SAML V2.0 Deployment Profiles for X.509 Subjects

~~Working~~Committee Draft 03

~~27 February~~11 March 2008

Specification URIs:

This Version:

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml2-profiles-deploy-x509-~~draft~~cd-03.html

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml2-profiles-deploy-x509-~~draft~~cd-03.odt

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml2-profiles-deploy-x509-~~draft~~cd-03.pdf

Previous Version:

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml2-profiles-deploy-x509-draft-03~~cd-02~~.html

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml2-profiles-deploy-x509-draft-03~~cd-02~~.odt

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml2-profiles-deploy-x509-draft-03~~cd-02~~.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

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

Abstract:

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

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

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

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical 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.

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

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

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

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

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

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

Table of Contents

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

3.10.5 Caching of Attributes 21
4 SAML Attribute Self-Query Deployment Profile for X.509 Subjects 22
4.1 Profile Overview (non-normative) 22
4.2 Required Information 23
4.3 Profile Description 24
4.3.1 <samlp:AttributeQuery> Issued by Principal 24
4.3.2 <samlp:Response> Issued by Identity Provider 24
4.4 Use of SAML Request-Response Protocol 24
4.4.1 <samlp:AttributeQuery> Usage 24
4.4.2 <samlp:Response> Usage 24
4.4.3 Processing Rules 25
4.5 Example 25
4.6 Use of Metadata 27
4.6.1 Identity Provider Metadata 27
4.7 Security and Privacy Considerations 28
4.8 Implementation Guidelines (non-normative) 28
4.8.1 Discovery 28
5 Implementation Conformance 30
6 Acknowledgments 31
7 Revision History 32

1 Introduction

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

1.1 Terminology

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

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]. 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].

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

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

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

1.2 Outline

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

1.3 Normative References

[FIPS 140-2] *Security Requirements for Cryptographic Modules*, May 2001. See http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[RFC 2119] S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. IETF RFC 2119, March 1997. See http://www.ietf.org/rfc/rfc2119.txt

[RFC2246] T. Dierks and C. Allen. *The TLS Protocol Version 1.0*. IETF RFC 2246, January 1999. See http://www.ietf.org/rfc/rfc2246.txt

[RFC2253] M. Wahl et al. *Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names*. IETF RFC 2253, December 1997. See http://www.ietf.org/rfc/rfc2253.txt

[RFC3280] R. Housley et al. *Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL)* Profile. IETF RFC 3280, April 2002. See http://www.ietf.org/rfc/rfc3280.txt

[SAMLBind] S. Cantor et al. *Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0.* OASIS Standard, March 2005. See http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf

[SAMLCore] S. Cantor et al. *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS Standard, March 2005. See http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

[SAMLMeta] S. Cantor et al. *Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS Standard, March 2005. See http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf

[SAMLMeta-Ext] T. Scavo and S. Cantor. *Metadata Extension for SAML V2.0 and V1.x Query Requesters*. OASIS Standard, November 2007. Document ID sstc-saml-metadata-ext-query-OS. See http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-ext-query-os.pdf

[SAMLProf] S. Cantor et al. *Profiles for the OASIS Security Assertion Markup Language*

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

[Schema1] H. S. Thompson et al. *XML Schema Part 1: Structures.* World Wide Web Consortium Recommendation, May 2001. See http://www.w3.org/TR/2001/REC-xmlschema-1-20010502/

[SSL3] A. Freier et al. *The SSL Protocol Version 3.0*, IETF Internet-Draft, November 1996. See http://wp.netscape.com/eng/ssl3/draft302.txt

[X509Query-XSD] *Schema for SAML V2.0 Deployment Profiles for X.509 Subjects*. OASIS, December 2006. Document ID sstc-saml-metadata-x509-query.xsd. See http://www.oasis-open.org/committees/documents.php?wg_abbrev=security

[XMLEnc] D. Eastlake et al. *XML Encryption Syntax and Processing*. World Wide Web Consortium Recommendation, December 2002. See http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/

[XMLEnc-XSD] *XML Encryption Schema*. World Wide Web Consortium Recommendation, December 2002. See http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/xenc-schema.xsd

[XMLSig] D. Eastlake et al. *XML-Signature Syntax and Processing*. World Wide Web Consortium Recommendation, February 2002. See http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/

[XMLSig-XSD] *Schema for XML Signatures*. World Wide Web Consortium Recommendation, February 2002. See http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/xmldsig-core-schema.xsd

1.4 Non-Normative References

[MACEAttrib] S. Cantor et al. *MACE-Dir SAML Attribute Profiles*. Internet2 MACE, December 2007. See http://middleware.internet2.edu/dir/docs/draft-internet2-mace-dir-saml-attributes-latest.pdf

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

[SAMLASP] R. Randall et al. *SAML V2.0 Attribute Sharing Profile for X.509 Authentication-Based Systems.* OASIS Committee Draft, August 2007. Document ID sstc-saml-x509-authn-attrib-profile-cd-04.

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

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

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

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

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

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

2.4 Example

An example of an unencrypted X.509 SAML Subject:

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

An example of an encrypted X.509 SAML Subject:

```
<!-- encrypted X.509 SAML Subject -->
<saml:Subject>
  <saml:EncryptedID
    xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
    <xenc:EncryptedData
      Type="http://www.w3.org/2001/04/xmlenc#Element">
      ...
    </xenc:EncryptedData>
    <xenc:EncryptedKey
      Recipient="https://idp.example.org/saml">
      ...
    </xenc:EncryptedKey>
  </saml:EncryptedID>
</saml:Subject>
```

3 SAML Attribute Query Deployment Profile for X.509 Subjects

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

3.1 Profile Overview (non-normative)

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

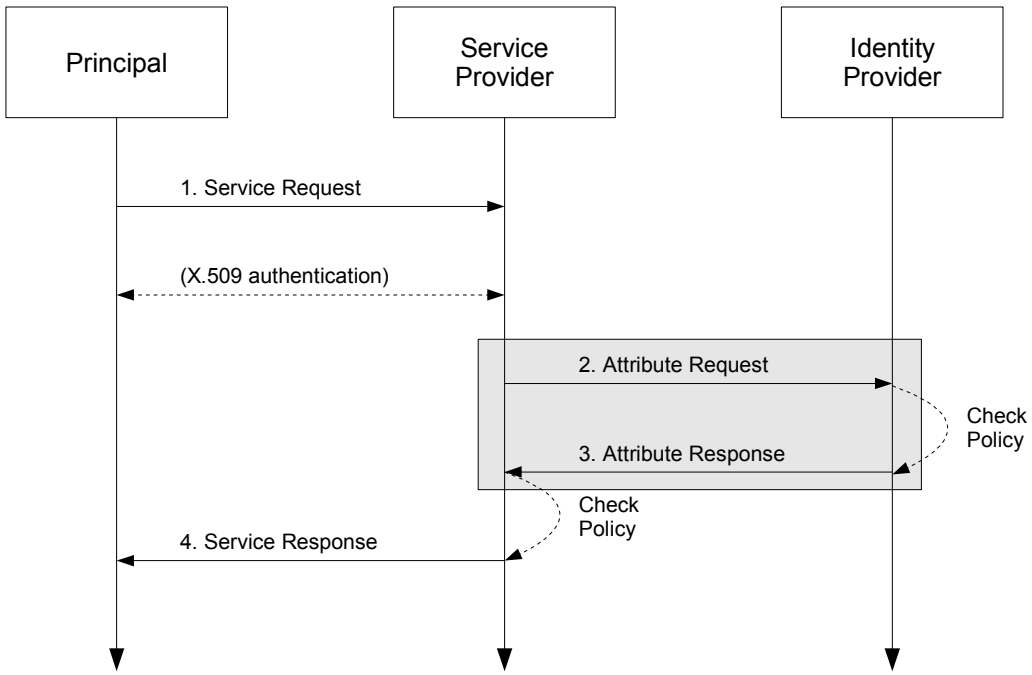
After the principal has been authenticated, the service provider requires additional information about the principal in order to determine whether to grant access to the resource. To obtain this information, the service provider uses the Subject Distinguished Name (DN) field (and perhaps other information)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

This use case is based upon the following assumptions:

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

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

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



1. **Service Request**

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

2. **Attribute Request**

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

3. **Attribute Response**

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

4. **Service Response**

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

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

3.2 Required Information

Identification:
`urn:oasis:names:tc:SAML:2.0:profiles:query:attribute:X509`

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

Description: Given below.

Updates: N/A

Extends: Assertion Query/Request Profile [SAMLProf]

3.3 Profile Description

This deployment profile 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 identity certificate. The attribute exchange MUST conform to the Assertion Query/Request Profile given in section 6 of [SAMLProf] unless otherwise specified below.

As outlined in section 3.1, a service provider sends a SAML V2.0 `<samlp:AttributeQuery>` message directly to an identity provider. This message contains a name identifier that identifies a principal who has 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.

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

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

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

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

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

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

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

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

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

3.4 Use of SAML Request-Response Protocol

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

3.4.1 <samlp:AttributeQuery> Usage

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

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

3.4.2 <samlp:Response> Usage

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

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

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

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

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

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

See section 3.6 for additional rules regarding encryption.

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

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

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

3.5 Example

For example, the requester issues the following attribute query:

```
<samlp:AttributeQuery
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  ID="aaf23196-1773-2113-474a-fe114412ab72"
  Version="2.0"
  IssueInstant="2006-07-17T22:26:40Z">
  <saml:Issuer>https://sp.example.org/saml</saml:Issuer>
  <saml:Subject>
    <saml:NameID
      Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
      CN=trscavo@uiuc.edu,OU=User,O=NCSA-TEST,C=US
    </saml:NameID>
  </saml:Subject>
  <saml:Attribute
    xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
    x500:Encoding="LDAP"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
    Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
    FriendlyName="eduPersonPrincipalName">
  </saml:Attribute>
  <saml:Attribute
    xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
    x500:Encoding="LDAP"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
    Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.1"
    FriendlyName="eduPersonAffiliation">
  </saml:Attribute>
</samlp:AttributeQuery>
```

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

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

```
    Version="2.0"
    IssueInstant="2006-07-17T22:26:41Z">
    <saml:Issuer>https://idp.example.org/saml</saml:Issuer>
    <saml:Subject>
      <saml:NameID
        Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName">
        CN=trscavo@uiuc.edu,OU=User,O=NCSA-TEST,C=US
      </saml:NameID>
    </saml:Subject>
    <saml:Conditions
      NotBefore="2006-07-17T22:21:41Z"
      NotOnOrAfter="2006-07-17T22:51:41Z">
      <saml:AudienceRestriction>
        <saml:Audience>https://sp.example.org/saml</saml:Audience>
      </saml:AudienceRestriction>
    </saml:Conditions>
    <saml:AttributeStatement>
      <saml:Attribute
        xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
        x500:Encoding="LDAP"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
        Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
        FriendlyName="eduPersonPrincipalName">
        <saml:AttributeValue xsi:type="xs:string">
          trscavo@uiuc.edu
        </saml:AttributeValue>
      </saml:Attribute>
      <saml:Attribute
        xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
        x500:Encoding="LDAP"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
        Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.1"
        FriendlyName="eduPersonAffiliation">
        <saml:AttributeValue xsi:type="xs:string">
          member
        </saml:AttributeValue>
        <saml:AttributeValue xsi:type="xs:string">
          staff
        </saml:AttributeValue>
      </saml:Attribute>
    </saml:AttributeStatement>
  </saml:Assertion>
</samlp:Response>
```

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

3.6 Use of Encryption

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

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

3.7 Use of Digital Signatures

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

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

3.8 Use of Metadata

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

3.8.1 Identity Provider Metadata

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

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

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

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

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

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

An example of identity provider metadata follows:

```
<!-- An Identity Provider supporting this deployment profile -->
<md:EntityDescriptor
  xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
  entityID="https://idp.example.org/saml">

  <md:AttributeAuthorityDescriptor
    protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">

```

```
    <md:AttributeService
      x509qry:supportsX509Query="true"
      xmlns:x509qry="urn:oasis:names:tc:SAML:metadata:X509:query"
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
      Location="https://idp.example.org:8443/saml-idp/AA"/>

    <md:NameIDFormat>
      urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName
    </md:NameIDFormat>

    <!-- see [MACEAttr] -->
    <md:AttributeProfile>
      urn:mace:dir:profiles:attribute:samlv2
    </md:AttributeProfile>

  </md:AttributeAuthorityDescriptor>

</md:EntityDescriptor>
```

3.8.2 Service Provider Metadata

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

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

An example of service provider metadata follows:

```
<!-- A Service Provider supporting this profile -->
<md:EntityDescriptor
  xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
  entityID="https://sp.example.org/saml">

  <md:RoleDescriptor
    xmlns:query="urn:oasis:names:tc:SAML:metadata:ext:query"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:type="query:AttributeQueryDescriptorType"
    protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">

    <md:NameIDFormat>
      urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName
    </md:NameIDFormat>

    <md:AttributeConsumingService isDefault="true" index="0">
      <md:ServiceName xml:lang="en">
        Grid Service Provider
      </md:ServiceName>
      <md:RequestedAttribute
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
        Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
        FriendlyName="eduPersonPrincipalName">
      </md:RequestedAttribute>
      <md:RequestedAttribute
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
        Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.1"
```

```
        FriendlyName="eduPersonAffiliation">
      </md:RequestedAttribute>
    </md:AttributeConsumingService>

  </md:RoleDescriptor>

</md:EntityDescriptor>
```

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

3.9 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.

3.9.1 Background

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

3.9.2 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 identity 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 (and other information) from the 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.

3.9.3 User Privacy

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

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

3.10 Implementation Guidelines (non-normative)

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

3.10.1 Discovery

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

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

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

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

3.10.2 Name Mapping

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

3.10.3 Canonicalization

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

3.10.4 Identity Provider Policy

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

3.10.5 Caching of Attributes

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

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

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

4.1 Profile Overview (non-normative)

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

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

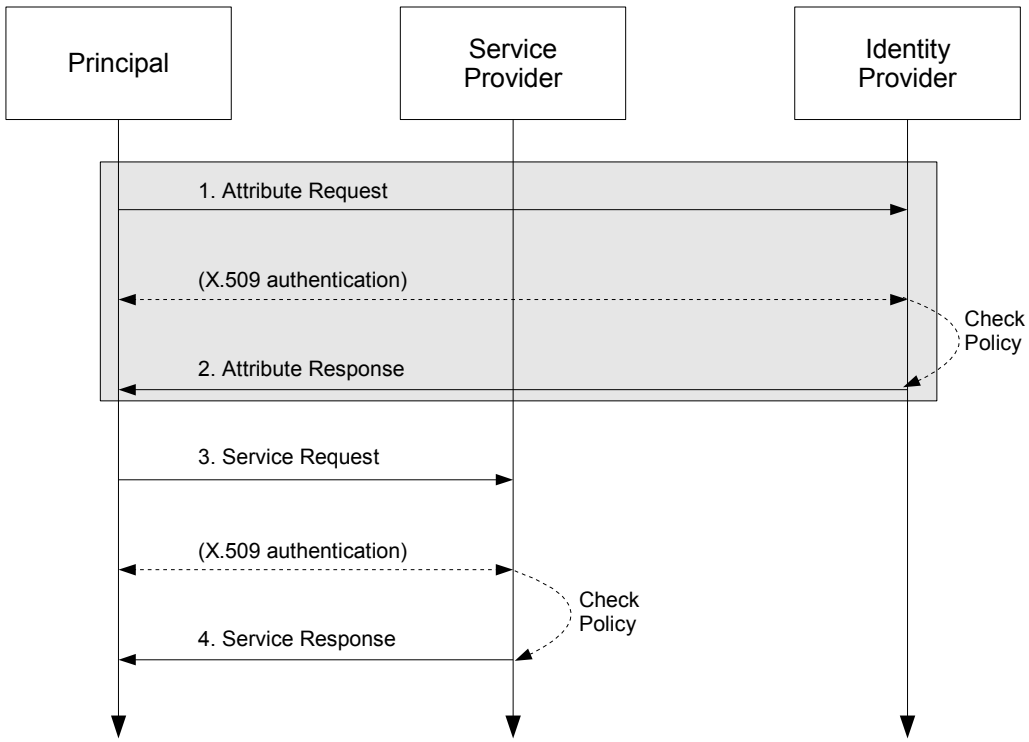
This use case is based on the following assumptions:

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

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

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

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



800

801 **1. Attribute Request**

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

807 **2. Attribute Response**

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

811 **3. Service Request**

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

816 **4. Service Response**

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

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

821 4.2 Required Information

822 **Identification:**
823 `urn:oasis:names:tc:SAML:2.0:profiles:query:attribute:X509-self`

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

Description: Given below.

Updates: N/A

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

4.3 Profile Description

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

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

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

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

4.3.1 <samlp:AttributeQuery> Issued by Principal

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

4.3.2 <samlp:Response> Issued by Identity Provider

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

4.4 Use of SAML Request-Response Protocol

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

4.4.1 <samlp:AttributeQuery> Usage

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

4.4.2 <samlp:Response> Usage

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

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

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

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

4.4.3 Processing Rules

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

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

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

4.5 Example

For example, the principal issues the following attribute query:

```
<samlp:AttributeQuery
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  ID="aaf23196-1773-2113-474a-fe114412ab72"
  Version="2.0"
  IssueInstant="2006-07-17T20:31:40Z">
  <saml:Issuer
    Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
    CN=trscavo@uiuc.edu,OU=User,O=NCSA-TEST,C=US
  </saml:Issuer>
  <saml:Subject>
    <saml:NameID
      Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
      CN=trscavo@uiuc.edu,OU=User,O=NCSA-TEST,C=US
    </saml:NameID>
  </saml:Subject>
  <saml:Attribute
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
    Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
    FriendlyName="eduPersonPrincipalName">
  </saml:Attribute>
  <saml:Attribute
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
    Name="urn:oid:2.5.4.42"
    FriendlyName="givenName">
  </saml:Attribute>
  <saml:Attribute
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
    Name="urn:oid:2.5.4.4"
    FriendlyName="sn">
  </saml:Attribute>
  <saml:Attribute
```

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

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

```
<!-- SAML Assertion for an X.509 Subject -->
<saml:Assertion
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  ID="_33776a319493ad607b7ab3e689482e45"
  Version="2.0"
  IssueInstant="2006-07-17T20:31:41Z">
  <saml:Issuer>https://idp.example.org/saml</saml:Issuer>
  <ds:Signature>...</ds:Signature>
  <saml:Subject>
    <saml:NameID
      Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
      CN=trscavo@uiuc.edu,OU=User,O=NCSA-TEST,C=US
    </saml:NameID>
    <saml:SubjectConfirmation
      Method="urn:oasis:names:tc:SAML:2.0:cm:holder-of-key">
      <saml:SubjectConfirmationData>
        <ds:KeyInfo>
          <ds:X509Data>
            <!-- principal's X.509 cert -->
            <ds:X509Certificate>
MIICiDCCAXACCQDE+9eiWrm62jANBgkqhkiG9w0BAQQFADBFMQswCQYDVQQGEwJV
UzESMBAGA1UEChMJTkNTQS1URVNUMQ0wCwYDVQQLEwRVc2VyMRMwEQYDVQQDEwpT
UC1TZXJ2aWNlMB4XDTA2MDcxNzIwMjE0MVoXDTA2MDcxODIwMjE0MVowSzELMAkG
A1UEBhMCVVMxEjAQBgNVBAoTCU5DU0EtVEVTVDENMAsGA1UECxMEVXNlcjEZMBcG
A1UEAwwQdHJzY2F2b0B1aXVjLmVkdTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkC
gYEAv9QMe4lRl3XbWPcflbCjGK9gty6zBJmp+tsaJINM0VaBaZ3t+tSXknelYife
nCc2O3yaX76aq53QMXy+5wKQYe8Rzdw28Nv3a73wfjXJXoUhGkvERcscs9EfIWcC
g2bHOg8uSh+Fbv3lHih4lBJ5MCS2buJfsR7dlr/xsadU2RcCAwEAATANBgkqhkiG
9w0BAQQFAAOCAQEAdyIcMTob7TVkelfJ7+I1j0LO24UlKvbLzd2OPvcFTCv6fVHx
Ejk0QxaZXJhreZ6+rIdiMXrEzlRdJEsNMxtDW8++sVp6avoB5EX1y3ez+CEAIL4g
cjvKZUR4dMryWshWIBHKFFul+r7urUgvWI12KbMeE9KP+kiiiiTskLcKgFzngw1J
selmHhTcTCrcDocn5yO2+d3dog52vSOtVFDBsBuvDixO2hv679JR6Hlqjtk4GExp
E9iVI0wdPE038uQIJJTXlhsMMLvUGVh/c0ReJBn92Vj4dI/yy6PtY/8ncYLYNkjg
oVN0J/ymOktn9lTlFyTiuY4OuJsZRO1+zWLy9g==
            </ds:X509Certificate>
          </ds:X509Data>
        </ds:KeyInfo>
      </saml:SubjectConfirmationData>
    </saml:SubjectConfirmation>
  </saml:Subject>
  <!-- assertion lifetime constrained by principal's X.509 cert -->
  <saml:Conditions
    NotBefore="2006-07-17T20:31:41Z"
    NotOnOrAfter="2006-07-18T20:21:41Z">
  </saml:Conditions>
  <saml:AuthnStatement
    AuthnInstant="2006-07-17T20:31:41Z">
    <saml:AuthnContext>
      <saml:AuthnContextClassRef>
          urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient
      </saml:AuthnContextClassRef>
    </saml:AuthnContext>
  </saml:AuthnStatement>
```

```
  <saml:AttributeStatement>
    <saml:Attribute
      xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
      x500:Encoding="LDAP"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
      Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
      FriendlyName="eduPersonPrincipalName">
      <saml:AttributeValue xsi:type="xs:string">
        trscavo@uiuc.edu
      </saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute
      xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
      x500:Encoding="LDAP"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
      Name="urn:oid:2.5.4.42"
      FriendlyName="givenName">
      <saml:AttributeValue xsi:type="xs:string">
        Tom
      </saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute
      xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
      x500:Encoding="LDAP"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
      Name="urn:oid:2.5.4.4"
      FriendlyName="sn">
      <saml:AttributeValue xsi:type="xs:string">
        Scavo
      </saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute
      xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
      x500:Encoding="LDAP"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
      Name="urn:oid:1.3.6.1.4.1.1466.115.121.1.26"
      FriendlyName="mail">
      <saml:AttributeValue xsi:type="xs:string">
        trscavo@gmail.com
      </saml:AttributeValue>
    </saml:Attribute>
  </saml:AttributeStatement>
</saml:Assertion>
```

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

4.6 Use of Metadata

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

4.6.1 Identity Provider Metadata

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

```
<xs:attribute
```

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

As before, use of this attribute is OPTIONAL.

An example of identity provider metadata follows:

```
<!-- An Identity Provider supporting both deployment profiles -->
<md:EntityDescriptor
  xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
  entityID="https://idp.example.org/saml">

  <md:AttributeAuthorityDescriptor
    protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">

    <md:AttributeService
      x509qry:supportsX509Query="true"
      x509qry:supportsX509SelfQuery="true"
      xmlns:x509qry="urn:oasis:names:tc:SAML:metadata:X509:query"
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
      Location="https://idp.example.org:8443/saml-idp/AA"/>

    <md:NameIDFormat>
      urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName
    </md:NameIDFormat>

    <!-- see [MACEAttr] -->
    <md:AttributeProfile>
      urn:mace:dir:profiles:attribute:samlv2
    </md:AttributeProfile>

  </md:AttributeAuthorityDescriptor>

</md:EntityDescriptor>
```

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

4.7 Security and Privacy Considerations

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

4.8 Implementation Guidelines (non-normative)

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

4.8.1 Discovery

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

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

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

5 Implementation Conformance

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

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

6 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:

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

7 Revision History

Document ID	Date	Committer	Comment
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
sstc-saml2-profiles-deploy-x509-draft-03	26 Feb 2008	T. Scavo	
sstc-saml2-profiles-deploy-x509-cd-03	11 Mar 2008	T. Scavo	Committee Draft