Using the Registered By InCommon Category

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

Contents

- IdP Uses of the Registered By InCommon Category
  - Releasing the Essential Attribute Bundle
  - Releasing the R&S Attribute Bundle
- SP Uses of the Registered By InCommon Category
  - Filtering Untrusted Metadata
  - Customizing Discovery Interfaces

IdP Uses of the Registered By InCommon Category

Typically, an IdP will use the `registered-by-incommon` entity attribute (if it uses it all) to constrain its attribute release policy. A number of sample policy rules are illustrated in the subsections below.

Do not filter SP metadata!

An interoperable IdP consumes all the SP metadata in the world, no exceptions. Consequently, *an IdP does not filter metadata*. Instead an interoperable IdP implements a rational set of attribute release rules, subject to local policy.

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. For various reasons, 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.

Here's how an instance of Shibboleth IdP V2 can 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 -->
<!-- (for Shib IdP V3, use type saml:EntityAttributeExactMatch instead)        -->
<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 all 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 ID for the InCommon registrar.

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"/>
```

An IdP configuration SHOULD NOT rely on the incommon.org R&S tag in SP metadata

Use of the legacy incommon.org R&S tag to configure attribute release policy at the IdP is **deprecated**. Eventually this tag will be removed from all SP metadata although a timeline for doing so has not yet been determined.

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 thought 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

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

<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 Research & Scholarship, consult the R&S Attribute Bundle Config topic in the wiki.

SP Uses of the Registered By InCommon Category

SPs typically leverage entity attributes up front when metadata is consumed. The `registered-by-incommon` entity attribute may be used to customize the discovery interface, or in some special circumstances, to filter metadata altogether.

See the Shibboleth Metadata Config topic for a complete example of a `MetadataProvider`. At most one of the following `MetadataFilter` elements may be added to that `MetadataProvider`.

Filtering Untrusted Metadata

To filter all but InCommon metadata, add the following `MetadataFilter` to your SP's `MetadataProvider`:

Filter all metadata not registered by InCommon

```
<!-- consume only InCommon metadata -->
<MetadataFilter type="Whitelist" matcher="EntityAttributes">
  <saml:Attribute
      Name="http://macedir.org/entity-category"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
    <saml:AttributeValue>http://id.incommon.org/category/registered-by-incommon</saml:AttributeValue>
  </saml:Attribute>
</MetadataFilter>
```

The above policy is severe but sometimes warranted. A more relaxed policy will simply filter the metadata from the discovery interface, as shown in the next section.

Customizing Discovery Interfaces

To show all IdPs with the `registered-by-incommon` entity attribute, add the following `MetadataFilter` to your SP's `MetadataProvider`:

Show only InCommon IdPs on the discovery interface

```
<!-- Show all IdPs with the registered-by-incommon entity attribute -->
<DiscoveryFilter type="Whitelist" matcher="EntityAttributes"
    attributeName="http://macedir.org/entity-category"
    attributeNameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
    attributeValue="http://id.incommon.org/category/registered-by-incommon"/>
```

Keep in mind that hiding an IdP from the discovery interface does **not** prevent the SP from accepting an assertion from that IdP.