

InCommon TAC Meeting 2016-03-17

Attending: Tom Barton, Mark Scheible, Kim Milford, Keith Hazelton, Janemarie Duh, Michael Gettes, Walter Hoehn, Steven Carmody,, Jim Jokl, Albert Wu, Tom Mitchell

With: Nick Roy, Dean Woodbeck, Ann West, David Walker, Tom Scavo, IJ Kim, Mike LaHaye, Paul Caskey, Kevin Morooney, Ian Young

Minutes from March 3

Approved

Limitations of InCommon Metadata

At least three items have been identified as limitations of InCommon Metadata that impact IdP operators. Changes to the Federation Manager could eliminate these limitations:

1. Improved support for encryption keys in SP metadata (currently, an encryption key is required)
2. Support for the md:NameIDFormat element in SP metadata (currently, there is no support for this attribute)
3. Support for md:SPSSODescriptor/@WantAssertionsSigned XML attribute in SP metadata (currently, there is no support for this attribute)

(AI) InCommon Operations will look at changing the software to support these items. TAC members should express any objections over the next week, or this will be considered approved by the TAC. The new Operations Advisory Group may be asked to review and comment.

Per-Entity Metadata Proof of Concept

Some IdP operators are interested in testing the per-entity metadata service (via the metadata-support email list). Tom Scavo has drafted a note to see if others are interested (<https://spaces.at.internet2.edu/display/InCCollaborate/Call+for+Participation+March+2016>)

(AI) Nick will develop a charge/outline for continuing this discussion, involving the Operations Advisory Group, with the focus on addressing what needs to be done to move this to production (and potentially other ways of solving the problem of the aggregate size).

(AI) Tom Scavo will change references to per-entity metadata from "pilot" to "proof of concept."

Interfederation Technical Policy Update

The UK federation help desk has filtered three InCommon SPs out of their metadata because the entities do not have https: protected endpoints (we don't have a policy to prevent that). (AI) Tom S will share the identity of the three SPs via email to TAC. He will also contact the SPs about this and report back at the next meeting.

InCommon Ops suggests adding the following policy rules:

1. Filter all imported entities (IdP and SP) with non-conforming entityIDs, implementing a whitelist of prefixes: "http://", "https://", "urn:mace" (there is one such entity in eduGAIN metadata)
2. Filter all imported IdP entities with an endpoint location that is not HTTPS-protected (there are 11 such IdPs in eduGAIN metadata - none from InCommon)
3. Filter all imported entities (IdP and SP) with a Logo URL that is not HTTPS-protected (there are 11 such IdPs and 3 such SPs in eduGAIN metadata)

Consider the following policy rules:

1. Filter all exported SP entities with an endpoint location that is not HTTPS-protected.
 - a. Not all InCommon SPs have HTTPS-protected endpoint locations in metadata
 - b. Currently 3 SPs with non-HTTPS-protected endpoint locations are exported to eduGAIN
2. Filter all imported SP entities with an endpoint location that is not HTTPS-protected.
 - a. There are 4 such SPs in eduGAIN metadata

The REFEDS MET tool can help uncover the filtered entities. (AI) Nick will write a blog about this tool to make it more widely known.

TAC 2016 Work Items

<https://docs.google.com/document/d/1uf7ZCTP-3brWqEldTZ9P2o5p0BSstAYbjov8S0ub7GA/edit#heading=h.g0jvd3ujm8b0>

InCommon has a set of 2016 goals, which need to be vetted by the Internet2 board before becoming public. Staff are still working to prioritize these. Two items high on the list are moving to a ticketing system (vs. the current email alias as the help mechanism), and prioritizing items from the ops review. Ann said that all of the items on the TAC document are on the list of goals - the question will be one of priority.

(AI) Ann/Kevin will review the TAC document to determine if there are any glaring omissions. (AI) TAC will review the list with an eye toward what can likely be accomplished (probably by working groups) in 2016.

Next Meeting - Thursday, March 31 - 1 pm ET