Recommendations

Introduction

As the globalization of federation continues to advance and the needs of our InCommon federation evolve, changes to the InCommon metadata will be needed. Historically, the InCommon metadata file contains, from a policy perspective, only one kind of entity—those under the control of a legal entity that has signed the InCommon Participation Agreement. On the other hand, interfederation will add metadata for entities registered under the policies and practices of other federations. Other sources will inject metadata for K–12 entities into the InCommon aggregate. A number of "new entity" use cases were analyzed and many options for remediating the impact of placing these new types of entities into InCommon metadata were discussed. We used the following questions to frame the analysis of each new use case:

1. How do we make it easy for existing InCommon participants to maintain current federation behavior as they work through campus policy issues?
2. What does an existing InCommon Identity Provider want or need to know about the new type of entity in the metadata?
3. What would an existing InCommon Service Provider want or need to know about the new type of entity in the metadata?

Using this framework, the New Entities WG developed the following set of recommendations.

Recommendations

1. The anticipated multiple sources of new entity metadata should not change metadata distribution practices. InCommon should continue to provide a single production metadata aggregate that contains both the existing and the new entities. The use of multiple metadata aggregates over the long run is not sustainable and runs counter to our goal of enabling interfederation and the use of the new types of entities that we place into the metadata. The remainder of these recommendations provide the technical and policy basis that enables a single aggregate to function.
2. InCommon should sufficiently annotate entity metadata so that IdP operators and SP owners can maintain current federation behavior in the short term and subsequently make informed policy decisions as needed.
    a. Every entity descriptor in metadata MUST have an `<mdrpi:RegistrationInfo>` element.
    b. The `mdrpi:RegistrationInfo/@registrationAuthority` XML attribute (which is required by the MD-RPI schema) takes on value "https://incommon.org" only if the entity metadata was registered in accordance with the InCommon Metadata Registration Practice Statement.
    c. InCommon should apply technical controls to ensure that the attribute value "https://incommon.org" is not accidentally imported from other metadata sources.
    d. InCommon should create a new entity category and automatically populate a new entity attribute having the precise semantics of the `mdrpi:RegistrationInfo/@registrationAuthority="https://incommon.org"` XML attribute.
    e. InCommon should create specific recommendations for deployers to address issues related to new types of entities in metadata.
3. InCommon should start to place metadata generated by the Quilt Initiative for K12 entities into the single InCommon aggregate subject to the following conditions:
    a. We use the "registrarID" entity attribute to convey both the name of the Registrar and the effective "RP/RPS" that the registrar used for this particular entity.
    b. If the entity is under the control of a legal organization that has signed the InCommon Participation Agreement and the entity has gone through the full InCommon registration process, the Registrar value will be set to: https://incommon.org. This will be true regardless of who performs the actual registration process work (i.e., InCommon staff or, for example, Quilt regional staff working under contract to InCommon).
    c. If the entity being entered into the metadata is under the control of legal organization that has not signed the InCommon Participation Agreement, the Registrar value will be different. The first such Quilt use case will be covered with a Registrar value that reflects the final outcome of the work of the InCommon/Quilt workgroup.
        i. If the Quilt/InCommon workgroup produces a single new RP/RPS and associated Quilt/InCommon Participation Agreement and InCommon assumes ownership of this process and subcontracts it to the regional, a Registrar value of https://steward.incommon.org will be used.
        ii. If the Quilt/InCommon workgroup produces a general framework but leaves the RP/RPS and equivalent entity Participation Agreement in the hands of each regional, then the Registrar value that will be used will be that of the regional - e.g., https://x.regional.net.
    d. The InCommon Participation Agreement requirement of 3.b and 3.c may be satisfied by either signing the full existing agreement or by signing a minimally modified version (as determined by InCommon legal) that contains all of the same requirements and protections as the main agreement but not providing direct membership in InCommon.
    e. We discussed other possibilities for the longer term involving attribute separation of the Registrar and the RP/RPS used in the process but are not bringing them forward here. See the Use Case Impact Section 1.d.iv.2 for more information and discussion on some longer-term possibilities.
    f. 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 and release this data** as part of the requirement for being included in the InCommon metadata aggregate.
4. InCommon should take no special action on proxy metadata entities beyond the constraints listed below for InCommon members
    a. Requests from InCommon members for proxy metadata entities are subject to the following constraints
        i. All entities/services behind the proxy are under the administrative control of the legal entity that has signed the InCommon participation agreement.
        ii. Members are advised that by aggregating too many services behind a proxy, they greatly complicate the formulation of IdP attribute release policies.
    b. eduGAIN and other metadata imported into the InCommon aggregate may contain proxy entities as long as the listed Registrar is not https://incommon.org.
5. InCommon should provide members with a mechanism to insert additional entity attributes into the metadata to support relationships with other entities and organizations within InCommon and other federations.
    a. Unverified Attributes - InCommon takes no action beyond incorporating the attribute into the entity's metadata. An example of an unverified attribute might be that the entity supports the EU Code of Conduct.
    b. Verified Attributes - InCommon takes appropriate actions as governed by an updated RPS to validate that the entity is allowed to assert the attribute before incorporating it into the metadata. An example of a verified attribute might be "UCTrust Approved" where only UC system members are allowed to assert the attribute.

    c. Our recommendation is that members are provided with a mechanism to add new attributes to their entities. This process could be governed via a (small) pre-approved list of attributes and some process for members to request that new attributes be added to the list.
    d. Note: there was not unanimous agreement that this issue is within the scope of this working group. However, since at least the example listed in 5.a is a direct result of a new-entities use case, the issue is documented here.
6. InCommon should plan to incorporate the metadata of other federations (via eduGAIN) into the InCommon production aggregate subject to the following conditions:
    a. Every entity descriptor imported from eduGAIN must satisfy the requirements outlined in #2 above.
    b. In particular, InCommon should apply technical controls to ensure that the value "https://incommon.org" is not accidentally imported from eduGAIN.
    c. InCommon should create specific recommendations for deployers to help prepare for eduGAIN metadata in the InCommon production aggregate.
    d. InCommon should publish configuration examples for Shibboleth2 and Shibboleth3 that show how to maintain current federation behavior.
    e. Sufficient time for adequate publicity, awareness, and campus implementation should be provided.
7. InCommon should allow any authorized Site Administrator to introduce metadata into the InCommon production aggregate subject to the following conditions:
    a. Every entity descriptor so introduced must satisfy the requirements outlined in #2 above.
    b. If the entity descriptor is submitted to the InCommon registrar for approval, and the metadata is subsequently approved by the registrar, the entity descriptor will be tagged with registrar ID "https://incommon.org" to indicate that the metadata was registered in full accordance with the InCommon Metadata Registration Practice Statement.
    c. If the entity descriptor is not submitted to the InCommon registrar or otherwise not approved by the InCommon registrar, the entity descriptor MAY be introduced into the InCommon production aggregate at the discretion of the Site Administrator and subject to the following conditions:
        i. The entity descriptor will be tagged with the registrar ID of the organization that submitted the metadata.
        ii. The entityID must be an absolute URL whose host part is rooted in a registered domain owned by the organization that submitted the metadata (as determined by the whois database).
8. Default attribute release policy
    a. While outside of the scope of the New Entities WG, the group notes that the changes, education, and outreach needed to support new entities (e.g., eduGAIN, Quilt, etc.) in 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.