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

OASIS Draft, 13 May 2005

Document identifier:
  sstc-saml-x509-authn-based-attribute-protocol-profile-2.0-draft-06

Location:

Editor:
  Rick Randall, Booz Allen Hamilton

Contributors:
  Thomas Wisniewski, Entrust
  Tom Scavo, NCSA/University of Illinois
  Scott Cantor, Internet2
  Santosh Chokhani, Orion Security
  Rebekah Metz, Booz Allen Hamilton
  Robert Mingo, SAIC
  Paul Madsen, Entrust

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

Status:
  Committee members should submit comments and potential errata to the security-services@lists.oasis-open.org list. Others should submit them to the security-services-comment@lists.oasis-open.org list (to post, you must subscribe; to subscribe, send a message to security-services-comment-request@lists.oasis-open.org with "subscribe" in the body) or use other OASIS-supported means of submitting comments. The committee will publish vetted errata on the Security Services TC web page (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 Intellectual Property Rights web page for the Security Services TC (http://www.oasis-open.org/committees/security/ipr.php).
1 SAML Attribute Sharing Profile for X.509 Authentication-based Systems

[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 [SAMLBind], and 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.

1.1 Required Information

Identification:

Two modes of operation are provided by this profile:


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

Description: Given below.

Updates: NA

Extends: Attribute Query/Request Profile

1.2 Motivating Use Case

1.2.1 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 (i.e., 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.

1.2.2 Sequence

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

Note: those steps constrained by this profile are hilted 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 (i.e., 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 3, 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 2 and 3 below.
2 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> 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, etc. If SAML 2.0 metadata is used, the <md:AttributeAuthorityDescriptor> element in [SAMLMeta] and the mdext:AttributeRequesterDescriptorType complex type in [SAMLMeta-Ext] SHOULD be used with this profile.

2.1 <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].

2.1.1 <AttributeQuery> Usage:

The <AttributeQuery> MUST conform to the following:

- 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.

2.2 <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].

2.2.1 <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:

- It MUST contain exactly one <Assertion> element.
The `<Assertion>` element MUST satisfy the following conditions:

- It MUST contain exactly one `<AttributeStatement>` that reflects the attributes of the principal to the service provider.

- The `<Assertion>` MUST contain an `<AudienceRestriction>` including 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.
3 Encrypted/Signed Mode

In this mode, a service provider uses the SAML SOAP Binding to send an \(<\text{AttributeQuery}\>\) message directly to an identity provider. 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 \(<\text{AttributeQuery}\>\) 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 \(<\text{Response}\>\) 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 \(<\text{Response}\>\) 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, etc. If SAML 2.0 metadata is used, the \(<\text{md:AttributeAuthorityDescriptor}\>\) element in [SAMLMeta] and the \(<\text{mdext:AttributeRequesterDescriptorType}\>\) complex type in [SAMLMeta-Ext] SHOULD be used with this profile.

3.1 \(<\text{AttributeQuery}\>\) Issued by Service provider to Identity Provider

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

All requests MUST be made over either SSL 3.0 [SSL3] or TLS 1.0 [RFC 3280] to maintain confidentiality and message integrity.

3.1.1 \(<\text{AttributeQuery}\>\) Usage

The \(<\text{AttributeQuery}\>\) MUST conform to the following:

- The \(<\text{Subject}\>\) element must contain an \(<\text{EncryptedID}\>\) element carrying the encrypted value of the \(<\text{NameID}\>\) 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 3.1.2 for details on the use of encryption.
- It MUST contain a \(<\text{Signature}\>\) element carrying the signature of the service provider.

3.1.2 Use of Encryption

[SAMLCore] defines the \(<\text{EncryptedID}\>\) element as a means of applying confidentiality to a name identifier.

In this mode the service provider MUST use the \(<\text{EncryptedID}\>\) to carry the Subject DN of the principal in the \(<\text{AttributeQuery}\>\).

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
\texttt{<xenc:EncryptedData>} element. The symmetric key MUST be encrypted with the identity provider's
public key and the resulting ciphertext placed in the \texttt{<exec: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
\texttt{<xenc:EncryptedData>} element and the \texttt{<EncryptedID>} element MUST NOT contain an
\texttt{<exec:EncryptedKey>} element.

### 3.1.3 Use of Digital Signatures

[SAMLCore] provides the \texttt{<Signature>} element as a means of providing integrity and authenticity for a
message.

In this mode, a service provider MUST sign the \texttt{<AttributeQuery>} containing the \texttt{<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.

### 3.2 \texttt{<Response> Issued by Identity Provider to Service Provider}

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

All responses MUST be made over either SSL 3.0 [SSL3] or TLS 1.0 [RFC 3280] to maintain
confidentiality and message integrity.

#### 3.2.1 \texttt{<Response>} Usage

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

- It MUST contain exactly one \texttt{<EncryptedAssertion>} element.

- The encrypted content of the \texttt{<EncryptedAssertion>} element is an \texttt{<Assertion>} element that MUST satisfy the following conditions:
  - It MUST contain exactly one \texttt{<AttributeStatement>} that reflects the attributes of
    the principal to the service provider.
  - The \texttt{<Assertion>} MUST contain a \texttt{<Signature>} element carrying the signature of
    the identity provider.
  - The \texttt{<Assertion>} MUST contain an \texttt{<AudienceRestriction>} including the
    service provider's unique identifier as an \texttt{<Audience>},
  - Other conditions (and other \texttt{<Audience>} elements) MAY be included as requested by
    the service provider or at the discretion of the identity provider.

#### 3.2.2 Use of Encryption

[SAMLCore] defines the \texttt{<EncryptedAssertion>} element as a mean of applying confidentiality to the
contents of an assertion.

In this mode the identity provider MUST use the \texttt{<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 <exec: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 <exec: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 <exec:EncryptedKey> element. A [FIPS 140-2] validated encryption algorithm SHALL be used for the encryption operation.

### 3.2.3 Use of Digital Signatures

[SAMLCore] provides the <Signature> element as a mean 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.
4 Implementation Guidance (informative)

The following guidance is informatively provided for implementers.

4.1 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.

4.2 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 (i.e., clear text) in cache files or the cache repository.
5 References


A. Acknowledgments

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

- Conor P. Cahill, AOL
- John Hughes, Atos Origin
- Hal Lockhart, BEA Systems
- Michael Beach, Boeing
- Rebekah Metz, Booz Allen Hamilton
- Tim Alsop, CyberSafe Limited
- Paul Madsen, Entrust
- Irving Reid, Hewlett-Packard
- Paula Austel, IBM
- Maryann Hondo, IBM
- Michael McIntosh, IBM
- Tony Nadalin, IBM
- Nick Ragouzis, Individual
- Scott Cantor, Internet2
- RL 'Bob' Morgan, Internet2
- Peter C Davis, Neustar
- Jeff Hodges, Neustar
- Frederick Hirsch, Nokia
- John Kemp, Nokia
- Charles Knouse, Oblix
- Steve Anderson, OpenNetwork
- Prateek Mishra, Principal Identity
- John Linn, RSA Security
- Rob Philpott, RSA Security
- Jahan Moreh, Sigaba
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.

Copyright © OASIS Open 2003-2005. All Rights Reserved.

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 paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to OASIS, except as needed for the purpose of developing OASIS specifications, in which case the procedures for copyrights defined in the OASIS Intellectual Property Rights document 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 RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. JavaScript is a trademark or registered trademark of Sun Microsystems, Inc. in the United States and other countries.