MACE-Dir SAML Attribute Profiles

April 2008

Document identifier:
internet2-mace-dir-saml-attributes-200804a

Location:
http://middleware.internet2.edu/dir

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

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

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

Table of Contents

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

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

This specification uses the following typographical conventions in text: `<ns:Element>`, `Attribute`, **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 **[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:
```

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

```
eduPersonScopedAffiliation
eduPersonPrimaryAffiliation
eduPersonAffiliation
eduPersonPrincipalName
```

```
eduPersonEntitlement
eduPersonTargetedID
eduPersonNickname
eduPersonPrimaryOrgUnitDN
eduPersonOrgUnitDN
eduPersonOrgDN
eduCourseMember
businessCategory
carLicense
cn
departmentNumber
description
displayName
employeeNumber
employeeType
facsimileTelephoneNumber
givenName
homePhone
homePostalAddress
initials
jpegPhoto
l
labeledURI
mail
manager
mobile
o
ou
pager
physicalDeliveryOfficeName
postalAddress
postalCode
postOfficeBox
preferredLanguage
roomNumber
seeAlso
sn
st
street
telephoneNumber
title
uid
userCertificate
userSMIMECertificate
```

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

2.2.2 ADFS Namespace Exception

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

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

2.2.3 Attribute Name Comparison

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

2.3 SAML Attribute Values

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

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

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

2.3.1 Scoped Attribute Values

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

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

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

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

2.3.1.1 Structured Encoding

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

Examples are shown in section 2.5 .

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

```
urn:mace:dir:attribute-def:eduPersonScopedAffiliation
urn:mace:dir:attribute-def:eduPersonPrincipalName
urn:mace:dir:attribute-def:eduPersonTargetedID
urn:mace:dir:attribute-def:eduCourseMember
```

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

2.3.1.2 Simple Encoding

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

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

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

2.3.2 Non-LDAP Attributes

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

2.3.2.1 eduPersonTargetedID

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

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

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

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

2.3.2.1.1 Recommended Name and Syntax

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

`urn:oid:1.3.6.1.4.1.5923.1.1.1.10`

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

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

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

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

2.3.2.1.2 Legacy Name and Syntax

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

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

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

2.4 NameIdentifier Usage

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

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

2.5 Examples

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3 MACE-Dir Attribute Profile for SAML 2.0

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

3.1 Required Information

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

Contact information: mace-dir@internet2.edu

Description: Given below

Updates: The SAML 1.x profile

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

3.2 SAML Attribute Naming

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

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

3.3 SAML Attribute Values

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

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

Examples are shown in section 3.5 .

3.3.1 Non-LDAP Attributes

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

3.3.1.1 eduPersonTargetedID

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

Abstractly, an eduPersonTargetedID value consists of a triple:

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

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

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

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

An example can be found in section 3.5 .

3.4 NameID Usage

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

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

3.5 Examples

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

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

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

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

```

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

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

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

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

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

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

4 References

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

4.1 Normative References

[eduPerson] MACE-Dir. *eduPerson Specification (200604a)*. Internet2-MACE, May 2007. http://www.nmi-edit.org/eduPerson/internet2-mace-dir-eduperson-200604.html.

[eduCourse] MACE-CourseID. *LDAP representations of eduCourse attributes and an auxiliary object class (200507)*. Internet2-MACE, July 2005. http://middleware.internet2.edu/courseid/docs/internet2-mace-dir-courseid-educourse-ldap-200507.html

[AttrDefs] MACE-Dir. *Attribute Registrations*. Internet2-MACE. http://middleware.internet2.edu/urn-mace/urn-mace-dir-attribute-def.html.

[RFC 2119] S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. IETF RFC 2119, March 1997. http://www.ietf.org/rfc/rfc2119.txt.

[RFC 2396] T. Berners-Lee et al. *Uniform Resource Identifiers (URI): Generic Syntax.* IETF RFC 2396, August, 1998. http://www.ietf.org/rfc/rfc2396.txt.

[RFC3061] M. Mealling. *A URN Namespace of Object Identifiers*. IETF RFC 3061, February 2001. See http://www.ietf.org/rfc/rfc3061.txt.

[SAMLCore] E. Maler et al. Assertions *and Protocols for the OASIS Security Assertion Markup Language (SAML)*. OASIS, September 2003. Document ID oasis-sstc-saml-core-1.1. http://www.oasis-open.org/committees/security/.

[SAML-XSD] E. Maler et al. *SAML assertion schema.* OASIS, September 2003. Document ID oasis-sstc-saml-schema-assertion-1.1. http://www.oasis-open.org/committees/security/.

[SAML2Core] S. Cantor et al., *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-core-2.0-os. See http://www.oasis-open.org/committees/security/.

[SAML-X500] S.Cantor., *SAML V2.0 X.500/LDAP Attribute Profile, Committee Specification 01*. OASIS SSTC, March 2008. Document ID sstc-saml-attribute-x500-cs-01. See http://wiki.oasis-open.org/security/.

[SAML2-XSD] S. Cantor et al. *SAML 2.0 Assertion Schema.* OASIS, March 2005. Document ID saml-schema-assertion-2.0. http://www.oasis-open.org/committees/security/.

[Schema2] P. V. Biron et al. *XML Schema Part 2: Datatypes*. World Wide Web Consortium Recommendation, May 2001. http://www.w3.org/TR/xmlschema-2/.

4.2 Non-Normative References

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