SAML V2.0 X.500/LDAP Attribute Profile

Committee Specification 01

27 March 2008

Specification URIs:

This Version:

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-attribute-x500-cs-01.html

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-attribute-x500-cs-01.odt

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-attribute-x500-cs-01.pdf

Previous Version:

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-attribute-x500-cd-03.html

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-attribute-x500-cd-03.odt

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-attribute-x500-cd-03.pdf

Latest Version:

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-attribute-x500.html

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-attribute-x500.odt

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-attribute-x500.pdf

Latest Approved Version:

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-attribute-x500-cd-03.html

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-attribute-x500-cd-03.odt

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-attribute-x500-cd-03.pdf

Technical Committee:

OASIS Security Services TC

Chair(s):

Hal Lockhart, BEA Systems, Inc.
Brian Campbell, Ping Identity Corporation

Editors:

Scott Cantor, Internet2

Related Work:

This specification supersedes the X.500/LDAP Attribute Profile in the original SAML 2.0 Profiles specification [SAML2Prof].

Declared XML Namespace(s):

urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500

Abstract:

This profile is a replacement for the X.500/LDAP Attribute Profile found in the original SAML 2.0 Profiles specification [SAML2Prof]. The original profile results in well-formed but schema-invalid XML and cannot be corrected without a normative change.

Status

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

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

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

The non-normative errata page for this specification is located at http://www.oasis-open.org/committees/security.

Notices

Table of Contents

1 Introduction

This profile supersedes the profile originally presented in the SAML 2.0 Profiles specification [SAML2Prof] and corrects a normative error in the use of XML extension attributes.

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].
`x500:`	urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500	This is the namespace defined by this document and its accompanying schema [SAMLX500-xsd].
`xsd:`	http://www.w3.org/2001/XMLSchema	This namespace is defined in the W3C XML Schema specification [Schema1]. In schema listings, this is the default namespace and no prefix is shown.
`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 Normative References

[ASN.1] Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation, ITU-T Recommendation X.680, July 2002. See http://www.itu.int/rec/recommendation.asp?type=folders&lang=e&parent=T-REC-X.680.

[eduPerson] eduPerson.ldif. See http://www.educause.edu/eduperson.

[LDAP] K. Zeilanga. *Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map*. IETF RFC 4510, June 2006. See http://www.ietf.org/rfc/rfc4510.txt.

[RFC3866] K. Zeilanga, Ed.. *Language Tags and Ranges in the Lightweight Directory Access Protocol (LDAP)*. IETF RFC 3866, July 2004. See http://www.ietf.org/rfc/rfc3866.txt.

[RFC2045] N. Freed et al. *Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies*. IETF RFC 2045, November 1996. See http://www.ietf.org/rfc/rfc2045.txt.

[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.

[RFC2798] M. Smith. *Definition of the inetOrgPerson LDAP Object Class*. IETF RFC 2798, April 2000. See http://www.ietf.org/rfc/rfc2798.txt.

[RFC3061] M. Mealling. *A URN Namespace of Object Identifiers*. IETF RFC 3061, February 2001. See http://www.ietf.org/rfc/rfc3061.txt.

[SAML2Core] 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.

[SAML2Prof] 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.

[SAMLX500-xsd] S. Cantor et al. SAML X.500/LDAP attribute profile schema. OASIS SSTC, March 2005. Document ID saml-schema-x500-2.0. See http://www.oasis-open.org/committees/security/.

[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/. Note that this specification normatively references Error: Reference source not found, listed below.

[Schema2] Paul V. Biron, Ashok Malhotra. *XML Schema Part 2: Datatypes*. World Wide Web Consortium Recommendation, May 2001. See http://www.w3.org/TR/2001/REC-xmlschema-2-20010502/.

[X.500] Information technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services. ITU-T Recommendation X.500, February 2001. See http://www.itu.int/rec/recommendation.asp?type=folders&lang=e&parent=T-REC-X.500.

1.3 Conformance

1.3.1 SAML 2.0 X.500/LDAP Attribute Profile

An asserting party implementation conforms to this profile if it can produce assertions and other SAML-defined content consistent with the normative text of section 2.

A relying party implementation conforms to this profile if it can accept assertions and other SAML-defined content consistent with the normative text of section 2.

2 SAML 2.0 X.500/LDAP Attribute Profile

2.1 Required Information

Identification: urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500 (this is also the target namespace assigned in the corresponding X.500/LDAP profile schema document [SAMLX500-xsd]).

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

Description: Given below.

Updates: Supersedes the erroneous profile in the SAML 2.0 Profiles specification [SAML2Prof].

2.2 Profile Overview

Directories based on the ITU-T X.500 specifications [X.500] and the related IETF Lightweight Directory Access Protocol specifications [LDAP] are widely deployed. Directory schema is used to model information to be stored in these directories. In particular, in X.500, attribute type definitions are used to specify the syntax and other features of attributes, the basic information storage unit in a directory (this document refers to these as “directory attributes”).

Directory attribute types are defined in schema in the X.500 and LDAP specifications themselves, schema in other public documents (such as the Internet2/Educause eduPerson schema Error: Reference source not found, or the inetOrgPerson schema [RFC2798]), and schema defined for private purposes. In any of these cases, it is useful for deployers to take advantage of these directory attribute types in the context of SAML attribute statements, without having to manually create SAML-specific attribute definitions for them, and to do this in an interoperable fashion.

The X.500/LDAP attribute profile defines a common convention for the naming and representation of such attributes when expressed as SAML attributes.

2.3 SAML Attribute Naming

The NameFormat XML attribute in <Attribute> elements MUST be urn:oasis:names:tc:SAML:2.0:attrname-format:uri.

To construct attribute names, the URN oid namespace described in IETF RFC 3061 [RFC3061] is used. In this approach the Name XML attribute is based on the OBJECT IDENTIFIER assigned to the directory attribute type.

Example:

```
Name="urn:oid:2.5.4.3"
```

Since X.500 procedures require that every attribute type be identified with a unique OBJECT IDENTIFIER, this naming scheme ensures that the derived SAML attribute names, for X.500 attribute types and LDAP attribute descriptions without any tagging options, are unambiguous.

Tagging options on LDAP attribute descriptions, including but not limited to language tags as in IETF RFC 3866 [RFC3866], are not transferred within the Name field of SAML attributes for the purposes of this profile, and their use is undefined.

For purposes of human readability, there may also be a requirement for some applications to carry an optional string name together with the OID URN. The optional XML attribute FriendlyName (defined in [SAML2Core]) MAY be used for this purpose. If the definition of the directory attribute type includes one or more descriptors (short names) for the attribute type, the `FriendlyName` value, if present, SHOULD be one of the defined descriptors.

2.3.1 Attribute Name Comparison

Two `<Attribute>` elements refer to the same SAML attribute if and only if their `Name` XML attribute values are equal in the sense of [RFC3061]. The `FriendlyName` attribute plays no role in the comparison.

Note that two SAML attributes resulting from two LDAP attributes with the same attribute type and different attribute descriptions (for example, tagging options) will also match for equality.

2.4 Profile-Specific XML Attributes

To represent the encoding rules in use for a particular attribute's values, the `<Attribute>` element MUST contain an XML attribute named `Encoding` defined in the XML namespace `urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500`. The value of the attribute is determined by the particular encoding rules in use.

2.5 SAML Attribute Values

Directory attribute type definitions for use in native X.500 directories specify the syntax of the attribute using ASN.1 [ASN.1]. For use in LDAP, directory attribute definitions additionally include an LDAP syntax that specifies how attribute or assertion values conforming to the syntax are to be represented when transferred in the LDAP protocol (known as an LDAP-specific encoding). The LDAP-specific encoding commonly produces Unicode characters in UTF-8 form. This SAML attribute profile specifies the form of SAML attribute values only for those directory attributes which have LDAP syntaxes. Future extensions to this profile may define attribute value formats for directory attributes whose syntaxes specify other encodings.

For any directory attribute with a syntax whose LDAP-specific encoding exclusively produces UTF-8 character strings as values, the SAML attribute value is encoded as simply the UTF-8 string itself, as the content of the `<AttributeValue>` element, with no additional whitespace. In such cases, the `xsi:type` XML attribute MUST be set to **xsd:string**. The profile-specific `Encoding` XML attribute is provided in the `<Attribute>` element, with a value of `LDAP`.

A list of some LDAP attribute syntaxes to which this applies is:

Attribute Type Description	1.3.6.1.4.1.1466.115.121.1.3
Bit String	1.3.6.1.4.1.1466.115.121.1.6
Boolean	1.3.6.1.4.1.1466.115.121.1.7
Country String	1.3.6.1.4.1.1466.115.121.1.11
DN	1.3.6.1.4.1.1466.115.121.1.12
Directory String	1.3.6.1.4.1.1466.115.121.1.15
Facsimile Telephone Number	1.3.6.1.4.1.1466.115.121.1.22
Generalized Time	1.3.6.1.4.1.1466.115.121.1.24
IA5 String	1.3.6.1.4.1.1466.115.121.1.26
INTEGER	1.3.6.1.4.1.1466.115.121.1.27
LDAP Syntax Description	1.3.6.1.4.1.1466.115.121.1.54
Matching Rule Description	1.3.6.1.4.1.1466.115.121.1.30
Matching Rule Use Description	1.3.6.1.4.1.1466.115.121.1.31
Name And Optional UID	1.3.6.1.4.1.1466.115.121.1.34
Name Form Description	1.3.6.1.4.1.1466.115.121.1.35
Numeric String	1.3.6.1.4.1.1466.115.121.1.36

Object Class Description	1.3.6.1.4.1.1466.115.121.1.37
Octet String	1.3.6.1.4.1.1466.115.121.1.40
OID	1.3.6.1.4.1.1466.115.121.1.38
Other Mailbox	1.3.6.1.4.1.1466.115.121.1.39
Postal Address	1.3.6.1.4.1.1466.115.121.1.41
Presentation Address	1.3.6.1.4.1.1466.115.121.1.43
Printable String	1.3.6.1.4.1.1466.115.121.1.44
Substring Assertion	1.3.6.1.4.1.1466.115.121.1.58
Telephone Number	1.3.6.1.4.1.1466.115.121.1.50
UTC Time	1.3.6.1.4.1.1466.115.121.1.53

For all other LDAP syntaxes, the attribute value is encoded, as the content of the `<AttributeValue>` element, by base64-encoding [RFC2045] the contents of the ASN.1 OCTET STRING-encoded LDAP attribute value (not including the ASN.1 OCTET STRING wrapper). The `xsi:type` XML attribute MUST be set to **xsd:base64Binary**. The profile-specific `Encoding` XML attribute is provided in the `<Attribute>` element, with a value of `LDAP`.

When comparing SAML attribute values for equality, the matching rules specified for the corresponding directory attribute type MUST be observed (case sensitivity, for example).

2.6 Profile-Specific Schema

The following schema listing shows how the profile-specific `Encoding` XML attribute is defined [SAMLX500-xsd]:

```
<schema
    targetNamespace="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
    xmlns="http://www.w3.org/2001/XMLSchema"
    elementFormDefault="unqualified"
    attributeFormDefault="unqualified"
    blockDefault="substitution"
    version="2.0">
    <annotation>
        <documentation>
            Document identifier: saml-schema-x500-2.0
            Location: http://docs.oasis-open.org/security/saml/v2.0/
            Revision history:
              V2.0 (March, 2005):
                Custom schema for X.500 attribute profile, first published in
SAML 2.0.
        </documentation>
    </annotation>
    <attribute name="Encoding" type="string"/>
</schema>
```

Note that this is the original schema included in the SAML 2.0 Profiles specification [SAML2Prof].

2.7 Examples

The following is an example of a mapping of the "givenName" directory attribute, representing the SAML assertion subject's first name. It's OBJECT IDENTIFIER is 2.5.4.42 and its LDAP syntax is Directory String.

```
<saml:Attribute
       xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
       NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
       Name="urn:oid:2.5.4.42" FriendlyName="givenName" x500:Encoding="LDAP">
   <saml:AttributeValue xsi:type="xsd:string">Steven</saml:AttributeValue>
```

```
</saml:Attribute>
```

Appendix A. Acknowledgements

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.
- Rob Philpott, EMC Corporation
- Scott Cantor, Internet2
- Bob Morgan, Internet2
- Eric Tiffany, Liberty Alliance Project
- Tom Scavo, National Center for Supercomputing Applications (NCSA)
- Peter Davis, Neustar, Inc.
- Jeff Hodges, Neustar, Inc.
- Frederick Hirsch, Nokia Corporation
- Abbie Barbir, Nortel Networks Limited
- Paul Madsen, NTT Corporation
- Ari Kermaier, Oracle Corporation
- Prateek Mishra, Oracle Corporation
- Brian Campbell, Ping Identity Corporation
- Anil Saldhana, Red Hat
- Eve Maler, Sun Microsystems
- Emily Xu, Sun Microsystems
- Kent Spaulding, Tripod Technology Group, Inc.
- David Staggs, Veterans Health Administration

The editors would also like to acknowledge the following contributors:

- Mark Wahl, Microsoft Corporation

Appendix B. Revision History

- Draft 01, initial correction of original profile to move Encoding attribute up to Attribute element.
- Committee Draft 01, boilerplate edits for CD status.
- Draft 02, incorporating feedback from public review.
- Draft 03, clarify attribute option handling as out of scope, and revise structure to match new OASIS requirements.
- Draft 04, fix references and make other copyedits.
- Committee Draft 02, boilerplate edits for CD status.
- Draft 05, add a contributor, clarify statement on naming equality.
- Committee Draft 03, boilerplate edits for CD status.