Consequences of eduGAIN Metadata

Consequences of eduGAIN Metadata

InCommon metadata registration practices, although just recently published, have remained more-or-less the same for over 10 years. During that time, the size of the metadata aggregate has grown significantly but the semantic content of the aggregate has not changed much (if at all). Indeed, the perception of metadata as a coherent bundle of trust anchors is a tightly held concept by most metadata consumers.

Two events are challenging long-held perceptions of the trusted metadata aggregate: interfederation and per-entity metadata. These forces will permanently alter our perception of trusted metadata.

The most disruptive such force is interfederation, specifically the import of eduGAIN metadata into trusted metadata aggregates such as the InCommon metadata aggregate. Since the provenance of entity descriptors in eduGAIN metadata is mostly unknown, combining eduGAIN metadata with more familiar InCommon metadata in a comprehensive aggregate will disrupt participant practices and IdP attribute release policies. As uncomfortable as it might seem, the import of eduGAIN metadata into the production aggregate is not only inevitable but advisable.

Recommendation

Import eduGAIN metadata directly into the production aggregate.

It's important to note that any meaning attached to the aggregate as a whole is lost when that aggregate is presented to the client as per-entity metadata. Today federation operators are paying close attention to entity attributes, MD-RPI elements, and other extension elements since these elements add value to entity metadata. The value of an aggregate, therefore, should properly be viewed as the sum of its individual entity descriptors. We must therefore sufficiently distinguish entity descriptors in metadata so that participants can enforce local policies that make sense to them.

The Name XML Attribute

For better or worse, InCommon metadata has a `Name` XML attribute on the root `<md:EntitiesDescriptor>` element:

```
<md:EntitiesDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
  ID="INC20140930T184956" Name="urn:mace:incommon" validUntil="2014-10-14T10:00:00Z" ...>
```

It is believed that a significant number of IdP operators currently base their attribute release policy on the `Name` XML attribute:

```
<afp:AttributeFilterPolicy id="releaseToAnyInCommonSP">
  <afp:PolicyRequirementRule
      xsi:type="saml:AttributeRequesterInEntityGroup" groupID="urn:mace:incommon"/>
  <!-- insert attribute rules here -->
</afp:AttributeFilterPolicy>
```

This is unfortunate since such a configuration will break the moment we import eduGAIN entities into InCommon metadata.

Avoid attribute release policy based on the Name XML attribute in metadata

We strongly RECOMMEND that IdPs do **not** rely on the `Name` XML attribute in InCommon metadata. Instead expose an entity attribute with similar semantics.

The problem is potentially worse than that. For example, consider the following attribute release policy:

```
<afp:AttributeFilterPolicy id="releaseToAnySP">
  <afp:PolicyRequirementRule xsi:type="basic:ANY"/>
  <!-- insert attribute rules here -->
</afp:AttributeFilterPolicy>
```

Did the deployer mean *any SP* or *any SP in this aggregate*?

Recommendation

IdP operators are advised to re-evaluate the use of the `basic:ANY` type in attribute release policy.

Registration Info

Every entity descriptor in eduGAIN metadata contains an `<mdrpi:RegistrationInfo>` element. For example:

```
<mdrpi:RegistrationInfo
    xmlns:mdrpi="urn:oasis:names:tc:SAML:metadata:rpi"
    registrationAuthority="https://incommon.org"/>
```

The actual value of the `registrationAuthority` XML attribute is the globally unique identifier of the metadata's registrar.

An IdP's attribute release policy could key off the `registrationAuthority` value but this immediately raises a number of questions and issues:

1. What are InCommon's recommended practices with respect to eduGAIN metadata? In particular, how is the `registrationAuthority` value best factored into an IdP's attribute release policy (if at all)?
2. What software supports MDRPI elements in metadata?
    a. Short answer: None. A 3rd-party plugin for Shibboleth IdP V2 exists. See the "Configuration Examples" section of the plugin documentation for specific configuration examples.
3. Should MDRPI info be routinely converted to entity attributes in metadata? If so, how?

The latter question stems from the fact that Shibboleth IdP V2 supports entity attributes out-of-the-box (but in any case, note that Shibboleth is the only SAML implementation that supports *any* of these extension elements).

Recommendation

De-emphasize the `<mdrpi:RegistrationInfo>` element as a direct source of attribute release policy. Instead expose the `registrationAuthority` XML attribute value as an entity attribute.

R&S Entity Category

In January 2014, REFEDS published a specification for a Research & Scholarship Entity Category that was heavily influenced by the existing InCommon Research & Scholarship Category, which opened its doors early in 2012. Currently there are a few dozen R&S entities in eduGAIN metadata (but that number seems to be steadily increasing). Here's what an SP entity attribute in eduGAIN metadata looks like, for example:

```
<mdattr:EntityAttributes xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
  <saml:Attribute Name="http://macedir.org/entity-category" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:uri">
    <saml:AttributeValue> http://refeds.org/category/research-and-scholarship </saml:AttributeValue>
  </saml:Attribute>
</mdattr:EntityAttributes>
```

An R&S SP in InCommon metadata is denoted similarly:

```
<mdattr:EntityAttributes xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
  <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/research-and-scholarship </saml:AttributeValue>
  </saml:Attribute>
</mdattr:EntityAttributes>
```

but the similarities between the two entity attributes are deceiving.

An InCommon R&S entity attribute value must **not** be exported to eduGAIN! Doing so will make it more difficult to migrate from InCommon R&S to REFEDS R&S.

Since InCommon R&S isn't recognized by the REFEDS community, we are left with the nagging problem of how to phase out the legacy InCommon R&S entity attribute value in an orderly fashion.