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

Working Draft, 13 February 2007

Document identifier:
sstc-saml-x509-authn-attrib-profile-draft-11

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

Editor:
Rick Randall, Booz Allen Hamilton
Rob Philpott, RSA Security
Tom Scavo, NCSA
Ari Kermaier, Oracle

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

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

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 of Contents

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 profile: Basic Mode (section) and Encrypted Mode (section). The Basic Mode profile extends the SAML V2.0 Assertion Query/Request Profile [SAMLProf]. The Encrypted Mode profile specifies the use of encryption to protect the privacy of the principal.

1.1 Notation

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

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

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

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

```
Listings of XML schemas appear like this.
```

```
Example code listings appear like this.
```

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

Prefix	*XML Namespace*	*Comments*
`saml:`	urn:oasis:names:tc:SAML:2.0:assertion	This is the SAML V2.0 assertion namespace [SAMLCore].
`samlp:`	urn:oasis:names:tc:SAML:2.0:protocol	This is the SAML V2.0 protocol namespace [SAMLCore].
`md:`	urn:oasis:names:tc:SAML:2.0:metadata	This is the SAML V2.0 metadata namespace [SAMLMeta].
`query:`	urn:oasis:names:tc:SAML:metadata:ext:query	This is the SAML metadata extension query requester namespace [SAMLMeta-Ext].
`ds:`	http://www.w3.org/2000/09/xmldsig#	This is the XML Signature namespace [XMLSig].
`xenc:`	http://www.w3.org/2001/04/xmlenc#	This is the XML Encryption namespace [XMLEnc].

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

1.2 Terminology

The term *identity provider* as used in this specification refers to an ordinary SAML attribute authority [SAMLGloss]. The term *service provider* refers to a SAML attribute requester. However, as used in this specification, a service provider is not a typical SAML service provider since it performs X.509

101 authentication in lieu of consuming a SAML authentication assertion.

102 The term *X.509 certificate* as used in this specification refers to an X.509 end entity certificate [RFC3280]
103 or a certificate based on an X.509 end entity certificate (such as an X.509 proxy certificate [RFC3820]).

104 1.3 Outline

105 The next section describes a typical use case scenario that motivates the Basic Mode profile. Then
106 sections 3 and 4 specify Basic Mode and Encrypted Mode, respectively. Security and privacy issues are
107 discussed in section 5. Finally, in section 6, some guidance for implementers is given.

2 Use Cases

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

2.1.1 Overview

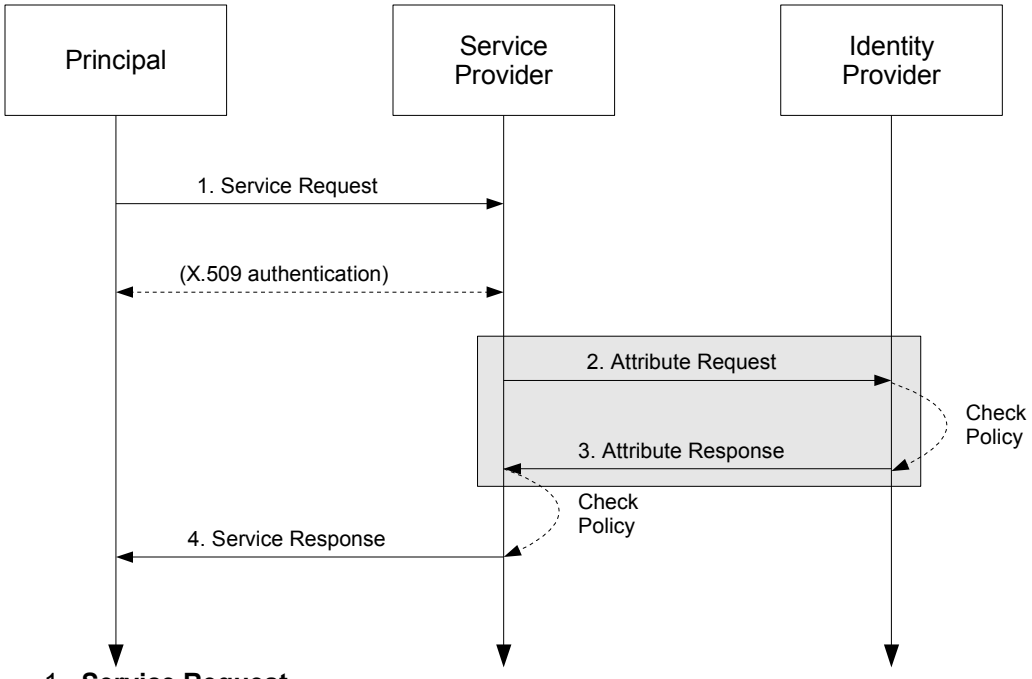
A principal attempts to access a secured resource maintained at a service provider. Principal authentication is accomplished by presenting a trusted X.509v3 certificate and by demonstrating proof of possession of the associated private key.

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.509v3 certificate to query an identity provider for the required information about the principal. When the identity provider returns the relevant attributes, the service provider is able to make an informed authorization decision.

2.1.2 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.509v3 certificate. Subject confirmation is performed by the service provider as part of this authentication. Presentation of the principal's certificate might occur via TLS with client certificate authentication, but the details of this step are out of scope for this profile.

2. **Attribute** Request

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

3. **Attribute** Response

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

4. Service Response

Based on the attributes received from the identity provider in step 3, the service provider returns the requested resource or an error, subject to policy.

Of the sequence 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 <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.

If the identity provider receiving the request can:

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

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

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

3.1 Required Information

Identification:

urn:oasis:names:tc:SAML:profiles:query:attributes: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 <AttributeQuery> Issued by Service Provider

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

3.2.1 <AttributeQuery> Usage

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

- The <Subject> element must contain a <NameID> element whose value is the Subject DN from the principal's X.509v3 certificate.
- The <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 <Response> Issued by Identity Provider

The identity provider processes the <AttributeQuery> element and any enclosed <Attribute> elements, as defined in [SAMLCore] and Section 6 of [SAMLProf], 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 <Response> message and any enclosed <Assertion> elements as described in [SAMLCore] and in Section 6 of [SAMLProf].

3.3.1 <Response> Usage

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

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

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

3.4 Use of Metadata

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

4 Encrypted Mode

In this mode, as in Basic Mode, a service provider sends a SAML V2.0 <AttributeQuery> message directly to an identity provider. The Encrypted Mode request differs from that of the 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.509v3 certificate.

If the identity provider receiving the request can:

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

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

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

4.1 Required Information

Identification:

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

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

Description: Given below.

Updates: N/A

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

4.2 <AttributeQuery> Issued by Service Provider

In Encrypted Mode, the service provider sends a SAML V2.0 <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 <AttributeQuery> Usage

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

- The <Subject> element must contain an <EncryptedID> element carrying the encrypted value of the <NameID> element (using XML Encryption as defined in [XMLEnc]). See Section 4.2.2 for details on the use of encryption.
- The <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 <EncryptedID> element as a means of applying confidentiality to a name identifier.

In Encrypted Mode the service provider MUST use the <EncryptedID> to carry the Subject DN of the principal in the <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.

  This procedure MUST be supported by the service provider.

- Optionally, 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 <EncryptedID> 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.

4.2.3 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 <AttributeQuery> containing the <EncryptedID> 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 <Response> Issued by Identity Provider

The identity provider processes the <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 <Response> message and through TLS or SSL server authentication.

4.3.1 <Response> Usage

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

- The <Response> element MUST contain a <ds:Signature> element carrying the signature of the identity provider.
- It MUST contain at least one <EncryptedAssertion> element.
- The encrypted content of each <EncryptedAssertion> element is an <Assertion> element that MUST satisfy the following conditions, in addition to the rules of section 3.3.1:
  - The <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 assertions in the <Response> message.

4.3.2 Use of Encryption

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

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

Exactly one of the following procedures MUST be followed:

- The identity provider generates a new symmetric key to encrypt the <Assertion>. After performing the encryption, the identity provider places the resulting ciphertext in the <xenc:EncryptedData> element. The symmetric key MUST be encrypted with the service provider's public key and the resulting ciphertext placed in the <xenc:EncryptedKey> element.

  This procedure MUST be supported by the identity provider.

- Optionally, and if supported by the service provider, the identity provider uses the symmetric key used by the service provider to encrypt the name identifier. After encrypting the <Assertion> using this key, the identity provider places the resulting ciphertext in the <xenc:EncryptedData> element. In this case, however, the <EncryptedAssertion> element MUST NOT contain an <xenc:EncryptedKey> element.

- Optionally, and if supported by the service provider, and if the service provider did not include a symmetric key in the <AttributeQuery> for decryption of the <EncryptedID>, the identity provider uses a previously established symmetric key to encrypt the <Assertion>. If the identity provider reuses a key in this manner, the <EncryptedAssertion> element MUST NOT contain an <xenc:EncryptedKey> element.

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

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

4.4 Use of Metadata

As in Basic Mode, the service provider and identity provider MAY use metadata in support of this profile. If SAML V2.0 metadata is used, 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 profile is to specify a secure means of obtaining SAML attributes in conjunction with X.509 authentication. As such, security considerations are highly important from the perspective of this profile.

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 username/password for a user. The authentication service must be securely linked to an identity provider that issues SAML authentication assertions based on that user's act of authentication. Similarly, this profile assumes that the system entity that performs the X.509 authentication is operating in a secure environment that includes the attribute requester.

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

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

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

The following non-normative guidance is provided for implementers.

6.1 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.

6.2 Caching of Attributes

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

7 References

7.1 Normative References

[FIPS 140-2] *Security Requirements for Cryptographic Modules*, May 2001. See http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.

[RFC 2119] S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. IETF RFC 2119, March 1997. See http://www.ietf.org/rfc/rfc2119.txt.

[RFC2246] T. Dierks and C. Allen. *The TLS Protocol Version 1.0*. IETF RFC 2246, January 1999. See http://www.ietf.org/rfc/rfc2246.txt

[RFC3280] S. Tuecke et al. *Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile*. IETF RFC 3820, June 2004. See http://www.ietf.org/rfc/rfc3820.txt

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

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

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

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

[SAMLMeta-Ext] T. Scavo and S. Cantor. *SAML Metadata Extension for SAML V2.0 and V1.x Query Requesters*. OASIS, September 2006. Document ID sstc-saml-metadata-ext-query-cd-02. See http://www.oasis-open.org/committees/security/.

[SSL3] A. Frier et al., *The SSL Protocol Version 3.0*, IETF Internet-Draft, November 1996. See http://wp.netscape.com/eng/ssl3/draft302.txt

[XMLEnc] D. Eastlake et al. *XML Encryption Syntax and Processing.* World Wide Web Consortium. See http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/.

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

7.2 Non-Normative References

[RFC3820] S. Tuecke et al. *Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile*. IETF RFC 3820, June 2004. See http://www.ietf.org/rfc/rfc3820.txt

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

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

A. Acknowledgments

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

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

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

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

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

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

B. Notices

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS's procedures with respect to rights in OASIS specifications can be found at the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification, can be obtained from the OASIS Executive Director.

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