

# InCommon TAC Meeting 2017-03-02

## Als From 2017-02-16 call

- (AI) Mark Scheible will add TIER packaging update (JimJ) to the top of the Information Items for the next meeting
- (AI) For the next TAC meeting, there will be a proposal about whether to have an open TAC discussion email list
- (AI) Dean to add information to the TAC public wiki: list of meeting dates and a way to contact TAC
- (AI) TAC - review and comment on the 2017 TAC work plan
- (AI) Mark S - Add a column to the work plan that reflects where the work should happen (e.g. REFEDS, TAC, Ops, etc)

## Minutes

**TAC Members Attending:** Mark Scheible, Eric Goodman, Janemarie Duh, Tom Mitchell, Albert Wu, Mike Grady, Walter Hoehn, Jim Jokl, Tom Barton, Chris Misra, Steve Carmody

**Others Attending:** David Walker, Ian Young, Dean Woodbeck, Kevin Morooney, Ann West, Tom Scavo, IJ Kim, Paul Caskey

## Action Items

- (AI) TAC members are asked to review the document regarding TIER and potential changes to Shibboleth and see if there is anything that should be added.
- (AI) Mark Scheible will send email to the TAC list with a reminder that the deadline for commenting on the 2017 TAC Work Plan is March 8.
- (AI) Dean Woodbeck will ping Mark Scheible about scheduling a webinar to present the TAC work plan.
- (AI) Mark Scheible will set up a discussion about potential TAC/community email list(s) via the TAC email list.
- (AI) Tom Scavo will report back on discussion about InCommon relaxing ownership of IdP domains.
- (AI) Tom Scavo will introduce the topic of requiring HTTPS-protected protocol endpoints on the TAC email list, including whether this should be an eduGAIN-wide discussion.
- (AI) Nick Roy and Tom Barton will send their meeting summaries to the TAC list and answer questions on the next call.
- (AI) David Walker will follow up with the OIDC Survey working group regarding a community review of their report and the possibility of scheduling a webinar.

## TIER Packaging

Jim Jokl reviewed the TIER packaging strategy of entity-attribute-based IdP configuration to greatly reduce the volume of XML file edits needed to bring new SPs online. Main points:

- There have been calls in the past for a UI for Shibboleth that would reduce the need to edit XML. The TIER packaging group is looking initially at a UI that would control filter configurations. This would also require a reworking of the Shibboleth backend files so the software will respond in the right way. See this very rough UI mock up for a sense of the group's direction. The goal is to have a demo on this at the Global Summit.
- The UI would be part of the build within the Docker container.
- This mechanism would also enable the production/creation/maintenance of a repository of Shibboleth settings for many different relying parties. What are the interactions with InCommon's work? Should such a repository, if created, be maintained by InCommon, TIER, user/community?
- These are JSON files.
- The TIER distribution of Shibboleth would have these changes built in.
- This tool will manage attribute release. The tool does not handle changes from the default initial configuration. TIER is pursuing other options to ease the initial configuration workload.

An extensive community survey conducted last year, along with follow-up working group discussions, have resulted in a list of desired Shibboleth configurations and software changes. Please note that none of this is final and is under consideration. (AI) TAC members are asked to review this document and see if there is anything that should be added.

## Ops Update

<https://spaces.at.internet2.edu/x/aoGTBg>

- Sent message to inc-ops-notifications concerning the Cloudbled incident
- The ops advisory group has recommended that InCommon relax its requirements regarding ownership of domains that appear in IdP metadata. This is under discussion internally. (AI) Tom Scavo will report the result of these discussions back to TAC. It could be that this will carry over to SP endpoints as well.
- There have been discussions about requiring HTTPS-protected protocol endpoints. (AI) Tom Scavo will introduce this topic on the TAC email list. Tom Barton recommended considering whether this topic should be approached eduGAIN-wide, rather than just in the U.S.
- InCommon is now producing signed per-entity metadata on a daily basis (thanks to a new version of the MD aggregator tool from Ian and thanks to IJ for installing). There remains testing to be done before this will be available publicly

## Trust and Identity Updates

- So far we have 9 nominees for CACTI. We continue to encourage community members to send nominations (including self nominations). Nominations close March 9.
- Trust and Identity has published the 2016 Trust and Identity Accomplishments report: [www.incommon.org/docs/2016TIRReport](http://www.incommon.org/docs/2016TIRReport)
- **Marketing/segmentation project** - The consultant, Mike Norris, provided an extensive report two weeks ago. There is a meeting with him March 3 to review a number of questions. Once the outcomes and recommendations are clarified, staff will develop a presentation for TAC, Steering and others. Kevin expects this to be the main topic for the Steering/TCIC meeting at the Global Summit.

## Transparency/Community Involvement

Mark summarized discussions regarding the possibility of opening TAC meetings and/or opening the TAC email list. After consideration, TAC determined that open meetings would likely make it harder to get through the agenda. The same is true with the email list.

The recommendation is to develop one or more separate email lists (possibly by topic) to fill the need for community discussion. (AI) Mark Scheible will set up this discussion via email.

## TAC Work Plan

The goal is to make this work plan public soon for community review. (AI) TAC members should review the work plan by COB Wednesday, March 8, and also sign up as a TAC champion or sponsor for area(s) in which they are interested. (AI) Mark Scheible will send a note to the email list. There was also discussion about a webinar concerning the work plan. (AI) Dean ping Mark about scheduling.

## OIDC/OAuth Survey WG

Albert Wu discussed the working group report, which includes the results of the survey. He reported that there is already considerable activity for deploying OIDC and OAuth support. These broad categories emerged:

- Managing security for APIs
- Native mobile app development and connections to APIs
- Leveraging social identities to access campus resources and the reverse (using campus SSO to access services wanting socialIDs)

The working group recommends that Internet2 should build OIDC and OAuth (in addition to SAML) into TIER

About half of the respondents want to see InCommon develop OIDC/OAuth federation standards and practices.

The discussion made these points:

- In terms of including this with TIER and/or InCommon developing OIDC/OAuth federation standards, it will not work without sufficient funding and support.
- Campuses are already building proxies to turn a SAML assertion into OAuth (or vice versa).
- The development of federation standards and practices) will take longer.

The working group will meet March 3 and discuss starting community review of this report, in order to have it completed by Global Summit. (AI) David Walker will follow up with the working group on this and also whether to schedule a webinar.

## TIIME Meeting

(AI) Nick Roy and Tom Barton will send their meeting summaries to the TAC list and answer questions on the next call.

Next Meeting - Thursday, March 16 - 1 pm ET