ConfiguringScopedAttributes

This page is being updated and refined - the information on it is not yet considered to be "official". Thanks for your understanding!

Handling Scoped Attributes in Shibboleth IDP and SP

With many campuses transitioning from 1.3 to 2.1, there have been some confusions over configuring Shibboleth to properly deliver and consume scoped attributes. Older versions of Shibboleth (1.3 and earlier) defined attribute names using MACE defined URN Strings. That is what most early Shibboleth adopter used when releasing attributes. SAML 2 (hence Shibboleth 2) introduced a new convention of naming attribute based on OID-style URN strings. This difference has created incompatibilities between IDP's and SP's running on different versions of Shibboleth software. This document illustrates the best practices we've developed to maintain maximum attribute compatibility between different versions of Shibboleth.

Since eduPersonPrincipleName (eppn) is the most heavily used scoped attribute, we will use eppn throughout this document as example.

There are two ways to define attribute names for eduPersonPrincipleName in Shbibboleth:

- Using MACE-defined URN: urn:mace:dir:attribute-def:eduPersonPrincipalName
- Using OID-style URN: urn:oid:1.3.6.1.4.1.5923.1.1.1.6

The rest of the documentation will show you the best practices for each version of IdP and SP.

Configuring eppn in IDP 1.3

Work in Progress

I am still working to determine the best way to handle IDP 1.3 configuration. Since OID-based attribute naming is a SAML 2 specification, it is difficult for 1.3 IDPs to just support OID-based attribute names. The example below is a guess. I am currently testing/researching whether it works. Stay tuned. With the example below, both attributes have to be released to an application in order for OID-based attribute to work. If MACE-defined attribute is not released as well the OID-based attribute will not be inline scoped and thus rejected by the SP's attribute-polcy.

Edit resolver.xml to include the following configuration:

```
<!-- replace 'urn:mace:ucla.edu:edimi:attributes:uclaLogonID' with the name of your NetID attribute -->
<SimpleAttributeDefinition id="urn:mace:dir:attribute-def:eduPersonPrincipalName"
                           smartScope="ucla.edu">
        <AttributeDependency requires="urn:mace:ucla.edu:edimi:attributes:uclaLogonID"/>
</SimpleAttributeDefinition>
<SimpleAttributeDefinition id="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
                           sourceName="urn:mace:dir:attribute-def:eduPersonPrincipalName">
        <AttributeDependency requires="urn:mace:dir:attribute-def:eduPersonPrincipalName"/>
</SimpleAttributeDefinition>
```

Configuring eppn in IDP 2.1

The following example was taken from Internet2's documentation.

Edit attribute-resolver.xml to include the following configuration:

```
<resolver:AttributeDefinition id="eduPersonPrincipalName"
                              xsi:type="Scoped"
                              xmlns="urn:mace:shibboleth:2.0:resolver:ad"
                              scope="example.org"
                              sourceAttributeID="uid">
    <resolver:Dependency ref="myLDAP" />
    <resolver:AttributeEncoder xsi:type="SAML1ScopedString"
                               xmlns="urn:mace:shibboleth:2.0:attribute:encoder"
                               name="urn:mace:dir:attribute-def:eduPersonPrincipalName" />

    <!-- additional definition for use with commercial SAML 1.1 SPs -->
    <resolver:AttributeEncoder xsi:type="SAML1ScopedString"
                               xmlns="urn:mace:shibboleth:2.0:attribute:encoder"
                               name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
                               scopeType="inline" />

    <resolver:AttributeEncoder xsi:type="SAML2ScopedString"
                               xmlns="urn:mace:shibboleth:2.0:attribute:encoder"
                               name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
                               friendlyName="eduPersonPrincipalName" />
</resolver:AttributeDefinition>
```

Configuring eppn in SP 1.3

The following xml snippit maps multiple attributes to a single header. It enables a 1.3 SP to accept either attribute name. This is the configuration we use for spaces.ais.ucla.edu.

Edit AAP.xml to include the following configuration:

```
<AttributeRule Name="urn:mace:dir:attribute-def:eduPersonPrincipalName"
               Scoped="true"
               Header="REMOTE_USER"
               Alias="user">
    <!-- Basic rule to pass through any value. -->
    <AnySite>
        <Value Type="regexp">^[ConfiguringScopedAttributes^@]+$</Value>
    </AnySite>
</AttributeRule>
<AttributeRule Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
               Scoped="false"
               Header="REMOTE_USER"
               Alias="user-alt">
    <AnySite>
        <AnyValue/>
    </AnySite>
</AttributeRule>
```

Configuring eppn in SP 2.1

We have not tested the following configuration. This is the configuration is recommend by Chad La Joie.

Edit attribute-map.xml to include the following configuration:

```
<Attribute name="urn:mace:dir:attribute-def:eduPersonPrincipalName"
           id="eppn">
    <AttributeDecoder xsi:type="ScopedAttributeDecoder"/>
</Attribute>
<Attribute name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
           id="eppn">
    <AttributeDecoder xsi:type="ScopedAttributeDecoder"/>
</Attribute>
```