
1 MACE-Dir SAML Attribute Profiles

2 April 2006

3 **Document identifier:**

4 internet2-mace-dir-saml-attributes-200604

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
18 2.0 specifications.

19 Table of Contents

20	1 Introduction.....	3
21	1.1 Notation.....	3
22	2 MACE-Dir Attribute Profile for SAML 1.x.....	4
23	2.1 Required Information.....	4
24	2.2 SAML Attribute Naming.....	4
25	2.2.1 Legacy Names.....	4
26	2.2.2 Attribute Name Comparison.....	5
27	2.3 SAML Attribute Values.....	6
28	2.3.1 Scoped Attribute Values.....	6
29	2.3.2 Non-LDAP Attributes.....	6
30	2.3.2.1 eduPersonTargetedID.....	6
31	2.3.2.1.1 Recommended Name and Syntax.....	7
32	2.3.2.1.2 Legacy Name and Syntax.....	7
33	2.4 Examples.....	7
34	3 MACE-Dir Attribute Profile for SAML 2.0.....	9
35	3.1 Required Information.....	9
36	3.2 SAML Attribute Naming.....	9
37	3.3 SAML Attribute Values.....	9
38	3.3.1 Non-LDAP Attributes.....	9
39	3.3.1.1 eduPersonTargetedID.....	9
40	3.4 Examples.....	10
41	4 References.....	12
42	4.1 Normative References.....	12
43	4.2 Non-Normative References.....	12
44		

1 Introduction

45

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

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

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

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

1.1 Notation

63

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

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

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

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

73 Listings of XML schemas appear like this.

74

75 Example code listings appear like this.

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

79 • The prefix `saml:` stands for the SAML 1.1 (and 1.0) assertion namespace,
80 `urn:oasis:names:tc:SAML:1.0:assertion`

81 • The prefix `saml2:` stands for the SAML 2.0 assertion namespace,
82 `urn:oasis:names:tc:SAML:2.0:assertion`

83 • The prefix `xsi:` stands for the W3C XML Schema-instance namespace,
84 `http://www.w3.org/2001/XMLSchema-instance`

85 • The prefix `xsd:` stands for the W3C XML Schema namespace,
86 `http://www.w3.org/2001/XMLSchema`
87 in example listings. In schema listings, this is the default namespace and no prefix is shown.

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

90 2 MACE-Dir Attribute Profile for SAML 1.x

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

94 2.1 Required Information

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

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

97 **Description:** Given below

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

100 2.2 SAML Attribute Naming

101 To ensure uniqueness, each attribute type is assigned a name in the form of a URI. To construct attribute
102 names, the URN `oid` namespace described in [RFC3061] is used. The `AttributeName` XML attribute
103 is based on the OBJECT IDENTIFIER assigned to the attribute type. This naming procedure mirrors the
104 X.500/LDAP attribute profile defined in [SAML2Prof].

105 Example:

```
106 urn:oid:2.5.4.3
```

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

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

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

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

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

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

120 2.2.1 Legacy Names

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

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

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

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

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

178 **2.2.2 Attribute Name Comparison**

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

181 **2.3 SAML Attribute Values**

182 With two significant exceptions, the syntax rules defined by the SAML 2.0 X.500/LDAP attribute profile in
183 [SAML2Prof] are to be applied, with the obvious caveat that the `<saml:AttributeValue>` element is
184 substituted for the `<saml2:AttributeValue>` element in that specification.

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

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

189 **2.3.1 Scoped Attribute Values**

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

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

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

202 Examples are shown in section 2.4.

203 The following attributes have been designated as scoped for the purposes of applying this exception to
204 the standard value profile:

```
205 urn:mace:dir:attribute-def:eduPersonScopedAffiliation  
206 urn:mace:dir:attribute-def:eduPersonPrincipalName  
207 urn:mace:dir:attribute-def:eduPersonTargetedID
```

208 Additional attributes MAY be designated as scoped when appropriate, and will be subject to these syntax
209 rules for consistency.

210 **2.3.2 Non-LDAP Attributes**

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

214 **2.3.2.1 eduPersonTargetedID**

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

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

- 220 • the unique identifier of the identity provider that created the value

- 221 • the unique identifier of the service provider or group for which the value was created
- 222 • the opaque string value itself

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

226 **2.3.2.1.1 Recommended Name and Syntax**

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

228 `urn:oid:1.3.6.1.4.1.5923.1.1.1.10`

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

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

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

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

235 **2.3.2.1.2 Legacy Name and Syntax**

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

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

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

243 **2.4 Examples**

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

```
247 <saml:Attribute AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri "  
248   AttributeName="urn:mace:dir:attribute-def:givenName">  
249   <saml:AttributeValue xsi:type="xsd:string">Scott</saml:AttributeValue>  
250 </saml:Attribute>
```

251 The following is an example mapping of an `eduPersonPrincipalName` directory attribute with the
252 LDAP value of "cantor.2@osu.edu". Its LDAP syntax is `Directory String`, but it is a scoped attribute, and
253 is therefore subject to alternative syntax rules. The resulting XML type of the value is therefore a
254 complex type and is omitted to ease interoperability.

```
256 <saml:Attribute AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri "  
257   AttributeName="urn:mace:dir:attribute-def:eduPersonPrincipalName">  
258   <saml:AttributeValue Scope="osu.edu">cantor.2</saml:AttributeValue>  
259 </saml:Attribute>
```

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

```
265 <saml:Attribute AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri "  
266     AttributeName="urn:oid:1.3.6.1.4.1.5923.1.6.1.1">  
267     <saml:AttributeValue xsi:type="xsd:anyURI"  
268         >urn:mace:uchicago.edu:classes:autumn2004:phys12100.003</saml:AttributeValue>  
269 </saml:Attribute>
```

270

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

```
275 <saml:Attribute AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri "  
276     AttributeName="urn:mace:dir:attribute-def:eduPersonTargetedID">  
277     <saml:AttributeValue  
278         Scope="https://idp.example.org/shibboleth">1234567890</saml:AttributeValue>  
279 </saml:Attribute>
```

280

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

```
282 <saml:Attribute AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri "  
283     AttributeName="urn:oid:1.3.6.1.4.1.5923.1.1.1.10">  
284     <saml:AttributeValue>  
285         <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent "  
286             NameQualifier="https://idp.example.org/shibboleth"  
287             SPNameQualifier="https://sp.example.org/shibboleth"  
288             >1234567890</saml2:NameID>  
289     </saml:AttributeValue>  
290 </saml:Attribute>
```

291 3 MACE-Dir Attribute Profile for SAML 2.0

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

298 3.1 Required Information

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

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

301 **Description:** Given below

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

303 **Depends On:** The X.500/LDAP attribute profile in [SAML2Prof].

304 3.2 SAML Attribute Naming

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

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

310 3.3 SAML Attribute Values

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

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

318 Examples are shown in section 3.4.

319 3.3.1 Non-LDAP Attributes

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

323 3.3.1.1 eduPersonTargetedID

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

327 Abstractly, an eduPersonTargetedID value consists of a triple:

- 328 • the unique identifier of the identity provider that created the value
- 329 • the unique identifier of the service provider or group for which the value was created
- 330 • the opaque string value itself

331 The <saml2:AttributeValue> element's content MUST be a <saml2:NameID> element with a
332 Format XML attribute of

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

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

336 An example can be found in section 3.4.

337 3.4 Examples

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

```
341 <saml2:Attribute xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"  
342   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"  
343   Name="urn:oid:2.5.4.42" FriendlyName="givenName">  
344   <saml2:AttributeValue xsi:type="xsd:string"  
345     x500:Encoding="LDAP">Steven</saml2:AttributeValue>  
346 </saml2:Attribute>
```

347
348 The following is an example mapping of an eduPersonPrincipalName directory attribute with the
349 LDAP value of "cantor.2@osu.edu". Its LDAP syntax is Directory String, and it is a scoped attribute, but
350 is covered by this profile directly without special treatment. Since the XML type of the value is a built-in
351 type, it is included within the xsi:type XML attribute.

```
352 <saml2:Attribute xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"  
353   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"  
354   Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6" FriendlyName="eduPersonPrincipalName">  
355   <saml2:AttributeValue xsi:type="xsd:string"  
356     x500:Encoding="LDAP">cantor.2@osu.edu</saml2:AttributeValue>  
357 </saml2:Attribute>
```

358

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

```
361 <saml2:Attribute xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"  
362   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"  
363   Name="urn:oid:1.3.6.1.4.1.5923.1.6.1.1" FriendlyName="eduCourseOffering">  
364   <saml2:AttributeValue xsi:type="xsd:anyURI" x500:Encoding="LDAP"  
365     >urn:mace:uchicago.edu:classes:autumn2004:phys12100.003</saml2:AttributeValue>  
366 </saml2:Attribute>
```

367

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

```
371 <saml2:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"  
372   Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.10"  
373   FriendlyName="eduPersonTargetedID">  
374   <saml2:AttributeValue>  
375     <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"  
376       NameQualifier="https://idp.example.org/shibboleth"
```

```
377     SPNameQualifier="https://sp.example.org/shibboleth"  
378     >1234567890</saml2:NameID>  
379     </saml2:AttributeValue>  
380 </saml2:Attribute>
```

4 References

381

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

4.1 Normative References

383

- 384 **[eduPerson]** MACE-Dir. *eduPerson Specification (200406)*. Internet2-MACE, April 2006.
385 <http://www.nmi-edit.org/eduPerson/internet2-mace-dir-eduperson-200406.html>.
- 386 **[AttrDefs]** MACE-Dir. *Attribute Registrations*. Internet2-MACE.
387 <http://middleware.internet2.edu/urn-mace/urn-mace-dir-attribute-def.html>.
- 388 **[RFC 2119]** S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. IETF
389 RFC 2119, March 1997. <http://www.ietf.org/rfc/rfc2119.txt>.
- 390 **[RFC 2396]** T. Berners-Lee et al. *Uniform Resource Identifiers (URI): Generic Syntax*. IETF
391 RFC 2396, August, 1998. <http://www.ietf.org/rfc/rfc2396.txt>.
- 392 **[RFC3061]** M. Mealling. *A URN Namespace of Object Identifiers*. IETF RFC 3061, February
393 2001. See <http://www.ietf.org/rfc/rfc3061.txt>.
- 394 **[SAMLCore]** E. Maler et al. *Assertions and Protocols for the OASIS Security Assertion
395 Markup Language (SAML)*. OASIS, September 2003. Document ID oasis-sstc-
396 saml-core-1.1. <http://www.oasis-open.org/committees/security/>.
- 397 **[SAML-XSD]** E. Maler et al. *SAML assertion schema*. OASIS, September 2003. Document ID
398 oasis-sstc-saml-schema-assertion-1.1. [http://www.oasis-
open.org/committees/security/](http://www.oasis-
399 open.org/committees/security/).
- 400 **[SAML2Core]** S. Cantor et al., *Assertions and Protocols for the OASIS Security Assertion
401 Markup Language (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-
402 core-2.0-os. See <http://www.oasis-open.org/committees/security/>.
- 403 **[SAML2Prof]** S. Cantor et al., *Profiles for the OASIS Security Assertion Markup Language
404 (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-profiles-2.0-os.
405 See <http://www.oasis-open.org/committees/security/>.
- 406 **[SAML2-XSD]** S. Cantor et al. *SAML 2.0 Assertion Schema*. OASIS, March 2005. Document ID
407 saml-schema-assertion-2.0. <http://www.oasis-open.org/committees/security/>.
- 408 **[Schema2]** P. V. Biron et al. *XML Schema Part 2: Datatypes*. World Wide Web Consortium
409 Recommendation, May 2001. <http://www.w3.org/TR/xmlschema-2/>.

4.2 Non-Normative References

410

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