
1 MACE-Dir SAML Attribute Profiles

2 **April 2 December 2006**

3 **Document identifier:**

4 [draft-internet2-mace-dir-saml-attributes-20060471202](#)

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`.

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 [\[SAML2Prof\]\[SAML-X500\]](#).

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:
```

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 [ifas](#) 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 | AttributeName 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 | [SAML2Profile]in [SAML-X500] are to be applied, with the obvious caveat that the
202 | <saml:AttributeValue> element is substituted for the <saml2:AttributeValue> element in that
203 | specification.

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

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

208 | **2.3.1 Scoped Attribute Values**

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

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

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

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

227 | **2.3.1.1 Structured Encoding**

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

233 | Examples are shown in section 2.5.

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

```
236 |     urn:mace:dir:attribute-def:eduPersonScopedAffiliation  
237 |     urn:mace:dir:attribute-def:eduPersonPrincipalName  
238 |     urn:mace:dir:attribute-def:eduPersonTargetedID  
239 |     urn:mace:dir:attribute-def:eduCourseMember
```

240 | Additional attributes MAY be designated as scoped when appropriate, and will may be subject to these
241 | syntax rules for consistency.

242 | **2.3.1.2 Simple Encoding**

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

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

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

253 | **2.3.2 Non-LDAP Attributes**

254 | This profile provides uniform treatment of attribute types whose values can be described in terms of X.
255 | 500/LDAP directory syntax. Other attribute types are addressed on a case by case basis below, or in other
256 | specifications as appropriate.

257 | **2.3.2.1 eduPersonTargetedID**

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

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

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

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

269 **2.3.2.1.1 Recommended Name and Syntax**

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

271 `urn:oid:1.3.6.1.4.1.5923.1.1.1.10`

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

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

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

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

278 **2.3.2.1.2 Legacy Name and Syntax**

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

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

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

285 **2.4 NameIdentifier Usage**

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

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

293 **2.5 Examples**

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

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

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

```
305 <saml:Attribute AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri"
```

```
307     AttributeName="urn:mace:dir:attribute-def:eduPersonPrincipalName">
308     <saml:AttributeValue Scope="osu.edu">cantor.2</saml:AttributeValue>
309 </saml:Attribute>
```

310

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

```
313 <saml:Attribute AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri"
314     AttributeName="urn:oid:1.3.6.1.4.1.5923.1.1.1.6">
315     <saml:AttributeValue xsi:type="xsd:string">cantor.2@osu.edu</saml:AttributeValue>
316 </saml:Attribute>
```

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

```
319 <saml:Attribute AttributeNamespace="http://schemas.xmlsoap.org/claims"
320     AttributeName="urn:oid:1.3.6.1.4.1.5923.1.1.1.6">
321     <saml:AttributeValue xsi:type="xsd:string">cantor.2@osu.edu</saml:AttributeValue>
322 </saml:Attribute>
```

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

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

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

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

335

336 The following is an example mapping of an eduPersonTargetedID attribute created by the identity
337 provider named "https://idp.example.org/shibboleth" for the service provider named
338 "https://sp.example.org/shibboleth" with the opaque value of "1234567890". The legacy name and value
339 syntax is used.

```
340 <saml:Attribute AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri"
341     AttributeName="urn:mace:dir:attribute-def:eduPersonTargetedID">
342     <saml:AttributeValue
343     Scope="https://idp.example.org/shibboleth">1234567890</saml:AttributeValue>
344 </saml:Attribute>
```

345

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

```
347 <saml:Attribute AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri"
348     AttributeName="urn:oid:1.3.6.1.4.1.5923.1.1.1.10">
349     <saml:AttributeValue>
350     <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
351     NameQualifier="https://idp.example.org/shibboleth"
352     SPNameQualifier="https://sp.example.org/shibboleth"
353     >1234567890</saml2:NameID>
354     </saml:AttributeValue>
355 </saml:Attribute>
```

3 MACE-Dir Attribute Profile for SAML 2.0

356

357 This profile defines the syntax for expressing attribute types defined (or referenced) by MACE-Dir Working
358 Group specifications in SAML 2.0. Most of the attribute types defined or referenced by MACE-Dir have (or
359 can be given) LDAP representations, and as a matter of procedure are always assigned an OBJECT
360 IDENTIFIER. Therefore, in the interest of expediency, the X.500/LDAP attribute profile defined in
361 [\[SAML2Prof\]\[SAML-X500\]](#) is adopted whenever possible. This profile directly addresses naming, the
362 mapping of directory syntax to XML syntax, comparison rules, etc. Exceptions to this general policy are
363 noted.

3.1 Required Information

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

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

366 **Description:** Given below

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

368 **Depends On:** The X.500/LDAP attribute profile in [\[SAML2Prof\]\[SAML-X500\]](#).

3.2 SAML Attribute Naming

370

371 All attribute types specified by MACE-Dir possess an OBJECT IDENTIFIER. Therefore attribute naming
372 and name comparison is in accordance with the X.500/LDAP attribute profile in [\[SAML2Prof\]\[SAML-](#)
373 [X500\]](#). If the `FriendlyName` XML attribute is used, then it SHOULD carry the short name of the attribute
374 type.

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

3.3 SAML Attribute Values

377

378 If an attribute type is associated with an X.500/LDAP directory syntax, then the syntax rules defined by the
379 X.500/LDAP attribute profile in [\[SAML2Prof\]\[SAML-X500\]](#) are to be applied directly. This includes scoped
380 attributes typed as Directory String, such as `eduPersonScopedAffiliation`.

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

385 Examples are shown in section 3.5.

3.3.1 Non-LDAP Attributes

386

387 This profile provides uniform treatment of attribute types whose values can be described in terms of X.
388 500/LDAP directory syntax. Other attribute types are addressed on a case by case basis below, or in other
389 specifications as appropriate.

390 3.3.1.1 eduPersonTargetedID

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

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

- 395 • the unique identifier of the identity provider that created the value
- 396 • the unique identifier of the service provider or group for which the value was created
- 397 • the opaque string value itself

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

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

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

403 An example can be found in section 3.5.

404 3.4 NameID Usage

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

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

412 3.5 Examples

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

```
416 <saml2:Attribute xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"  
417   x500:Encoding="LDAP"  
418   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"  
419   Name="urn:oid:2.5.4.42" FriendlyName="givenName">  
420   <saml2:AttributeValue xsi:type="xsd:string" x500:Encoding="LDAP"  
421 >Steven</saml2:AttributeValue>  
422 </saml2:Attribute>
```

423
424 The following is an example mapping of an `eduPersonPrincipalName` directory attribute with the
425 LDAP value of "cantor.2@osu.edu". Its LDAP syntax is Directory String, and it is a scoped attribute, but is
426 covered by this profile directly without special treatment. Since the XML type of the value is a built-in type,
427 it is included within the `xsi:type` XML attribute.

```
428 <saml2:Attribute xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"  
429   x500:Encoding="LDAP"  
430   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"  
431   Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6" FriendlyName="eduPersonPrincipalName">  
432   <saml2:AttributeValue xsi:type="xsd:string" x500:Encoding="LDAP"  
433 >cantor.2@osu.edu</saml2:AttributeValue>
```

434 </saml2:Attribute>
435

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

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

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

```
442 <saml2:Attribute xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"  
443 x500:Encoding="LDAP"  
444 NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"  
445 Name="urn:oid:1.3.6.1.4.1.5923.1.6.1.1" FriendlyName="eduCourseOffering">  
446 <saml2:AttributeValue xsi:type="xsd:anyURI" x500:Encoding="LDAP"  
447 >urn:mace:uchicago.edu:classes:autumn2004:phys12100.003</saml2:AttributeValue>  
448 </saml2:Attribute>
```

449 The following is an example mapping of an eduPersonTargetedID attribute created by the identity
450 provider named "https://idp.example.org/shibboleth" for the service provider named
451 "https://sp.example.org/shibboleth" with the opaque value of "1234567890".
452

```
453 <saml2:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"  
454 Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.10"  
455 FriendlyName="eduPersonTargetedID">  
456 <saml2:AttributeValue>  
457 <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"  
458 NameQualifier="https://idp.example.org/shibboleth"  
459 SPNameQualifier="https://sp.example.org/shibboleth"  
460 >1234567890</saml2:NameID>  
461 </saml2:AttributeValue>  
462 </saml2:Attribute>
```

4 References

463

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

4.1 Normative References

465

- 466 **[eduPerson]** MACE-Dir. *eduPerson Specification (200361204a)*. Internet2-MACE,
467 December 2003. [http://www.nmi-edit.org/eduPerson/internet2-mace-dir-](http://www.nmi-edit.org/eduPerson/internet2-mace-dir-eduperson-200312.html)
468 [eduperson-200312.html](http://www.nmi-edit.org/eduPerson/internet2-mace-dir-eduperson-200312.html)
469 [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).
- 470 **[eduCourse]** MACE-CourseID. *LDAP representations of eduCourse attributes and an auxiliary*
471 *object class (200507)*. Internet2-MACE, July 2005.
472 [http://middleware.internet2.edu/courseid/docs/internet2-mace-dir-courseid-](http://middleware.internet2.edu/courseid/docs/internet2-mace-dir-courseid-educourse-ldap-200507.html)
473 [educourse-ldap-200507.html](http://middleware.internet2.edu/courseid/docs/internet2-mace-dir-courseid-educourse-ldap-200507.html)
- 474 **[AttrDefs]** MACE-Dir. *Attribute Registrations*. Internet2-MACE.
475 <http://middleware.internet2.edu/urn-mace/urn-mace-dir-attribute-def.html>.
- 476 **[RFC 2119]** S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. IETF
477 RFC 2119, March 1997. <http://www.ietf.org/rfc/rfc2119.txt>.
- 478 **[RFC 2396]** T. Berners-Lee et al. *Uniform Resource Identifiers (URI): Generic Syntax*. IETF
479 RFC 2396, August, 1998. <http://www.ietf.org/rfc/rfc2396.txt>.
- 480 **[RFC3061]** M. Mealling. *A URN Namespace of Object Identifiers*. IETF RFC 3061, February
481 2001. See <http://www.ietf.org/rfc/rfc3061.txt>.
- 482 **[SAMLCore]** E. Maler et al. *Assertions and Protocols for the OASIS Security Assertion Markup*
483 *Language (SAML)*. OASIS, September 2003. Document ID oasis-sstc-saml-
484 core-1.1. <http://www.oasis-open.org/committees/security/>.
- 485 **[SAML-XSD]** E. Maler et al. *SAML assertion schema*. OASIS, September 2003. Document ID
486 oasis-sstc-saml-schema-assertion-1.1. [http://www.oasis-](http://www.oasis-open.org/committees/security/)
487 [open.org/committees/security/](http://www.oasis-open.org/committees/security/).
- 488 **[SAML2Core]** S. Cantor et al., *Assertions and Protocols for the OASIS Security Assertion*
489 *Markup Language (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-
490 core-2.0-os. See <http://www.oasis-open.org/committees/security/>.
- 491 ~~**[SAML2Prof]** S. Cantor et al., *Profiles for the OASIS Security Assertion Markup Language*~~
492 ~~*(SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-profiles-2.0-os. See~~
493 ~~<http://www.oasis-open.org/committees/security/>: **[SAML-X500]** S. Cantor.,~~
494 ~~[SAML V2.0 X.500/LDAP Attribute Profile, Committee Draft 02](http://www.oasis-open.org/committees/security/). OASIS SSTC.,~~
495 ~~November 2007. Document ID sstc-saml-attribute-x500-cd-02. See~~
496 ~~<http://wiki.oasis-open.org/security/FrontPage>.~~
- 497 **[SAML2-XSD]** S. Cantor et al. *SAML 2.0 Assertion Schema*. OASIS, March 2005. Document ID
498 saml-schema-assertion-2.0. <http://www.oasis-open.org/committees/security/>.
- 499 **[Schema2]** P. V. Biron et al. *XML Schema Part 2: Datatypes*. World Wide Web Consortium
500 Recommendation, May 2001. <http://www.w3.org/TR/xmlschema-2/>.

4.2 Non-Normative References

501

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