Use Case Impact

Use Case Impact (This section retained to help explain/document how the final recommendations were developed)

1. **Quilt - InCommon Initiative to Extend Federation to K12 and Community Colleges**
    a. What does an InCommon SP need to know
        i. In real time, if individual in question is under age 13 (if collecting PII from user - see: http://www.coppa.org/comply.htm)
        ii. If the request is from an InCommon Member (entity *signed* the InCommon participation agreement) (Models 1, 2, 3)
        iii. In Model 4, the Full Service Steward Model", the InCommon member (the Steward) is required to pass the terns and conditions of the InCommon participation agreement on to its Represented Constituents. The Steward assumes liability for the actions of the entities listed in the metadata. A globally unique URI from the QUILT aggregator will be used as the registrar in the metadata. (Note: incommon.org is always asserted as the registrar in cases of an entity having full InCommon membership (participation agreement signed) e.g., Case ii).
        iv. Model 5, Full Federation Operator, is an interfederation issue and is not discussed here,
    b. What does an InCommon IdP need to know (What's the scenario here? Why would another IdP need to know anything? Are we talking about an SP run by an entity that is not a member - Model 4?)
        i. If the request is from an entity that is operating under the terms of the InCommon participation agreement - Models 1, 2, 3 (or 4 if it's the Steward)
    c. Additional Information
        i. The general question of student age and the different legal responsibilities that exist for different age groups is an issue, but not an issue for metadata and hence not the purview of this working group. This group recommends that IdPs serving the K-12 community that are placed into the InCommon metadata be required to use new, yet to be defined eduPerson / k12Person attribute(s), to describe the age classification of the end user.
        ii. Does the group recommend that InCommon SPs that serve the K-12 community, K-20, or the general public, be required to "consume" the above referred to attribute(s)?
    d. **2015-01-08 Discussion Summary - start here on our next call.**
        i. One of our goals is to make it easy (e.g., via a simple Shibboleth configuration) for relying parties to be able to emulate the existing InCommon metadata distribution. Fundamentally, this means transmitting knowledge if the metadata entity is operated by a legal organization that has signed the InCommon participation agreement and gone through the InCommon registration processes.
        ii. Carrying this concept forward, think of "has signed the InCommon participation agreement" as the existing proxy for what in the PKI world would be a CP/CPS. We call it here a InCommon Registration RP/RPS. While the overall RPS includes other steps, the key item that an InCommon relying party wants to know is if the legal organization that operates the entity in the metadata has signed the participation agreement.
        iii. There will be new RP/RPS cases in the InCommon metadata in the future. The first such case is a relatively rare Quilt use case where a school district is running their own IdP, the school district has elected not to execute the InCommon participation agreement, and the metadata for their entity is placed into the InCommon aggregate by a third party under contract to Internet2 (e.g., a regional network).
        iv. Proposal:
            1. Short Term (where *t* is some small integer - a year or two)
                a. We use the "registrarID" entity attribute to convey both the name of the registrar and the "RP/RPS" that the registrar used for this particular entity.
                b. If the entity is operated by a legal organization that has signed the InCommon Participation Agreement, the Registrar value will be: https://incommon.org. This will be true regardless of who performs the actual registration process work (i.e., InCommon staff or Quilt regional staff working under contract to InCommon). If the entity being placed in the metadata has gone through the full InCommon registration process (including signing the participation agreement) then the Registrar value used will always be https://incommon.org.
                c. If the entity being entered into the metadata is operated by a 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 workrgroup 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.
            2. Longer Term (where *t* is some larger integer, likely a few years from now)
                a. The registrar and policy/practices concepts would be split into two different variables
                b. The RegistrarID entity attribute would be the name of the entity that performed the registration work. A value of https://incommon.org ~~https\://example.org~~ would be used for entities that were directly registered by InCommon and for entities that are registered by third parties under contract to InCommon. We are not presently aware of entities that InCommon would add to the metadata that would not be listed with https://incommon.org
                ~~https\://example.org~~ as the RegistrarID.
                c. A new "RP/RPS" entity attribute would be added to the metadata to specify the policy/practices of the registration. Some initial known values would be terms such as: incommon-participant (has signed InCommon agreement RP/RPS) and steward-participant (some steward RP/RPS).
            3. We do need to consider transition issues in our discussion. Another topic might be if our threshold should be the number of different RP/PRS categories instead of time.
2. **IdP Proxy (proxying either IdPs or SPs) as a Metadata Entry**
    a. There is no fundamental problem with multiple services being offered behind a single entity-id in the InCommon metdata.
        i. InCommon policy should clearly state that such entities must be under the administrative control of the same legal entity. This *administrative control* includes vendor provisioned services that are under contract to the InCommon legal entity.
        ii. Note that a proxy SP registered in InCommon metadata is still subject to section 9 of the InCommon participation agreement. That is, the proxy is responsible for ensuring appropriate use of the data by all of the SPs that it proxies for.

iii. Advice to service providers should be documented to advise against the over-aggregation of services as it will make it less likely that IdPs will releae attributes to overly aggregated SPs

b. What does an InCommon SP need to know
   i. No metadata changes needed
c. What does an InCommon IdP need to know
   i. No metadata changes needed
d. Additional Information
   i. IdP proxies that cache might be problematic as they might not accurately mirror the source IdPs attribute release policies.
   ii. The committee suggests that, for now, InCommon policy clearly state IdP Proxies and their "proxied IdPs" must all be under the control of the same legal entity.
   iii. Add an exemption for Use Case #1 above
   iv. InCommon is currently not capable of dealing with a single entity-id that is used for both an IdP and SP. This committee does not, at least at this time, recommend that this capability be added to InCommon's infrastructure. We do not know why anyone would need this capability even though we see some of this type of entity in the eduGAIN metadata.

3. **EU IDP accessing SP at Brown**
   a. What does an InCommon SP need to know
      i. No metadata changes needed
   b. What does an EU IdP need to know
      i. Which attributes are required/optional for this SP
      ii. That the SP will only use the asserted attributes in a manner compatible with the Code of Conduct.
   c. Additional Information
      i. This need to assert that an InCommon SP follows the EU Privacy Directive could also be considered as an interfederation issue.
      ii. Group: do we recommend that InCommon members be given a way to self-assert a fixed set of attributes about their SPs in the InCommon metadata? (The proposal described in the "MARI plan and next steps" may simplify how this set of attributes is expressed.)
      iii. Steve Carmody took an action item on this topic – expectation by end of February
      iv. See also Section 4.c

4. **Course with US-based and EU-based students, LMS is commercial and based in the US**
   a. What does an InCommon SP need to know
   b. What does an EU IdP need to know
      i. Which attributes are required/optional for this SP
      ii. That the SP will only use the asserted attributes in a manner compatible with the Code of Conduct.
   c. Additional Information
      i. While perhaps slightly out of scope but certainly interrelated, one of the main questions with #3 and #4 is if InCommon is willing and able to support a set of self-asserted entity attributes such as EU Code of Conduct. The import of eduGAIN metadata will be less useful if InCommon entities are not able to populate metadata with needed attributes.

5. **eduGAIN Metadata (jaj to consolidate around just the registrar tag as an entity attribute)**
   a. What does an InCommon SP need to know
      i. Some SPs might require the ability to act differently depending on the source of the metadata.
      ii. Importing IdPs into InCommon metadata will alter discovery interfaces across the Federation. Some SPs will want to filter such IdPs from their discovery interfaces.
   b. What does an InCommon IdP need to know
      i. Some IdPs might require the ability to act differently depending on the source of the metadata.
      ii. Some InCommon IdPs will require the ability to craft their attribute release policy based on if the SP is operating under the terms of the InCommon Participation Agreement or not.
         1. What is it about the InCommon Participation Agreement that IdPs are focused on, do we know?
      iii. Many IdPs will require the ability to act differently depending on if the SP is a member of the R&S Category or not.
         1. The InCommon R&S category or the REFEDS R&S category?
      iv. Some IdPs will require the ability to act differently based on multiple SP characteristics (e.g., an R&S SP that is operating under the terms of the InCommon Participation Agreement).
      v. Importing SPs into InCommon metadata will cause some IdPs to automatically release attributes to those SPs. This may or may not be what those IdPs intended. We need to give IdPs a way to restrict attribute release, at least until they've had a chance to broach the subject with local data stewards.
      vi. When SPs are imported into the production aggregate, an IdP that releases attributes to *any SP* is affected:
      `<PolicyRequirementRule xsi:type="basic:ANY"/>`
      Likewise an IdP that releases attributes based on the *Name XML attribute* in metadata is affected:
      `<PolicyRequirementRule xsi:type="saml:AttributeRequesterInEntityGroup" groupID="urn:mace:incommon"/>`
      IdPs need a way to mitigate these effects.
   c. Additional Information (chronological order)
      i. *Discussion Recommendation*: Tag every entity descriptor in the InCommon aggregate with a new entity attribute value (TBD). Resist the urge to create a new aggregate.
      ii. *Discussion Recommendation*: Import eduGAIN metadata directly into the production aggregate. Begin by importing IdP metadata from eduGAIN since the impact on InCommon SPs is less than what it will be for InCommon IdPs.
      iii. *Discussion Recommendation*: 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.
      iv. *Discussion Recommendation*: Consider the `<mdrpi:RegistrationInfo>` element as a direct source of attribute release policy. Avoid exposing the `registrationAuthority` XML attribute value as an entity attribute.
      v. *Discussion Recommendation*: 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). **Is this out of scope?**
      vi. *Discussion Recommendation*: 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. **Is this necessary? All entities in InCommon metadata were submitted by orgs that have signed the InCommon PA.**
      vii. Should we recommend that InCommon maintain separate metadata distributions for InCommon-only and InCommon + Interfederation
         1. (No, otherwise we force deployments away from production metadata. See: Importing eduGAIN Metadata)

d. Plan Discussion - as of 20141218
    i. InCommonOrgPolicy - the only current known value will be "this entity is under the control of an organization that has signed the InCommon Member Agreement" **What is "InCommonOrgPolicy" and what is meant by "under the control of"?** We will add a new metadata entity attribute that states that the entity is an InCommon member with a signed InCommon participation agreement in place. **Is this necessary?**
    ii. RegistrationAuthority - Values: InCommon, eduGAIN, etc.; See 5.c.4 for how this eduGAIN requirement works Following the eduGAIN requirements for a Registrar entity-attribute solves some other use case issues.
    iii. With (i) and (ii) above, we recommend a single production metadata aggregate
    iv. Question: 5.d.i and 5.d.ii are redundant if we will never have a second defined value for 5.d.i. Which use cases drive this? Will it always be the case that InCommon will only add an entity to the metadata when it is certified that the entity is under the **direct control of** an organization that has signed the InCommon participation agreement? **What is meant by "under the direct control of"?**
    v. Transition plan: next topic
    vi. Question: any discussion / recommendation for InCommon filtering of eduGAIN data (proxies, etc.)?
e. Final Discussion
    i. As part of our revisited discussion on the Quilt use cases, we determined that a single entity attribute listing the registrar could be overloaded to meet the eduGain use case needs as long as we imposed a strict definition that a value of incommon.org means that the entity is under the control of a legal organization that has signed the incommon participation agreement. Since this requirement is part of the existing registration practices, it should impose no additional burden.

6. **LIGO as an International Virtual Organization** (what does LIGO have to do with new entities in metadata?)
    a. What does an InCommon SP need to know
        i. No metadata changes are needed
    b. What does an InCommon IdP need to know
        i. No metadata changes are needed
    c. Additional Information
        i. LIGO would benefit from a larger percentage of IdPs supporting R&S
        ii. LIGO would benefit if more IdPs were to change their default attribute release policy to release EPPN even if they don't support R&S.
            1. (No, LIGO filters all but R&S IdPs, so LIGO would **not** benefit from this)
        iii. LIGO would benefit from the migration to a single R&S category (instead of the separate InCommon and REFEDs work).
            1. (I don't see how this matters)
        iv. LIGO would benefit from more accurate metadata. Existing metadata contains too much incorrect data, often issues in the area of support for ECP and Artifact Resolution. This may become more prevalent as the size of the metadata aggregate expands.
            1. (*Everyone* would benefit from more accurate metadata)
        v. LIGO *might* benefit if we tested and tagged interoperable IdPs
            1. (LIGO would first have to be persuaded to consume all InCommon metadata)

7. **Campus metadata in InCommon Metadata**
    a. Should there be a difference in the registration authority metadata for entities where the campus entered volumes of local metadata (e.g., the CMU case)?
        i. *Recommendation*: 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. Recommended value: {{ http://id.incommon.org/category /organizational-valid-metadata}}
        ii. Recommendation (updated 20150212) no new entity attribute, use registrar field. .local not allowed (registrar must be full campus name: e.g., urn:mace:incommon:cmu.edu). Still being discussed if this enables a single aggregate or not.