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

Committee Draft, 28 March 2006

Document identifier:
sstc-saml-x509-authn-attrib-profile-cd-02

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 attribute queries and assertions to support distributed authorization in support of X.509v3-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 attribute queries and assertions to support distributed authorization in support of X.509v3-based authentication.

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.
```

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

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

The SAML V2.0 Assertions and Protocols specification [SAMLCore] defines an Attribute Query/Response Protocol for retrieving a principal's attributes. This profile describes the use of this protocol with the SOAP binding defined in the SAML V2.0 Bindings specification [SAMLBind], and provides additional guidelines for protecting the privacy of the principal with encryption, to support the retrieval of attributes of a principal authenticated using an X.509v3 [RFC3280] certificate.

This profile specifies two modes of operation: Basic Mode and Encrypted Mode.

2.1 Required Information

Identification:

Two modes of operation are provided by this profile, each represented by a URI:

```
urn:oasis:names:tc:SAML:profiles:query:attributes:X509-basic
urn:oasis:names:tc:SAML:profiles:query:attributes:X509-encrypted
```

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

Description: Given below.

Updates: N/A

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

2.2 Motivating Use Case

2.2.1 Overview

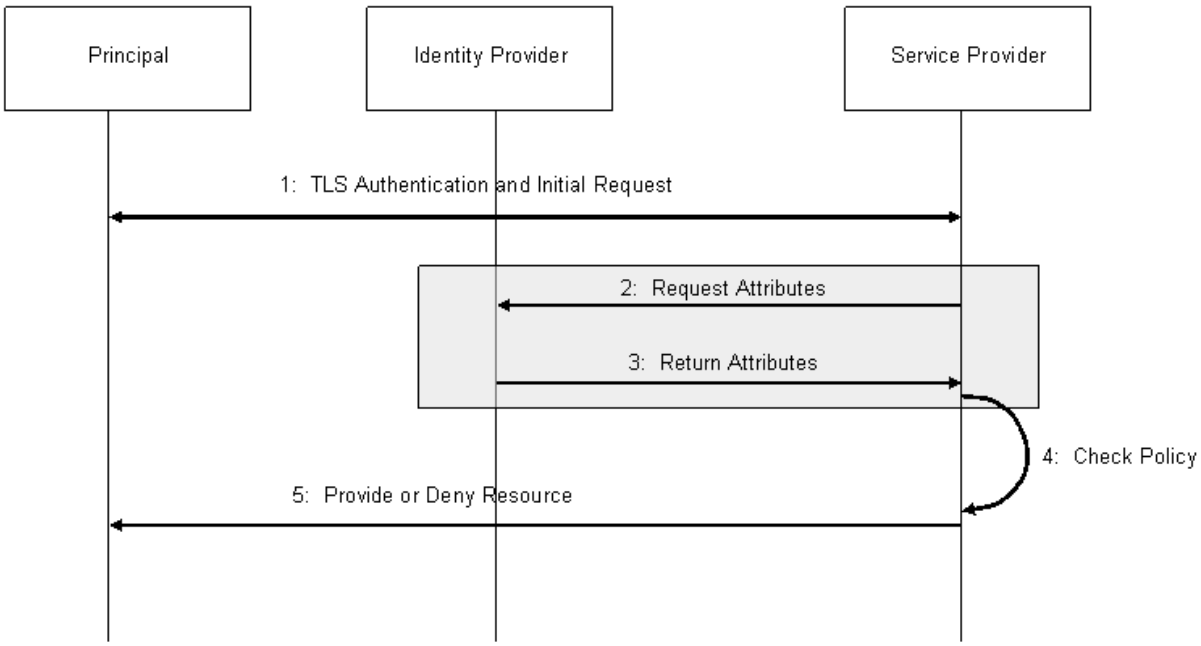
A principal attempts to access a web resource maintained at a service provider. Principal authentication is accomplished through the presentation of a trusted X.509v3 certificate (that is, the federated credential is a certificate, and not a SAML assertion) and by the demonstration of proof of possession 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 some privileged resource(s). To get this information the service provider uses the Subject DistinguishedName (Subject DN) field of the principal's X.509v3 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.

2.2.2 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. **TLS Authentication and Initial Request**

In step 1, the principal requests a secured resource from a service provider. The service provider requests that the principal be authenticated. The principal authenticates to the service provider with an X.509v3 certificate. The service provider authenticates to the principal at the same time (that is, TLS or SSL mutual authentication is performed). Subject confirmation is performed by the service provider as part of the TLS authentication.

2. **Request Attributes**

In step 2, the service provider sends a SAML `<AttributeQuery>` to the identity provider using a SAML SOAP Binding, using the Subject DN from the principal's X.509v3 certificate (presented in step 1 above) within the `<Subject>` element. The `<Subject>` element will contain a `<NameID>` with the value of the Subject DN from the principal's X.509v3 certificate and a format with the value of `urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName`. In the Encrypted/Signed mode, the service provider will sign the attribute request so that the identity provider will be able to verify its origin and integrity.

The service provider shall determine the location of an appropriate identity provider for the request based upon the contents of the Subject DN or the Issuer DN in the principal's certificate. The details of locating the identity provider from the DN information are not specified by this profile.

3. **Return Attributes**

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.

In the Encrypted/Signed mode, the attributes returned in the `<Response>` message are encrypted as described in Section 4, and the `<Response>` message is signed by the identity provider so that the service provider will be able to verify the origin and integrity of the message.

4. **Check Policy**

Based on the results of the `<Response>` message from the identity provider in step 3, the service provider evaluates the access control policy for the resource being requested to determine whether the

principal should be granted access to the resource.

5. **Return Resource**

Based on the results of steps 3 and 4, the service returns the requested resource or returns an error.

Of the sequence steps described above, it is steps 2 and 3 that are profiled in Sections 3 and 4 below.

3 Basic Mode

In this mode, a service provider uses the SAML SOAP Binding to send an <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 certificate.

The service provider MAY authenticate to the identity using this mode. In addition, the requester MAY use TLS or SSL client authentication.

If the identity provider receiving the request can:

- Recognize the name identifier; and
- Fulfill the request based on authentication of the requester and any applicable policies;

it will respond with a successful <Response> containing the relevant attributes for the identified principal.

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

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 **mdext:AttributeRequesterDescriptorType** complex type defined by the SAML metadata extension specification [SAMLMeta-Ext] SHOULD be used with this profile.

3.1 <AttributeQuery> Issued by Service Provider to Identity Provider

The identity provider MUST process the <AttributeQuery> message and any enclosed <Attribute> elements as described in [SAMLCore] and in Section 6 of [SAMLProf].

3.1.1 <AttributeQuery> Usage

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

- The <Subject> element must contain a <NameID> with the value of the Subject DN from the principal's X.509v3 certificate and a format with the value of urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName.

3.2 <Response> Issued by Identity Provider to Service Provider

The service provider MUST process the <Response> message and any enclosed <Assertion> elements as described in [SAMLCore] and in Section 6 of [SAMLProf].

3.2.1 <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 <Assertion> element.
- The <Assertion> element MUST satisfy the following conditions:
  - It MUST contain exactly one <AttributeStatement> element that reflects 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 Encrypted/Signed Mode

In this mode, a service provider uses the SAML SOAP Binding to send an <AttributeQuery> message directly to an identity provider. It differs from the basic mode in that this message contains an encrypted name identifier assigned to a principal that authenticated to the service provider using an X.509v3 certificate.

The service provider MUST authenticate to the identity provider by signing the <AttributeQuery> message. In addition, the requester MAY use TLS or SSL client authentication.

If the identity provider receiving the request can:

- Decrypt and recognize the name identifier; and
- Fulfill the request based on authentication of the requester and any applicable policies;

it will respond with a successful <Response> containing the relevant attributes for the identified principal. The returned attributes MUST be encrypted as described below.

The responding identity provider MUST authenticate to the requester, both by signing the <Response> message and through TLS or SSL server authentication. 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 **mdext:AttributeRequesterDescriptorType** complex type defined by the SAML metadata extension specification [SAMLMeta-Ext] SHOULD be used with this profile.

4.1 <AttributeQuery> Issued by Service Provider to Identity Provider

The identity provider MUST process the <AttributeQuery> message and any enclosed <Attribute> elements as described in [SAMLCore] and in Section 6 of [SAMLProf].

All requests MUST be made over either SSL 3.0 [SAMLSecure] or TLS 1.0 [RFC3280] to maintain confidentiality and message integrity.

4.1.1 <AttributeQuery> Usage

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

- The <Subject> element must contain an <EncryptedID> element carrying the encrypted value of the <NameID> (using XML Encryption as defined in [XMLEnc]) with the value of the principal's Subject DN from the principal's X.509v3 certificate and a format with the value of urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName. See Section 4.1.2 for details on the use of encryption.
- It MUST contain a <ds:Signature> element carrying the signature of the service provider.

4.1.2 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 this mode the service provider MUST use the <EncryptedID> to carry the Subject DN of the principal in the <AttributeQuery>.

The service provider MUST be able to generate a new symmetric key for encrypting the principal's name identifier containing the Subject DN to conform to the Encrypted/Signed Mode. After performing the encryption using this method, the service provider then 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.

Optionally, and if supported by an identity provider, the Service Provider MAY use a previously established symmetric key for encrypting the principal's name identifier containing the Subject DN. After performing the encryption using this method, the service provider then places the resulting ciphertext in the <xenc:EncryptedData> element and the <EncryptedID> element MUST NOT contain an <xenc:EncryptedKey> element.

4.1.3 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, a service provider MUST sign the <AttributeQuery> containing the <EncryptedID> to allow the identity provider to authenticate its origin and verify its integrity. A [FIPS 140-2] validated digital signing algorithm SHALL be used for the digital signature operation.

4.2 <Response> Issued by Identity Provider to Service Provider

The service provider MUST process the <Response> message and any enclosed <Assertion> elements as described in [SAMLCore] and in Section 6 of [SAMLProf].

All responses MUST be made over either SSL 3.0 [SAMLSecure] or TLS 1.0 [RFC3280] to maintain confidentiality and message integrity.

4.2.1 <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:
  - It MUST contain exactly one <AttributeStatement> element that reflects the attributes of the principal to the service provider.
  - The <Assertion> element MUST contain a <ds:Signature> element carrying the signature of the identity 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.

4.2.2 Use of Encryption

The SAML V2.0 assertions and protocols specification [SAMLCore] defines the <EncryptedAssertion> element as a mean of applying confidentiality to the contents of an assertion.

In this mode the identity provider MUST use the <EncryptedAssertion> element to carry the returned attribute values for the principal.

The identity provider MUST be able to generate a new symmetric key for encrypting the <Assertion> to

conform to the Encrypted/Signed Mode. After performing the encryption using this method, the identity provider then 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.

Optionally, and if supported by a service provider, the Service Provider MAY use the symmetric key used in the <AttributeQuery> for encrypting the name identifier containing the Subject DN in order to encrypt the returned <Assertion>. If the identity provider reuses the key in this manner, the <EncryptedAssertion> element MUST NOT contain an <xenc:EncryptedKey> element.

Optionally, if supported by a service provider and the service provider did not include a symmetric key in the <AttributeQuery> for encrypting the name identifier containing the Subject DN, the Service Provider MAY use a previously established symmetric key in order to encrypt the returned <Assertion>. If the identity provider reuses the key in this manner, the <EncryptedAssertion> element MUST NOT contain an <xenc:EncryptedKey> element. A [FIPS 140-2] validated encryption algorithm SHALL be used for the encryption operation.

4.2.3 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 [FIPS 140-2] validated digital signing algorithm SHALL be used for the digital signature operation.

5 Security Considerations

As is the case with other processing profiles of SAML that rely on an earlier act of user authentication, this profile assumes that the system entity that performs the actual validation of user credentials is operating in a secure environment that includes the SAML system entity initiating the profile. For example, when considering the SAML Web Browser SSO Profile [SAMLProf], an authentication service that validates a username/password for a user must be securely linked to an identity provider that issues SAML web SSO assertions based on that user's act of authentication.

In this profile, an end user uses 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 by obtaining the X.509 subject name from the end-user certificate and issuing a SAML <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 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 relies on the SAML SOAP Binding [SAMLBind], the relevant security considerations described in the SAML Security and Privacy Considerations [SAMLSecure] specification should also be observed. While not mandated by the Basic Mode of this profile, the Encrypted/Signed Mode requires the service provider to successfully authenticate to the attribute authority in order to obtain the requested subject's attributes.

6 Implementation Guidance (Informative)

The following non-normative guidance is provided for implementers.

6.1 Identity Provider Policy

The motivation for this profile is to specify a secure means of using X.509 authentication in association with SAML attributes. As such, security considerations are highly important from the perspective of the profile. The policy configuration of identity providers SHOULD permit only a strictly limited list of attribute responses in SAML assertions.

6.2 Caching of Attributes

A capability to cache user attributes that are returned in assertions SHOULD be provided. Cache expiration settings SHOULD be configurable by administrators. The identity of the principal for which the assertion was issued SHOULD NOT be human readable (that is, clear text) in cache files or the cache repository.

7 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.

[RFC3280] *The TLS Protocol Version 1.0*, http://www.ietf.org/rfc/rfc3280.txt

[SAMLBind] S. Cantor et al *Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0.* OASIS,. 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. *Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML V2.0)*. OASIS, March 2005. Document ID sstc-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] S. Cantor et al. *SAML Metadata Extension for a Standalone Attribute Requester*. OASIS, March 2005. Document ID sstc-saml-metadata-2.0-cd-01. See http://www.oasis-open.org/committees/security/.

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

[SSL3] A. Frier et al., *The SSL 3.0 Protocol*, Netscape Communications Corp, November 1996.

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

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
- Santosh Chokhani
- Robert Mingo

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.