Applying the Registered By InCommon Category

This page shows some sample Shibboleth IdP configurations that leverage the proposed Registered By InCommon Category.

This document contains DRAFT material intended for discussion and comment by the InCommon participant community. Comments and questions should be sent to the InCommon participants mailing list (participants@incommon.org).

Releasing the Essential Attribute Bundle

A Shibboleth IdP uses type `basic:ANY` to activate a policy for **any** requester. For example, here's a default attribute release policy that releases the Essential Attribute Bundle to **all** SPs:

A Shib IdP config that releases attributes to ALL SPs

```
<afp:AttributeFilterPolicy id="releaseEssentialAttributeBundle">

  <!-- this policy is active for ANY requester -->
  <afp:PolicyRequirementRule xsi:type="basic:ANY"/>

  <!-- the Essential Attribute Bundle -->

  <afp:AttributeRule attributeID="eduPersonPrincipalName">
    <afp:PermitValueRule xsi:type="basic:ANY"/>
  </afp:AttributeRule>
  <afp:AttributeRule attributeID="email">
    <afp:PermitValueRule xsi:type="basic:ANY"/>
  </afp:AttributeRule>
  <afp:AttributeRule attributeID="displayName">
    <afp:PermitValueRule xsi:type="basic:ANY"/>
  </afp:AttributeRule>
  <afp:AttributeRule attributeID="givenName">
    <afp:PermitValueRule xsi:type="basic:ANY"/>
  </afp:AttributeRule>
  <afp:AttributeRule attributeID="surname">
    <afp:PermitValueRule xsi:type="basic:ANY"/>
  </afp:AttributeRule>

</afp:AttributeFilterPolicy>
```

A default policy (such as the previous policy) takes on a different meaning in the presence of eduGAIN metadata. It is believed that some IdPs will want to retain the semantics of their current default policy, at least for a time. This is why the Registered By InCommon Category was created.

An instance of Shibboleth IdP V2 may leverage the `registered-by-incommon` entity attribute to retain its current default policy:

A Shib IdP V2 rule that releases attributes to all SPs registered by InCommon

```
<!-- this policy is active for a requester with the following entity attribute -->
<afp:PolicyRequirementRule xsi:type="saml:AttributeRequesterEntityAttributeExactMatch"
    attributeName="http://macedir.org/entity-category"
    attributeValue="http://id.incommon.org/category/registered-by-incommon"/>
```

An instance of Shibboleth IdP V3 will either leverage the `registered-by-incommon` entity attribute (as above) or the `<mdrpi:RegistrationInfo>` element directly, as shown in the following example:

A Shib IdP V3 rule that releases attributes to SPs registered by InCommon

```
<!-- this policy is active for a requester whose registrar has the given ID -->
<afp:PolicyRequirementRule xsi:type="saml:RegistrationAuthority"
    registrars="https://incommon.org"/>
```

The value of the `registrars` XML attribute above is the globally unique registrar ID for InCommon.

Releasing the R&S Attribute Bundle

Most of the Research & Scholarship (R&S) IdPs in the InCommon Federation are configured with a policy rule that releases attributes to R&S SPs tagged with the legacy InCommon R&S entity attribute value:

A Shib IdP V2 rule that releases attributes to legacy R&S SPs

```
<afp:PolicyRequirementRule xsi:type="saml:AttributeRequesterEntityAttributeExactMatch"
    attributeName="http://macedir.org/entity-category"
    attributeValue="http://id.incommon.org/category/research-and-scholarship"/>
```

R&S IdPs should instead be configured with a policy that releases the R&S Attribute Bundle to **all** R&S SPs, including R&S SPs in other federations:

A Shib IdP config that releases the R&S bundle to ALL R&S SPs

```
<afp:AttributeFilterPolicy id="releaseRandSAttributeBundle">

  <!-- for Shib IdP V3, use type saml:EntityAttributeExactMatch instead -->

  <afp:PolicyRequirementRule xsi:type="saml:AttributeRequesterEntityAttributeExactMatch"
      attributeName="http://macedir.org/entity-category"
      attributeValue="http://refeds.org/category/research-and-scholarship"/>

  <!-- a fixed subset of the Research & Scholarship Attribute Bundle -->

  <afp:AttributeRule attributeID="eduPersonPrincipalName">
    <afp:PermitValueRule xsi:type="basic:ANY"/>
  </afp:AttributeRule>

  <!-- if your deployment of ePPN is non-reassigned, release of ePTID is OPTIONAL -->
  <afp:AttributeRule attributeID="eduPersonTargetedID">
    <afp:PermitValueRule xsi:type="basic:ANY"/>
  </afp:AttributeRule>

  <afp:AttributeRule attributeID="email">
    <afp:PermitValueRule xsi:type="basic:ANY"/>
  </afp:AttributeRule>

  <!-- either displayName or (givenName and sn) is REQUIRED but all three are RECOMMENDED -->
  <afp:AttributeRule attributeID="displayName">
    <afp:PermitValueRule xsi:type="basic:ANY"/>
  </afp:AttributeRule>
  <afp:AttributeRule attributeID="givenName">
    <afp:PermitValueRule xsi:type="basic:ANY"/>
  </afp:AttributeRule>
  <afp:AttributeRule attributeID="surname">
    <afp:PermitValueRule xsi:type="basic:ANY"/>
  </afp:AttributeRule>

  <!-- release of ePSA is OPTIONAL -->
  <afp:AttributeRule attributeID="eduPersonScopedAffiliation">
    <afp:PermitValueRule xsi:type="basic:ANY"/>
  </afp:AttributeRule>

</afp:AttributeFilterPolicy>
```

To facilitate the migration suggested by the previous examples, all R&S SPs registered by InCommon have a multivalued R&S entity attribute in metadata.

It is believed that some R&S IdPs will want to retain their current attribute release policy for a time. An instance of Shibboleth IdP V2 may leverage the Registered By InCommon Category to retain its current attribute release policy but without relying on the legacy InCommon R&S entity attribute value:

A Shib IdP V2 rule that releases attributes to R&S SPs registered by InCommon

```
<afp:PolicyRequirementRule xsi:type="basic:AND">
  <basic:Rule xsi:type="saml:AttributeRequesterEntityAttributeExactMatch"
      attributeName="http://macedir.org/entity-category"
      attributeValue="http://refeds.org/category/research-and-scholarship"/>
  <basic:Rule xsi:type="saml:AttributeRequesterEntityAttributeExactMatch"
      attributeName="http://macedir.org/entity-category"
      attributeValue="http://id.incommon.org/category/registered-by-incommon"/>
</afp:PolicyRequirementRule>
```

An instance of Shibboleth IdP V3 will either leverage the `registered-by-incommon` entity attribute (as above) or the `<mdrpi:RegistrationInfo>` element directly, as shown in the following example:

A Shib IdP V3 rule that releases attributes to R&S SPs registered by InCommon

```
<afp:PolicyRequirementRule xsi:type="basic:AND">
  <basic:Rule xsi:type="saml:EntityAttributeExactMatch"
      attributeName="http://macedir.org/entity-category"
      attributeValue="http://refeds.org/category/research-and-scholarship"/>
  <basic:Rule xsi:type="saml:RegistrationAuthority"
      registrars="https://incommon.org"/>
</afp:PolicyRequirementRule>
```

For more information about configuring an IdP for R&S, consult the R&S Attribute Bundle Config topic in the wiki.