
1 MACE-Dir SAML Attribute Profiles

2 April 2008

3 **Document identifier:**

4 internet2-mace-dir-saml-attributes-200804

5 **Location:**

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

7 **Editors:**

8 Scott Cantor (cantor.2@osu.edu), The Ohio State University

9 Keith Hazelton (hazelton@doit.wisc.edu), University of Wisconsin-Madison

10 **Contributors:**

11 RL "Bob" Morgan, University of Washington

12 Tom Barton, University of Chicago

13 Walter Hoehn, University of Memphis

14 Tom Scavo, NCSA

15 **Abstract:**

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

Table of Contents

20	1 Introduction.....	3
21	1.1 SAML Profile Reference.....	3
22	1.2 Notation.....	3
23	2 MACE-Dir Attribute Profile for SAML 1.x.....	5
24	2.1 Required Information.....	5
25	2.2 SAML Attribute Naming.....	5
26	2.2.1 Legacy Names.....	5
27	2.2.2 ADFS Namespace Exception.....	6
28	2.2.3 Attribute Name Comparison.....	7
29	2.3 SAML Attribute Values.....	7
30	2.3.1 Scoped Attribute Values.....	7
31	2.3.1.1 Structured Encoding.....	7
32	2.3.1.2 Simple Encoding.....	8
33	2.3.2 Non-LDAP Attributes.....	8
34	2.3.2.1 eduPersonTargetedID.....	8
35	2.3.2.1.1 Recommended Name and Syntax.....	8
36	2.3.2.1.2 Legacy Name and Syntax.....	9
37	2.4 NameIdentifier Usage.....	9
38	2.5 Examples.....	9
39	3 MACE-Dir Attribute Profile for SAML 2.0.....	11
40	3.1 Required Information.....	11
41	3.2 SAML Attribute Naming.....	11
42	3.3 SAML Attribute Values.....	11
43	3.3.1 Non-LDAP Attributes.....	11
44	3.3.1.1 eduPersonTargetedID.....	11
45	3.4 NameID Usage.....	12
46	3.5 Examples.....	12
47	4 References.....	14
48	4.1 Normative References.....	14
49	4.2 Non-Normative References.....	14
50		

1 Introduction

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

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

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

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

1.1 SAML Profile Reference

The original X.500/LDAP attribute profile from the SAML 2.0 standard has been deprecated by the SAML TC due to an XML schema error involving the `Encoding XML` attribute. This document references a committee draft version of the replacement profile.

1.2 Notation

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

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 [RFC 2119]:

...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:

- The prefix `saml:` stands for the SAML 1.1 (and 1.0) assertion namespace, `urn:oasis:names:tc:SAML:1.0:assertion`
- The prefix `saml2:` stands for the SAML 2.0 assertion namespace, `urn:oasis:names:tc:SAML:2.0:assertion`

- 92 • The prefix `xsi:` stands for the W3C XML Schema-instance namespace,
93 `http://www.w3.org/2001/XMLSchema-instance`
- 94 • The prefix `xsd:` stands for the W3C XML Schema namespace,
95 `http://www.w3.org/2001/XMLSchema`
96 in example listings. In schema listings, this is the default namespace and no prefix is shown.
- 97 This specification uses the following typographical conventions in text: `<ns:Element>`, `Attribute`,
98 **Datatype**, `OtherCode`.

99 2 MACE-Dir Attribute Profile for SAML 1.x

100 This profile defines the syntax for expressing attribute types defined (or referenced) by MACE-Dir Working
101 Group specifications in SAML 1.1. With respect to attribute representation, SAML 1.0 is identical to SAML
102 1.1; therefore, this profile applies to both specifications equally.

103 2.1 Required Information

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

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

106 **Description:** Given below

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

109 2.2 SAML Attribute Naming

110 To ensure uniqueness, each attribute type is assigned a name in the form of a URI. To construct attribute
111 names, the URN `oid` namespace described in [RFC3061] is used. The `AttributeName` XML attribute is
112 based on the OBJECT IDENTIFIER assigned to the attribute type. This naming procedure mirrors the
113 X.500/LDAP attribute profile defined in [SAML-X500].

114 Example:

```
115 urn:oid:2.5.4.3
```

116 Since MACE-Dir procedures require that every attribute type be identified with a unique OBJECT
117 IDENTIFIER, this naming scheme ensures that the derived SAML attribute names are unambiguous.

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

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

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

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

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

129 2.2.1 Legacy Names

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

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

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

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

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

188 **2.2.2 ADFS Namespace Exception**

189 An additional exception to the rules defined in section 2.2 applies to the use of SAML 1.1 attributes with
190 the WS-Federation passive profile implemented by Microsoft's ADFS product, among others.

191 Implementation experience suggests that interoperability is best achieved by using an
192 `AttributeNameSpace` XML attribute of `http://schemas.xmlsoap.org/claims`, matching the
193 value used for the predefined "claim" types defined by Microsoft.

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

196 2.2.3 Attribute Name Comparison

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

199 2.3 SAML Attribute Values

200 With two significant exceptions, the syntax rules defined by the SAML 2.0 X.500/LDAP attribute profile
201 [SAML-X500] are to be applied, with the obvious caveat that the `<saml:AttributeValue>` element is
202 substituted for the `<saml2:AttributeValue>` element in that specification.

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

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

207 2.3.1 Scoped Attribute Values

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

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

216 Unfortunately, this convention, while absolutely legal with respect to the SAML 1.1 [SAMLCore]
217 specification, has proven to be virtually impossible to support in commercial products, creating limitations
218 on interoperability between them and the Shibboleth System software. Therefore, a set of two alternate
219 encoding rules for scoped attribute values has been developed. To maximize compatibility with existing
220 deployments, the `AttributeName` XML attribute is used as a signal for which set of encoding rules to
221 use.

222 Essentially, the older `urn:mace:dir:attribute-def` naming convention is used to signal the
223 structured encoding rules in section 2.3.1.1, while the newer OID-style naming convention is used to
224 signal the simple non-exceptional encoding rules in section 2.3.1.2.

225 2.3.1.1 Structured Encoding

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

231 Examples are shown in section 2.5.

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

234 `urn:mace:dir:attribute-def:eduPersonScopedAffiliation`
235 `urn:mace:dir:attribute-def:eduPersonPrincipalName`
236 `urn:mace:dir:attribute-def:eduPersonTargetedID`
237 `urn:mace:dir:attribute-def:eduCourseMember`

238 Additional attributes MAY be designated as scoped when appropriate, and may be subject to these syntax
239 rules for consistency.

240 **2.3.1.2 Simple Encoding**

241 To facilitate interoperability with SAML implementations incapable of handling the full range of attribute
242 value behavior permitted by the standard, an alternate simplified encoding may be used that follows the
243 new syntax rules defined by the SAML 2.0 X.500/LDAP attribute profile in [SAML-X500]. Specifically both
244 the *value* and *scope* are carried directly within the `<saml:AttributeValue>` element, with the @
245 separator.

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

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

251 **2.3.2 Non-LDAP Attributes**

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

255 **2.3.2.1 eduPersonTargetedID**

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

260 Abstractly, an `eduPersonTargetedID` value consists of a triple:

- 261 • the unique identifier of the identity provider that created the value
- 262 • the unique identifier of the service provider or group for which the value was created
- 263 • the opaque string value itself

264 For compatibility with legacy implementations, this profile provides for two alternate representations
265 distinguished by the name used to identify the attribute. Examples of both representations can be found in
266 section 2.5.

267 **2.3.2.1.1 Recommended Name and Syntax**

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

269 `urn:oid:1.3.6.1.4.1.5923.1.1.1.10`

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

272 urn:oasis:names:tc:SAML:2.0:nameid-format:persistent

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

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

276 2.3.2.1.2 Legacy Name and Syntax

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

278 urn:mace:dir:attribute-def:eduPersonTargetedID

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

283 2.4 NameIdentifier Usage

284 Some attributes uniquely identify principals that are the subject of SAML assertions. To maximize
285 interoperability, it is useful to be able to express such attributes, when single-valued, using a
286 `<saml:NameIdentifier>` element.

287 To accomplish this using this profile, the attribute must have a single value and be expressible as a simple
288 string value. The string value is used as the content of the `<saml:NameIdentifier>` element. The
289 attribute's name is placed into the `Format` XML attribute. The `NameQualifier` attribute MUST be
290 omitted.

291 2.5 Examples

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

```
295 <saml:Attribute AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri"  
296   AttributeName="urn:mace:dir:attribute-def:givenName">  
297   <saml:AttributeValue xsi:type="xsd:string">Scott</saml:AttributeValue>  
298 </saml:Attribute>
```

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

```
303 <saml:Attribute AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri"  
304   AttributeName="urn:mace:dir:attribute-def:eduPersonPrincipalName">  
305   <saml:AttributeValue Scope="osu.edu">cantor.2</saml:AttributeValue>  
306 </saml:Attribute>
```

307 The following is the same attribute as in the previous example, but using its OID-style name to signal the
308 use of the simple encoding rules, for compatibility with a wider range of software.

```
309 <saml:Attribute AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri"  
310   AttributeName="urn:oid:1.3.6.1.4.1.5923.1.1.1.6">  
311   <saml:AttributeValue xsi:type="xsd:string">cantor.2@osu.edu</saml:AttributeValue>  
312 </saml:Attribute>
```

313 The following is the same attribute again, but using the conventions defined for ADFS-interoperable
314 deployment.

```
315 <saml:Attribute AttributeNamespace="http://schemas.xmlsoap.org/claims"  
316   AttributeName="urn:oid:1.3.6.1.4.1.5923.1.1.1.6">
```

```
317     <saml:AttributeValue xsi:type="xsd:string">cantor.2@osu.edu</saml:AttributeValue>
318 </saml:Attribute>
```

319 Finally, the same attribute expressed as a `<saml:NameIdentifier>` element.

```
320 <saml:NameIdentifier Format="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
321     >cantor.2@osu.edu</saml:NameIdentifier>
```

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

```
326 <saml:Attribute AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri"
327     AttributeName="urn:oid:1.3.6.1.4.1.5923.1.6.1.1">
328     <saml:AttributeValue xsi:type="xsd:anyURI"
329         >urn:mace:uchicago.edu:classes:autumn2004:phys12100.003</saml:AttributeValue>
330 </saml:Attribute>
```

331 The following is an example mapping of an `eduPersonTargetedID` attribute created by the identity
332 provider named "`https://idp.example.org/shibboleth`" for the service provider named
333 "`https://sp.example.org/shibboleth`" with the opaque value of "1234567890". The legacy name and value
334 syntax is used.

```
335 <saml:Attribute AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri"
336     AttributeName="urn:mace:dir:attribute-def:eduPersonTargetedID">
337     <saml:AttributeValue
338         Scope="https://idp.example.org/shibboleth">1234567890</saml:AttributeValue>
339 </saml:Attribute>
```

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

```
341 <saml:Attribute AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri"
342     AttributeName="urn:oid:1.3.6.1.4.1.5923.1.1.1.10">
343     <saml:AttributeValue>
344         <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
345             NameQualifier="https://idp.example.org/shibboleth"
346             SPNameQualifier="https://sp.example.org/shibboleth"
347             >1234567890</saml2:NameID>
348     </saml:AttributeValue>
349 </saml:Attribute>
```

3 MACE-Dir Attribute Profile for SAML 2.0

350

351 This profile defines the syntax for expressing attribute types defined (or referenced) by MACE-Dir Working
352 Group specifications in SAML 2.0. Most of the attribute types defined or referenced by MACE-Dir have (or
353 can be given) LDAP representations, and as a matter of procedure are always assigned an OBJECT
354 IDENTIFIER. Therefore, in the interest of expediency, the X.500/LDAP attribute profile defined in [SAML-
355 X500] is adopted whenever possible. This profile directly addresses naming, the mapping of directory
356 syntax to XML syntax, comparison rules, etc. Exceptions to this general policy are noted.

3.1 Required Information

357

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

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

360 **Description:** Given below

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

362 **Depends On:** The X.500/LDAP attribute profile in [SAML-X500].

3.2 SAML Attribute Naming

363

364 All attribute types specified by MACE-Dir possess an OBJECT IDENTIFIER. Therefore attribute naming
365 and name comparison is in accordance with the X.500/LDAP attribute profile in [SAML-X500]. If the
366 `FriendlyName` XML attribute is used, then it SHOULD carry the short name of the attribute type.

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

3.3 SAML Attribute Values

369

370 If an attribute type is associated with an X.500/LDAP directory syntax, then the syntax rules defined by the
371 X.500/LDAP attribute profile in [SAML-X500] are to be applied directly. This includes scoped attributes
372 typed as Directory String, such as `eduPersonScopedAffiliation`.

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

377 Examples are shown in section 3.5.

3.3.1 Non-LDAP Attributes

378

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

3.3.1.1 `eduPersonTargetedID`

382

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

386 Abstractly, an eduPersonTargetedID value consists of a triple:

- 387 • the unique identifier of the identity provider that created the value
- 388 • the unique identifier of the service provider or group for which the value was created
- 389 • the opaque string value itself

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

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

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

395 An example can be found in section 3.5.

396 3.4 NameID Usage

397 Some attributes uniquely identify principals that are the subject of SAML assertions. To maximize
398 interoperability, it is useful to be able to express such attributes, when single-valued, using a
399 `<saml2:NameID>` element.

400 To accomplish this using this profile, the attribute must have a single value and be expressible as a simple
401 string value. The string value is used as the content of the `<saml2:NameID>` element. The attribute's
402 name is placed into the Format XML attribute. The `NameQualifier` and `SPNameQualifier` attributes
403 MUST be omitted.

404 3.5 Examples

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

```
408 <saml2:Attribute xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"  
409     x500:Encoding="LDAP"  
410     NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"  
411     Name="urn:oid:2.5.4.42" FriendlyName="givenName">  
412     <saml2:AttributeValue xsi:type="xsd:string">Steven</saml2:AttributeValue>  
413 </saml2:Attribute>
```

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

```
418 <saml2:Attribute xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"  
419     x500:Encoding="LDAP"  
420     NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"  
421     Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6" FriendlyName="eduPersonPrincipalName">  
422     <saml2:AttributeValue xsi:type="xsd:string">cantor.2@osu.edu</saml2:AttributeValue>  
423 </saml2:Attribute>
```

424 The following is an example of the same `eduPersonPrincipalName` directory attribute expressed as a
425 `<saml2:NameID>` element.

```
426 <saml2:NameID Format="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"  
427     >cantor.2@osu.edu</saml2:NameID>
```

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

```
430 <saml2:Attribute xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"  
431   x500:Encoding="LDAP"  
432   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"  
433   Name="urn:oid:1.3.6.1.4.1.5923.1.6.1.1" FriendlyName="eduCourseOffering">  
434   <saml2:AttributeValue xsi:type="xsd:anyURI"  
435     >urn:mace:uchicago.edu:classes:autumn2004:phys12100.003</saml2:AttributeValue>  
436 </saml2:Attribute>
```

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

```
440 <saml2:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"  
441   Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.10"  
442   FriendlyName="eduPersonTargetedID">  
443   <saml2:AttributeValue>  
444     <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"  
445       NameQualifier="https://idp.example.org/shibboleth"  
446       SPNameQualifier="https://sp.example.org/shibboleth"  
447       >1234567890</saml2:NameID>  
448   </saml2:AttributeValue>  
449 </saml2:Attribute>
```

4 References

450

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

4.1 Normative References

452

- 453 **[eduPerson]** MACE-Dir. *eduPerson Specification (200604a)*. Internet2-MACE, May 2007.
454 <http://www.nmi-edit.org/eduPerson/internet2-mace-dir-eduperson-200604.html>.
- 455 **[eduCourse]** MACE-CourseID. *LDAP representations of eduCourse attributes and an auxiliary*
456 *object class (200507)*. Internet2-MACE, July 2005.
457 [http://middleware.internet2.edu/courseid/docs/internet2-mace-dir-courseid-](http://middleware.internet2.edu/courseid/docs/internet2-mace-dir-courseid-educourse-ldap-200507.html)
458 [educourse-ldap-200507.html](http://middleware.internet2.edu/courseid/docs/internet2-mace-dir-courseid-educourse-ldap-200507.html)
- 459 **[AttrDefs]** MACE-Dir. *Attribute Registrations*. Internet2-MACE.
460 <http://middleware.internet2.edu/urn-mace/urn-mace-dir-attribute-def.html>.
- 461 **[RFC 2119]** S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. IETF
462 RFC 2119, March 1997. <http://www.ietf.org/rfc/rfc2119.txt>.
- 463 **[RFC 2396]** T. Berners-Lee et al. *Uniform Resource Identifiers (URI): Generic Syntax*. IETF
464 RFC 2396, August, 1998. <http://www.ietf.org/rfc/rfc2396.txt>.
- 465 **[RFC3061]** M. Mealling. *A URN Namespace of Object Identifiers*. IETF RFC 3061, February
466 2001. See <http://www.ietf.org/rfc/rfc3061.txt>.
- 467 **[SAMLCore]** E. Maler et al. *Assertions and Protocols for the OASIS Security Assertion Markup*
468 *Language (SAML)*. OASIS, September 2003. Document ID oasis-sstc-saml-
469 core-1.1. <http://www.oasis-open.org/committees/security/>.
- 470 **[SAML-XSD]** E. Maler et al. *SAML assertion schema*. OASIS, September 2003. Document ID
471 oasis-sstc-saml-schema-assertion-1.1. [http://www.oasis-](http://www.oasis-open.org/committees/security/)
472 [open.org/committees/security/](http://www.oasis-open.org/committees/security/).
- 473 **[SAML2Core]** S. Cantor et al., *Assertions and Protocols for the OASIS Security Assertion*
474 *Markup Language (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-
475 core-2.0-os. See <http://www.oasis-open.org/committees/security/>.
- 476 **[SAML-X500]** S.Cantor., *SAML V2.0 X.500/LDAP Attribute Profile, Committee Draft 02*. OASIS
477 SSTC, November 2007. Document ID sstc-saml-attribute-x500-cd-02. See [http://](http://wiki.oasis-open.org/security/FrontPage)
478 wiki.oasis-open.org/security/FrontPage.
- 479 **[SAML2-XSD]** S. Cantor et al. *SAML 2.0 Assertion Schema*. OASIS, March 2005. Document ID
480 saml-schema-assertion-2.0. <http://www.oasis-open.org/committees/security/>.
- 481 **[Schema2]** P. V. Biron et al. *XML Schema Part 2: Datatypes*. World Wide Web Consortium
482 Recommendation, May 2001. <http://www.w3.org/TR/xmlschema-2/>.

4.2 Non-Normative References

483

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