Enrolled User Policy Profiles Attribute
draft-wahl-schema-eupp-attribute-01

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on November 9, 2007.

Copyright Notice

Copyright (C) The IETF Trust (2007).
Abstract

This document defines an attribute of a user identity which contains a list of the identifiers of enrollment policy profiles for that user. This attribute is generated by an identity provider that manages the user’s identity. An encoding of the attribute is defined for transport in the Lightweight Directory Access Protocol (LDAP), in the Security Assertion Markup Language (SAML), the OpenID Attribute Exchange Protocol, and as an Information Card claim.
1. Introduction

In an identity metasystem [15], when an end user requests access to a service, the network interactions for authenticating and authorizing that user can involve three parties: a relying party, an identity provider, and the end user. The relying party is the network entity which requires the identity of a user in order to make an access control decision. The identity provider is the network entity which establishes the identity of the end user.

For example, a company which provides a free blog hosting service to the Internet might operate as an identity provider. When a customer of the service logs in to update their blog, the company will authenticate the user and record the last login time. Another Internet service, such as a free digital photo hosting service, might act as relying party and leverage that blog hosting service identity provider. An identity provider - relying party relationship between these two organizations will enable a customer of that blog hosting service to be able to access the digital photo hosting service without needing to maintain a separate copy of their account authentication credentials at the digital photo hosting service.

A relying party can make use of claims issued by an identity provider in order to determine whether the user requesting access to a service has been authenticated, and if so, whether access should be granted. Whether the relying party will permit access depends on the relying party’s access control decision function. One input to that function is an assessment on the reliability of the information provided in those claims, which might be based on the practices and procedures employed by the identity provider which led to those claims being generated. Another input is the suitability of the identity and the associated claims to the service provided by the relying party. In order to assist the relying party with this decision, the identity provider might wish to indicate under which set of practices the user’s identity is managed (their identity as known to the identity provider was established or revised), particularly if the identity provider has multiple practices for enrollment, or these practices change over time.

In a typical deployment, the identity provider and relying party have a relationship established before a user identified by the identity provider is allowed access to a relying party. The specifications agreed in that relationship might include, for example, the community of users served by the identity provider, the practices by which identity provider identifies and authenticates users, or the formats of the attributes generated by the identity provider.

In some cases, an identity provider might offer claim generation
services to user community that includes multiple, potentially overlapping, categories of users. The identification of the category of user might be of interest to the relying parties in order to enable the relying party to make a better access control decision.

To continue the previous example, the blog hosting service might have a policy that all of their employees have accounts in the service, and that individuals whose employment is terminated are allowed to keep their blog hosting accounts. The blog hosting service might wish to indicate to the relying parties whether the user’s account is for

- a current employee
- a former employee
- a user with no employment history with the identity provider

The degree of verification used to establish the user’s account might potentially be greater for current and former employees than for non-employee users (e.g., if the employee process incorporated an in-person identity document verification process), and the degree of authentication used to identify the requestor as a user might be greater for current employees than for former employees or non-employee users (e.g., if current employees are required to perform multi-factor authentication, but other users simply rely on password-based authentication).

Frequently, these categorizations are connected with the different communities of users supported by the identity provider. A large company operating an in-house identity provider might have multiple categories of individuals accessing their internal network, such as employees, contractors, employees and contractors of outsourced service providers, auditors, employees and contractors of partners and customers, etc. The company will have different policies for how each category of user that is enrolled into the identity provider service.

Even for customers or employees as a whole, the enrollment practices that an identity provider follows may change over time. For example, regulation might require that the identity provider use stronger verification methods for new customers.

This document defines an attribute of a user identity that is intended for use in an identity metasystem, for an identity provider to specify the enrolled user policy or policies which establish and maintain the user identity at that identity provider.
The words "MUST", "SHOULD" and "MAY" are used as defined in RFC 2119 [1].

Please send comments to the author at mark.wahl@informed-control.com.
2. Attribute definition

This document defines an attribute of a user identity that is generated by an identity provider to specify the enrolled user policy profiles under which the user's identity is managed by the identity provider. The value of an attribute of this type consists of an ordered list of one or more enrolled user policy profile identifiers. Each identifier specifies a single enrolled user policy profile supported by the identity provider, under which the user was enrolled into the identity provider’s user community. If this attribute is present in a user's identity and more than one enrolled user policy profile identifier is present in the value of the attribute, then all of the enrolled user policy profiles identified in that value apply to the identity.

2.1. Enrolled user policy profile

An enrolled user policy profile is a named set of rules that indicates the applicability of a user identity to a particular community and/or class of application with common security requirements. An enrolled user policy profile for a user may be based on the practices of the identity provider, on the user community served by the identity provider, on the credentials by which the user established their identity with the identity provider, or other factors. This policy is similar in concept to a certificate policy, which is defined in X.509 [16] and expanded in RFC 3647 [2].

An identity provider can categorize a user’s identity into zero, one, or more than one enrolled user policy profiles. There may be multiple enrolled user policy profiles by which a particular user is categorized, and this set may change over time. However, an enrolled user policy profile is not intended to change to indicate a transitory state that is still within conditions acceptable to the identity provider. Other protocols, such as the OpenID assertion quality extension [17], SHOULD be used to indicate parameters that change, such as the authentication method most recently selected by a user.

2.2. Enrolled user policy profile identifier forms

An enrolled user policy profile is named by a Uniform Resource Identifier [3] (URI). The URI MUST be encoded into US-ASCII characters, and any embedded whitespace MUST be encoded. URIs MUST be normalized by the identity provider generating them, to enable relying parties to compare two URIs for equality using a US ASCII case exact match string comparison function.

While a value of the attribute can contain URIs that are URNs or URLs
of any scheme, the identity provider SHOULD use URIs that are either of the OBJECT IDENTIFIER identifier form, or the HTTP identifier form, as described below.

2.2.1. OBJECT IDENTIFIER identifier form choice

The OBJECT IDENTIFIER identifier form of an enrolled user policy profile identifier is intended for use by an identity provider that is also a X.509 certification authority (CA) or registration authority (RA). A CA or RA already might have a OBJECT IDENTIFIER that specifies the certificate policy by which an end user certificate is issued, for use in the Internet X.509 Public Key Infrastructure [4].

The URI of the enrolled user policy profile identifier consists of a Uniform Resource Name in the "oid" namespace [5]. A URI in this form will resemble

    urn:oid:1.3.6.1.2.1.27

2.2.2. HTTP identifier form choice

The HTTP identifier form of an enrolled user policy profile identifier is intended for use by any identity provider.

The URI of the enrolled user policy profile identifier consists of a Uniform Resource Locator in either the "http" [6] or "https" [7] schemes. The URI MAY contain a query, and MAY contain a fragment.
3. Representing the attribute in an identity metasystem

The value of an attribute of this type consists of an ordered list of one or more enrolled user policy profile identifiers. Each enrolled user policy profile is identified by a URI, as discussed in the previous section, and are separated in the enrolled user policy profile identifiers value from other URIs by a US-ASCII space character (SP).

3.1. Representation as an LDAP attribute

This attribute can be part of a user’s entry held in a directory server based on the LDAP [8] data model. The schema definitions are based on the LDAP directory information models [9].

The attribute type is defined as follows (with lines wrapped for readability):

```plaintext
attributeTypes: ( 1.3.6.1.4.1.21008.97.74.4.1
    NAME 'enrolledUserPolicyProfiles'
    EQUALITY caseExactMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
    SINGLE-VALUE )
```

The caseExactMatch and Directory String syntax are defined in RFC 4517 [10].

In order to allow this class to be present on objects of many different structural classes, an auxiliary object class is defined.

```plaintext
objectClasses: ( 1.3.6.1.4.1.21008.97.74.4.2
    NAME 'enrolledUserPolicyProfilesClass'
    AUXILIARY
    MAY ( enrolledUserPolicyProfiles ) )
```

This auxiliary class might most usefully be combined with the person object class.

Clients MUST NOT assume the absence of this class in an entry’s objectClass implies that the enrolledUserPolicyProfiles attribute is not present in the entry, as this attribute might be part of a privately-defined schema object class, or be provided through collective attributes.
3.2. Representation as a SAML 1.1 attribute

This attribute can be expressed as a SAML 1.1 attribute. The attribute is represented as if it is translated from LDAP to SAML 1.1 using the method described in the MAC-Dir SAML Attribute Profile [11].

In this representation, the SAML attribute name is

urn:oid:1.3.6.1.4.1.21008.97.74.4.1

The AttributeNamespace is

urn:mace:shibboleth:1.0:attributeNamespace:uri

An example SAML 1.1 attribute is

\[
\text{<saml:Attribute AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri" AttributeName="urn:oid:1.3.6.1.4.1.21008.97.74.4.1">
\text{<saml:AttributeValue xsi:type="xsd:string">}
\text{https://www.example.com/policy/cur.html#pfc urn:oid:1.1}
\text{</saml:AttributeValue>}
\text{</saml:Attribute>}
\]

3.3. Representation as a SAML 2.0 attribute

This attribute can be expressed as a SAML 2.0 attribute. The attribute is represented as if it is translated from LDAP to SAML 2.0 using the method described in the SAML V2.0 X.500/LDAP Attribute Profile [12].

In this representation, the SAML attribute name is

urn:oid:1.3.6.1.4.1.21008.97.74.4.1

The FriendlyName is "enrolledUserPolicyProfiles".

The attribute NameFormat is

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

3.4. Representation in OpenID Attribute Exchange

This attribute can be transferred using the OpenID Attribute Exchange protocol [13].
The attribute type identifier URI is

http://www.ldap.com/1/schema/eupp/eupp.rdf#EnrolledUserPolicyProfiles

The data format URI is

http://www.ldap.com/1/schema/eupp/eupp.xml#spaceSeparatedUriList

The data type is

<xsd:simpleType name="spaceSeparatedUriList">
  <xsd:restriction base="xsd:string">
    </xsd:restriction>
  </xsd:simpleType>

3.5. Representation as an Information Card claim

This attribute can be expressed as an Information Card claim [14].

The claim type URI is

http://www.ldap.com/1/schema/eupp/eupp.rdf#EnrolledUserPolicyProfiles

The data type is "xs:string".
4. Sample identifiers

This section provides sample categories of enrolled user policy profiles.

4.1. Unverified

The URI "http://www.ldap.com/1/schema/eupp/id/unverified.rdf" indicates that the identity provider has not performed any verification of the identity.

4.2. Provisional

The URI "http://www.ldap.com/1/schema/eupp/id/provisional.rdf" indicates that the identity provider has not completed performing the verification tasks which are normally performed for a new user enrollment.

4.3. Shared account

The URI "http://www.ldap.com/1/schema/eupp/id/shared.rdf" indicates that the identity is known by the identity provider to be used as a shared account by a potentially large number of users.

4.4. Fictitious

The URI "http://www.ldap.com/1/schema/eupp/id/fictitious.rdf" indicates that the identity is known by the identity provider to be a fictitious persona, e.g. if the user has registered with a name of "Mickey Mouse".
5. Security Considerations

As with the certificate policy defined in RFC 3647 [2], the enrolled user policy profiles attribute MAY be used by a relying party to help in deciding whether an identity is sufficiently trustworthy and otherwise appropriate for a particular application. This attribute is purely advisory and is provided voluntarily by the identity provider. This attribute in itself is not sufficient for a relying party to establish trust in an identity provider, or for a relying party to establish trust in a particular identity: additional attributes and trust mechanisms are required, that are outside of the scope of this document.
6. IANA Considerations

The LDAP attribute and object class defined in this document will be registered with IANA.

Subject: Request for LDAP Descriptor Registration
Descriptor (short name): enrolledUserPolicyProfiles
Object Identifier: 1.3.6.1.4.1.21008.97.74.4.1
Person & email address to contact for further information:
Mark Wahl <Mark.Wahl@informed-control.com>
Usage: attribute type
Specification: RFC XXXX
Author/Change Controller: IESG
Comments:

Subject: Request for LDAP Descriptor Registration
Descriptor (short name): enrolledUserPolicyProfilesClass
Object Identifier: 1.3.6.1.4.1.21008.97.74.4.2
Person & email address to contact for further information:
Mark Wahl <Mark.Wahl@informed-control.com>
Usage: object class
Specification: RFC XXXX
Author/Change Controller: IESG
Comments:
7. References

7.1. Normative References


7.2. Informative References


Appendix A. Copyright

Copyright (C) The IETF Trust (2007). This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights. This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.
Author’s Address

Mark Wahl
Informed Control Inc.
PO Box 90626
Austin, TX  78709
US

Email: mark.wahl@informed-control.com