

2018-06-04

InCommon Steering Committee Minutes - June 4, 2018

Attending: Melissa Woo, Michael Gettes, Sean Reynolds, Mark Scheible, Brett Bieber, Von Welch, Ann West, Celeste Schwartz, Klara Jelinkova, Pankaj Shah, Ted Hanss, Laura Paglione, Mike Erickson, Marty Ringle, Dave Vernon, Dee Childs

With: Kevin Morooney, Dean Woodbeck, Steve Zoppi, Tom Barton

TAC Charter Revision

Mark Scheible, chair of the InCommon Technical Advisory Committee (TAC), discussed the proposed revised TAC charter, which was distributed in advance of the meeting. Mark reviewed the reasons for the changes

- The first TAC charter was adopted in 2015. This was pre-eduGAIN, and TAC was much more focused on federation in the U.S. TAC was made up mainly of campus IdP operators to provide technical support for InCommon operations. Since then, an Operations Advisory Group formed to do the latter.
- Additional Internet2 staff have been hired, also reducing the need for TAC operational support
- The changes better reflect the broader focus and make-up of the TAC



Vote on TAC Charter Revision

It was moved, seconded and unanimously approved to accept the revised charter.

Baseline Expectations Update

Brett Bieber, chair of the InCommon Community Trust and Assurance Board (CTAB) provided an update on the Baseline Expectations program. The changes to the InCommon Participation Agreement go into effect on June 15. CTAB and InCommon staff view that date as a continuation of the education outreach process, not the flipping of a switch.

Ann West has drafted a transition plan, which CTAB will review and comment on, detailing how InCommon operations and the community will continue efforts to help participants meet the Baseline. The monthly health checks, started in February 2018, have had a large impact, with those meeting all expectations at about 46% (identity providers) and 36% (service providers). The goal is to reach 90-95%.

InCommon is hiring two contractors, both well known in the community, who will talk to participants that are not in conformance to uncover the main roadblocks. The results will inform the plan for the next few months.

Brett noted that a special newsletter went out last week with CTAB guidance on logos and privacy policies, which seem to be the largest issues among the community at this time, as well as information about the progress made by the health checks. This graph is tracking the progress made by the metadata health checks. In addition, the Federation Manager now includes warnings if there are items that do not meet Baseline Expectations. At some point, this will move to being required. The timing will be based on progress that is made in the community. Brett emphasized that, once we reach that point, we will work with those who have developed action plans to meet Baseline. For those that don't, we will begin the process of removing them from the federation.

Kevin mentioned that we are starting an effort to add InCommon CIOs to the Internet2 Salesforce database. When InCommon started, it was expected that the InCommon Exec role would be filled by CIOs, but that has become less so over time. This will help as we target critical communications to campuses.

Federation Software Ecosystem Dynamics

At the Global Summit, Steering briefly heard about the dynamics of the software ecosystem that supports federation. This will become a priority item for the next couple of Steering meetings, since the TIER investment is ending in 2018, but the community wants continued progress on software development. The big question for Steering will be to help figure out how to pay for that (and some other things, like Shibboleth support for participants). Klara suggested a half-day meeting at TechEx. Kevin also mentioned that it might be helpful to create a task force that would take a deep dive into the issues and develop some potential recommendations.

Globus and ePPN

Tom Barton joined the call to discuss an issue raised by Globus (which was developed at the University of Chicago) concerning the eduPersonPrincipalName (ePPN) specification. Steve Tuecke of Globus had emailed that the spec could allow an identity provider to use a particular user@domain string as the ePPN for one person, but that same string as the email address for another person, which he feels is a potential security threat. This affects the Globus Online service, which is a cloud-based service aimed at small- and medium-sized organizations.

The concern was raised with MACE-DIR, the group with responsibility for the eduPerson specifications. Rather than fix the ePPN spec, that group took the approach of proposing changes to the SAML profile, which is a more time-consuming international process.

While this is a problem with the eduPerson spec, operationally it is highly unlikely to happen. An organization using, say, tbarton@uchicago.edu for Tom Barton's ePPN, but Timothy Barton's email, would cause major operational problems for the organization (like issuing paychecks). So Tom feels that the risk is actually negligible, but it's still a spec bug that should be fixed.

There was concern expressed by Steering members that Globus may be thinking of disengaging from federated identity management. Tom does not believe that to be the case, and will have a conversation with Steve Tuecke to determine the depth of his concern.

Next Meeting: Monday, July 2, 2018 - 4 pm ET