SAML V2.0 Subject Management Protocol Version 1.0 Working Draft 07 March 2010

Specification URIs:

This Version:

Previous Version:

Latest Version:

Technical Committee:

OASIS Security Services TC

Chair(s):

Hal Lockhart, BEA Systems, Inc.
Thomas Hardjono, MIT

Editors:

Phil Hunt, Oracle Corporation

Contributors:

Based on NSN Draft: SAML V2.0Attributes Management Protocol Version 1.0 Working Draft 06 November 2009

Declared XML Namespace(s):

`urn:oasis:names:tc:SAML:2.0:mgmt`

Abstract:

The SAML V2.0 Management Protocol describes the request and response messages for managing subject entity and attribute information.

Status

This is initial draft of Subject Management Protocol based on NSN proposal (http://www.oasis-open.org/apps/org/workgroup/security/document.php?document_id=34222)

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.

Notices

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

The Subject Management Protocol is a message exchange protocol by which a service provider requests an identity provider to update or store authorized subject entity or attribute information. This message exchange protocol uses the SAML Protocols V2.0 [SAML2Core].

1.1 Notation

This specification uses normative text. 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 [RFC2119]:

> …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 defined in the SAML V2.0 core specification [SAML2Core].
`ds:`	http://www.w3.org/2000/09/xmldsig#	This is the XML Signature namespace [XMLSig].
`xs:`	http://www.w3.org/2001/XMLSchema	This is the XML Schema namespace [Schema1].
`xsi:`	http://www.w3.org/2001/XMLSchema-instance	This is the XML Schema namespace for schema-related markup that appears in XML instances [Schema1].

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

1.2 Terminology

1.3 Normative References

[RFC2119] S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels.* IETF RFC 2119, March 1997. http://www.ietf.org/rfc/rfc2119.txt

[RFC4514] K. Zeilenga. *Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names.* IETF RFC 4514, June 2006. http://www.ietf.org/rfc/rfc4514.txt

[RFC5280] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.* IETF RFC 5280, May 2008. http://www.ietf.org/rfc/rfc5280.txt

[SAML2Core] OASIS Standard, *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0.* March 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

[SAML2Prof] OASIS Standard, *Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0.* March 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf

[Schema1] H. S. Thompson et al. *XML Schema Part 1: Structures.* World Wide Web Consortium Recommendation, May 2001. See http://www.w3.org/TR/2001/REC-xmlschema-1-20010502/

[XMLSig] D. Eastlake, J. Reagle, D. Solo, F. Hirsch, T. Roessler. *XML Signature Syntax and Processing (Second Edition).* World Wide Web Consortium Recommendation, 10 June 2008. http://www.w3.org/TR/xmldsig-core/

[XMLEnc] D. Eastlake, J. Reagle. XML Encryption Syntax and Processing. World Wide Web Consortium Recommendation, 10 December 2002. http://www.w3.org/TR/xmlenc-core/

1.4 Non-normative References

[RFC3820] S. Tuecke, V. Welch, D. Engert, L. Pearlman, M. Thompson. *Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile.* IETF RFC 3820, June 2004. http://www.ietf.org/rfc/rfc3820.txt

[RFC4346] T. Dierks, E. Rescorla. *The Transport Layer Security (TLS) Protocol Version 1.1.* IETF RFC 4346, April 2006. http://www.ietf.org/rfc/rfc4346.txt

[SAML2ConDel] S. Cantor. *SAML V2.0 Condition for Delegation Restriction*. OASIS SSTC Committee Draft 01, 10 March 2009. http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-delegation-cd-01.pdf

2 SAML V2.0 Subject Management Protocol

2.1 Required Information

Identification: urn:oasis:names:tc:SAML:2.0:mgmt

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

Description: Given below.

Updates: None.

2.2 Description

The SAML Subject Management Protocol is a message exchange protocol by which the Service Provider (SP) requests the Identity Provider (IdP) to update or store the authorized subject information. This message exchange protocol uses the SAML Protocols V2.0 [SAML2Core] and SAML Profile specifications [SAMLProf].

When a Service Provider wishing to register a new subject and/or add, replace, or remove attribute values of a Subject, the Service Provider informs the Identify Provider of the change by sending them a <ManageSubjectRequest> message.

After successfully processing the request, the Identity Provider responses with a <samlp:ManageSubjectResponse> to the request.

2.3 Elements <ManageSubjectRequest>

A Service Provider sends a <ManageSubjectRequest> message containing either an <AddSubject> or <ModifySubject> sub-element.

This message has the complex type ManageSubjectRequestType, which extends RequestAbstractType.

2.3.1 Element <AddSubject>

The <AddSubject> element has the complex type <AddSubjectType> which requires that either a <saml:Assertion> or <saml:EncryptedAssertion> be provided. The provided assertion constitutes the entire object that the SP wishes to provide. The IdP may choose to accept the request by either creating a new record, or by modifying or mapping the request to one that makes sense within the IDP's context. This is useful in cases where a SP may perceive that a subject entity is new, but to the IDP, the change represents only a role change or provisioning state change.

Example

A SP may request to add a subject by providing a SAML assertion containing one or more attributes to be used in the add request.

In this request, the <saml:Issuer> is the subject identifier of the party issuing the information (typically the SP). The <saml:Subject> is an identifier representing the requested unique identifier for the subject. The IdP is not obligated to accept the identifier, but should return the actual identifier in its response.

```
    <AddSubject>
        <saml:Assertion IssueInstant="2006-07-17T20:31:40Z" ID="bbf23196-1773-2113-474a-
fe114412ab73"
            Version="2.0">
            <saml:Issuer
```

```
                Format="urn:oasis:names:tc:SAML:1.1:nameidformat:X509SubjectName">
                C=US, O=NCSA-TEST, OU=Apps, CN=hrsvc@uiuc.edu
            </saml:Issuer>
            <saml:Subject>
                <saml:NameID
                    Format="urn:oasis:names:tc:SAML:1.1:nameidformat:X509SubjectName">
                    C=US, O=NCSA-TEST, OU=User, CN=trscavo@uiuc.edu
                </saml:NameID>
            </saml:Subject>
            <saml:AttributeStatement>
                <saml:Attribute
                    xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
                    x500:Encoding="LDAP" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:uri"
                    Name="urn:oid:2.5.4.42" FriendlyName="givenName">
                    <saml:AttributeValue>
                        John
                    </saml:AttributeValue>
                </saml:Attribute>
                <saml:Attribute
                    xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
                    x500:Encoding="LDAP" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:uri"
                    Name="urn:oid:1.3.6.1.4.1.1466.115.121.1.26" FriendlyName="mail">
                    <saml:AttributeValue>johndoe@gmail.com
                    </saml:AttributeValue>
                </saml:Attribute>
            </saml:AttributeStatement>
        </saml:Assertion>
    </AddSubject>
</samlm:ManageSubjectRequest>
```

2.3.2 Element <ModifySubject>

The <ModifySubject> element is used to update the attributes of an existing subject. Operations allowed are:

- AddAttributeValue – To add one or more values to an attribute (which may or may not have an existing value).
- DeleteAttributeValue – To remove a specific value or to remove all values of an Attribute. If no values are specified, all values are to be deleted. If specific values are provided than only those values are to be deleted.
- ReplaceAttributeValue – To replace the existing attribute values with a new set of values.

A <ModifySubject> element includes a <saml:Subject> which is used to reference the target of the modify operation and one or more of the above operations.

Example

```
<samlm:ManageSubjectRequest xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:samlm="urn:oasis:names:tc:SAML:2.0:mgmt"
    ID="aaf23196-1773-2113-474a-fe114412ab72" Version="2.0"
    IssueInstant="2006-07-17T20:31:40Z">
    <saml:Subject>
        <saml:NameID
            Format="urn:oasis:names:tc:SAML:1.1:nameidformat:X509SubjectName">
            C=US, O=NCSA-TEST, OU=User, CN=trscavo@uiuc.edu
        </saml:NameID>
```

```
    </saml:Subject>
    <ModifySubject>
        <saml:NameID
            Format="urn:oasis:names:tc:SAML:1.1:nameidformat:X509SubjectName">
            C=US, O=NCSA-TEST, OU=User, CN=trscavo@uiuc.edu
        </saml:NameID>
        <AddAttributeValue>
            <saml:Attribute xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
                x500:Encoding="LDAP" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
                Name="urn:oid:2.5.4.42" FriendlyName="givenName">
                <saml:AttributeValue>John
                </saml:AttributeValue>
            </saml:Attribute>
        </AddAttributeValue>
        <ReplaceAttributeValue>
            <saml:Attribute xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
                x500:Encoding="LDAP" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
                Name="urn:oid:1.3.6.1.4.1.1466.115.121.1.26" FriendlyName="mail">
                <saml:AttributeValue>johndoe@gmail.com
                </saml:AttributeValue>
            </saml:Attribute>
        </ReplaceAttributeValue>
    </ModifySubject>
</samlm:ManageSubjectRequest>
```

2.3.3 Delete Operation

The delete operation is not directly covered in this specification as it is already covered by the existing <samlp:ManageNameIDRequest> element. In this case, a subject deletion is handled by providing the <saml:NameID> identifier of a subject to be deleted in conjuction with the element <samlp:Terminate>

Example

```
<samlp:ManageNameIDRequest
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    ID="aaf23196-1773-2113-474a-fe114412ab72" Version="2.0"
    IssueInstant="2006-07-17T20:31:40Z">
    <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameidformat:X509SubjectName">
        C=US, O=NCSA-TEST, OU=User, CN=trscavo@uiuc.edu
    </saml:NameID>
    <samlp:Terminate />
</samlp:ManageNameIDRequest>
```

2.4 Elements <ManageSubjectResponse>

The recipient of the <ManageSubjectRequest> message MUST respond with a <ManageSubjectResponse> message, which is of StatusResponseType.

2.4.1 Management Related Status Response Codes

In addition to status codes values specified in section 3.2.2.2 of [SAML2Core], the following additional <StatusCode> responses are defined:

`urn:oasis:names:tc:SAML:2.0:status:SubjectNotUnique`

The target subject already exists. Usually in response to an AddSubject operation of a ManageSubjectRequest.

`urn:oasis:names:tc:SAML:2.0:status:NoSuchContext`

The domain or IDP for subject could not be located, or is not valid within the current IDP.

`urn:oasis:names:tc:SAML:2.0:status:Schema`

The attribute or set of attributes defined is not valid for the specified operation. In the case of an AddSubject, the IDP may have a minimum set of attributes required to perform an AddSubject operation. The <StatusDetail> element MAY contain the minimum attributes required for the operation requested.

`urn:oasis:names:tc:SAML:2.0:status:Consent`

The operation was not performed or was partially completed due to a consent exception. <StatusDetail> MAY contain details of failure.

2.4.2 Example

The following XML fragment exemplifies the <ManageSubjectResponse> element:

```
<samlm:ManageAttributeResponse
   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
   xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
   ID="aaf23196-1773-2113-474a-fe114412ab72"
   Version="2.0"
   IssueInstant="2006-07-17T20:31:40Z">
   <samlp:Status
      xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
      <samlp:StatusCode
      xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
      Value="urn:oasis:names:tc:SAML:2.0:status:Success">
      </samlp:StatusCode>
   </samlp:Status>
</samlp:ManageAttributeResponse>
```

2.5 Processing Rules

If the Service Provider requests that a Subject entity be added or modified and/or stored at the Identity Provider, the Service Provider MUST include a <samlp:ManageSubjectRequest> specifying either <AddSubject> or <ModifySubject> elements.

To perform a delete subject operation, the Service Provider MAY include a <ManageNameIDRequest> element with the <Terminate> element as specified in [SAML2Core].

On receiving a request, an IDP may process the request within its own context and security policies. On completion, or rejection of the request, the IDP must respond with a <ManageSubjectResponse> element including the appropriate <StatusCode>.

3 Conformance

Appendix A. Acknowledgments

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

- TBD

The editor would also like to acknowledge the contribution of an earlier draft from NSN entitled: “SAML V2.0Attributes Management Protocol Version 1.0 Working Draft 06 November 2009“, upon which this document attempts to incorporate supporting requirements from.

Appendix B. Revision History

Document ID	Date	Committer	Comment
sstc-saml2-attributes-management-protocol-01	05/11/09	Thinh Nguyenphu	Initial draft