Preparing for eduGAIN Metadata

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).

Importing eduGAIN metadata into the production InCommon metadata aggregate will have at least the following consequences:

1. Importing global IdP metadata into InCommon metadata will alter discovery interfaces across the Federation.
2. Importing global IdP metadata into InCommon metadata will cause some SPs to automatically accept attributes from those IdPs.
3. Importing global SP metadata into InCommon metadata will cause some IdPs to automatically release attributes to those SPs.

The following recommendations and guidelines are intended to help SP owners and IdP operators prepare for the introduction of eduGAIN metadata into the InCommon metadata aggregate.

Registered By InCommon Category

In general, SP owners and IdP operators can mitigate the effects of eduGAIN metadata by leveraging the Registered By InCommon Category.

Tips for SP Owners

Importing eduGAIN metadata will increase the number of IdPs in the InCommon aggregate by an order of magnitude, from a few hundred to over 1500 IdPs. Roughly 6000 IdPs are known to be deployed in R&E federations around the world, and it is expected that most of these IdPs will be eventually exported to eduGAIN.

Approximately 10% of global IdP entities belong to the Hide From Discovery Category. A much smaller proportion of InCommon IdPs are tagged with the h `ide-from-discovery` entity attribute but this will increase as the inevitable categorization of IdPs unfolds.

In most cases, SP deployments are well advised to filter IdPs tagged with the `hide-from-discovery` entity attribute. However, SP deployments with highly customized discovery interfaces may choose to ignore it. For example, a specialized SP with no discovery interface can completely ignore the `hide-from-discovery` entity attribute.

It is thought that importing global IdP entities into InCommon metadata will have little (or no) effect on most federated apps. If an app exposes all IdPs on its discovery interface (except perhaps IdPs tagged with the `hide-from-discovery` entity attribute), additional IdPs will be exposed as a result of importing global IdPs, but more often than not, that is precisely what's intended. If for some reason only InCommon IdPs are to be exposed (which should be the exception, not the rule), non-InCommon IdPs can be filtered from the discovery interface (assuming your software is capable of doing so).

Keep in mind that filtering IdPs from your discovery interface does not prevent those same IdPs from pushing a SAML assertion to your SP. If the latter is what you really want to do, then filter IdP metadata in conjunction with your metadata refresh process.

If you must limit your IdP partners, do it in one of two ways:

1. Filter IdPs from your discovery interface
2. Filter IdPs from your metadata refresh process

Avoid making access control decisions based on the characteristics of entity metadata (such as IdP entityID, entity attributes, and registration info).

Tips for R&S SP Owners

The recommendations above apply equally well to R&S SP owners but R&S SPs that filter based on the legacy InCommon R&S entity attribute value

http://id.incommon.org/category/research-and-scholarship

may also want to filter on the REFEDS R&S entity attribute value

http://refeds.org/category/research-and-scholarship

since global IdPs that support REFEDS R&S will carry the latter (and only the latter) in their metadata. Many R&S IdPs registered by InCommon will support REFEDS R&S so they too will carry the REFEDS R&S entity attribute value in their metadata.

In general, R&S SPs should avoid filtering on the R&S entity attribute in IdP metadata since doing so will tend to overlook non-R&S IdPs with relaxed attribute release policies. In any case, keep in mind that R&S IdPs will carry exactly one of the two R&S entity attribute values shown above.

Tips for IdP Operators

IdP operators should avoid attribute release policy based on properties of the metadata aggregate itself. In particular, avoid basing your attribute release policy on the `md:EntitiesDescriptor/@Name` XML attribute in metadata. Such a policy is invariably based on implicit assumptions that will prove to be false as new methods of metadata aggregation and distribution become the norm.

In general, base your attribute release policy on the characteristics of entity metadata only: SP entityID, entity attributes, and registration info. Avoid policy based on the characteristics of the aggregate itself.

IdP operators should also review their default attribute release policy. By definition, a *default attribute release policy* specifies a set of attributes to be released to any SP. The key phrase is *any SP*, which takes on new meaning in the presence of eduGAIN metadata.

If your IdP is configured with a default attribute release policy, you should review it *before* global SP metadata is imported into the InCommon production aggregate, otherwise you may start releasing attributes to unintended relying parties.

For example, if you're using the Shibboleth IdP software, a `PolicyRequirementRule` based on the `basic:ANY` type usually indicates a default policy is in effect. An IdP operator can leverage the `registered-by-incommon` entity attribute to scope their default policy to InCommon.

If you don't have a default policy, now is an excellent time to craft a default attribute release policy that will improve the overall interoperability of your IdP.

Special Notes for R&S IdP Operators

In the InCommon Federation, IdPs that support R&S are currently migrating to REFEDS R&S. Instead of recognizing the legacy InCommon R&S entity attribute value:

> http://id.incommon.org/category/research-and-scholarship

R&S IdPs are reconfiguring their attribute release policy rules to recognize the REFEDS R&S entity attribute value:

> http://refeds.org/category/research-and-scholarship

An R&S IdP has two choices:

1. Release attributes to **all** R&S SPs, including R&S SPs in other federations
2. Release attributes to R&S SPs registered by InCommon only

An IdP chooses exactly one of these two R&S configuration options.

An IdP that releases attributes to all R&S SPs will carry the REFEDS R&S entity attribute value in its metadata while an IdP that releases attributes to R&S SPs registered by InCommon only will carry the InCommon R&S entity attribute value in metadata. Only the REFEDS R&S entity attribute value will be exported to eduGAIN; the legacy InCommon R&S entity attribute value will be filtered from metadata exported to eduGAIN.