SAML eduPerson Attribute Profiles

Working Draft 01, 18 April 2005

Document identifier:

draft-internet2-mace-dir-eduPerson-SAML-01

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

Abstract:

This document contains a pair of SAML attribute profiles addressing the use of eduPerson attribute definitions with the SAML 1.x and SAML 2.0 specifications

Table of Contents

1 Introduction

The eduPerson specification ([eduPerson]) defines 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. This profile specifies a mapping of these attribute types to the SAML 1.1 ([SAMLCore]) and SAML 2.0 ([SAML2Core]) specifications. SAML provides a general framework for expressing attribute information but does not define specific attribute types or impose other requirements on applications. This profile enables SAML applications that wish to exchange eduPerson 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 implementatations of the Shibboleth specification ([ShibProt]) 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.

1.1 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 `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 eduPerson Attribute Profile for SAML 1.x

This profile defines the syntax for expressing attribute types defined (or referenced) by [eduPerson] in SAML 1.1. SAML 1.0 is identical to SAML 1.1 with respect to attribute representation and this profile should be considered to apply to it as well.

2.1 Required Information

Identification: urn:mace:dir:eduperson:profiles: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.

SAML 1.1 does not specify any interoperable means of establishing the kind of name used, so the convention used is that the `AttributeNamespace` XML attribute in `<saml:Attribute>` elements MUST be set to `urn:mace:shibboleth:1.0:attributeNamespace:uri`

Unless specified below, 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].

Example:

```
urn:oid:2.5.4.3
```

Since [eduPerson] 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.

2.2.1 Legacy Names

Unfortunately, this profile post-dates the establishment of an alternate naming convention designed to improve the human-readability of attribute information. 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:

```
urn:mace:dir:attribute-def:eduPersonScopedAffiliation
urn:mace:dir:attribute-def:eduPersonPrimaryAffiliation
urn:mace:dir:attribute-def:eduPersonAffiliation
urn:mace:dir:attribute-def:eduPersonPrincipalName
urn:mace:dir:attribute-def:eduPersonEntitlement
urn:mace:dir:attribute-def:eduPersonTargetedID
urn:mace:dir:attribute-def:eduPersonNickname
urn:mace:dir:attribute-def:eduPersonPrimaryOrgUnitDN
```

```
urn:mace:dir:attribute-def:eduPersonOrgUnitDN
urn:mace:dir:attribute-def:eduPersonOrgDN
urn:mace:dir:attribute-def:businessCategory
urn:mace:dir:attribute-def:carLicense
urn:mace:dir:attribute-def:cn
urn:mace:dir:attribute-def:departmentNumber
urn:mace:dir:attribute-def:description
urn:mace:dir:attribute-def:displayName
urn:mace:dir:attribute-def:employeeNumber
urn:mace:dir:attribute-def:employeeType
urn:mace:dir:attribute-def:facsimileTelephoneNumber
urn:mace:dir:attribute-def:givenName
urn:mace:dir:attribute-def:homePhone
urn:mace:dir:attribute-def:homePostalAddress
urn:mace:dir:attribute-def:initials
urn:mace:dir:attribute-def:jpegPhoto
urn:mace:dir:attribute-def:l
urn:mace:dir:attribute-def:labeledURI
urn:mace:dir:attribute-def:mail
urn:mace:dir:attribute-def:manager
urn:mace:dir:attribute-def:mobile
urn:mace:dir:attribute-def:o
urn:mace:dir:attribute-def:ou
urn:mace:dir:attribute-def:pager
urn:mace:dir:attribute-def:physicalDeliveryOfficeName
urn:mace:dir:attribute-def:postalAddress
urn:mace:dir:attribute-def:postalCode
urn:mace:dir:attribute-def:postOfficeBox
urn:mace:dir:attribute-def:preferredLanguage
urn:mace:dir:attribute-def:roomNumber
urn:mace:dir:attribute-def:seeAlso
urn:mace:dir:attribute-def:sn
urn:mace:dir:attribute-def:st
urn:mace:dir:attribute-def:street
urn:mace:dir:attribute-def:telephoneNumber
urn:mace:dir:attribute-def:title
urn:mace:dir:attribute-def:uid
urn:mace:dir:attribute-def:userCertificate
urn:mace:dir:attribute-def:userSMIMECertificate
```

This is obviously 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 if new attribute types emerge.

2.2.2 Attribute Name Comparison

Two `<saml:Attribute>` elements refer to the same SAML attribute if and only if their `AttributeName` XML attribute values are byte-equal (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 in [SAML2Prof] 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.

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.

Instead, an unqualified 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).

Examples are shown in section 2.4.

The following attributes 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
```

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

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 must be addressed on a case by case basis at this time.

2.3.2.1 eduPersonTargetedID

The "eduPersonTargetedID" attribute is an outlier because its abstract representation cannot easily be bound to an LDAP directory syntax, nor 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 URI of the identity provider that created the value
- the URI 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.

The legacy `AttributeName`, `urn:mace:dir:attribute-def:eduPersonTargetedID`, is bound to an older representation in which the attribute is considered to be scoped (as described in section 2.3.1) and the value is expressed with a scope representing the identity provider. The scope MAY be in any form, possibly but not specifically a URI. The service provider value is not represented.

The OBJECT IDENTIFIER-derived `AttributeName`, `urn:oid:1.3.6.1.4.1.5923.1.1.1.10`, is bound to a new, expanded representation that leverages the equivalence in semantics between this attribute type and the SAML 2.0 subject name identifier format of

`urn:oasis:names:tc:SAML:2.0:nameid-format:persistent` (see section 8.3.7 of [SAML2Core]). The newer representation places a `<saml2:NameID>` element expressing the attribute value directly within the `<saml:AtributeValue>` element. The identity provider and service provider identifiers map directly into the `NameQualifier` and `SPNameQualifier` XML attributes, as defined in [SAML2Core].

Examples of both representations can be found in section 2.4.

2.4 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. 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 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. The scope "example.org" is used to stand-in for the identity provider's full name.

```
<saml:Attribute AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri"
       AttributeName="urn:mace:dir:attribute-def:eduPersonTargetedID">
   <saml:AttributeValue Scope="example.org">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 eduPerson Attribute Profile for SAML 2.0

This profile defines the syntax for expressing attribute types defined (or referenced) by [eduPerson] in SAML 2.0. Most of the attribute types defined or referenced by [eduPerson] 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 [SAML2Prof] 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:eduperson:profiles:samlv2

Contact information: mace-dir@internet2.edu

Description: Given below.

Updates: The SAML 1.x profile

3.2 SAML Attribute Naming

All [eduPerson] attribute types possess an OBJECT IDENTIFIER. Therefore attribute naming and name comparison is in accordance with the X.500/LDAP attribute profile in [SAML2Prof].

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 [SAML2Prof] 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 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 COTS SAML software.

Examples are shown in section 3.4.

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 must be addressed on a case by case basis at this time.

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

Since this attribute type is assigned an OBJECT IDENTIFIER, its `Name` is derived in accordance with this profile as `urn:oid:1.3.6.1.4.1.5923.1.1.1.10`.

The value syntax defined by this profile leverages the equivalence in semantics between this attribute type and the SAML 2.0 subject name identifier format of `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent` (see section 8.3.7 of [SAML2Core]). This representation places a `<saml2:NameID>` element expressing the attribute value directly within the `<saml2:AtributeValue>` element. The identity provider and service provider identifiers map directly into the `NameQualifier` and `SPNameQualifier` XML attributes, as defined in [SAML2Core].

An example can be found in section 3.4.

3.4 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"
      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"
      x500:Encoding="LDAP">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"
      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"
      x500:Encoding="LDAP">cantor.2@osu.edu</saml2:AttributeValue>
</saml2:Attribute>
```

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"
      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" x500:Encoding="LDAP"
      >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">
   <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 (200312)*. Internet2-MACE, December 2003. http://www.nmi-edit.org/eduPerson/internet2-mace-dir-eduperson-200312.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/.

[SAML2Prof] S. Cantor et al., *Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-profiles-2.0-os. See http://www.oasis-open.org/committees/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, February 2005. http://shibboleth.internet2.edu/shibboleth-documents.html.