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

Committee Draft 04

28 August 2007

Specification URIs:

This Version:
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-x509-authn-attrib-profile-cd-04.html
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-x509-authn-attrib-profile-cd-04.odt
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-x509-authn-attrib-profile-cd-04.pdf

Previous Version:
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-x509-authn-attrib-profile-cd-03.html
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-x509-authn-attrib-profile-cd-03.odt
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-x509-authn-attrib-profile-cd-03.pdf

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

Latest Approved Version:
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-x509-authn-attrib-profile-cd-04.html
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-x509-authn-attrib-profile-cd-04.odt
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-x509-authn-attrib-profile-cd-04.pdf

Technical Committee:
OASIS Security Services TC

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

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

Contributor(s):
Scott Cantor, Internet2
Paul Madsen, NTT Corporation
Related Work:
This specification is an alternative to the SAML V2.0 Deployment Profiles for X.509 Subjects [SAMLX509].

Declared XML Namespace(s):
N/A

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

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

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

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

The non-normative errata page for this specification is located at http://www.oasis-open.org/committees/security.
Copyright © OASIS Open 2007. All Rights Reserved.

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.................................................................................................................. 5
2 Use Cases..................................................................................................................... 8
3 Basic Mode.................................................................................................................. 10
4 Encrypted Mode......................................................................................................... 12
5 Security and Privacy Considerations....................................................................... 15
6 Implementation Conformance.................................................................................... 16
7 Implementation Guidance (Informative)................................................................. 17

1.1 Notation.................................................................................................................... 5
1.2 Terminology............................................................................................................. 5
1.3 Outline..................................................................................................................... 6
1.4 Normative References............................................................................................. 6
1.5 Non-Normative References..................................................................................... 6
2.1.1 Overview............................................................................................................... 8
2.1.2 Sequence............................................................................................................... 8
3.1 Required Information.............................................................................................. 10
3.2 <samlp:AttributeQuery> Issued by Service Provider........................................ 10
3.2.1 <samlp:AttributeQuery> Usage......................................................................... 10
3.3 <samlp:Response> Issued by Identity Provider.................................................... 10
3.3.1 <samlp:Response> Usage.................................................................................... 11
3.4 Use of Metadata..................................................................................................... 11
4.1 Required Information.............................................................................................. 12
4.2 <samlp:AttributeQuery> Issued by Service Provider........................................ 12
4.2.1 <samlp:AttributeQuery> Usage......................................................................... 12
4.2.2 Use of Encryption............................................................................................... 12
4.2.3 Use of Digital Signatures.................................................................................... 13
4.3 <samlp:Response> Issued by Identity Provider.................................................... 13
4.3.1 <samlp:Response> Usage.................................................................................... 13
4.3.2 Use of Encryption............................................................................................... 14
4.3.3 Use of Digital Signatures.................................................................................... 14
4.4 Use of Metadata..................................................................................................... 14
5.1 Background............................................................................................................ 15
5.2 General Security Requirements............................................................................ 15
5.3 User Privacy........................................................................................................... 15
6.1 Overview.................................................................................................................. 16
6.2 Sequence................................................................................................................ 17
7.1 Identity Provider Policy ......................................................................................... 17
7.2 Caching of Attributes............................................................................................. 17
1 Introduction

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

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

1.1 Notation

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

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

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

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

Listings of XML schemas appear like this.

Example code listings appear like this.

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

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

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

1.2 Terminology

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

### 1.3 Outline

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

### 1.4 Normative References


### 1.5 Non-Normative References


2 Use Cases

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

2.1.1 Overview

A principal attempts to access a secured resource maintained at a service provider. Principal authentication 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 (Subject DN) field of the principal’s X.509 identity 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.

2.1.2 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.509 identity certificate. The details of this step are out of scope for this deployment profile.

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

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 in step 3, 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 and 4 of this
specification.
3 Basic Mode

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

If the identity provider receiving the request can:

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

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

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

3.1 Required Information

Identification:

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

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

Description: Given below.

Updates: N/A

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

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

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

3.2.1 `<samlp:AttributeQuery>` Usage

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

- The `<saml:Subject>` element must contain a `<saml:NameID>` element whose value is the Subject DN from the principal’s X.509 identity certificate.
- The `<saml:NameID>` element MUST have a `Format` attribute whose value is `urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName`, as defined in section 8.3.3 of [SAMLCore].

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

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

The service provider MUST process the `<samlp:Response>` message and any enclosed
<saml:Assertion> elements as described in section 6 of [SAMLProf].

### 3.3.1 <samlp:Response> Usage

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

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

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

### 3.4 Use of Metadata

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

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

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

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

If the identity provider receiving the request can:

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

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

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

4.1 Required Information

Identification:


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

Description: Given below.

Updates: N/A

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

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

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

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

4.2.1 `<samlp:AttributeQuery>` Usage

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

- The `<saml:Subject>` element must contain an `<saml:EncryptedID>` element carrying the encrypted value of the `<saml:NameID>` element (using XML Encryption as specified in [XMLEnc]).
  
  See section 4.2.2 for details on the use of encryption.

- The `<samlp:AttributeQuery>` MUST contain a `<ds:Signature>` element carrying the signature of the service provider.

4.2.2 Use of Encryption

The SAML V2.0 Assertions and Protocols specification [SAMLCore] defines the `<saml:EncryptedID>` element as a means of applying confidentiality to a name identifier.
In Encrypted Mode the service provider MUST use the `<saml:EncryptedID>` to carry the Subject DN of the principal in the `<samlp:AttributeQuery>`.

Exactly one of the following encryption 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, 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 service provider as a previously established symmetric key.

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

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

### 4.3 `<samlp:Response>` Issued by Identity Provider

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

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

### 4.3.1 `<samlp:Response>` Usage

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

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

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

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

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

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

### 4.3.2 Use of Encryption

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

In Encrypted Mode the identity provider MUST use the `<saml: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 `<saml: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 `<saml:Assertion>` 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.

- If the service provider did not include a symmetric key in the `<samlp:AttributeQuery>` for decryption of the `<saml:EncryptedID>`, the identity provider uses a previously established symmetric key to encrypt the `<saml:Assertion>`. If the identity provider reuses a key in this manner, the `<saml: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.

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

### 4.4 Use of Metadata

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

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

5.1 Background

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

5.2 General Security Requirements

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

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

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

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

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

5.3 User Privacy

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

An implementation of this specification shall be a conforming Basic Mode X.509 Attribute Query/Requester or a conforming Encrypted Mode X.509 Attribute Query/Requester (or both). An Encrypted Mode X.509 Attribute Query/Requester is a functional superset of a Basic Mode X.509 Attribute Query/Requester.

A Basic Mode X.509 Attribute Query/Requester MUST conform to the normative statements in section 3. An Encrypted Mode X.509 Attribute Query/Requester MUST conform to the normative statements in section 4, which includes references to normative portions of section 3.
7 Implementation Guidance (Informative)

The following non-normative guidance is provided for implementers.

7.1 Identity Provider Policy

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

7.2 Caching of Attributes

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

<table>
<thead>
<tr>
<th>Document ID</th>
<th>Date</th>
<th>Committer</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Draft-01</td>
<td>22 Jun 2004</td>
<td></td>
<td>Initial draft</td>
</tr>
<tr>
<td>Draft-02</td>
<td>03 Feb 2005</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sstc-saml-x509-authn-based-attribute-protocol-profile-2.0-draft-05</td>
<td>02 May 2005</td>
<td>R. Randall</td>
<td></td>
</tr>
<tr>
<td>sstc-saml-x509-authn-based-attribute-protocol-profile-2.0-draft-06</td>
<td>13 May 2005</td>
<td>R. Randall</td>
<td></td>
</tr>
<tr>
<td>sstc-saml-x509-authn-attrib-profile-cd-01</td>
<td>01 Jun 2005</td>
<td>E. Maler</td>
<td>Committee Draft</td>
</tr>
<tr>
<td>sstc-saml-x509-authn-attrib-profile-cd-02</td>
<td>28 Mar 2006</td>
<td>R. Philpott</td>
<td>Committee Draft</td>
</tr>
<tr>
<td>sstc-saml-x509-authn-attrib-profile-cd-03</td>
<td>05 Jul 2006</td>
<td>T. Scavo</td>
<td></td>
</tr>
</tbody>
</table>

Copyright © OASIS Open 2007. All Rights Reserved.
B. Acknowledgments

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

- George Fletcher, AOL
- Hal Lockhart, BEA Systems, Inc.
- Steve Anderson, BMC Software
- Jeff Bohren, BMC Software
- Carolina Canales-Valenzuela, Ericsson
- Greg Whitehead, Hewlett-Packard
- Eric Tiffany, IEEE Industry Standards and Technology Org (IEEE-ISTO)
- Conor Cahill, Intel Corporation
- Scott Cantor, 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
- Ari Kermaier, Oracle Corporation
- Eve Maler, Sun Microsystems
- Emily Xu, Sun Microsystems
- Sampo Kellomki, Symlabs, S.A.
- David Staggs, Veterans Health Administration

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

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