Metadata Registration and Publication Info

The SAML V2.0 Metadata Extensions for Registration and Publication Information is a specification for a set of extension elements to SAML metadata. These elements are particularly important for the purposes of interfederation. For example, every entity descriptor exported to eduGAIN must include the globally unique identifier of the registrar that registered that entity descriptor. See the sidebar for a complete list of registrars currently exporting metadata to eduGAIN.

Registration Info

Since metadata registrars rely on a wide variety of operating principles, we expect some metadata consumers to care who the registrar is, at least in the short term. To accommodate this potential need, a globally unique identifier for the InCommon registrar will be inserted into metadata:

The RegistrationInfo Element

```
<md:Extensions
    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    xmlns:mdrpi="urn:oasis:names:tc:SAML:metadata:rpi">
  <mdrpi:RegistrationInfo registrationAuthority="https://incommon.org"/>
</md:Extensions>
```

According to the MD-RPI specification, the above extension element (and therefore the registrar's ID) may be inserted either at the aggregate level or the entity level. To accommodate per-entity metadata, the `<mdrpi:RegistrationInfo>` element will be inserted at the entity level. Consequently, the introduction of the MD-RPI schema will necessarily *touch every entity descriptor* in metadata.

Besides the `registrationAuthority` XML attribute, the `<mdrpi:RegistrationInfo>` element has two other (optional) components:

- the `registrationInstant` attribute
- the `<mdrpi:RegistrationPolicy>` child element

This optional information will not be included in InCommon metadata, however. The rest of this section gives a rationale for this decision.

Since InCommon maintains a repository of every metadata aggregate ever published, the `registrationInstant` for each entity descriptor may be computed, but since the utility of this attribute has not been demonstrated, the computation (and subsequent publication) of the per-entity `registrationInstant` value will be omitted.

On the other hand, the `<mdrpi:RegistrationPolicy>` child element appears to be more interesting. Note, however, that the MD-RPI specification contains the following explicit requirement:

> *The URL MUST represent a single, immutable, policy document. Any changes made to an existing policy document MUST result in a new URL.*

Consequently, the value of the `<mdrpi:RegistrationPolicy>` element is not particularly useful as a component of an IdP's attribute release policy since the metadata registration practices of Federations worldwide are expected to change while registration procedures converge to a common standard. In particular, the InCommon Metadata Registration Practice Statement is subject to change, and therefore the `<mdrpi:RegistrationPolicy>` element represents a potential maintenance issue for IdP operators. For this reason, the element will not be included in entity metadata, at least not at this time.

Global Registrar IDs

- http://aai.arnes.si
- http://aai.grnet.gr/
- http://cafe.rnp.br
- http://cofre.reuna.cl
- http://colfire.co
- http://eduid.at
- http://eduid.hu
- http://federation.belnet.be/
- http://feide.no/
- http://iif.iucc.ac.il
- http://laife.lanet.lv/
- http://rr.aai.switch.ch/
- http://ukfederation.org.uk
- http://www.canarie.ca
- http://www.csc.fi/haka
- http://www.eduid.cz/
- http://www.heanet.ie
- http://www.idem.garr.it/
- http://www.rediris.es/
- http://www.srce.hr
- http://www.surfconext.nl/
- http://www.swamid.se/
- https://aai.pionier.net.pl
- https://federation.renater.fr/
- https://fedi.litnet.lt
- https://incommon.org
- https://minga.cedia.org.ec
- https://www.aai.dfn.de
- https://www.gakunin.jp
- https://www.wayf.dk

Attribute Release Policy

As suggested earlier, the registrar ID may be used to formulate an IdP's attribute release policy (although the extent to which IdP operators will actually want to do this is unknown). What follows are some practical considerations for deployers of the Shibboleth IdP software.

Unfortunately, Shibboleth IdP 2.x does not support the MD-RPI schema out-of-the-box. However, a plugin for Shibboleth IdP V2 that adds support for the `registrationAuthority` XML attribute has been developed by the UK Federation. An IdP outfitted with this plugin may be configured to release attributes based on the SP's registrar. See the "Configuration Examples" section of the plugin documentation for specific examples.

In contrast, support for the MD-RPI schema is native to Shibboleth IdP 3.x. Documentation is still kind of sketchy but see the AttributeFilterConfiguration topic in the Shibboleth wiki for an example of the new syntax.

Publication Info

The MD-RPI specification also defines an `<mdrpi:PublicationInfo>` element with the following three XML attributes:

1. `publisher` (required)
2. `creationInstant`

3. `publicationId`

The latter will be omitted from InCommon metadata but the other two are a welcome addition. In particular, the publisher XML attribute will take on the location of the metadata aggregate, which will positively identify the source of the metadata. This is useful for debugging and perhaps other purposes.

The PublicationInfo Element

```
<md:Extensions
    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    xmlns:mdrpi="urn:oasis:names:tc:SAML:metadata:rpi">
  <mdrpi:PublicationInfo
      publisher="http://md.incommon.org/InCommon/InCommon-metadata-preview.xml"
      creationInstant="2015-02-04T10:00:00Z"/>
</md:Extensions>
```

Unlike the `<mdrpi:RegistrationInfo>` element, the `<mdrpi:PublicationInfo>` element is intended to be used exclusively on the root element of the metadata, which implies the latter element should appear at the aggregate level, not the entity level.

Migration Strategy

Metadata aggregates are brittle by their very nature (which is yet another reason to embrace per-entity metadata) especially when introducing new XML schema into the mix. So as to minimize the risk of breakage, we will first introduce the MD-RPI schema into the *preview aggregate*. If all goes well, we will later sync the preview aggregate with the well-known *main aggregate* (which is sometimes called the *production aggregate* even though all aggregates published by InCommon are production-quality aggregates). The final step is to sync the main aggregate with the *fallback aggregate*. See the Metadata Aggregates wiki page for more info about this process.

By the way, if you have a test deployment handy (either IdP or SP), by all means point it at the preview aggregate and leave it that way indefinitely