

---

# MACE-Dir SAML Attribute Profiles

~~April~~November 20067

## Document identifier:

~~draft-internet2-mace-dir-saml-attributes-2006~~04711

## Location:

<http://middleware.internet2.edu/dir>

## Editors:

Scott Cantor ([cantor.2@osu.edu](mailto:cantor.2@osu.edu)), The Ohio State University  
Keith Hazelton ([hazelton@doit.wisc.edu](mailto:hazelton@doit.wisc.edu)), University of Wisconsin-Madison

## Contributors:

RL "Bob" Morgan, University of Washington  
Tom Barton, University of Chicago  
Walter Hoehn, University of Memphis  
Tom Scavo, NCSA

## Abstract:

This document contains a pair of SAML attribute profiles addressing the recommended use of attribute definitions from the Internet2 MACE-Dir Working Group with the SAML 1.x and SAML 2.0 specifications.

## Table of Contents

20	1 Introduction.....	3
21	1.1 Notation.....	3
22	2 MACE-Dir Attribute Profile for SAML 1.x.....	4
23	2.1 Required Information.....	4
24	2.2 SAML Attribute Naming.....	4
25	2.2.1 Legacy Names.....	4
26	2.2.2 ADFS Namespace Exception.....	5
27	2.2.3 Attribute Name Comparison.....	6
28	2.3 SAML Attribute Values.....	6
29	2.3.1 Scoped Attribute Values.....	6
30	2.3.1.1 Structured Encoding.....	6
31	2.3.1.2 Simple Encoding.....	7
32	2.3.2 Non-LDAP Attributes.....	7
33	2.3.2.1 eduPersonTargetedID.....	7
34	2.3.2.1.1 Recommended Name and Syntax.....	7
35	2.3.2.1.2 Legacy Name and Syntax.....	8
36	2.4 Examples.....	8
37	3 MACE-Dir Attribute Profile for SAML 2.0.....	10
38	3.1 Required Information.....	10
39	3.2 SAML Attribute Naming.....	10
40	3.3 SAML Attribute Values.....	10
41	3.3.1 Non-LDAP Attributes.....	10
42	3.3.1.1 eduPersonTargetedID.....	10
43	3.4 Examples.....	11
44	4 References.....	13
45	4.1 Normative References.....	13
46	4.2 Non-Normative References.....	13
47		

---

# 1 Introduction

48

49 MACE-Dir Working Group specifications, including the eduPerson specification [eduPerson], define a set  
50 of LDAP object classes and associated attribute types at a level of detail sufficient to achieve  
51 interoperability with respect to the LDAP representation of those attribute types. It also provides  
52 clarifications and suggestions regarding the use of certain other common LDAP attribute types often used  
53 in conjunction with eduPerson.

54 These profiles specify a recommended mapping of these attribute types to the SAML 1.1 [SAMLCore] and  
55 SAML 2.0 [SAML2Core] specifications for use in the Internet2 Middleware Initiative community. SAML  
56 provides a general framework for expressing attribute information but does not define specific attribute  
57 types or impose other requirements on applications. These profiles enable SAML applications that wish to  
58 exchange MACE-Dir-specified and profiled attributes to interoperate.

59 Much of the SAML 1.1 profile should be understood as a retroactive effort to document practices  
60 developed in handling these attribute types in the implementation and deployments of the Shibboleth  
61 specification [ShibProt] and Shibboleth System software in support of the InCommon Federation  
62 (<http://www.incommonfederation.org/>).

63 The SAML 2.0 profile reflects both the enhanced capabilities and additional profiles defined in that  
64 specification, and the experiences gained working with the SAML 1.1 profile in the Shibboleth community.

## 1.1 Notation

65

66 This specification uses normative text to describe the use of SAML capabilities.

67 The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD  
68 NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this specification are to be interpreted as  
69 described in [RFC 2119]:

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

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

75       Listings of XML schemas appear like this.

76

77       Example code listings appear like this.

78 Conventional XML namespace prefixes are used throughout the listings in this specification to stand for  
79 their respective namespaces as follows, whether or not a namespace declaration is present in the  
80 example:

- 81 • The prefix `saml:` stands for the SAML 1.1 (and 1.0) assertion namespace,  
82     `urn:oasis:names:tc:SAML:1.0:assertion`
- 83 • The prefix `saml2:` stands for the SAML 2.0 assertion namespace,  
84     `urn:oasis:names:tc:SAML:2.0:assertion`
- 85 • The prefix `xsi:` stands for the W3C XML Schema-instance namespace,  
86     `http://www.w3.org/2001/XMLSchema-instance`
- 87 • The prefix `xsd:` stands for the W3C XML Schema namespace,  
88     `http://www.w3.org/2001/XMLSchema`  
89     in example listings. In schema listings, this is the default namespace and no prefix is shown.

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

---

## 2 MACE-Dir Attribute Profile for SAML 1.x

This profile defines the syntax for expressing attribute types defined (or referenced) by MACE-Dir Working Group specifications in SAML 1.1. With respect to attribute representation, SAML 1.0 is identical to SAML 1.1; therefore, this profile applies to both specifications equally.

### 2.1 Required Information

**Identification:** urn:mace:dir:profiles:attribute:samlv1

**Contact information:** mace-dir@internet2.edu

**Description:** Given below

**Updates:** Various informal documents and drafts describing the use of eduPerson attribute types in SAML 1.1

### 2.2 SAML Attribute Naming

To ensure uniqueness, each attribute type is assigned a name in the form of a URI. To construct attribute names, the URN `oid` namespace described in [RFC3061] is used. The `AttributeName` XML attribute is based on the OBJECT IDENTIFIER assigned to the attribute type. This naming procedure mirrors the X.500/LDAP attribute profile defined in [\[SAML2Pref\]](#).

Example:

```
urn:oid:2.5.4.3
```

Since MACE-Dir 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.

SAML 1.1 does not specify any interoperable means of establishing the kind of name used, so the convention used within this profile is that the `AttributeNamespace` XML attribute in `<saml:Attribute>` elements MUST be set to

```
urn:mace:shibboleth:1.0:attributeNamespace:uri
```

The meaning of this URI is best understood as "the corresponding SAML `AttributeName` is in the form of a URI and uniquely identifies the SAML attribute". It is analagous to the SAML 2.0 `NameFormat` value of

```
urn:oasis:names:tc:SAML:2.0:attrname-format:uri
```

Despite the use of this particular URI value, this profile does not depend specifically on [ShibProt] nor on the Shibboleth System's implementation of SAML. Note also that other attribute profiles are free to define naming conventions of their own.

#### 2.2.1 Legacy Names

This profile post-dates the establishment of an alternate naming convention designed to improve the human-readability of attribute information in the absence of a facility such as the `FriendlyName` XML attribute supported by [SAML2Core]. Most existing attribute types have already been assigned URI names using a convention based on appending the attribute type's "short name" to the URN prefix:

```
urn:mace:dir:attribute-def:
```

128 The following legacy attribute names have been formally assigned in [AttrDefs], and the corresponding  
129 attribute types are exempt from the naming convention described in the previous section when bound to  
130 SAML 1.x:

131 eduPersonScopedAffiliation  
132 eduPersonPrimaryAffiliation  
133 eduPersonAffiliation  
134 eduPersonPrincipalName  
135 eduPersonEntitlement  
136 eduPersonTargetedID  
137 eduPersonNickname  
138 eduPersonPrimaryOrgUnitDN  
139 eduPersonOrgUnitDN  
140 eduPersonOrgDN  
141 [eduCourseMember](#)  
142 businessCategory  
143 carLicense  
144 cn  
145 departmentNumber  
146 description  
147 displayName  
148 employeeNumber  
149 employeeType  
150 facsimileTelephoneNumber  
151 givenName  
152 homePhone  
153 homePostalAddress  
154 initials  
155 jpegPhoto  
156 l  
157 labeledURI  
158 mail  
159 manager  
160 mobile  
161 o  
162 ou  
163 pager  
164 physicalDeliveryOfficeName  
165 postalAddress  
166 postalCode  
167 postOfficeBox  
168 preferredLanguage  
169 roomNumber  
170 seeAlso  
171 sn  
172 st  
173 street  
174 telephoneNumber  
175 title  
176 uid  
177 userCertificate  
178 userSMIMECertificate

179 This is a fairly exhaustive list of existing LDAP attribute types referenced by [eduPerson] (and a few that  
180 aren't). Thus, the new naming convention is likely to be applied only [ifas](#) new attribute types emerge.

## 181 | **2.2.2 ADFS Namespace Exception**

182 | An additional exception to the rules defined in section 2.2 applies to the use of SAML 1.1 attributes with  
183 | the WS-Federation passive profile implemented by Microsoft's ADFS product, among others.  
184 | Implementation experience suggests that interoperability is best achieved by using an  
185 | AttributeName XML attribute of <http://schemas.xmlsoap.org/claims>, matching the  
186 | value used for the predefined "claim" types defined by Microsoft.

187 | Deployers MAY use this alternate namespace value if necessary, but SHOULD avoid its use with SAML-  
188 | only deployments.

## 189 | **2.2.3 Attribute Name Comparison**

190 | Two `<saml:Attribute>` elements refer to the same SAML attribute if and only if their `AttributeName`  
191 | XML attribute values are equal (using a case-sensitive, binary comparison).

## 192 | **2.3 SAML Attribute Values**

193 | With two significant exceptions, the syntax rules defined by the SAML 2.0 X.509/LDAP attribute profile in  
194 | [\[SAML2Prof\]](#) are to be applied, with the obvious caveat that the `<saml:AttributeValue>` element is  
195 | substituted for the `<saml2:AttributeValue>` element in that specification.

196 | The first exception is that the XML attribute named `Encoding` defined by that profile is NOT specified for  
197 | use with this profile.

198 | The second exception is more significant and pertains to "scoped" attributes, which are discussed in the  
199 | next section.

### 200 | **2.3.1 Scoped Attribute Values**

201 | In the course of developing implementations and producing the informal attribute bindings that have led to  
202 | this profile, a few attribute types were identified as consisting of a relation between two separate pieces of  
203 | data, termed a *value* and a *scope* or *domain*. For policy reasons, it seemed useful to distinguish the two  
204 | halves of the value in a more explicit fashion than merely by using a separator character (typically the @  
205 | symbol).

206 | As a result, attribute types identified as having this characteristic were given special treatment and for  
207 | compatibility reasons are considered exceptions to the standard syntax rules, which would normally  
208 | dictate that the entire `value@scope` string be placed within the `<saml:AttributeValue>` element.

209 | Unfortunately, this convention, while absolutely legal with respect to the SAML 1.1 [\[SAMLCore\]](#)  
210 | specification, has proven to be virtually impossible to support in commercial products, creating limitations  
211 | on interoperability between them and the Shibboleth System software. Therefore, a set of two alternate  
212 | encoding rules for scoped attribute values has been developed. To maximize compatibility with existing  
213 | deployments, the `AttributeName` XML attribute is used as a signal for which set of encoding rules to  
214 | use.

215 | Essentially, the older `urn:mace:dir:attribute-def` naming convention is used to signal the  
216 | structured encoding rules in section 2.3.1.1, while the newer OID-style naming convention is used to  
217 | signal the simple non-exceptional encoding rules in section 2.3.1.2. This also aligns attribute name and  
218 | value conventions used in SAML 1.1 with the rules adopted for use with SAML 2.0.

### 219 | **2.3.1.1 Structured Encoding**

220 | When using the structured encoding, ~~instead~~, an XML attribute named `Scope` is used to carry the so-  
221 | called "right-hand side" of the scope/domain-qualified string, with the left-hand side placed within the  
222 | `<saml:AttributeValue>` element. No separator character appears in either location (as the halves are  
223 | already carried separately and need no additional separator). The `Scope` XML attribute is NOT  
224 | namespace-qualified.

225 | Examples are shown in section 2.4.

226 | The following attributes ss (when using the associated `AttributeName`) have been designated as scoped  
227 | for the purposes of applying this exception to the standard value profile:

```
228 |     urn:mace:dir:attribute-def:eduPersonScopedAffiliation  
229 |     urn:mace:dir:attribute-def:eduPersonPrincipalName  
230 |     urn:mace:dir:attribute-def:eduPersonTargetedID  
231 |     urn:mace:dir:attribute-def:eduCourseMember
```

232 | Additional attributes MAY be designated as scoped when appropriate, and willmay be subject to these  
233 | syntax rules for consistency.

### 234 | **2.3.1.2 Simple Encoding**

235 | To facilitate interoperability with SAML implementations incapable of handling the full range of attribute  
236 | value behavior permitted by the standard, an alternate simplified encoding may be used that follows the  
237 | new syntax rules defined by the SAML 2.0 X.500/LDAP attribute profile in . Specifically both the `value` and  
238 | `scope` are carried directly within the `<saml:AttributeValue>` element, with the `@` separator.

239 | To avoid collision with the previously deployed encoding described in the previous section, the newly  
240 | defined OID-style attribute names MUST be used when following the simple encoding rules.

241 | For example, when following the simpler encoding rules, the `eduPersonPrincipalName` attribute is  
242 | assigned an `AttributeName` of `urn:oid:1.3.6.1.4.1.5923.1.1.1.6` instead of the typical name of  
243 | `urn:mace:dir:attribute-def:eduPersonPrincipalName`.

## 244 | **2.3.2 Non-LDAP Attributes**

245 | This profile provides uniform treatment of attribute types whose values can be described in terms of  
246 | X.500/LDAP directory syntax. Other attribute types are addressed on a case by case basis below, or in  
247 | other specifications as appropriate.

### 248 | **2.3.2.1 eduPersonTargetedID**

249 | The `eduPersonTargetedID` attribute is an outlier in the current set of attribute types specified by  
250 | MACE-Dir because its abstract representation cannot easily be bound to an LDAP directory syntax, nor  
251 | are its semantics easily implemented using an LDAP directory. It therefore requires special treatment  
252 | within this profile.

253 | Abstractly, an `eduPersonTargetedID` value consists of a triple:

- 254 | • the unique identifier of the identity provider that created the value
- 255 | • the unique identifier of the service provider or group for which the value was created
- 256 | • the opaque string value itself

257 For compatibility with legacy implementations, this profile provides for two alternate representations  
258 distinguished by the name used to identify the attribute. Examples of both representations can be found in  
259 section 2.4.

### 260 2.3.2.1.1 Recommended Name and Syntax

261 If the `AttributeName` attribute of the `<saml:Attribute>` element has value

262 `urn:oid:1.3.6.1.4.1.5923.1.1.1.10`

263 then the `<saml:AttributeValue>` element's content MUST be a `<saml2:NameID>` element with a  
264 `Format` XML attribute of

265 `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent`

266 as described in section 8.3.7 of [SAML2Core]. The unique identifiers of the identity provider and service  
267 provider map directly to the `NameQualifier` and `SPNameQualifier` XML attributes, respectively.

268 New applications are encouraged to use this newer syntax, when possible.

### 269 2.3.2.1.2 Legacy Name and Syntax

270 If the `AttributeName` attribute of the `<saml:Attribute>` element has the value

271 `urn:mace:dir:attribute-def:eduPersonTargetedID`

272 then the `<saml:AttributeValue>` element's content MUST be the opaque string identifier value and it  
273 MUST have a `Scope` XML attribute. It is RECOMMENDED that the value of this XML attribute be set to  
274 the unique identifier of the identity provider (although other values are permitted). The unique identifier of  
275 the service provider is not represented in this case and must be derived from the surrounding context.

## 276 2.4 Examples

277 The following is an example of a mapping of the `givenName` directory attribute, representing the SAML  
278 assertion subject's first name. Its LDAP syntax is Directory String. Since the XML type of the value is a  
279 built-in type, it is included within the `xsi:type` XML attribute.

```
280 <saml:Attribute AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri"  
281   AttributeName="urn:mace:dir:attribute-def:givenName">  
282   <saml:AttributeValue xsi:type="xsd:string">Scott</saml:AttributeValue>  
283 </saml:Attribute>
```

284 The following is an example mapping of an `eduPersonPrincipalName` directory attribute with the  
285 LDAP value of "cantor.2@osu.edu". Its LDAP syntax is Directory String, but it is a scoped attribute, and is  
286 therefore subject to alternative syntax rules ([when using its non-OID-style name](#)). The resulting XML type  
287 of the value is therefore a complex type and is omitted to ease interoperability.

```
289 <saml:Attribute AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri"  
290   AttributeName="urn:mace:dir:attribute-def:eduPersonPrincipalName">  
291   <saml:AttributeValue Scope="osu.edu">cantor.2</saml:AttributeValue>  
292 </saml:Attribute>
```

294 [The following is the same attribute as in the previous example, but using its OID-style name to signal the  
295 use of the simple encoding rules, for compatibility with a wider range of software.](#)

```
296 <saml:Attribute AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri"  
297   AttributeName="urn:oid:1.3.6.1.4.1.5923.1.1.1.6">  
298   <saml:AttributeValue xsi:type="xsd:string">cantor.2@osu.edu</saml:AttributeValue>  
299 </saml:Attribute>
```

300

301 [The following is the same attribute again, but using the conventions defined for ADFS-interoperable](#)  
302 [deployment.](#)

```
303 <saml:Attribute AttributeNamespace="http://schemas.xmlsoap.org/claims"  
304     AttributeName="urn:oid:1.3.6.1.4.1.5923.1.1.1.6">  
305     <saml:AttributeValue xsi:type="xsd:string">cantor.2@osu.edu</saml:AttributeValue>  
306 </saml:Attribute>
```

308 The following is an example mapping of an eduCourseOffering directory attribute. Its LDAP syntax is  
309 URI. Since the XML type of the value is a built-in type, it is carried within the xsi:type XML attribute.  
310 Since it is a relatively new attribute type, it does not have an assigned "legacy" name and is therefore  
311 named in accordance with its OBJECT IDENTIFIER, 1.3.6.1.4.1.5923.1.6.1.1.

```
312 <saml:Attribute AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri"  
313     AttributeName="urn:oid:1.3.6.1.4.1.5923.1.6.1.1">  
314     <saml:AttributeValue xsi:type="xsd:anyURI"  
315     >urn:mace:uchicago.edu:classes:autumn2004:phys12100.003</saml:AttributeValue>  
316 </saml:Attribute>
```

317  
318 The following is an example mapping of an eduPersonTargetedID attribute created by the identity  
319 provider named "https://idp.example.org/shibboleth" for the service provider named  
320 "https://sp.example.org/shibboleth" with the opaque value of "1234567890". The legacy name and value  
321 syntax is used.

```
322 <saml:Attribute AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri"  
323     AttributeName="urn:mace:dir:attribute-def:eduPersonTargetedID">  
324     <saml:AttributeValue  
325     Scope="https://idp.example.org/shibboleth">1234567890</saml:AttributeValue>  
326 </saml:Attribute>
```

327  
328 The following is the same attribute shown with the newer, recommended name and value syntax.

```
329 <saml:Attribute AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri"  
330     AttributeName="urn:oid:1.3.6.1.4.1.5923.1.1.1.10">  
331     <saml:AttributeValue>  
332     <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"  
333     NameQualifier="https://idp.example.org/shibboleth"  
334     SPNameQualifier="https://sp.example.org/shibboleth"  
335     >1234567890</saml2:NameID>  
336     </saml:AttributeValue>  
337 </saml:Attribute>
```

---

## 3 MACE-Dir Attribute Profile for SAML 2.0

338

339 This profile defines the syntax for expressing attribute types defined (or referenced) by MACE-Dir Working  
340 Group specifications in SAML 2.0. Most of the attribute types defined or referenced by MACE-Dir have (or  
341 can be given) LDAP representations, and as a matter of procedure are always assigned an OBJECT  
342 IDENTIFIER. Therefore, in the interest of expediency, the X.500/LDAP attribute profile defined in  
343 [\[SAML2Prof\]](#) is adopted whenever possible. This profile directly addresses naming, the mapping of  
344 directory syntax to XML syntax, comparison rules, etc. Exceptions to this general policy are noted.

### 3.1 Required Information

346 **Identification:** urn:mace:dir:profiles:attribute:samlv2

347 **Contact information:** mace-dir@internet2.edu

348 **Description:** Given below

349 **Updates:** The SAML 1.x profile

350 **Depends On:** The X.500/LDAP attribute profile in [\[SAML2Prof\]](#).

### 3.2 SAML Attribute Naming

352 All attribute types specified by MACE-Dir possess an OBJECT IDENTIFIER. Therefore attribute naming  
353 and name comparison is in accordance with the X.500/LDAP attribute profile in [\[SAML2Prof\]](#). If the  
354 `FriendlyName` XML attribute is used, then it SHOULD carry the short name of the attribute type.

355 The legacy names assigned for use with the SAML 1.x attribute profile MUST NOT be used with this  
356 profile.

### 3.3 SAML Attribute Values

358 If an attribute type is associated with an X.500/LDAP directory syntax, then the syntax rules defined by the  
359 X.500/LDAP attribute profile in [\[SAML2Prof\]](#) are to be applied directly. This includes scoped attributes  
360 typed as Directory String, such as `eduPersonScopedAffiliation`.

361 Diverging from the SAML 1.x profile, both the *value* and *scope* are always carried directly within the  
362 `<saml2:AttributeValue>` element, with the `@` separator. Such attribute types are therefore no longer  
363 "exception" cases. The intent is to ease directory integration and compatibility with the limitations of  
364 standard SAML software, commercial and otherwise.

365 Examples are shown in section 3.4.

#### 3.3.1 Non-LDAP Attributes

367 This profile provides uniform treatment of attribute types whose values can be described in terms of  
368 X.500/LDAP directory syntax. Other attribute types are addressed on a case by case basis below, or in  
369 other specifications as appropriate.

##### 3.3.1.1 eduPersonTargetedID

371 The `eduPersonTargetedID` attribute is an outlier because its abstract representation cannot easily be  
372 bound to an LDAP directory syntax, nor are its semantics easily implemented using an LDAP directory. It  
373 therefore requires special treatment within this profile.

374 Abstractly, an eduPersonTargetedID value consists of a triple:

- 375 • the unique identifier of the identity provider that created the value
- 376 • the unique identifier of the service provider or group for which the value was created
- 377 • the opaque string value itself

378 The `<saml2:AttributeValue>` element's content MUST be a `<saml2:NameID>` element with a  
379 Format XML attribute of

```
380 urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
```

381 as described in section 8.3.7 of [SAML2Core]. The unique identifiers of the identity provider and service  
382 provider map directly to the NameQualifier and SPNameQualifier XML attributes, respectively.

383 An example can be found in section 3.4.

### 384 3.4 Examples

385 The following is an example of a mapping of the givenName directory attribute, representing the SAML  
386 assertion subject's first name. Its LDAP syntax is Directory String. Since the XML type of the value is a  
387 built-in type, it is included within the xsi:type XML attribute.

```
388 <saml2:Attribute xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"  
389   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"  
390   Name="urn:oid:2.5.4.42" FriendlyName="givenName">  
391   <saml2:AttributeValue xsi:type="xsd:string"  
392     x500:Encoding="LDAP">Steven</saml2:AttributeValue>  
393 </saml2:Attribute>
```

394  
395 The following is an example mapping of an eduPersonPrincipalName directory attribute with the  
396 LDAP value of "cantor.2@osu.edu". Its LDAP syntax is Directory String, and it is a scoped attribute, but is  
397 covered by this profile directly without special treatment. Since the XML type of the value is a built-in type,  
398 it is included within the xsi:type XML attribute.

```
399 <saml2:Attribute xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"  
400   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"  
401   Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6" FriendlyName="eduPersonPrincipalName">  
402   <saml2:AttributeValue xsi:type="xsd:string"  
403     x500:Encoding="LDAP">cantor.2@osu.edu</saml2:AttributeValue>  
404 </saml2:Attribute>
```

406 The following is an example mapping of an eduCourseOffering directory attribute. Its LDAP syntax is  
407 URI. Since the XML type of the value is a built-in type, it is carried within the xsi:type XML attribute.

```
408 <saml2:Attribute xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"  
409   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"  
410   Name="urn:oid:1.3.6.1.4.1.5923.1.6.1.1" FriendlyName="eduCourseOffering">  
411   <saml2:AttributeValue xsi:type="xsd:anyURI" x500:Encoding="LDAP"  
412     >urn:mace:uchicago.edu:classes:autumn2004:phys12100.003</saml2:AttributeValue>  
413 </saml2:Attribute>
```

414  
415 The following is an example mapping of an eduPersonTargetedID attribute created by the identity  
416 provider named "https://idp.example.org/shibboleth" for the service provider named  
417 "https://sp.example.org/shibboleth" with the opaque value of "1234567890".

```
418 <saml2:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"  
419   Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.10"  
420   FriendlyName="eduPersonTargetedID">  
421   <saml2:AttributeValue>  
422     <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"  
423       NameQualifier="https://idp.example.org/shibboleth"
```

```
424         SPNameQualifier="https://sp.example.org/shibboleth"  
425         >1234567890</saml2:NameID>  
426     </saml2:AttributeValue>  
427 </saml2:Attribute>
```

---

## 4 References

428

429 The following works are cited in the body of this specification.

### 4.1 Normative References

430

- 431 **[eduPerson]** MACE-Dir. *eduPerson Specification (200361204a)*. Internet2-MACE,  
432 December 2003. [http://www.nmi-edit.org/eduPerson/internet2-mace-dir-](http://www.nmi-edit.org/eduPerson/internet2-mace-dir-eduperson-200312.html)  
433 [eduperson-200312.html](http://www.nmi-edit.org/eduPerson/internet2-mace-dir-eduperson-200312.html)  
434 [http://www.nmi-edit.org/eduPerson/internet2-mace-dir-](http://www.nmi-edit.org/eduPerson/internet2-mace-dir-eduperson-200604.html)  
[eduperson-200604.html](http://www.nmi-edit.org/eduPerson/internet2-mace-dir-eduperson-200604.html).
- 435 **[eduCourse]** MACE-CourseID. *LDAP representations of eduCourse attributes and an auxiliary*  
436 *object class (200507)*. Internet2-MACE, July 2005.  
437 [http://middleware.internet2.edu/courseid/docs/internet2-mace-dir-courseid-](http://middleware.internet2.edu/courseid/docs/internet2-mace-dir-courseid-educourse-ldap-200507.html)  
438 [educourse-ldap-200507.html](http://middleware.internet2.edu/courseid/docs/internet2-mace-dir-courseid-educourse-ldap-200507.html)
- 439 **[AttrDefs]** MACE-Dir. *Attribute Registrations*. Internet2-MACE.  
440 <http://middleware.internet2.edu/urn-mace/urn-mace-dir-attribute-def.html>.
- 441 **[RFC 2119]** S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. IETF  
442 RFC 2119, March 1997. <http://www.ietf.org/rfc/rfc2119.txt>.
- 443 **[RFC 2396]** T. Berners-Lee et al. *Uniform Resource Identifiers (URI): Generic Syntax*. IETF  
444 RFC 2396, August, 1998. <http://www.ietf.org/rfc/rfc2396.txt>.
- 445 **[RFC3061]** M. Mealling. *A URN Namespace of Object Identifiers*. IETF RFC 3061, February  
446 2001. See <http://www.ietf.org/rfc/rfc3061.txt>.
- 447 **[SAMLCore]** E. Maler et al. *Assertions and Protocols for the OASIS Security Assertion Markup*  
448 *Language (SAML)*. OASIS, September 2003. Document ID oasis-sstc-saml-core-  
449 1.1. <http://www.oasis-open.org/committees/security/>.
- 450 **[SAML-XSD]** E. Maler et al. *SAML assertion schema*. OASIS, September 2003. Document ID  
451 oasis-sstc-saml-schema-assertion-1.1. [http://www.oasis-](http://www.oasis-open.org/committees/security/)  
452 [open.org/committees/security/](http://www.oasis-open.org/committees/security/).
- 453 **[SAML2Core]** S. Cantor et al., *Assertions and Protocols for the OASIS Security Assertion*  
454 *Markup Language (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-  
455 core-2.0-os. See <http://www.oasis-open.org/committees/security/>.
- 456 **[SAML2Prof]** S. Cantor et al., *Profiles for the OASIS Security Assertion Markup Language*  
457 *(SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-profiles-2.0-os. See  
458 <http://www.oasis-open.org/committees/security/>.
- 459 **[SAML-X500]** S. Cantor., *SAML V2.0 X.500/LDAP Attribute Profile, Committee Draft 02*. OASIS  
460 SSTC, November 2007. Document ID sstc-saml-attribute-x500-cd-02. See  
461 <http://www.oasis-open.org/committees/security/>.
- 462 **[SAML2-XSD]** S. Cantor et al. *SAML 2.0 Assertion Schema*. OASIS, March 2005. Document ID  
463 saml-schema-assertion-2.0. <http://www.oasis-open.org/committees/security/>.
- 464 **[Schema2]** P. V. Biron et al. *XML Schema Part 2: Datatypes*. World Wide Web Consortium  
465 Recommendation, May 2001. <http://www.w3.org/TR/xmlschema-2/>.

### 4.2 Non-Normative References

466

- 467 **[ShibProt]** S. Cantor et al. *Shibboleth Architecture: Protocols and Profiles*. Internet2-MACE,  
468 September 2005. [http://shibboleth.internet2.edu/docs/draft-mace-shibboleth-arch-](http://shibboleth.internet2.edu/docs/draft-mace-shibboleth-arch-protocols-latest.pdf)  
469 [protocols-latest.pdf](http://shibboleth.internet2.edu/docs/draft-mace-shibboleth-arch-protocols-latest.pdf).