



# SAML V2.0 X.500/LDAP Attribute Profile

## Committee Draft 01, 19 December 2006

### Document identifier:

sstc-saml-attribute-x500-cd-01

### Location:

[http://www.oasis-open.org/committees/documents.php?wg\\_abbrev=security](http://www.oasis-open.org/committees/documents.php?wg_abbrev=security)

### Technical Committee:

OASIS Security Services TC

### Chair(s):

Hal Lockhart, BEA Systems, Inc.

Prateek Mishra, Oracle Corporation

### Editors:

Scott Cantor, Internet2

### Related Work:

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

### 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.

Technical Committee members should send comments on this specification to the Technical Committee's email list. Others should send comments to the Technical Committee by using the "Send A Comment" button on the Technical Committee'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 Intellectual Property Rights web page for the Security Services TC (<http://www.oasis-open.org/committees/security/ipr.php>).

## 33 **Table of Contents**

34	1 Introduction.....	3
35	1.1 Notation.....	3
36	2 SAML 2.0 X.500/LDAP Attribute Profile.....	4
37	2.1 Required Information.....	4
38	2.2 Profile Overview.....	4
39	2.3 SAML Attribute Naming.....	4
40	2.3.1 Attribute Name Comparison.....	5
41	2.4 Profile-Specific XML Attributes.....	5
42	2.5 SAML Attribute Values.....	5
43	2.6 Profile-Specific Schema.....	6
44	2.7 Examples.....	6
45	3 References.....	7
46	3.1 Normative References.....	7
47	Appendix A. Acknowledgements.....	8
48	Appendix B. Notices.....	9
49		

# 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.

## 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](mailto: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:

```
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 are unambiguous.

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.

### 108 2.3.1 Attribute Name Comparison

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

## 112 2.4 Profile-Specific XML Attributes

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

## 117 2.5 SAML Attribute Values

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

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

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

132	Attribute Type Description	1.3.6.1.4.1.1466.115.121.1.3
133	Bit String	1.3.6.1.4.1.1466.115.121.1.6
134	Boolean	1.3.6.1.4.1.1466.115.121.1.7
135	Country String	1.3.6.1.4.1.1466.115.121.1.11
136	DN	1.3.6.1.4.1.1466.115.121.1.12
137	Directory String	1.3.6.1.4.1.1466.115.121.1.15
138	Facsimile Telephone Number	1.3.6.1.4.1.1466.115.121.1.22
139	Generalized Time	1.3.6.1.4.1.1466.115.121.1.24
140	IA5 String	1.3.6.1.4.1.1466.115.121.1.26
141	INTEGER	1.3.6.1.4.1.1466.115.121.1.27
142	LDAP Syntax Description	1.3.6.1.4.1.1466.115.121.1.54
143	Matching Rule Description	1.3.6.1.4.1.1466.115.121.1.30
144	Matching Rule Use Description	1.3.6.1.4.1.1466.115.121.1.31
145	Name And Optional UID	1.3.6.1.4.1.1466.115.121.1.34
146	Name Form Description	1.3.6.1.4.1.1466.115.121.1.35
147	Numeric String	1.3.6.1.4.1.1466.115.121.1.36
148	Object Class Description	1.3.6.1.4.1.1466.115.121.1.37
149	Octet String	1.3.6.1.4.1.1466.115.121.1.40
150	OID	1.3.6.1.4.1.1466.115.121.1.38
151	Other Mailbox	1.3.6.1.4.1.1466.115.121.1.39
152	Postal Address	1.3.6.1.4.1.1466.115.121.1.41
153	Presentation Address	1.3.6.1.4.1.1466.115.121.1.43
154	Printable String	1.3.6.1.4.1.1466.115.121.1.44

155 Substring Assertion 1.3.6.1.4.1.1466.115.121.1.58  
156 Telephone Number 1.3.6.1.4.1.1466.115.121.1.50  
157 UTC Time 1.3.6.1.4.1.1466.115.121.1.53

158 For all other LDAP syntaxes, the attribute value is encoded, as the content of the <AttributeValue>  
159 element, by base64-encoding [RFC2045] the encompassing ASN.1 OCTET STRING-encoded LDAP  
160 attribute value. The xsi:type XML attribute MUST be set to **xsd:base64Binary**. The profile-specific  
161 Encoding XML attribute is provided in the <Attribute> element, with a value of LDAP.

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

## 164 2.6 Profile-Specific Schema

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

167

```
168 <schema  
169   targetNamespace="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"  
170   xmlns="http://www.w3.org/2001/XMLSchema"  
171   elementFormDefault="unqualified"  
172   attributeFormDefault="unqualified"  
173   blockDefault="substitution"  
174   version="2.0">  
175   <annotation>  
176     <documentation>  
177       Document identifier: saml-schema-x500-2.0  
178       Location: http://docs.oasis-open.org/security/saml/v2.0/  
179       Revision history:  
180         V2.0 (March, 2005):  
181         Custom schema for X.500 attribute profile, first published  
182 in SAML 2.0.  
183     </documentation>  
184   </annotation>  
185   <attribute name="Encoding" type="string"/>  
186 </schema>
```

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

## 188 2.7 Examples

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

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

## 3 References

198

199 The following works are referenced in the body of this specification.

### 3.1 Normative References

200

- 201 **[ASN.1]** Information technology - Abstract Syntax Notation One (ASN.1): Specification of  
202 basic notation, ITU-T Recommendation X.680, July 2002. See  
203 <http://www.itu.int/rec/recommendation.asp?type=folders&lang=e&parent=T-REC-X.680>.  
204
- 205 **[eduPerson]** eduPerson.Idif. See <http://www.educause.edu/eduperson>.
- 206 **[LDAP]** J. Hodges et al. *Lightweight Directory Access Protocol (v3): Technical  
207 Specification*. IETF RFC 3377, September 2002. See  
208 <http://www.ietf.org/rfc/rfc3377.txt>.
- 209 **[RFC2045]** N. Freed et al. *Multipurpose Internet Mail Extensions (MIME) Part One: Format  
210 of Internet Message Bodies*. IETF RFC 2045, November 1996. See  
211 <http://www.ietf.org/rfc/rfc2045.txt>.
- 212 **[RFC2119]** S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. IETF  
213 RFC 2119, March 1997. <http://www.ietf.org/rfc/rfc2119.txt>.
- 214 **[RFC2798]** M. Smith. *Definition of the inetOrgPerson LDAP Object Class*. IETF RFC 2798,  
215 April 2000. See <http://www.ietf.org/rfc/rfc2798.txt>.
- 216 **[RFC3061]** M. Mealling. *A URN Namespace of Object Identifiers*. IETF RFC 3061, February  
217 2001. See <http://www.ietf.org/rfc/rfc3061.txt>.
- 218 **[SAML2Core]** S. Cantor et al. *Assertions and Protocols for the OASIS Security Assertion  
219 Markup Language (SAML) V2.0*. OASIS Standard, March 2005. Document ID  
220 saml-core-2.0-os. See <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>.  
221
- 222 **[SAML2Prof]** S. Cantor et al. *Profiles for the OASIS Security Assertion Markup Language  
223 (SAML) V2.0*. OASIS Standard, March 2005. Document ID saml-profiles-2.0-os.  
224 See <http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf>.
- 225 **[SAMLX500-xsd]** S. Cantor et al. *SAML X.500/LDAP attribute profile schema*. OASIS SSTC,  
226 March 2005. Document ID saml-schema-x500-2.0. See <http://www.oasis-open.org/committees/security/>.  
227
- 228 **[Schema1]** H. S. Thompson et al. *XML Schema Part 1: Structures*. World Wide Web  
229 Consortium Recommendation, May 2001. See <http://www.w3.org/TR/2001/REC-xmlschema-1-20010502/>. Note that this specification normatively references  
230 [Schema2], listed below.  
231
- 232 **[Schema2]** Paul V. Biron, Ashok Malhotra. *XML Schema Part 2: Datatypes*. World Wide  
233 Web Consortium Recommendation, May 2001. See  
234 <http://www.w3.org/TR/2001/REC-xmlschema-2-20010502/>.
- 235 **[X.500]** Information technology - Open Systems Interconnection - The Directory:  
236 Overview of concepts, models and services. ITU-T Recommendation X.500,  
237 February 2001. See  
238 <http://www.itu.int/rec/recommendation.asp?type=folders&lang=e&parent=T-REC-X.500>.  
239  
240

## 241 **Appendix A. Acknowledgements**

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

- 244 • Hal Lockhart, BEA Systems, Inc.
- 245 • Steve Anderson, BMC Software
- 246 • Christopher Laskowski, Booz Allen Hamilton
- 247 • Rebekah Metz, Booz Allen Hamilton
- 248 • Carolina Canales-Valenzuela, Ericsson
- 249 • Dana Kaufman, Forum Systems, Inc.
- 250 • Ashish Patel, France Telecom
- 251 • Greg Whitehead, Hewlett-Packard
- 252 • Guy Denton, IBM
- 253 • Heather Hinton, IBM
- 254 • Anthony Nadalin, IBM
- 255 • Eric Tiffany, IEEE Industry Standards and Technology Org (IEEE-ISTO)
- 256 • Scott Cantor, Internet2
- 257 • Bob Morgan, Internet2
- 258 • Tom Scavo, National Center for Supercomputing Applications (NCSA)
- 259 • Peter Davis, Neustar, Inc.
- 260 • Jeff Hodges, Neustar, Inc.
- 261 • Frederick Hirsch, Nokia Corporation
- 262 • Abbie Barbir, Nortel Networks Limited
- 263 • Paul Madsen, NTT Corporation
- 264 • Ari Kermaier, Oracle Corporation
- 265 • Prateek Mishra, Oracle Corporation
- 266 • Brian Campbell, Ping Identity Corporation
- 267 • Rob Philpott, RSA Security
- 268 • Bhavna Bhatnagar, Sun Microsystems
- 269 • Eve Maler, Sun Microsystems
- 270 • Emily Xu, Sun Microsystems
- 271 • David Staggs, Veterans Health Administration



## 272 **Appendix B. Notices**

273 Copyright © OASIS Open 2006. All Rights Reserved.

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

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

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

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

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

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

305 OASIS takes no position regarding the validity or scope of any intellectual property or other  
306 rights that might be claimed to pertain to the implementation or use of the technology  
307 described in this document or the extent to which any license under such rights might or  
308 might not be available; neither does it represent that it has made any effort to identify any  
309 such rights. Information on OASIS' procedures with respect to rights in any document or  
310 deliverable produced by an OASIS Technical Committee can be found on the OASIS  
311 website. Copies of claims of rights made available for publication and any assurances of  
312 licenses to be made available, or the result of an attempt made to obtain a general license

313 or permission for the use of such proprietary rights by implementers or users of this OASIS  
314 Committee Specification or OASIS Standard, can be obtained from the OASIS TC  
315 Administrator. OASIS makes no representation that any information or list of intellectual  
316 property rights will at any time be complete, or that any claims in such list are, in fact,  
317 Essential Claims.