SAML V1.1 Profiles for X.509 Subjects

OASIS Draft, 29 August 2006

Document identifier: sstc-saml1-profiles-x509-draft-01


Editor: Tom Scavo, NCSA/University of Illinois

Contributors: Von Welch, NCSA/University of Illinois

Abstract: This related set of SAML V1.1 profiles specifies how a principal who has been issued an X.509 certificate is represented as a SAML Subject, how an assertion regarding such a principal is produced, and finally how two entities exchange attributes about such a principal.

Status: This is a Working Draft of the Security Services Technical Committee.

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>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.8.5 Caching of Attributes</td>
<td>19</td>
</tr>
<tr>
<td>5 SAML Attribute Self-Query Profile for X.509 Subjects</td>
<td>20</td>
</tr>
<tr>
<td>5.1 Profile Overview (non-normative)</td>
<td>20</td>
</tr>
<tr>
<td>5.2 Required Information</td>
<td>21</td>
</tr>
<tr>
<td>5.3 Profile Description</td>
<td>22</td>
</tr>
<tr>
<td>5.3.1 <a href="">samlp:Request</a> Issued by Principal</td>
<td>22</td>
</tr>
<tr>
<td>5.3.2 <a href="">samlp:Response</a> Issued by Identity Provider</td>
<td>22</td>
</tr>
<tr>
<td>5.4 Use of SAML Request-Response Protocol</td>
<td>22</td>
</tr>
<tr>
<td>5.4.1 <a href="">samlp:Request</a> Usage</td>
<td>22</td>
</tr>
<tr>
<td>5.4.2 <a href="">samlp:Response</a> Usage</td>
<td>22</td>
</tr>
<tr>
<td>5.4.3 Processing Rules</td>
<td>23</td>
</tr>
<tr>
<td>5.5 Example</td>
<td>23</td>
</tr>
<tr>
<td>5.6 Use of Metadata</td>
<td>24</td>
</tr>
<tr>
<td>5.6.1 Identity Provider Metadata</td>
<td>24</td>
</tr>
<tr>
<td>5.7 Security and Privacy Considerations</td>
<td>25</td>
</tr>
<tr>
<td>5.8 Implementation Guidelines (non-normative)</td>
<td>25</td>
</tr>
<tr>
<td>5.8.1 Discovery</td>
<td>25</td>
</tr>
<tr>
<td>6 References</td>
<td>26</td>
</tr>
<tr>
<td>6.1 Normative References</td>
<td>26</td>
</tr>
<tr>
<td>6.2 Non-Normative References</td>
<td>26</td>
</tr>
</tbody>
</table>
1 Introduction

This related set of SAML V1.1 Profiles for X.509 Subjects describes how a principal who has been issued an X.509 certificate is represented as a SAML Subject, how an assertion regarding such a principal is produced and consumed, and finally how two entities exchange attributes about such a principal.

1.1 Notation

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

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

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

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

Listings of XML schemas appear like this.

Example code listings appear like this.

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

<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:1.1:assertion</td>
<td>This is the SAML V1.1 assertion namespace [SAMLCore]. This is the default namespace used throughout this document.</td>
</tr>
<tr>
<td>samlp:</td>
<td>urn:oasis:names:tc:SAML:1.1:protocol</td>
<td>This is the SAML V1.1 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 [SAML2Meta].</td>
</tr>
<tr>
<td>query:</td>
<td>urn:oasis:names:tc:SAML:metadata:ext:query</td>
<td>This is the SAML metadata query extension namespace [SAMLMeta-Ext].</td>
</tr>
<tr>
<td>x509qry:</td>
<td>urn:oasis:names:tc:SAML:1.1:profiles:X509:query:attribute</td>
<td>This is the SAML V1.1 X.509 query namespace defined by this document and its accompanying schema [X509Query-XSD].</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>xs:</td>
<td><a href="http://www.w3.org/2001/XMLSchema">http://www.w3.org/2001/XMLSchema</a></td>
<td>This is the XML Schema namespace [Schema1].</td>
</tr>
<tr>
<td>xsi:</td>
<td><a href="http://www.w3.org/2001/XMLSchema-instance">http://www.w3.org/2001/XMLSchema-instance</a></td>
<td>This is the XML Schema namespace for schema-related markup that appears in XML instances [Schema1].</td>
</tr>
</tbody>
</table>

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

The SAML V2.0 roles of "identity provider" and "service provider" correspond to the roles "source site" and "destination site" described in the SAML V1.1 specifications. This specification adopts the SAML V2.0 terminology [SAML2Gloss].

The term identity provider as used in this specification refers to a typical SAML attribute authority [SAML2Gloss]. 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 v3 end entity certificate [RFC3280] or a certificate based on an X.509 v3 end entity certificate (such as an X.509 proxy certificate [RFC3820]).

1.3 Outline

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

The X.509 SAML Subject Profile describes how a principal who has been issued an X.509 certificate is represented as a SAML V1.1 Subject.

2.1 Required Information


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

Description: Given below.

Updates: N/A

Extends: N/A

2.2 Profile Description

This profile specifies a SAML V1.1 <saml:Subject> element that represents a principal who has been issued an X.509 certificate. An entity that produces a <saml:Subject> element according to this profile MUST have previously determined that the principal does in fact possess the corresponding private key.

2.3 <saml:Subject> Usage

The following requirements MUST be satisfied:

- The <saml:Subject> element MUST contain a <saml:NameIdentifier> element whose value is the Subject Distinguished Name (DN) from the principal’s X.509 certificate.
- The <saml:NameIdentifier> element MUST have a Format attribute whose value is urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName. Thus the DN value of the <saml:NameIdentifier> element MUST satisfy the rules of section 7.3.3 of [SAMLCore].
- The NameQualifier attribute of the <saml:NameIdentifier> element SHOULD be omitted.

Note that the <saml:Subject> element MAY contain one or more <saml:SubjectConfirmation> elements that are out of scope for this profile.

2.4 Example

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

The SAML Assertion Profile for X.509 Subjects describes how a SAML V1.1 assertion regarding a principal who has been issued an X.509 certificate is produced. As such, this profile relies on the X.509 SAML Subject Profile specified in section 2.

See section 2 of the SAML V1.1 Assertions and Protocols specification [SAMLCore] for general requirements regarding SAML assertions.

3.1 Required Information

Identification:


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

Description: Given below.

Updates: N/A

Extends: N/A

3.2 Profile Description

This profile specifies the contents and processing rules associated with SAML V1.1 assertions regarding a principal who has been issued an X.509 certificate. As such, this profile relies on the X.509 SAML Subject Profile specified in section 2 of this document.

3.3 <saml:Assertion> Usage

The following general requirements for all assertion subjects MUST be satisfied:

- Every statement in the assertion MUST have a type derived from abstract type saml:SubjectStatementAbstractType.

- If the <saml:Assertion> element contains more than one statement, each pair of <saml:Subject> elements MUST very strongly match, which we now define. Let S1 and S2 be two <saml:Subject> elements. These two <saml:Subject> elements very strongly match if and only if S1 strongly matches S2 and S2 strongly matches S1. Note that this definition depends on the notion of strongly matches defined in section 3.4.4 of [SAMLCore].

- The <saml:Assertion> element MUST contain a <saml:Conditions> element with NotBefore and NotOnOrAfter attributes. The value of NotBefore MUST be less than (earlier than) the value for NotOnOrAfter.

- The <saml:Assertion> element MAY contain an <saml:Audience> element whose value is the unique identifier of the service provider expected to consume the assertion, or the name of a group of service providers to which the target service provider belongs.

- Other conditions (including other <saml:Audience> elements) MAY be included as required by the service provider or at the discretion of the identity provider.

The following requirements for X.509 assertion subjects MUST be satisfied:

- The SAML Subject of each statement MUST conform to the X.509 SAML Subject Profile specified in section 2 of this document.

- If a <saml:Subject> element contains a <saml:ConfirmationMethod> element having value "urn:oasis:names:tc:SAML:1.0:cm:holder-of-key" (in which case all
<saml:Subject> elements contain such an element since each pair of <saml:Subject> elements very strongly matches), the following additional requirements MUST be satisfied:

- A <saml:SubjectConfirmationData> element MUST be present and it MUST contain a <ds:KeyInfo> element that refers to the principal's X.509 certificate.

- The value of the NotBefore attribute (resp., the NotOnOrAfter attribute) MUST be greater than or equal to (resp., less than or equal to) the NotBefore field (resp., the NotOnOrAfter field) of the certificate.

- The <saml:Assertion> element SHOULD be signed.

### 3.4 Example

The following SAML assertion was obtained by a principal who authenticated to an identity provider via TLS [RFC2246] client authentication. See section 5 for a specific attribute query that might have resulted in this assertion.

```xml
<!-- SAML Assertion for an X.509 Subject -->
<saml:Assertion
 xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
 xmlns:xs="http://www.w3.org/2001/XMLSchema"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
 AssertionID="_33776a319493ad607b7ab3e689482e45"
 IssueInstant="2006-07-17T20:31:41Z"
 Issuer="https://idp.example.org/saml"
 MajorVersion="1" MinorVersion="0">
  <!-- assertion lifetime constrained by principal's X.509 cert -->
  <saml:Conditions
    NotBefore="2006-07-17T20:31:41Z"
    NotOnOrAfter="2006-07-18T20:21:41Z">
  </saml:Conditions>
  <saml:AuthenticationStatement
    AuthenticationInstant="2006-07-17T20:31:41Z"
    AuthenticationMethod="urn:ietf:rfc:2246">
    <saml:Subject
      xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
      <saml:NameIdentifier
        Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
        C=US, O=NCSA-TEST, OU=User, CN=trscavo@uiuc.edu
      </saml:NameIdentifier>
      <saml:SubjectConfirmation
        xmlns:xs="http://www.w3.org/2001/XMLSchema"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <saml:ConfirmationMethod>
          urn:oasis:names:tc:SAML:1.0:cm:holder-of-key
        </saml:ConfirmationMethod>
        <saml:SubjectConfirmationData
          xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
          <ds:KeyInfo>
            <ds:X509Data>
              <!-- principal's X.509 cert -->
              MIICidCCAXGCCDQDE+9e1wrm6jzJNBgqkhkG9w0BAQYFFABqFQwswCQYDVQQGEwJV
              UaESMBQAgA1UECjMTJmNTQ19UVVQ0Q0OwCwYDVQQLEwRCZyMwEwQYDVQQDEwPT
              UC1TZXJ2aWN1MB4XDTA2MDCxNzIwMjE0Mw0DTA2MDc0MjE0Mw0SzELMAkG
              A1UHEhMCVVMzEjAqBQNVaToTCUS5U0EtVEVTVDENNAxGALUEcHREVXNjEGZBMcG
              A1UEAwQdHJyZyZrFi08B8A8IxVjlmVkdTCBZANBnkqhkG9w0BAQEBFAABojQAawgYKc
              qgYEAv9QMe41R1kxWpcfliCBcgK9gty6zBjMpt=saJINMOVaBa23t+txSKxnelYife
              nCcv203yaX76a053XmWY+5wKXYE8Rzd28XN5a37wffyJXsUhgkEvRccs99EfiWcC
              g2hBoDg6uhg+Fbv3Rlnh4tbJ5sCsb2bu77r7dilr=xsadU2BcJAwEAATANBnqkhkIG
              9w0BAQQFAAOCAsEDytrrMTotT7TVkelfJ7+I1j0LO24UlKvbLzd2OPvcFTCv6FvHx
              Ejk0Qxa2XJhreZ6fr+i7dImXrE1rRdJE5MkTdx8w+sVp6a0cB5Ex1y3ezzCEA14g
              c0XuKr4mDMyWnHlBFkU1r7urUgWII12KbMeE9KP+kiiiiTskLEkGfZwwg1wJ
              selmHhTcCTcKc3Iny20oz3d0g52vOSrFDBsBvui02h679J6H1q7tk4GExp
              E91Vi0wPE03BuQ1JXTXhMMLVgVh/c0ReJbn92Vj34I/yiy6PtY/8ncYLYnkjg
              oVNOJ/ymOktn91TLFiTyiuY40ujsZ2R01+zWLkY9g==
            </ds:X509Certificate>
          </ds:KeyInfo>
        </saml:SubjectConfirmationData>
      </saml:Subject>
    </saml:AuthenticationStatement>
  </saml:Conditions>
</saml:Assertion>
```
<saml:NameIdentifier Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
C=US, O=NCISA-TEST, OU=User, CN=trscavo@uiuc.edu
</saml:NameIdentifier>

<saml:ConfirmationMethod>
urn:oasis:names:tc:SAML:1.0:cm:holder-of-key
</saml:ConfirmationMethod>

<saml:SubjectConfirmationData>
<ds:KeyInfo>
<ds:X509Data>
<!-- principal's X.509 cert -->
<ds:X509Certificate>MIICiDCCAXACQCDDE+9eiWrm62jJANBgkqhkiG9w0BAQQFADBFMQswCQYDVQQGEwJy
UzESMBAgaJUEcmMjTqNTQs1URVNUMQ0wCwYDVQQLEwRVc2VyMRwEQRwEQYDVQQGEwJy
UCITZXj2aWN1MB4XDTA2MDcxNzIwMjE0MVoXDTA2MDcxNTIxMjE0MVoXzEELMAkGA1UE
AwwQdHJzY2F2b0B1aXVjLmVkdTCbnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAv9Q
Me41R13XbWpcf1bcGxK9tgy6zBjmp+tsajJINMoVaBaZ3tt+5SXkne1Yife
nCc203yya76aq53QMWy+5wQY8eRzd28NV3a73wfjXJXouHgkERcscs9EFiWcC
q2bhoQgBuSh+Fv3f1ll4lJ5MCs2bu5RdR7drl/xsadvU2RcCAWAEATANBgkqhkiG
9wBAQQFAOCAQGEdiy1TcTob7TVke1fJ7+1l10i24U1VbLz20PvcCTc6VfhX
EjkK0xa2XHr2e+rr+IdiXrEz1RjdJESNMxtJW8+svP6avoB5EXy3el+CEAIL4g
cjVXZUR4dMryWshWIBHKFu1r+7urugwWIIKZlMeE9RP+kiiiiTskLkcFzngwJl
selmHhTcTCrcDocn5y02+3dodg52sVoTFDBsBuVdx02hv679JR6Hlq1gtk4GExp
E91V10wpE038uQ1JXJTXlhasMMLvUGVh/c0ReJbn92Vj4dI/yy6PtY/8ncYLNLkjg
oVNOJ/y/ymOktn91lLFyTiuY4OuJsZRO1+zWLx9g==
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</saml:SubjectConfirmationData>

<saml:Attribute>
<AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri" AttributeName="urn:mace:dir:attribute-def:eduPersonPrincipalName">
<trscavo>
</saml:AttributeValue>
</saml:Attribute>

<saml:Attribute>
<AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri" AttributeName="urn:mace:dir:attribute-def:givenName">
<Tom>
</saml:AttributeValue>
</saml:Attribute>

<saml:Attribute>
<AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri" AttributeName="urn:mace:dir:attribute-def:sn">
<Scavo>
</saml:AttributeValue>
</saml:Attribute>

<saml:Attribute>
<AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri" AttributeName="urn:mace:dir:attribute-def:mail">
</saml:AttributeValue>
</saml:Attribute>
<saml:AttributeValue xsi:type="xs:string">
<trscavo@gmail.com></saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
<ds:Signature>...</ds:Signature>
</saml:Assertion>

The attributes in the above example conform to the MACE-Dir Attribute Profile for SAML 1.x [MACEAttrib] and are for illustration purposes only.
4 SAML Attribute Query Profile for X.509 Subjects

The SAML Attribute Query Profile for X.509 Subjects specifies how a service provider and an identity provider exchange attributes about a principal who has been issued an X.509 certificate. As such, the profile relies on the X.509 SAML Subject Profile and the SAML Assertion Profile for X.509 Subjects specified in sections 2 and 3 (resp.) of this document. Note that the profile specified in section 5 is an extension of this profile.

4.1 Profile Overview (non-normative)

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

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

This use case is based upon the following assumptions:

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

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

Note: The steps constrained by this profile are highlighted with a gray box. The other steps are shown only for completeness; the profile does not constrain them.
1. **Service Request**
   In step 1, the principal requests a secured resource from a service provider who requires that the principal be authenticated. The principal authenticates to the service provider with an X.509 certificate.

2. **Attribute Request**
   In step 2, the service provider sends a SAML V1.1 `<samlp:AttributeQuery>` message to the identity provider using a SAML SOAP Binding. The Subject DN from the principal's X.509 certificate (presented in step 1) is used to construct the `<saml:Subject>` element.

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

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

Of the sequence of steps described above, it is steps 2 and 3 that are profiled in sections 4.3 and 4.4 of this profile.

### 4.2 Required Information

**Identification:**

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

**Description:** Given below.

**Updates:** N/A

**Extends:** N/A
4.3 Profile Description

As outlined in section 4.1, a service provider sends a SAML V1.1 \(<\text{samlp:AttributeQuery}>\) message directly to an identity provider. This message contains a name identifier that identifies a principal who has authenticated to the service provider using an X.509 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 \(<\text{samlp:Response}>\) containing the relevant attributes for the identified principal.

4.3.1 \(<\text{samlp:Request}>\) Issued by Service Provider

To initiate the profile, the service provider uses a synchronous binding such as the SAML SOAP Binding \([\text{SAMLBind}]\) to send a SAML V1.1 \(<\text{samlp:Request}>\) message containing a \(<\text{samlp:AttributeQuery}>\) element to an Attribute Service endpoint at the identity provider. The service provider uses information obtained from the principal's X.509 certificate to construct the query. SAML metadata (section 4.6) MAY be used to determine the endpoint locations and bindings supported by the identity provider.

As required by the X.509 SAML Subject Profile (section 2), the service provider MUST have previously determined that the principal does in fact possess the corresponding private key. The details of this step are out of scope for this profile.

The service provider MUST authenticate itself to the identity provider. SSL 3.0 \([\text{SSL3}]\) or TLS 1.0 \([\text{RFC2246}]\) with client authentication MAY be used for this purpose and to provide integrity protection and confidentiality. Moreover, the \(<\text{samlp:Request}>\) element MAY be signed.

4.3.2 \(<\text{samlp:Response}>\) Issued by Identity Provider

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

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

The identity provider processes the \(<\text{samlp:AttributeQuery}>\) element and any enclosed \(<\text{saml:AttributeDesignator}>\) elements before returning an assertion containing a \(<\text{saml:AttributeStatement}>\) to the requester. If no \(<\text{saml:AttributeDesignator}>\) elements are included in the query, the identity provider returns all attributes for this principal, subject to policy. SAML metadata (section 4.6) MAY be used to determine the attribute requirements of the service provider. If the identity provider is unable to resolve attributes for this principal (for any reason), it MUST return an error.

The identity provider MUST authenticate itself to the service provider. Also, either the \(<\text{samlp:Response}>\) element or the \(<\text{saml:Assertion}>\) element (or both) MAY be signed.
### 4.4 Use of SAML Request-Response Protocol

#### 4.4.1 `<samlp:Request>` Usage

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

- **Resource** attribute MUST be present and its value MUST be the unique identifier of the service provider that will ultimately consume the assertion.
- The `<samlp:AttributeQuery>` element MAY include one or more `<samlp:AttributeDesignator>` elements.

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

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

- The `<samlp:Response>` element MUST contain at least one `<saml:Assertion>` element.
- Each `<saml:Assertion>` element MUST satisfy the following conditions:
  - The `<saml:Assertion>` element MUST conform to the SAML Assertion Profile for X.509 Subjects specified in section 3 of this document.
  - The **Issuer** attribute on the `<saml:Assertion>` element MUST be set to the unique identifier of the identity provider that issued the assertion.
  - The `<saml:Assertion>` element SHOULD contain an `<Audience>` element whose value is identical to the value of the **Resource** attribute.
  - The `<saml:Assertion>` element MUST contain at least one `<saml:AttributeStatement>` element and SHOULD contain only `<saml:AttributeStatement>` elements.
  - The `<saml:Subject>` element contained by the `<saml:AttributeStatement>` element SHOULD NOT contain a `<saml:SubjectConfirmation>` element. If, however, any `<saml:Subject>` element contains a `<saml:SubjectConfirmation>` element, then *all* `<saml:Subject>` elements MUST contain such an element (since each pair of `<saml:Subject>` elements very strongly matches).

If the request is unsuccessful, the `<samlp:Response>` element MUST NOT contain a `<saml:Assertion>` element.

### 4.5 Example

For example, the requester issues the following attribute query:

```xml
<samlp:Request
  xmlns:samlp="urn:oasis:names:tc:SAML:1.0:protocol"
  MajorVersion="1" MinorVersion="1"
  IssueInstant="2006-07-17T22:26:40Z"
  RequestID="aaf23196-1773-2113-474a-fell14412ab72">
  <samlp:AttributeQuery
    Resource="https://sp.example.org/saml"/>
</samlp:Request>
```
After processing the request, the identity provider issues the following response:

```xml
<samlp:Response
    xmlns:samlp="urn:oasis:names:tc:SAML:1.0:protocol"
    InResponseTo="aaf23196-1773-2113-474a-fell14412ab72"
    IssueInstant="2006-07-17T22:26:41Z"
    MajorVersion="1" MinorVersion="1"
    ResponseID="b07b804c-7c29-ea16-7300-4f3d6f7928ac">
    <samlp:Status>
        <samlp:StatusCode Value="samlp:Success"/>
    </samlp:Status>
    <saml:Assertion
        xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
        xmlns:xs="http://www.w3.org/2001/XMLSchema"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        MajorVersion="1" MinorVersion="1"
        IssueInstant="2006-07-17T22:26:41Z"
        Issuer="https://idp.example.org/saml">
        <Conditions
            NotBefore="2006-07-17T22:21:41Z"
            NotOnOrAfter="2006-07-17T22:51:41Z">
            <saml:AudienceRestrictionCondition>
                <saml:Audience>https://sp.example.org/saml</saml:Audience>
            </saml:AudienceRestrictionCondition>
        </Conditions>
        <saml:AttributeStatement>
            <saml:Attribute
                AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri"
                AttributeName="urn:mace:dir:attribute-def:eduPersonPrincipalName"/>
            <saml:Attribute
                AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri"
                AttributeName="urn:mace:dir:attribute-def:eduPersonAffiliation"/>
        </saml:AttributeStatement>
        <saml:NameIdentifier
            Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
            C=US, O=NCSA-TEST, OU=User, CN=trscavo@uiuc.edu
        </saml:NameIdentifier>
    </saml:Assertion>
</samlp:Response>
```
The attributes in the above example (eduPersonAffiliation and eduPersonPrincipalName) conform to the MACE-Dir Attribute Profile for SAML 1.x [MACEAttr] and are for illustration purposes only.

4.6 Use of Metadata

The identity provider and the service provider MAY use metadata for locating endpoints, communicating key information, and so forth. If SAML V2.0 metadata [SAML2Meta] is used, which is RECOMMENDED, the SAML 1.x Metadata Profile [SAMLMeta] MUST also be followed. In this case, the rules in sections 4.6.1 and 4.6.2 apply as well.

Since an entity requires the means to call out its support of this profile, an XML attribute has been specified for this purpose [X509Query-XSD]:

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

Use of this attribute is specified in the following subsection.

4.6.1 Identity Provider Metadata

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

- The containing `<md:EntityDescriptor>` element MUST have an `entityID` attribute whose value is the same unique identifier given as the `Issuer` attribute in assertions issued by the identity provider.
- If the identity provider supports this profile, the `<md:AttributeAuthorityDescriptor>` element MUST include at least one `<md:AttributeService>` element having attribute `supportsX509Query` set to "true".
- At least one `<md:AttributeService>` element having attribute `supportsX509Query` set to "true" MUST have its `Binding` attribute set to "urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding".
- 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.

An example of identity provider metadata follows:

```xml
<!-- An Identity Provider supporting the SAML attribute query profile -->
<md:EntityDescriptor
    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    entityID="https://idp.example.org/saml">
    <md:AttributeAuthorityDescriptor
        protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.1:protocol">
        <md:AttributeService
            x509qry:supportsX509Query="true"
```

Copyright © OASIS Open 2006. All Rights Reserved.
4.6.2 Service Provider Metadata

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

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

An example of service provider metadata follows:

```xml
<!-- 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:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:type="query:AttributeQueryDescriptorType"
      protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.1:protocol">
      <md:NameIDFormat>
        urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName
      </md:NameIDFormat>
   </md:RoleDescriptor>

</md:EntityDescriptor>
```
4.7 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.

4.7.1 Background

The SAML Security and Privacy specification [SAMLSecure] provides general background material relevant to all SAML bindings and profiles. Section 5.3 of [SAMLSecure], in particular, considers the security requirements of the SAML SOAP Binding, and is therefore pertinent to this profile. In addition, section 3.1 of the SAML Bindings specification [SAMLBind] provides further security guidelines regarding the SAML SOAP Binding.

4.7.2 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 [SAMLBind] 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 (and other information) from the certificate and issuing a SAML V1.1 <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 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.

4.7.3 User Privacy

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

4.8 Implementation Guidelines (non-normative)

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

4.8.1 Discovery

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

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

- The identity provider's unique identifier may be preconfigured at the service provider. This is useful, for instance, if there is only one identity provider per deployment.
- The subject DN of the principal's X.509 certificate may include a reference to the identity provider.

New deployments are discouraged from decorating long-lived DNs in this manner, however, since
this practice may lessen interoperability with existing PKIs. For short-lived DNs, this practice may be satisfactory.

- The issuer DN or the issuer alternative name may provide clues about the principal’s preferred identity provider. This technique may not be practical, however, since SAML authorities do not typically issue X.509 credentials.

- A reference to the identity provider may be inserted into a non-critical X.509 extension [RFC3280] at the time the credential is issued. For long-term credentials, this practice may not be feasible, however. For short-term credentials, this technique may be satisfactory.

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

### 4.8.2 Name Mapping

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

### 4.8.3 Canonicalization

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

### 4.8.4 Identity Provider Policy

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

### 4.8.5 Caching of Attributes

A service provider will most likely provide a capability to cache user attributes returned in assertions. If so, cache expiration settings should be configurable by administrators.
5 SAML Attribute Self-Query Profile for X.509 Subjects

The SAML Attribute Self-Query Profile for X.509 Subjects specifies how a principal who has been issued an X.509 certificate self-queries an identity provider for attributes. The profile extends the SAML Attribute Query Profile for X.509 Subjects specified in section 4 of this document. Where the two profiles conflict, this profile takes precedence.

5.1 Profile Overview (non-normative)

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

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

This use case is based on the following assumptions:

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

Note that in the case of a self-query, the client possesses significantly more functionality than the client alluded to in section 4.1.

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

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

In step 1, the principal sends a SAML V1.1 `<samlp:Request>` message containing a `<samlp:AttributeQuery>` element to the identity provider using a SAML SOAP Binding. The Subject DN from the principal's X.509 certificate is used to construct the `<saml:Subject>` element of the query. The identity provider requires that the principal be authenticated. The principal authenticates to the identity provider using the same X.509 credential used to construct the query.

2. **Attribute Response**

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

3. **Service Request**

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

4. **Service Response**

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

Of the sequence of steps described above, it is steps 1 and 2 that are profiled in sections 5.3 and 5.4 of this profile.

5.2 **Required Information**

**Identification:**


**Contact information:** security-services-comment@lists.oasis-open.org
5.3 Profile Description

This profile extends the SAML Attribute Query Profile for X.509 Subjects described in section 4.3.

As outlined in section 5.1, a principal sends a SAML V1.1 <samlp:AttributeQuery> message directly to an identity provider. The principal authenticates to the identity provider using an X.509 certificate. If the identity provider receiving the request can:

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

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

To determine that the requester is the principal, the identity provider MUST authenticate the principal.

5.3.1 <samlp:Request> Issued by Principal

To initiate the profile, the principal uses a synchronous binding such as the SAML SOAP Binding [SAMLBind] to send a SAML V1.1 <samlp:Request> message containing a <samlp:AttributeQuery> element as described in section 4.3. The principal uses information obtained from its X.509 certificate to construct the query. The principal MUST authenticate itself to the identity provider using the same X.509 credential used to construct the query.

5.3.2 <samlp:Response> Issued by Identity Provider

The identity provider MUST process the request as outlined in section 4.3.

5.4 Use of SAML Request-Response Protocol

5.4.1 <samlp:Request> Usage

The <samlp:Request> element MUST contain a <samlp:AttributeQuery> element that conforms to the rules of section 4.4.1 except as noted below:

- The Resource attribute MAY be omitted. If present, its value MUST be set to the unique identifier of the service provider that will ultimately consume the assertion.

5.4.2 <samlp:Response> Usage

If the request is successful, the <samlp:Response> element MUST conform to the rules of section 4.4.2 except as noted below:

- If there is a Resource attribute on the <samlp:AttributeQuery> element, the <Assertion> element SHOULD contain an <Audience> element whose value is identical to the value of the Resource attribute.
- The <saml:Assertion> element MAY include a <saml:AuthenticationStatement>
The `<saml:Subject>` element MUST contain a `<saml:ConfirmationMethod>` element having value "urn:oasis:names:tc:SAML:1.0:cm:holder-of-key". See section 3.2 for some important consequences of this rule.

5.4.3 Processing Rules

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

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

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

5.5 Example

For example, the principal issues the following attribute query:

```xml
<samlp:Request
 xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
 xmlns:samlp="urn:oasis:names:tc:SAML:1.0:protocol"
 MajorVersion="1" MinorVersion="1"
 IssueInstant="2006-07-17T20:31:40Z"
 RequestID="aaf23196-1773-2113-474a-fe114412ab72">
 <samlp:AttributeQuery>
 <saml:Subject>
 <saml:NameIdentifier Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
   C=US, O=NCSA-TEST, OU=User, CN=trscavo@uiuc.edu
 </saml:NameIdentifier>
 </saml:Subject>
 <saml:NameIdentifier>
   <saml:NameIdentifier>
     <saml:AttributeDesignator
       AttributeName="urn:mace:shibboleth:1.0:attributeNamespace:uri"
    />
     <saml:AttributeDesignator
       AttributeName="urn:mace:dir:attribute-def:eduPersonPrincipalName"/>
     <saml:AttributeDesignator
       AttributeName="urn:mace:dir:attribute-def:givenName"/>
     <saml:AttributeDesignator
       AttributeName="urn:mace:dir:attribute-def:sn"/>
     <saml:AttributeDesignator
       AttributeName="urn:mace:dir:attribute-def:mail"/>
   </saml:NameIdentifier>
 </samlp:AttributeQuery>
</samlp:Request>
```

The requested attributes (eduPersonPrincipalName, givenName, sn, and mail) in the previous example conform to the MACE-Dir Attribute Profile for SAML 1.x [MACEAttrib] and are for illustration purposes only.

After processing the request, the identity provider issues a response containing an assertion such as the one listed in section 3.4.
5.6 Use of Metadata

As outlined in section 4.6, the use of SAML V2.0 metadata [SAML2Meta] is RECOMMENDED, but since a principal is not expected to publish metadata about itself, only the use of identity provider metadata is profiled below. Note, however, that the principal may wield a client that relies on service provider metadata (see, e.g., section 5.8.1), in which case the rules in section 4.6.2 apply.

Since an entity requires the means to call out its support of this profile, an XML attribute has been specified for this purpose [X509Query-XSD]:

```xml
<xs:attribute
  name="supportsX509SelfQuery" type="boolean" use="optional"/>
```

Use of this attribute is specified in the following subsection.

5.6.1 Identity Provider Metadata

An identity provider that uses SAML V2.0 metadata MUST include an `<md:AttributeAuthorityDescriptor>` element that satisfies the rules given in section 4.6.1 in addition to the following rules:

- If the identity provider supports this profile, the `<md:AttributeAuthorityDescriptor>` element MUST include at least one `<md:AttributeService>` element having attribute `supportsX509SelfQuery` set to "true".
- At least one `<md:AttributeService>` element having attribute `supportsX509SelfQuery` set to "true" MUST have its `Binding` attribute set to "urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding".

An example of identity provider metadata follows:

```xml
<!-- An Identity Provider supporting both attribute query profiles -->
<md:EntityDescriptor
  xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
  entityID="https://idp.example.org/saml">
  <md:AttributeAuthorityDescriptor
    protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.1:protocol">
    <md:AttributeService
      x509qry:supportsX509Query="true"
      x509qry:supportsX509SelfQuery="true"
      Binding="urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding"
      Location="https://idp.example.org:8443/saml-idp/AA"/>
  </md:AttributeAuthorityDescriptor>
</md:EntityDescriptor>
```

</saml:Attribute>
<saml:Attribute>
  NameFormat="urn:mace:shibboleth:1.0:attributeNamespace:uri"
  Name="urn:mace:dir:attribute-def:eduPersonPrincipalName"
</saml:Attribute>
<saml:Attribute>
  NameFormat="urn:mace:shibboleth:1.0:attributeNamespace:uri"
  Name="urn:mace:dir:attribute-def:givenName"
</saml:Attribute>
<saml:Attribute>
Note that this identity provider supports both attribute query profiles at the same endpoint location.

5.7 Security and Privacy Considerations

TBD

5.8 Implementation Guidelines (non-normative)

In addition to the guidelines outlined in section 4.8, the following non-normative guidelines are provided for the convenience of implementers.

5.8.1 Discovery

In the SAML Attribute Query Profile for X.509 Subjects (section 4), we encounter the problem of identity provider discovery (section 4.8.1). In the case where the principal self-queries for attributes, we encounter a different problem, which we call service provider discovery. In both cases, we assume the client knows the principal's preferred identity provider, so identity provider discovery is a non-issue in the case of self-queries, but in that case the client is faced with a self-query for unknown attributes.

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

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

6.1 Normative References


6.2 Non-Normative References


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
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 2006. 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.