
1 MACE-Dir SAML Attribute Profiles

2 **2 December 2007**

3 **Document identifier:**

4 draft-internet2-mace-dir-saml-attributes-20071202

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

51

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

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

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

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

1.1 SAML Profile Reference

68

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

1.2 Notation

72

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

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

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

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

82 Listings of XML schemas appear like this.

83 Example code listings appear like this.

84
85 Conventional XML namespace prefixes are used throughout the listings in this specification to stand for
86 their respective namespaces as follows, whether or not a namespace declaration is present in the
87 example:

- 88 • The prefix `saml:` stands for the SAML 1.1 (and 1.0) assertion namespace,
89 `urn:oasis:names:tc:SAML:1.0:assertion`
- 90 • The prefix `saml2:` stands for the SAML 2.0 assertion namespace, `urn:oasis:names:tc:SAML:`
91 `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 X.
113 500/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.

187 **2.2.2 ADFS Namespace Exception**

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

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

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

194 **2.2.3 Attribute Name Comparison**

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

197 **2.3 SAML Attribute Values**

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

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

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

205 **2.3.1 Scoped Attribute Values**

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

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

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

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

221 **2.3.1.1 Structured Encoding**

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

223 Examples are shown in section 2.5.

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

226 `urn:mace:dir:attribute-def:eduPersonScopedAffiliation`
227 `urn:mace:dir:attribute-def:eduPersonPrincipalName`
228 `urn:mace:dir:attribute-def:eduPersonTargetedID`
229 `urn:mace:dir:attribute-def:eduCourseMember`

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

231 **2.3.1.2 Simple Encoding**

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

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

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

242 **2.3.2 Non-LDAP Attributes**

243 This profile provides uniform treatment of attribute types whose values can be described in terms of X.
244 500/LDAP directory syntax. Other attribute types are addressed on a case by case basis below, or in other
245 specifications as appropriate.

246 **2.3.2.1 eduPersonTargetedID**

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

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

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

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

258 **2.3.2.1.1 Recommended Name and Syntax**

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

260 `urn:oid:1.3.6.1.4.1.5923.1.1.1.10`

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

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

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

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

267 2.3.2.1.2 Legacy Name and Syntax

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

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

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

274 2.4 NameIdentifier Usage

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

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

282 2.5 Examples

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

```
286 <saml:Attribute AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri"  
287   AttributeName="urn:mace:dir:attribute-def:givenName">  
288   <saml:AttributeValue xsi:type="xsd:string">Scott</saml:AttributeValue>  
289 </saml:Attribute>
```

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

```
294 <saml:Attribute AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri"  
295   AttributeName="urn:mace:dir:attribute-def:eduPersonPrincipalName">  
296   <saml:AttributeValue Scope="osu.edu">cantor.2</saml:AttributeValue>  
297 </saml:Attribute>
```

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

```
300 <saml:Attribute AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri"  
301   AttributeName="urn:oid:1.3.6.1.4.1.5923.1.1.1.6">  
302   <saml:AttributeValue xsi:type="xsd:string">cantor.2@osu.edu</saml:AttributeValue>  
303 </saml:Attribute>
```

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

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

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

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

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

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

```
317 <saml:Attribute AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri"
318 AttributeName="urn:oid:1.3.6.1.4.1.5923.1.6.1.1">
319 <saml:AttributeValue xsi:type="xsd:anyURI"
320 >urn:mace:uchicago.edu:classes:autumn2004:phys12100.003</saml:AttributeValue>
321 </saml:Attribute>
```

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

```
326 <saml:Attribute AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri"
327 AttributeName="urn:mace:dir:attribute-def:eduPersonTargetedID">
328 <saml:AttributeValue
329 Scope="https://idp.example.org/shibboleth">1234567890</saml:AttributeValue>
330 </saml:Attribute>
```

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

```
332 <saml:Attribute AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri"
333 AttributeName="urn:oid:1.3.6.1.4.1.5923.1.1.1.10">
334 <saml:AttributeValue>
335 <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
336 NameQualifier="https://idp.example.org/shibboleth"
337 SPNameQualifier="https://sp.example.org/shibboleth"
338 >1234567890</saml2:NameID>
339 </saml:AttributeValue>
340 </saml:Attribute>
```

3 MACE-Dir Attribute Profile for SAML 2.0

341

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

3.1 Required Information

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

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

350 **Description:** Given below

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

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

3.2 SAML Attribute Naming

354
355 All attribute types specified by MACE-Dir possess an OBJECT IDENTIFIER. Therefore attribute naming
356 and name comparison is in accordance with the X.500/LDAP attribute profile in [SAML-X500]. If the
357 `FriendlyName` XML attribute is used, then it SHOULD carry the short name of the attribute type.

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

3.3 SAML Attribute Values

360
361 If an attribute type is associated with an X.500/LDAP directory syntax, then the syntax rules defined by the
362 X.500/LDAP attribute profile in [SAML-X500] are to be applied directly. This includes scoped attributes
363 typed as Directory String, such as `eduPersonScopedAffiliation`.

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

368 Examples are shown in section 3.5.

3.3.1 Non-LDAP Attributes

369
370 This profile provides uniform treatment of attribute types whose values can be described in terms of X.
371 500/LDAP directory syntax. Other attribute types are addressed on a case by case basis below, or in other
372 specifications as appropriate.

3.3.1.1 `eduPersonTargetedID`

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

377 Abstractly, an eduPersonTargetedID value consists of a triple:

- 378 • the unique identifier of the identity provider that created the value
- 379 • the unique identifier of the service provider or group for which the value was created
- 380 • the opaque string value itself

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

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

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

386 An example can be found in section 3.5.

387 3.4 NameID Usage

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

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

395 3.5 Examples

396 The following is an example of a mapping of the givenName directory attribute, representing the SAML
397 assertion subject's first name. Its LDAP syntax is Directory String. Since the XML type of the value is a
398 built-in type, 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   x500:Encoding="LDAP"  
401   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"  
402   Name="urn:oid:2.5.4.42" FriendlyName="givenName">  
403   <saml2:AttributeValue xsi:type="xsd:string">Steven</saml2:AttributeValue>  
404 </saml2:Attribute>
```

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

```
409 <saml2:Attribute xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"  
410   x500:Encoding="LDAP"  
411   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"  
412   Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6" FriendlyName="eduPersonPrincipalName">  
413   <saml2:AttributeValue xsi:type="xsd:string">cantor.2@osu.edu</saml2:AttributeValue>  
414 </saml2:Attribute>
```

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

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

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

```
421 <saml2:Attribute xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"  
422   x500:Encoding="LDAP"  
423   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"  
424   Name="urn:oid:1.3.6.1.4.1.5923.1.6.1.1" FriendlyName="eduCourseOffering">  
425   <saml2:AttributeValue xsi:type="xsd:anyURI"  
426     >urn:mace:uchicago.edu:classes:autumn2004:phys12100.003</saml2:AttributeValue>  
427 </saml2:Attribute>
```

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

```
431 <saml2:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"  
432   Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.10"  
433   FriendlyName="eduPersonTargetedID">  
434   <saml2:AttributeValue>  
435     <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"  
436       NameQualifier="https://idp.example.org/shibboleth"  
437       SPNameQualifier="https://sp.example.org/shibboleth"  
438       >1234567890</saml2:NameID>  
439   </saml2:AttributeValue>  
440 </saml2:Attribute>
```

4 References

441

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

4.1 Normative References

443

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

4.2 Non-Normative References

474

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