InCommon TAC Meeting 2018-03-01

InCommon Technical Advisory Committee Meeting - March 1, 2018

Action Items from Past Meetings

- AI: Mark, Janemarie, Nick to distill salient points from 2018-02-01 TAC discussion into suggestions for new TAC charter and share with group and share with TAC mailing list

Minutes

Attending: Janemarie Duh, Eric Goodman, Eric Kool-Brown, Keith Wessel, Mike Grady

With: Ian Young, David Walker, Nick Roy, Kevin Morooney, Dean Woodbeck, Brett Bieber (Guest), Shannon Roddy, Ann West, Dave Shafer

Janemarie chaired today's call.

All Internet2 activities are governed by the [Internet2 Intellectual Property Framework](#)

Ops Update

Discontinuation of legacy metadata download endpoint - The last good copy of MD from that endpoint went bad on Feb. 27, 2018 at 2:44 pm ET. There are 146 distinct host names still retrieving from that. We have only had a couple of emails concerning this. Many of these may be systems no longer in use, or very lightly used.

Upgrade of MDA rules to InCommon-v8 delayed to March 7 - Partly because of the timing of discontinuing the legacy metadata download endpoint, and also some other activities in Ann Arbor, this was delayed for a week.

Test security incident across eduGAIN last week

Security advisory from the Shibboleth Consortium was received this week. Shannon Roddy developed additional information and shared that with the participants list and the inc-ops-notifications list. Nick, Shannon, and Kim Milford have discussed using REN-ISAC as an anonymized location for SP status. Kim is taking this to REN-ISAC leadership.

There was clarification today that simpleSAML.php is affected by a bug, but it is a different bug than the Shibboleth issue.

Trust and Identity Updates

Ann shared the trust/identity project portfolio as an update.

This will be a standing agenda item for TAC.

Working Group Updates

Streaming SP Onboarding - no report

OIDC - no report

Deployment Profile - hoping to release a report in the next couple of weeks

Attribute Release - no report

Baseline Expectations

Brett Bieber, chair of Community Trust and Assurance Board (CTAB), joined to provide an overview of Baseline and lead a discussion with TAC.

Last year was spent developing:

- How will we maintain Baseline Expectations?
- What are the legal changes needed?

CTAB succeeded the AAC and has a new charter. The membership has changed and doubled.

Metadata Health Checks

- First was sent in mid-February
- Over three days after the health checks went out, InCommon saw 150 changes in metadata, so we are making some progress
- The plan is to send these monthly

Brett shared a pie chart that shows the percentage of IdPs and SPs meeting Baseline Expectations overall. blocked URL

SPs meeting BE went from 312 to 458 after the first health check. But that is still only 10 percent. This demonstrates how broken the user experience can be.

Another major change Baseline provides a way to alter metadata or remove an entity from the federation. Also eventually these elements will be required when someone enters metadata in the FM.

CTAB is planning additional communications to support BE. Areas include CTAB members looking at providing support materials for MDUI information, privacy policy, and working through the community consensus process. Hope to have more webinars around these issues.

CTAB will be receiving the dispute information and will need to work as a moderator for these disputes and to try to help resolve things. Part of this is understanding the scope of what the CTAB will face. Would use a couple of examples that CTAB could use to walk through the community consensus process and dispute resolution. One of the issues for arriving at consensus, there is a process that will prevent one loud voice from taking over the conversation.

- One example is response (or non-response) to security issues
- Another - what if the federating software doesn't support encryption?

Are there services/tools that the federation can provide to help improve the user experience? For example, discovery packages, default packaging /configuration of software. Nick - there is a requirement of the federation operator to encourage use of things like entity categories. There is no corresponding requirement among IdPs and SPs. Should R&S become part of Baseline? Once Baseline is part of the PA, it may help alleviate fears of IdPs for releasing attributes (because there would be consequences if the SP doesn't abide by the agreement for use and protection of information).

Next iteration of Baseline will include an error URL, which will also help the user experience.

Would like to move to a portal page that draws information out of the metadata.

There is a significant amount of work to be done. The roadmap shows the work that will need to be done by Steering, CTAB, InCommon staff, participants, and others.

Assurance program - This is another topic the CTAB will tackle over the next year. What do we do with this program? If we no longer offer the program, what will happen to current Bronze and Silver participants.

Question - Should we plan periodic shared calls with the TAC and CTAB? This was excellent discussion and interaction today.

Next Meeting - Thursday, March 15 - 1 pm ET