



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-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>

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

33 **Abstract:**

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

37 **Status**

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

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

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

47 The non-normative errata page for this specification is located at [http://www.oasis-](http://www.oasis-open.org/committees/security)
48 [open.org/committees/security](http://www.oasis-open.org/committees/security).

49 Notices

50 Copyright © OASIS Open 2008. All Rights Reserved.

51 All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual
52 Property Rights Policy (the "OASIS IPR Policy"). The full Policy may be found at the OASIS website.

53 This document and translations of it may be copied and furnished to others, and derivative works that
54 comment on or otherwise explain it or assist in its implementation may be prepared, copied, published,
55 and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice
56 and this section are included on all such copies and derivative works. However, this document itself may
57 not be modified in any way, including by removing the copyright notice or references to OASIS, except as
58 needed for the purpose of developing any document or deliverable produced by an OASIS Technical
59 Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be
60 followed) or as required to translate it into languages other than English.

61 The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors
62 or assigns.

63 This document and the information contained herein is provided on an "AS IS" basis and OASIS
64 DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY
65 WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY
66 OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A
67 PARTICULAR PURPOSE.

68 OASIS requests that any OASIS Party or any other party that believes it has patent claims that would
69 necessarily be infringed by implementations of this OASIS Committee Specification or OASIS Standard, to
70 notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such
71 patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced
72 this specification.

73 OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any
74 patent claims that would necessarily be infringed by implementations of this specification by a patent
75 holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR
76 Mode of the OASIS Technical Committee that produced this specification. OASIS may include such
77 claims on its website, but disclaims any obligation to do so.

78 OASIS takes no position regarding the validity or scope of any intellectual property or other rights that
79 might be claimed to pertain to the implementation or use of the technology described in this document or
80 the extent to which any license under such rights might or might not be available; neither does it represent
81 that it has made any effort to identify any such rights. Information on OASIS' procedures with respect to
82 rights in any document or deliverable produced by an OASIS Technical Committee can be found on the
83 OASIS website. Copies of claims of rights made available for publication and any assurances of licenses
84 to be made available, or the result of an attempt made to obtain a general license or permission for the
85 use of such proprietary rights by implementers or users of this OASIS Committee Specification or OASIS
86 Standard, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any
87 information or list of intellectual property rights will at any time be complete, or that any claims in such list
88 are, in fact, Essential Claims.

89 The name "OASIS" is a trademark of OASIS, the owner and developer of this specification, and should be
90 used only to refer to the organization and its official outputs. OASIS welcomes reference to, and
91 implementation and use of, specifications, while reserving the right to enforce its marks against
92 misleading uses. Please see <http://www.oasis-open.org/who/trademark.php> for above guidance.

93 **Table of Contents**

94 1 Introduction.....5
95 1.1 Notation.....5
96 1.2 Normative References.....5
97 1.3 Conformance.....6
98 1.3.1 SAML 2.0 X.500/LDAP Attribute Profile.....6
99 2 SAML 2.0 X.500/LDAP Attribute Profile.....7
100 2.1 Required Information.....7
101 2.2 Profile Overview.....7
102 2.3 SAML Attribute Naming.....7
103 2.3.1 Attribute Name Comparison.....8
104 2.4 Profile-Specific XML Attributes.....8
105 2.5 SAML Attribute Values.....8
106 2.6 Profile-Specific Schema.....9
107 2.7 Examples.....9
108 Appendix A. Acknowledgements.....10
109 Appendix B. Revision History.....11
110

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.Idif. See <http://www.educause.edu/eduperson>.

138	[LDAP]	K. Zeilanga. <i>Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map</i> . IETF RFC 4510, June 2006. See http://www.ietf.org/rfc/rfc4510.txt .
139		
140		
141	[RFC3866]	K. Zeilanga, Ed.. <i>Language Tags and Ranges in the Lightweight Directory Access Protocol (LDAP)</i> . IETF RFC 3866, July 2004. See http://www.ietf.org/rfc/rfc3866.txt .
142		
143		
144	[RFC2045]	N. Freed et al. <i>Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies</i> . IETF RFC 2045, November 1996. See http://www.ietf.org/rfc/rfc2045.txt .
145		
146		
147	[RFC2119]	S. Bradner. <i>Key words for use in RFCs to Indicate Requirement Levels</i> . IETF RFC 2119, March 1997. http://www.ietf.org/rfc/rfc2119.txt .
148		
149	[RFC2798]	M. Smith. <i>Definition of the inetOrgPerson LDAP Object Class</i> . IETF RFC 2798, April 2000. See http://www.ietf.org/rfc/rfc2798.txt .
150		
151	[RFC3061]	M. Mealling. <i>A URN Namespace of Object Identifiers</i> . IETF RFC 3061, February 2001. See http://www.ietf.org/rfc/rfc3061.txt .
152		
153	[SAML2Core]	S. Cantor et al. <i>Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0</i> . 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 .
154		
155		
156		
157	[SAML2Prof]	S. Cantor et al. <i>Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0</i> . 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 .
158		
159		
160	[SAMLX500-xsd]	S. Cantor et al. <i>SAML X.500/LDAP attribute profile schema</i> . OASIS SSTC, March 2005. Document ID saml-schema-x500-2.0. See http://www.oasis-open.org/committees/security/ .
161		
162		
163	[Schema1]	H. S. Thompson et al. <i>XML Schema Part 1: Structures</i> . World Wide Web Consortium Recommendation, May 2001. See http://www.w3.org/TR/2001/REC-xmlschema-1-20010502/ . Note that this specification normatively references , listed below.
164		
165		
166		
167	[Schema2]	Paul V. Biron, Ashok Malhotra. <i>XML Schema Part 2: Datatypes</i> . World Wide Web Consortium Recommendation, May 2001. See http://www.w3.org/TR/2001/REC-xmlschema-2-20010502/ .
168		
169		
170	[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 .
171		
172		
173		

174 **1.3 Conformance**

175 **1.3.1 SAML 2.0 X.500/LDAP Attribute Profile**

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

178 A relying party implementation conforms to this profile if it can accept assertions and other SAML-defined
179 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 , 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.

221 2.3.1 Attribute Name Comparison

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

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

227 2.4 Profile-Specific XML Attributes

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

232 2.5 SAML Attribute Values

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

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

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

247 Attribute Type Description	1.3.6.1.4.1.1466.115.121.1.3
248 Bit String	1.3.6.1.4.1.1466.115.121.1.6
249 Boolean	1.3.6.1.4.1.1466.115.121.1.7
250 Country String	1.3.6.1.4.1.1466.115.121.1.11
251 DN	1.3.6.1.4.1.1466.115.121.1.12
252 Directory String	1.3.6.1.4.1.1466.115.121.1.15
253 Facsimile Telephone Number	1.3.6.1.4.1.1466.115.121.1.22
254 Generalized Time	1.3.6.1.4.1.1466.115.121.1.24
255 IA5 String	1.3.6.1.4.1.1466.115.121.1.26
256 INTEGER	1.3.6.1.4.1.1466.115.121.1.27
257 LDAP Syntax Description	1.3.6.1.4.1.1466.115.121.1.54
258 Matching Rule Description	1.3.6.1.4.1.1466.115.121.1.30
259 Matching Rule Use Description	1.3.6.1.4.1.1466.115.121.1.31
260 Name And Optional UID	1.3.6.1.4.1.1466.115.121.1.34
261 Name Form Description	1.3.6.1.4.1.1466.115.121.1.35
262 Numeric String	1.3.6.1.4.1.1466.115.121.1.36
263 Object Class Description	1.3.6.1.4.1.1466.115.121.1.37
264 Octet String	1.3.6.1.4.1.1466.115.121.1.40
265 OID	1.3.6.1.4.1.1466.115.121.1.38
266 Other Mailbox	1.3.6.1.4.1.1466.115.121.1.39
267 Postal Address	1.3.6.1.4.1.1466.115.121.1.41

268	Presentation Address	1.3.6.1.4.1.1466.115.121.1.43
269	Printable String	1.3.6.1.4.1.1466.115.121.1.44
270	Substring Assertion	1.3.6.1.4.1.1466.115.121.1.58
271	Telephone Number	1.3.6.1.4.1.1466.115.121.1.50
272	UTC Time	1.3.6.1.4.1.1466.115.121.1.53

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

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

280 2.6 Profile-Specific Schema

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

283

```

284 <schema
285   targetNamespace="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
286   xmlns="http://www.w3.org/2001/XMLSchema"
287   elementFormDefault="unqualified"
288   attributeFormDefault="unqualified"
289   blockDefault="substitution"
290   version="2.0">
291   <annotation>
292     <documentation>
293       Document identifier: saml-schema-x500-2.0
294       Location: http://docs.oasis-open.org/security/saml/v2.0/
295       Revision history:
296         V2.0 (March, 2005):
297         Custom schema for X.500 attribute profile, first published in
298 SAML 2.0.
299     </documentation>
300   </annotation>
301   <attribute name="Encoding" type="string"/>
302 </schema>

```

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

304 2.7 Examples

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

```

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

```

314 **Appendix A. Acknowledgements**

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

- 317 • Hal Lockhart, BEA Systems, Inc.
- 318 • Rob Philpott, EMC Corporation
- 319 • Eric Tiffany, Liberty Alliance Project
- 320 • Scott Cantor, Internet2
- 321 • Bob Morgan, Internet2
- 322 • Tom Scavo, National Center for Supercomputing Applications (NCSA)
- 323 • Peter Davis, Neustar, Inc.
- 324 • Jeff Hodges, Neustar, Inc.
- 325 • Frederick Hirsch, Nokia Corporation
- 326 • Abbie Barbir, Nortel Networks Limited
- 327 • Paul Madsen, NTT Corporation
- 328 • Ari Kermaier, Oracle Corporation
- 329 • Prateek Mishra, Oracle Corporation
- 330 • Brian Campbell, Ping Identity Corporation
- 331 • Anil Saldhana, Red Hat
- 332 • Eve Maler, Sun Microsystems
- 333 • Emily Xu, Sun Microsystems
- 334 • Kent Spaulding, Tripod Technology Group, Inc.
- 335 • David Staggs, Veterans Health Administration

336 The editors would also like to acknowledge the following contributors:

- 337 • Mark Wahl, Microsoft Corporation

338 **Appendix B. Revision History**

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