



SAML V2.0 X.500/LDAP Attribute Profile

Working Draft 04, 14 October 2007

Specification URIs:

TBD

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>.

34 Notices

35 Copyright © OASIS Open 2007. All Rights Reserved.

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

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

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

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

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

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

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

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

78 **Table of Contents**

79 1 Introduction..... 4
80 1.1 Notation..... 4
81 1.2 Normative References..... 4
82 1.3 Conformance..... 5
83 1.3.1 SAML 2.0 X.500/LDAP Attribute Profile..... 5
84 2 SAML 2.0 X.500/LDAP Attribute Profile..... 6
85 2.1 Required Information..... 6
86 2.2 Profile Overview..... 6
87 2.3 SAML Attribute Naming..... 6
88 2.3.1 Attribute Name Comparison..... 7
89 2.4 Profile-Specific XML Attributes..... 7
90 2.5 SAML Attribute Values..... 7
91 2.6 Profile-Specific Schema..... 8
92 2.7 Examples..... 8
93 Appendix A. Acknowledgements..... 9
94 Appendix B. Revision History..... 10
95

96 1 Introduction

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

99 1.1 Notation

100 This specification uses normative text.

101 The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD
102 NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this specification are to be interpreted as
103 described in [RFC2119]:

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

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

109 Listings of XML schemas appear like this.

110 Example code listings appear like this.

112 Conventional XML namespace prefixes are used throughout the listings in this specification to stand for
113 their respective namespaces as follows, whether or not a namespace declaration is present in the
114 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].

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

117 1.2 Normative References

- 118 **[ASN.1]** Information technology - Abstract Syntax Notation One (ASN.1): Specification of
119 basic notation, ITU-T Recommendation X.680, July 2002. See
120 [http://www.itu.int/rec/recommendation.asp?type=folders&lang=e&parent=T-REC-](http://www.itu.int/rec/recommendation.asp?type=folders&lang=e&parent=T-REC-X.680)
121 [X.680](http://www.itu.int/rec/recommendation.asp?type=folders&lang=e&parent=T-REC-X.680).
122 **[eduPerson]** eduPerson.Idif. See <http://www.educause.edu/eduperson>.

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

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

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

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

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

136 **[RFC3061]** M. Mealling. *A URN Namespace of Object Identifiers*. IETF RFC 3061, February
137 2001. See <http://www.ietf.org/rfc/rfc3061.txt>.

138 **[SAML2Core]** S. Cantor et al. *Assertions and Protocols for the OASIS Security Assertion*
139 *Markup Language (SAML) V2.0*. OASIS Standard, March 2005. Document ID
140 saml-core-2.0-os. See [http://docs.oasis-open.org/security/saml/v2.0/saml-core-](http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf)
141 [2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf).

142 **[SAML2Prof]** S. Cantor et al. *Profiles for the OASIS Security Assertion Markup Language*
143 *(SAML) V2.0*. OASIS Standard, March 2005. Document ID saml-profiles-2.0-os.
144 See <http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf>.

145 **[SAMLX500-xsd]** S. Cantor et al. *SAML X.500/LDAP attribute profile schema*. OASIS SSTC, March
146 2005. Document ID saml-schema-x500-2.0. See [http://www.oasis-](http://www.oasis-open.org/committees/security/)
147 [open.org/committees/security/](http://www.oasis-open.org/committees/security/).

148 **[Schema1]** H. S. Thompson et al. *XML Schema Part 1: Structures*. World Wide Web
149 Consortium Recommendation, May 2001. See [http://www.w3.org/TR/2001/REC-](http://www.w3.org/TR/2001/REC-xmlschema-1-20010502/)
150 [xmlschema-1-20010502/](http://www.w3.org/TR/2001/REC-xmlschema-1-20010502/). Note that this specification normatively references
151 [Schema2], listed below.

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

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

160 **1.3 Conformance**

161 **1.3.1 SAML 2.0 X.500/LDAP Attribute Profile**

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

164 A relying party implementation conforms to this profile if it can accept assertions and other SAML-defined
165 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 [eduPerson], 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.

207 2.3.1 Attribute Name Comparison

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

211 Note that two SAML attributes resulting from two LDAP attributes with the same attribute type and
212 different attribute descriptions will also match for equality.

213 2.4 Profile-Specific XML Attributes

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

218 2.5 SAML Attribute Values

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

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

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

233	Attribute Type Description	1.3.6.1.4.1.1466.115.121.1.3
234	Bit String	1.3.6.1.4.1.1466.115.121.1.6
235	Boolean	1.3.6.1.4.1.1466.115.121.1.7
236	Country String	1.3.6.1.4.1.1466.115.121.1.11
237	DN	1.3.6.1.4.1.1466.115.121.1.12
238	Directory String	1.3.6.1.4.1.1466.115.121.1.15
239	Facsimile Telephone Number	1.3.6.1.4.1.1466.115.121.1.22
240	Generalized Time	1.3.6.1.4.1.1466.115.121.1.24
241	IA5 String	1.3.6.1.4.1.1466.115.121.1.26
242	INTEGER	1.3.6.1.4.1.1466.115.121.1.27
243	LDAP Syntax Description	1.3.6.1.4.1.1466.115.121.1.54
244	Matching Rule Description	1.3.6.1.4.1.1466.115.121.1.30
245	Matching Rule Use Description	1.3.6.1.4.1.1466.115.121.1.31
246	Name And Optional UID	1.3.6.1.4.1.1466.115.121.1.34
247	Name Form Description	1.3.6.1.4.1.1466.115.121.1.35
248	Numeric String	1.3.6.1.4.1.1466.115.121.1.36
249	Object Class Description	1.3.6.1.4.1.1466.115.121.1.37
250	Octet String	1.3.6.1.4.1.1466.115.121.1.40
251	OID	1.3.6.1.4.1.1466.115.121.1.38
252	Other Mailbox	1.3.6.1.4.1.1466.115.121.1.39
253	Postal Address	1.3.6.1.4.1.1466.115.121.1.41

254	Presentation Address	1.3.6.1.4.1.1466.115.121.1.43
255	Printable String	1.3.6.1.4.1.1466.115.121.1.44
256	Substring Assertion	1.3.6.1.4.1.1466.115.121.1.58
257	Telephone Number	1.3.6.1.4.1.1466.115.121.1.50
258	UTC Time	1.3.6.1.4.1.1466.115.121.1.53

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

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

266 2.6 Profile-Specific Schema

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

269

```

270 <schema
271   targetNamespace="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
272   xmlns="http://www.w3.org/2001/XMLSchema"
273   elementFormDefault="unqualified"
274   attributeFormDefault="unqualified"
275   blockDefault="substitution"
276   version="2.0">
277   <annotation>
278     <documentation>
279       Document identifier: saml-schema-x500-2.0
280       Location: http://docs.oasis-open.org/security/saml/v2.0/
281       Revision history:
282         V2.0 (March, 2005):
283         Custom schema for X.500 attribute profile, first published in
284 SAML 2.0.
285     </documentation>
286   </annotation>
287   <attribute name="Encoding" type="string"/>
288 </schema>

```

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

290 2.7 Examples

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

```

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

```

300 **Appendix A. Acknowledgements**

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

303 TBD

304 **Appendix B. Revision History**

- 305 ● Draft 01, initial correction of original profile to move Encoding attribute up to Attribute element.
- 306 ● Committee Draft 01, boilerplate edits for CD status.
- 307 ● Draft 02, incorporating feedback from public review.
- 308 ● Draft 03, clarify attribute option handling as out of scope, and revise structure to match new
309 OASIS requirements.
- 310 ● Draft 04, fix references and make other copyedits.