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

Committee Draft, ~~26 June~~5 July 2006

Document identifier:
sstc-saml-x509-authn-attrib-profile-cd-0~~4~~3

Location:
http://www.oasis-open.org/committees/documents.php?wg_abbrev=security

Editor:
Rick Randall, Booz Allen Hamilton
Rob Philpott, RSA Security

Contributors:
Rebekah Metz, Booz Allen Hamilton
Thomas Wisniewski, Entrust
Scott Cantor, Internet2
Paul Madsen, NTT

Abstract:
This profile specifies the use of SAML V2.0 attribute queries and assertions to support distributed authorization in support of ~~X.509v3~~X.509-based authentication.

Status:
This is a **Committee Draft** approved by the Security Services Technical Committee on 28 March 2006.

Committee members should submit comments and potential errata to the security-services@lists.oasis-open.org list. Others should submit them by filling out the web form located at http://www.oasis-open.org/committees/comments/form.php?wg_abbrev=security. The committee will publish on its web page (http://www.oasis-open.org/committees/security) a catalog of any changes made to this document as a result of comments.

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 Intellectual Property Rights web page for the Security Services TC (http://www.oasis-open.org/committees/security/ipr.php).

Table of Contents

1 Introduction

~~This profile specifies the use of SAML V2.0 attribute queries and assertions to support distributed authorization in support of X.509v3-based authentication.~~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 profile: Basic Mode (section 4) and Enhanced Mode (section 5). The Basic Mode profile extends the SAML V2.0 Assertion Query/Request Profile [SAMLProf]. The Enhanced Mode 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 ~~V2.0~~ metadata query extension namespace [SAMLMeta-Ext].
`x509qry:`	urn:oasis:names:tc:SAML:2.0:profiles:query:X509	This is the SAML V2.0 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 XML Signature namespace [XMLSig].
`xenc:`	http://www.w3.org/2001/04/xmlenc#	This is the XML Encryption namespace [XMLEnc].
`xs:`	http://www.w3.org/2001/XMLSchema	This is the XML Schema namespace [Schema1].
`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: `<SAMLElement>`, `<ns:ForeignElement>`, `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 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 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]).

1.3 Outline

The next section describes a typical use case scenario that motivates the Basic Mode profile. Then sections 4 and 5 specify Basic Mode and Enhanced Mode, respectively. Section 6 specifies the use of SAML V2.0 metadata in support of this profile, while security and privacy issues are discussed in section 7. Finally, in section 8, some guidance for implementers is given.

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

~~This 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.509v3 [RFC3280] certificate. In addition, the profile specifies the use of encryption to protect the privacy of the principal.~~

~~There are two modes of operation specified in this profile: Basic Mode (section 4) and Encrypted/Signed Mode (section 5).~~

3 ~~Motivating~~ Use Case~~s~~

We now~~The following non-normative material~~ describe~~s~~ a typical use case that motivates the Basic Mode profile described in section 4.

3.1 Overview

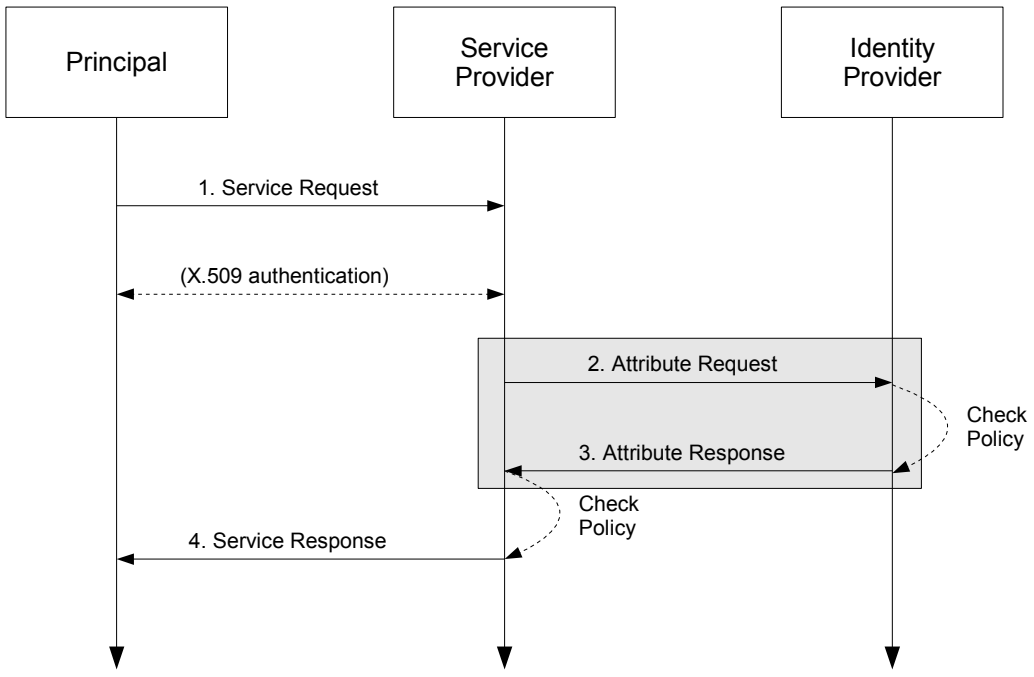
A principal attempts to access a secured resource maintained at a service provider. Principal authentication is accomplished by presenting a trusted ~~X.509v3~~X.509 certificate (that is, the federated credential is a certificate, not a SAML assertion) and by demonstrating proof of possession of the associated private key.

After the principal has been authenticated, the service provider requires additional information about the principal in order to determine whether to grant access to the resource. To obtain this information, the service provider uses the Subject Distinguished Name (Subject DN) field of the principal's ~~X.509v3~~X.509 certificate to query an identity provider for the required information about the principal. When the identity provider returns the relevant attributes, the service provider is able to make an informed authorization decision.

3.2 Sequence

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

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



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.509v3~~X.509 certificate. The details of the X.509 authentication step are out of scope.

2. **Attribute Request**

In step 2, the service provider sends a SAML V2.0 <AttributeQuery> to the identity provider using a SAML SOAP Binding. The Subject DN from the principal's ~~X.509v3~~X.509 certificate (presented in step 1 above) is used to construct the <Subject> element. Thus the <Subject> element will contain a <NameID> with the value of the Subject DN from the principal's ~~X.509v3~~X.509 certificate.

3. **Attribute Response**

In step 3, after verifying that the service provider is a valid requester, the identity provider issues a <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**

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 4 and ~~5~~5 (resp.) of this specification.

4 Basic Mode

In this mode, a service provider sends a SAML V2.0 <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.509v3~~X.509 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 <Response> containing the relevant attributes for the identified principal.

The <AttributeQuery>, <Response>, and <Assertion> elements MAY be signed using this mode.

4.1 Required Information

Identification:
urn:oasis:names:tc:SAML:2.0:profiles:query:X509:basic~~attributes:X509-basic~~

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

Description: Given below.

Updates: N/A

Extends: Assertion Query/Request Profile specified in [SAMLProf]

4.2 <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 <AttributeQuery> message to an identity provider. The query MUST conform to the Assertion Query/Request Profile given in section 6 of [SAMLProf] unless otherwise specified below.

4.2.1 <AttributeQuery> Usage

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

- The <Subject> element MUST contain a <NameID> element whose value is the Subject DN from the principal's ~~X.509v3~~X.509 certificate.
- The <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 <NameID> element MUST satisfy the rules of section 8.3.3 of [SAMLCore]. In particular, the format of the DN SHOULD comply with RFC 2253 [RFC2253].
- The <NameID> element ~~MUST~~SHOULD have a NameQualifier attribute whose value is the Issuer DN from the principal's ~~X.509v3~~X.509 certificate. The format of this DN SHOULD also comply with [RFC2253].

4.3 <Response> Issued by Identity Provider

The identity provider processes the <AttributeQuery> element and any enclosed <Attribute> elements before returning an attribute assertion to the service provider. The response MUST conform to the Assertion Query/Request Profile given in section 6 of [SAMLProf] unless otherwise specified below.

4.3.1 <Response> Usage

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

- The <Response> MUST contain exactly one <Assertion> element.
- The <Assertion> element MUST satisfy the following conditions:
  - The <Assertion> element MUST contain exactly one <AttributeStatement> element that conveys the attributes of the principal to the service provider.
  - The <Assertion> element MUST contain an <AudienceRestriction> element that includes the service provider's unique identifier as an <Audience>.
  - Other conditions (and other <Audience> elements) MAY be included as requested by the service provider or at the discretion of the identity provider.

4.3.2 Error Processing

If the identity provider wishes to return an error, it MUST NOT include any assertions in the <Response> message. Possible error responses include the following:

- If the identity provider does not support this profile, it MAY return the following status code:
  urn:oasis:names:tc:SAML:2.0:status:UnknownAttrProfile
- If the identity provider does not recognize the <NameID> or otherwise is unable to map the <NameID> to a local principal name, it MAY return the following status code:
  urn:oasis:names:tc:SAML:2.0:status:UnknownPrincipal

- ~~**Use of Metadata**~~

~~The service provider and identity provider MAY use metadata in support of this profile for locating endpoints, communicating key information, and so on. If SAML V2.0 metadata is used, the <md:AttributeAuthorityDescriptor> element defined by the SAML metadata specification [SAMLMeta] and the **query:AttributeQueryDescriptorType** complex type defined by the SAML metadata extension specification [SAMLMeta-Ext] SHOULD be used with this profile.~~

5 ~~Encrypted/Signed Mode~~Enhanced Mode

In this mode, as in ~~basic mode~~Basic Mode, a service provider sends a SAML V2.0 <AttributeQuery> message directly to an identity provider. ~~Encrypted/Signed Mode~~Enhanced Mode differs from ~~the basic mode~~Basic Mode in that the message contains an encrypted name identifier assigned to a principal that authenticated to the service provider using an ~~X.509v3~~X.509 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 <Response> containing the relevant attributes for the identified principal. The returned attributes are encrypted as described below.

The <AttributeQuery>, <Response>, and <Assertion> elements MUST be signed using this mode.

5.1 Required Information

Identification:
urn:oasis:names:tc:SAML:2.0:profiles:query:X509:enhanced~~attributes:X509-encrypted~~

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

Description: Given below.

Updates: N/A

Extends: The Basic Mode Attribute Sharing Profile specified in section 4 of this document

5.2 <AttributeQuery> Issued by Service Provider

In ~~Encrypted/Signed Mode~~Enhanced Mode, the service provider sends a SAML V2.0 <AttributeQuery> message to an identity provider as described in section 4. In addition to the requirements of Basic Mode, this mode has the following additional requirements.

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

5.2.1 <AttributeQuery> Usage

In addition to the Basic Mode rules of section 4.2.1, the <AttributeQuery> element MUST conform to the following rules:

- The <Subject> element MUST contain an <EncryptedID> element carrying the encrypted value of the <NameID> element (using XML Encryption as defined in the W3C XML Encryption specification [XMLEnc]). See section 4.2~~1~~.2 for details on the use of encryption.
- The <AttributeQuery> element MUST contain a <ds:Signature> element carrying the signature of the service provider.

5.2.2 Use of Encryption

The SAML V2.0 Assertions and Protocols specification [SAMLCore] defines the <EncryptedID> element as a means of applying confidentiality to a name identifier. In ~~Encrypted/Signed Mode~~Enhanced

Mode, the service provider MUST use the <EncryptedID> element to carry the Subject DN of the principal in the <AttributeQuery>.

Exactly one of the following procedures MUST be followed:

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

5.2.3 Use of Digital Signatures

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

In this mode, a service provider MUST sign the <AttributeQuery> element containing the <EncryptedID> element to allow the identity provider to authenticate the origin and integrity of the request. A signing algorithm satisfying FIPS 140-2 Security Requirements [FIPS 140-2] SHALL be used for the digital signature operation.

5.3 <Response> Issued by Identity Provider

The identity provider responds to the query by returning an attribute assertion to the service provider as described in section 4. In addition to the requirements of Basic Mode, this mode has the following additional requirements.

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

5.3.1 <Response> Usage

If the identity provider wishes to return an error, it MUST NOT include any assertions in the <Response> message. Otherwise, if the request is successful, the <Response> element MUST conform to the following rules:

- It MUST contain exactly one <EncryptedAssertion> element.
- The encrypted content of the <EncryptedAssertion> element is an <Assertion> element that MUST satisfy the following conditions in addition to the rules of section 4.3.1:
  - The <Assertion> element MUST contain a <ds:Signature> element carrying the signature of the identity provider.

5.3.2 Use of Encryption

The SAML V2.0 Assertions and Protocols specification [SAMLCore] defines the <EncryptedAssertion> element as a means of applying confidentiality to the contents of an assertion. In ~~Encrypted/Signed Mode~~Enhanced Mode, the identity provider MUST use the <EncryptedAssertion> element to carry the returned attribute values for the principal.

Exactly one of the following procedures MUST be followed:

- The identity provider generates a new symmetric key to encrypt the <Assertion>. 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 the symmetric key used by the service provider to encrypt the name identifier. After encrypting the <Assertion> using this key, the identity provider places the resulting ciphertext in the <xenc:EncryptedData> element. In this case, however, the <EncryptedAssertion> element MUST NOT contain an <xenc:EncryptedKey> element.
- Assuming the service provider did not include a symmetric key in the <AttributeQuery>, the identity provider uses a previously established symmetric key to encrypt the <Assertion>. If the identity provider reuses a key in this manner, the <EncryptedAssertion> element MUST NOT contain an <xenc:EncryptedKey> element.

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

5.3.3 Use of Digital Signatures

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

In this mode, the identity provider MUST sign the <Assertion> in order to allow the service provider to verify its integrity. The signature is calculated before the encryption operation. A signing algorithm satisfying FIPS 140-2 Security Requirements [FIPS 140-2] SHALL be used for the digital signature operation.

5.4 ~~Use of Metadata~~

~~As in Basic Mode, the service provider and identity provider MAY use metadata in support of this profile. If SAML V2.0 metadata is used, the following rules are specified in addition to the rules of section :~~

- ~~If the service provider uses a previously established symmetric key, there SHOULD be at least one <md:KeyDescriptor> element with attribute use="encryption" in service provider metadata.~~
- ~~Similarly, if the identity provider uses a previously established symmetric key, there SHOULD be at least one <md:KeyDescriptor> element with attribute use="encryption" in identity provider metadata.~~

6 Use of Metadata

The identity provider and service provider MAY use metadata for locating endpoints, communicating key information, and so forth. If SAML V2.0 metadata is used, which is RECOMMENDED, the rules in sections 6.1 and 6.2 apply.

Since an entity requires the means to call out its support of Basic Mode or Enhanced Mode (or both), a pair of XML attributes has been specified for this purpose [X509Query-XSD]:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  targetNamespace="urn:oasis:names:tc:SAML:2.0:profiles:query:X509"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  elementFormDefault="qualified"
  attributeFormDefault="unqualified"
  blockDefault="substitution"
  version="2.0">

  <xs:annotation>
    <xs:documentation>
      Document title: Schema for SAML V2.0 Attribute Sharing Profile for
X.509 Authentication-Based Systems
      Document identifier: sstc-saml-x509-authn-attrib-profile.xsd
      Location: http://www.oasis-
open.org/committees/documents.php?wg_abbrev=security
      Revision history:
        V1.0 (July 2006):
          Initial version.
    </xs:documentation>
  </xs:annotation>

  <xs:attribute name="hasBasicSupport" type="boolean" use="optional"/>
  <xs:attribute name="hasEnhancedSupport" type="boolean" use="optional"/>

</xs:schema>
```

Use of these attributes is specified in the following sections.

6.1 Identity Provider Metadata

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

- If the identity provider supports Basic Mode, the `<md:AttributeAuthorityDescriptor>` element MUST include at least one `<md:AttributeService>` element having attribute `hasBasicSupport` set to `"true"`.
- If the identity provider supports Enhanced Mode, the `<md:AttributeAuthorityDescriptor>` element MUST include at least one `<md:AttributeService>` element having attribute `hasEnhancedSupport` set to `"true"`.
- Any `<md:AttributeService>` element having attributes `hasBasicSupport` or `hasEnhancedSupport` set to `"true"` MUST have its `Binding` attribute set to `"urn:oasis:names:tc:SAML:2.0:bindings:SOAP"`.
- The `<md:AttributeAuthorityDescriptor>` element MUST include an `<md:NameIDFormat>` element with value `"urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName"`.
- Zero 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. Unless a method of dynamic metadata exchange exists, it is recommended that identity providers

omit this list entirely.

Also, if the identity provider has previously established a symmetric key with the service provider, there SHOULD be at least one `<md:KeyDescriptor>` element with attribute `use="encryption"` in identity provider metadata.

An example of identity provider metadata follows:

```
<!-- An Identity Provider supporting both Basic and Enhanced Mode -->
<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">

    <!-- a public key to be used by service providers to
         encrypt previously established symmetric keys -->
    <md:KeyDescriptor use="encryption">
      <ds:KeyInfo>...</ds:KeyInfo>
    </md:KeyDescriptor>

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

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

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

  </md:AttributeAuthorityDescriptor>

</md:EntityDescriptor>
```

6.2 Service Provider Metadata

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

- 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"`.

Also, if the service provider has previously established a symmetric key with the identity provider, there SHOULD be at least one `<md:KeyDescriptor>` element with attribute `use="encryption"` in service provider metadata.

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">

    <!-- a public key to be used by identity providers to
         encrypt previously established symmetric keys -->
    <md:KeyDescriptor use="encryption">
      <ds:KeyInfo>...</ds:KeyInfo>
    </md:KeyDescriptor>

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

  </md:RoleDescriptor>

</md:EntityDescriptor>
```

7 Security and Privacy Considerations

The motivation for this 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 profile.

7.1 Background

The SAML Security and Privacy specification ~~[SAMLSecure]~~ [SAMLSecure] provides general background material relevant to all SAML profiles. In addition ~~to that specification~~, 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.

7.2 General Security Requirements

SAML profiles often ~~include~~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 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 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 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 service provider that subsequently initiates this profile. The latter must have a secure means of obtaining the X.509 subject name from the end ~~user~~ entity certificate and issuing a SAML V2.0 `<AttributeQuery>` for that subject to the appropriate asserting party. The mechanism by which these system entities are linked is out of scope for this profile.

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

Since this 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/Signed Mode~~Enhanced Mode, ~~this profile specifies~~ a requester MUST authenticate and ensure message integrity to the responder, and vice versa.

Generally speaking, Basic Mode is applicable in point-to-point situations where transport-level security suffices. Thus mutually authenticated SSL/TLS will be the norm. On the other hand, ~~Encrypted/Signed Mode~~Enhanced Mode applies 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. Thus digital signatures are required in ~~Encrypted/Signed Mode~~Enhanced Mode. To ensure privacy, message-level encryption is also required.

7.3 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 (if applicable).

8 Implementation Guidance (Informative)

The following non-normative guidance is provided for implementers.

8.1 Identity Provider 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 profile are listed below:

- The identity provider's unique identifier may be preconfigured at the service provider. This is useful if there is only one identity provider per deployment, for example.
- The subject DN of the principal's ~~X.509v3~~X.509 certificate may provide a reference to the identity provider. New deployments are discouraged from decorating DNs in this manner, however, since ~~the~~this practice ~~will~~may lessen interoperability with existing PKIs.
- The issuer DN may provide clues about the principal's preferred identity provider. Generally, however, this will not be the case 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. ~~This is only feasible for new deployments, and as previously implied, there is a potential loss of interoperability associated with any discovery method that imposes a particular structure on the X.509 certificate~~For long-term credentials, this practice may not be feasible, however.

This profile does not specify a particular discovery method.

8.2 Canonicalization

According to this specification, the format of the DN used as the value of the <NameID> element SHOULD conform to [RFC2253]. Since the latter allows some flexibility in the precise format of the DN, it may be necessary for the identity provider to canonicalize the DN during the course of mapping it to a local principal name. The details of the canonicalization process are of concern only to the identity provider, however. As long as the service provider provides a DN whose canonicalization is recognized by the identity provider, the correct mapping will occur.

8.3 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), it is the identity provider that determines the actual attributes returned to the service provider. Thus a responsible identity provider will institute and enforce policy that strictly limits the attributes released to service providers.

8.4 Caching of Attributes

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

9 References

9.1 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. Document ID saml-bindings-2.0-os. 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. Document ID saml-core-2.0-os. See http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

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

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

[SAMLMeta-Ext] T. Scavo and S. Cantor. *SAML Metadata Extension for Query Requesters*. OASIS, March 2006. Document ID sstc-saml-metadata-ext-query-cd-01. See http://www.oasis-open.org/committees/download.php/18052/sstc-saml-metadata-ext-query-cd-01.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 Attribute Sharing Profile for X.509 Authentication-Based Systems*. OASIS, July 2006. Document ID sstc-saml-x509-authn-attrib-profile.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/

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

9.2 Non-Normative References

[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

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

A. 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
- Steve Anderson, BMC Software
- Rick Randall, Booz Allen Hamilton
- Nick Ragouzis, Enosis Group LLC
- Sharon Boeyen, Entrust
- Thomas Wisniewski, Entrust
- Carolina Canales-Valenzuela, Ericsson
- Dana Kaufman, Forum Systems
- Ashish Patel, France Telecom
- Irving Reid, Hewlett-Packard
- Greg Whitehead, Hewlett-Packard
- Guy Denton, IBM
- Heather Hinton, IBM
- Anthony Nadalin, IBM
- Eric Tiffany, IEEE
- Prasanta Behera, Individual
- Scott Cantor, Internet2
- Bob Morgan, Internet2
- Jeff Hodges, NeuStar
- Frederick Hirsch, Nokia
- Paul Madsen, NTT USA
- Ari Kermaier, Oracle
- Prateek Mishra, Oracle
- Vamsi Motukuru, Oracle
- John Hughes, PA Consulting
- Brian Campbell, Ping Identity
- Rob Philpott, RSA Security
- Jahan Moreh, Sigaba
- Bhavna Bhatnagar, Sun Microsystems
- Eve Maler, Sun Microsystems
- David Staggs, Veterans Health Administration

The editors also would like to acknowledge the following non-voting SSTC members for their contributions to this or previous versions of this specification:

- Maryann Hondo, IBM
- Peter Michalek, Individual
- Conor P. Cahill, Intel
- Wendy Gray, JPMorganChase
- Peter Davis, NeuStar
- Senthil Sengodan, Nokia
- Cameron Morris, Novell
- Darren Platt, Ping Identity
- Alberto Squassabia, Ping Identity
- Jim Lien, RSA Security
- John Linn, RSA Security

- Ron Monzillo, Sun Microsystems
- Mike Beach, The Boeing Company

Finally, the editors wish to acknowledge the following people for their contributions of material used as input to this specification:

- Tom Scavo, NCSA/University of Illinois
- Santosh Chokhani, Orion Security
- Robert Mingo, SAIC

B. Notices

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's procedures with respect to rights in OASIS specifications can be found at 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 implementors or users of this specification, can be obtained from the OASIS Executive Director.

OASIS invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to implement this specification. Please address the information to the OASIS Executive Director.