Recommendations (old)

Old Recommendations - This section was not deleted as it contains some useful information on concepts that we later rejected. Hopefully maintaining this page will help prevent another group from spending as much time on these ideas as we did.

1. An *entity-type* attribute should be added to the InCommon metadata in such a way that Shibboleth can be easily configured to use the entity-type as part of attribute release decisions. We need a controlled vocabulary for the metadata *entity-type* field using terms such as: K12, Higher Education, Research Lab, Commercial, Sponsored, Aggregator, Library, Museum, Proxy, etc. Can we use SCHAC definitions (http://www.terena.org/activities/tf-emc2/docs/schac/schac-20061212-1.3.0.schema.txt) or perhaps a subset of these definitions? Is SCHAC maintained any more? There may also be a schema that has already been developed as part of the NSTIC grant work. (Use cases:)

2. Some InCommon IdPs and SPs need to know and be able to act on data that specifies if the entity is under the full direct control of an organization that has signed the InCommon participation. In order to meet this need, we recommend that InCommon expose the value of the `registrationAuthority` XML attribute of `<mdrpi:RegistrationInfo>` element as an entity attribute. (Use cases: 1)

3. With the inclusion of K12 data, some InCommon service providers will need to know if the authenticated users are underage. While not an InCommon metadata issue and thus outside of the purview of this working group, this group recommends an expansion of eduPerson or k12Person to add the necessary attribute(s) to indicate age classification. Furthermore, this group recommends that k12 IdPs be required to populate this data as part of the requirement for being included in the InCommon metadata. (Use cases: 1)

4. We agreed to re-discuss the issues associated with Proxies in the metadata. The discussion to date has been to allow these **only** if all of the components are under the direct administrative control of the same InCommon legal entity (Use case: 2).

5. Issues related to the ability of InCommon members to have self-asserted data stored in the InCommon metadata remains to be discussed. (Use cases: 3,4)

6. Incorporation of eduGAIN Metadata
   a. A more focused discussion on a transition plan is still needed. See the more specific Item 5 notes. The general feeling is that if it becomes trivial for schools to configure Shibboleth to "simulate the current InCommon-only metadata", that we may be able to avoid the use of separate aggregates (see i below)
   b. Tag every entity descriptor in the production aggregate with a new entity attribute value (extended-validation-metadata). Resist the urge to create a new aggregate.
   c. Import eduGAIN metadata directly into the production aggregate. Start by importing IdP metadata from eduGAIN since the impact on InCommon SPs is less than what it will be for InCommon IdPs.
   d. Strongly recommend against the use of the AttributeRequesterInEntityGroup type in IdP attribute release policy. Advise IdP operators to re-evaluate the use of the basic:ANY type in attribute release policy.
   e. 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.
   f. Bring the beta metadata query server (mdq-beta.incommon.org) to production (mdq.incommon.org) as a distinct server environment (i.e., distinct from md.incommon.org).
   g. InCommon should tag all InCommon SPs and IdPs operating under the terms of the InCommon Participation Agreement with an entity attribute that specifies InCommon membership status.
   h. Consider introducing a new entity attribute that indicates whether or not an entity's metadata has been registered by InCommon but not vetted by the InCommon RA. (This addresses emerging use cases such as the Quilt use cases.) Recommended value: {{ http://id.incommon.org/category/organizational-valid-metadata}}
   i. We recommend a long-term goal of not maintaining separate metadata distributions for InCommon-only and InCommon + Interfederation Tag every entity descriptor in the production aggregate with a new entity attribute value (extended-validation-metadata). Resist the urge to create a new aggregate.

7. While outside of the scope of the new-entities workgroup, the group notes that the site changes/education needed to support eduGAIN in the InCommon metadata might also be an ideal time to push more on the idea of additional default attribute release, at least for entities from sites that have signed the InCommon Participation Agreement.

8. Provide IDPs with a cookbook describing how to configure and control attribute release in various scernarios (e.g., no release outside of InCommon, etc.