terminology

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

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

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

1.3 Outline

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

1.4 Normative References

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

1.5 Non-Normative References

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

208 (SAML) V2.0. OASIS Standard, March 2005. See http://docs.oasis-
209 open.org/security/saml/v2.0/saml-glossary-2.0-os.pdf

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

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

215 2 Use Cases

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

218 2.1.1 Overview

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

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

228 2.1.2 Sequence

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

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

232

233
234   1. **Service Request**
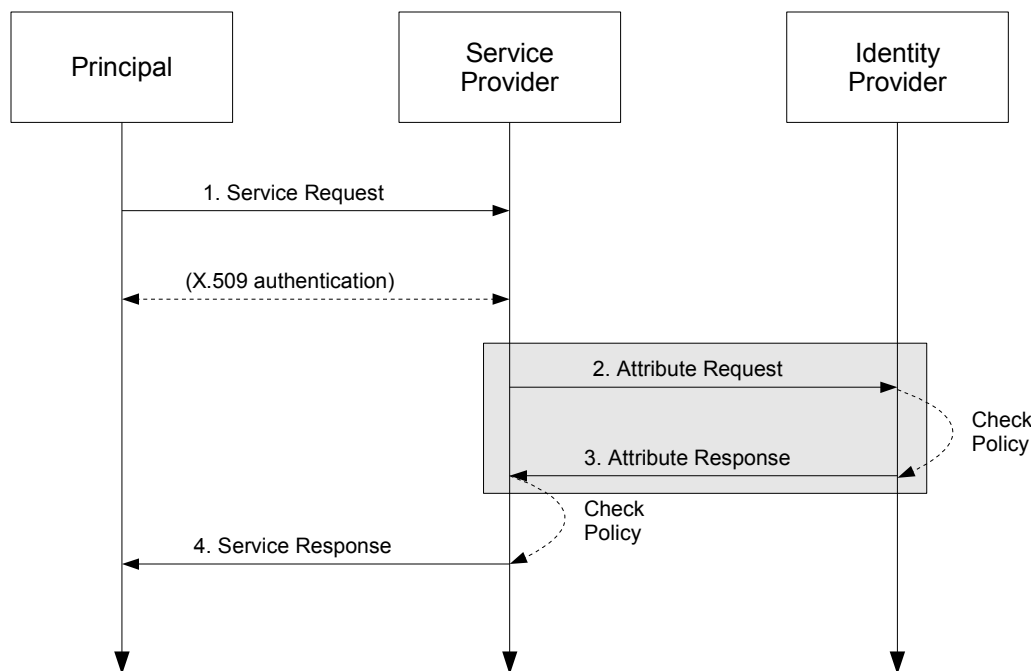
235   In step 1, the principal requests a secured resource from a service provider who requires that the
236   principal be authenticated. The principal authenticates to the service provider with an X.509 identity
237   certificate. The details of this step are out of scope for this deployment profile.

238   2. **Attribute Request**

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

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

3. **Attribute Response**

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

4. Service Response

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

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

3 Basic Mode

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

If the identity provider receiving the request can:

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

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

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

3.1 Required Information

Identification:

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

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

Description: Given below.

Updates: N/A

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

3.2 <samlp:AttributeQuery> Issued by Service Provider

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

3.2.1 <samlp:AttributeQuery> Usage

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

- The `<saml:Subject>` element must contain a `<saml:NameID>` element whose value is the Subject 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, as defined in section 8.3.3 of [SAMLCore].

3.3 <samlp:Response> Issued by Identity Provider

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

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

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

3.3.1 <samlp:Response> Usage

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

292   • Any `<saml:Assertion>` element(s) MUST satisfy the following conditions:

293
294
295   • The `<saml:Assertion>` element MUST contain at least one `<saml:AttributeStatement>` element that conveys the attributes of the principal to the service provider.

296
297   • The `<saml:Assertion>` element MUST contain an `<saml:AudienceRestriction>` element that includes the service provider's unique identifier as an `<saml:Audience>`.

298
299   • Other conditions (and other `<saml:Audience>` elements) MAY be included as requested by the service provider or at the discretion of the identity provider.

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

3.4 Use of Metadata

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

305
306   • The identity provider SHOULD use the `<md:AttributeAuthorityDescriptor>` element defined by the SAML metadata specification [SAMLMeta].

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

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

4 Encrypted Mode

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

If the identity provider receiving the request can:

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

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

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

4.1 Required Information

Identification:
> urn:oasis:names:tc:SAML:2.0:profiles:query:attribute:X509-encrypted

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

Description: Given below.

Updates: N/A

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

4.2 <samlp:AttributeQuery> Issued by Service Provider

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

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

4.2.1 <samlp:AttributeQuery> Usage

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

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

4.2.2 Use of Encryption

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

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

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

352 • The service provider generates a new symmetric key to encrypt the principal's name identifier
353   containing the Subject DN. After performing the encryption, the service provider places the resulting
354   ciphertext in the `<xenc:EncryptedData>` element. The symmetric key MUST be encrypted with
355   the identity provider's public key and the resulting ciphertext placed in the `<xenc:EncryptedKey>`
356   element.

357 • The service provider uses a previously established symmetric key to encrypt the principal's name
358   identifier containing the Subject DN. After performing the encryption, the service provider places the
359   resulting ciphertext in the `<xenc:EncryptedData>` element. In this case, the
360   `<saml:EncryptedID>` element MUST NOT contain an `<xenc:EncryptedKey>` element.

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

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

4.2.3 Use of Digital Signatures

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

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

4.3   <samlp:Response> Issued by Identity Provider

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

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

4.3.1 <samlp:Response> Usage

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

381 • The `<samlp:Response>` element MUST contain a `<ds:Signature>` element carrying the
382   signature of the identity provider.

383 • It MUST contain at least one `<saml:EncryptedAssertion>` element (but no
384   `<saml:Assertion>` elements).

385 • The encrypted content of each `<saml:EncryptedAssertion>` element is a
386   `<saml:Assertion>` element that MUST satisfy the following conditions, in addition to the rules of
387   section 3.3.1:

388   • The `<saml:Assertion>` element MUST contain a `<ds:Signature>` element carrying the
389   signature of the identity provider.

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

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

4.3.2 Use of Encryption

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

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

398   Exactly one of the following procedures MUST be followed:

399   • The identity provider generates a new symmetric key to encrypt the `<saml:Assertion>`. After
400   performing the encryption, the identity provider places the resulting ciphertext in the
401   `<xenc:EncryptedData>` element. The symmetric key MUST be encrypted with the service
402   provider's public key and the resulting ciphertext placed in the `<xenc:EncryptedKey>` element.

403   • The identity provider uses the symmetric key used by the service provider to encrypt the name
404   identifier. After encrypting the `<saml:Assertion>` using this key, the identity provider places the
405   resulting ciphertext in the `<xenc:EncryptedData>` element. In this case, however, the
406   `<saml:EncryptedAssertion>` element MUST NOT contain an `<xenc:EncryptedKey>`
407   element.

408   • If the service provider did not include a symmetric key in the `<samlp:AttributeQuery>` for
409   decryption of the `<saml:EncryptedID>`, the identity provider uses a previously established
410   symmetric key to encrypt the `<saml:Assertion>`. If the identity provider reuses a key in this
411   manner, the `<saml:EncryptedAssertion>` element MUST NOT contain an
412   `<xenc:EncryptedKey>` element.

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

4.3.3 Use of Digital Signatures

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

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

4.4 Use of Metadata

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

5 Security and Privacy Considerations

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

5.1 Background

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

5.2 General Security Requirements

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

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

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

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

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

5.3 User Privacy

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

6 Implementation Conformance

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

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

7 Implementation Guidance (Informative)

The following non-normative guidance is provided for implementers.

7.1 Identity Provider Policy

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

7.2 Caching of Attributes

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

486 A. Revision History

487 TBA

Document ID	Date	Committer	Comment
Draft-01	22 Jun 2004		Initial draft
Draft-02	03 Feb 2005		
sstc-saml-x509-authn-based-attribute-protocol-profile-2.0-draft-03	25 Mar 2005	R. Randall	
sstc-saml-x509-authn-based-attribute-protocol-profile-2.0-draft-04	14 Apr 2005	R. Randall	
sstc-saml-x509-authn-based-attribute-protocol-profile-2.0-draft-05	02 May 2005	R. Randall	
sstc-saml-x509-authn-based-attribute-protocol-profile-2.0-draft-06	13 May 2005	R. Randall	
sstc-saml-x509-authn-based-attribute-protocol-profile-2.0-draft-07	23 May 2005	R. Randall	
sstc-saml-x509-authn-attrib-profile-cd-01	01 Jun 2005	E. Maler	Committee Draft
sstc-saml-x509-authn-attrib-profile-draft-08	14 Mar 2006	R. Philpott	
sstc-saml-x509-authn-attrib-profile-cd-02	28 Mar 2006	R. Philpott	Committee Draft
sstc-saml-x509-authn-attrib-profile-draft-09	26 Jun 2006	T. Scavo	
sstc-saml-x509-authn-attrib-profile-draft-10	05 Jul 2006	T. Scavo	
sstc-saml-x509-authn-attrib-profile-draft-11	13 Feb 2007	A. Kermaier	
sstc-saml-x509-authn-attrib-profile-draft-12	26 Mar 2007	T. Scavo	
sstc-saml-x509-authn-attrib-profile-draft-13	12 Apr 2007	A. Kermaier	
sstc-saml-x509-authn-attrib-profile-cd-03	07 Jun 2007	T. Scavo	Committee Draft
sstc-saml-x509-authn-attrib-profile-cd-04	28 Aug 2007	T. Scavo	Committee Draft
sstc-saml-x509-authn-attrib-profile-draft-14	06 Mar 2008	T. Scavo	
sstc-saml-x509-authn-attrib-profile-cd-05	11 Mar 2008	T. Scavo	Committee Draft

B. Acknowledgments

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

- Hal Lockhart, BEA Systems, Inc.
- Rob Philpott, EMC Corporation
- Eric Tiffany, Liberty Alliance Project
- Scott Cantor, Internet2
- Bob Morgan, Internet2
- Tom Scavo, National Center for Supercomputing Applications (NCSA)
- Peter Davis, Neustar, Inc.
- Jeff Hodges, Neustar, Inc.
- Frederick Hirsch, Nokia Corporation
- Abbie Barbir, Nortel Networks Limited
- Paul Madsen, NTT Corporation
- Ari Kermaier, Oracle Corporation
- Prateek Mishra, Oracle Corporation
- Brian Campbell, Ping Identity Corporation
- Anil Saldhana, Red Hat
- Eve Maler, Sun Microsystems
- Emily Xu, Sun Microsystems
- Kent Spaulding, Tripod Technology Group, Inc.
- David Staggs, Veterans Health Administration

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

- Rick Randall, Booz Allen Hamilton
- Rebekah Metz, Booz Allen Hamilton
- Thomas Wisniewski, Entrust