

# InCommon TAC Meeting 2022-05-05

## Minutes

### Attending

Judith Bush, Heather Flanagan, Keith Wessel, Joanne Boomer, Matthew Economou, Steven Premeau, Matt Porter

**With (Also Starring):** Nicole Roy, Kevin Morooney, IJ Kim, Johnny Lasker, David Bantz, David Walker, Les LaCroix, Steve Zoppi

**Regrets:** Mark Rank

### Notes

<https://spaces.at.internet2.edu/pages/viewpage.action?spaceKey=inctac&title=TAC+Meeting+2022-05-05>

1. **Intellectual Property Reminder** - All Internet2 activities are governed by the [Internet2 Intellectual Property Framework](#).
2. **Public Content Notice** - TAC minutes are public documents. Please let the TAC and note taker know if you plan to discuss something of a sensitive nature.
3. **Call for scribe volunteers ( 2 per call) - recording / transcription available**
4. **Agenda Bash + request for notable working and advisory group updates**
5. **Status Updates - Q&A** (10 minutes)
  - a. Trust & Identity
    - Remember to submit CAMP proposals.
    - Internet2 is running a leadership academy.
  - b. Wallets working group
    - Concern with the level of community engagement for the Wallets and Federation workgroup
    - It's an important topic but not yet urgent.
    - Needs more engagement to be successful
    - How much does TAC want to help drive this process (vs. just being informed/aware that it's an issue)
    - Keith notes that he's still a little unclear on the scope of the workgroup, and if that's a common issue that may be driving the lack of engagement.
    - At IIW, it was discussed that the term "Wallet" is overloaded which may further drive confusion.
    - CACTI is also considering this general issue. That may help define InCommon's investment in this work.
    - One of the general issues is typically the trust model (more so than the technology of the underlying technologies).
    - One approach is to let CACTI figure it out (and not address it in TAC)
    - 5/6/2022 (tomorrow at the time of the TAC meeting) is the InCommon Quarterly workgroup leaders meeting, so maybe this can be added to that meeting to discuss how to move forward.
    - We also need a real and concrete way for people to hold on to responsibility for this process. Again discussed potentially focusing on the trust model.
    - Maybe the first step isn't establishing a workgroup, but more an IAM online to outline the issue and try to stimulate a discussion among the community.
    - Heather has cooler travel plans than the rest of us. Auf wiedersehen!
6. (30 min) Updates from Deployment Profile Rollout Group
  - Have a starting point for a value statement.
  - [https://docs.google.com/document/d/1HnCMY-2\\_JZy8myR2np8CmPTpJrhjPnRT88j-3n0L\\_Y/edit#heading=h.px3fed6f6ap6](https://docs.google.com/document/d/1HnCMY-2_JZy8myR2np8CmPTpJrhjPnRT88j-3n0L_Y/edit#heading=h.px3fed6f6ap6)
  - Discussion: What kinds of things should be included in the overall value statements.
    - Covers a lot of "if we knew earlier what the issues would be we would have addressed them this way" kinds of information.
    - E.g., privacy is generally more an IdP concern, and the new identifiers address this reasonably.
    - SPs care about consistent Identifiers. Major impetus for a lot of design is the fact that there is frequently not an available and consistent identifier. (Converse is SPs requiring special IDs)
    - Configuration via metadata addresses scaling (of trust, largely).
    - IdPaaS could make all of the deployment profile details less directly relevant to (much of) the community. E.g., if you can set up a Cirrus-oid solution and we are working with those solution providers, then the customers don't necessarily need to focus on the implementation details that support the deployment profile (because the solutions all support them "natively").
    - Mostly "federation" is not used, but the metadata requirements (configuring peer connectivity solely through metadata and validating the metadata via signature or TLS cert) are specifically there to support the underlying trust capabilities that a federation supports.
    - Mark: Should not dwell on the hurdles, should focus on the value and positive aspects. What's in it for me?
    - ME: Likes the problem statement. If the intent is to keep it short and sweet, it's really a nice approach.
    - It does talk about both the IdP/SP issues at a high level. Are there any things to call out that are specific to either that should be called out?
    - NR: The user should never see an error message, but rather something useful/informative
    - The value of the federation is supposed to be that "the plumbing is just there". There's extra effort, but the deployment profile is fitting services into that plumbing. I.e., allowing deployment of newer services to be more straightforward.
    - If you have people at your institution that need access to scholarly materials/research needs, this work is worth the up front investment
    - Call to a sense of community.
    - DB: Nicole's framing of effort/benefit is important and applies more broadly that research and scholarship needs are emphasized; same work can also benefit other service integrations that are the bulk of work "below" R1. We don't want to position this as a niche for those in top tier only.
    - Would be good to pick and choose some specific scenarios to add to illustrate specific value.

- How do we make this more compelling, especially for leadership? (Agreement that it's a hard question, but no clear suggestions.)
  - This all hooks into IdPaaS.
  - Discussion of how well federation is supported in the profile.
7. (remainder) Open floor discussion - agenda
- Ran out of time

## Email Updates

### International, SeamlessAccess, Browser, Wallet updates

Subject: International, SeamlessAccess, Browser, Wallet updates - 5 May 2022

From: Heather Flanagan

Date: Wednesday, May 4, 2022

#### International Update

##### REFEDS

- One consultation is currently open: eduPersonDisplayPronoun. The consultation is open until May 25. More information can be found on the consultations page: <https://wiki.refeds.org/display/CON>
- The next REFEDS Community Chat is scheduled for Thursday, 19 May and will focus on REFEDS' managed schemas. This is likely the last community chat until September.
- The most active working groups in REFEDS right now are the Sirtfi, Assurance, R&S 2.0, and Federation 2.0 working groups.

#### SeamlessAccess

The WAYF Entry Disambiguation Working Group is sending out its recommendations document to the SeamlessAccess Advisory and Outreach committees for feedback before publishing it on their website.

The product roadmap is always available to the public: <https://seamlessaccess.org/services/>

#### Browser Interactions

Several active members of the Federated Identity Community Group met at IIW last week in person for the first time. That helped move several conversations forward, including discussions around the limitations of backchannel logout and Shared Signals and Events. Google will be hosting its browser-focused conference called Blinkon on May 18 and 19; they need more identity people to attend and participate, much in the same way that identity conferences need more browser developer representation. If you're interested, it is online and registration is free: <https://hopin.com/events/blinkon-16/registration>

#### Wallets and Federation

A notice went out to InCommon participants; only one organization has responded. TAC and CACTI need to consider how we want to move this forward given the Important-but-not-Urgent nature of the topic.

## Federation 2.0 update

Subject: Fed 2.0 report

From: Judith Bush

Date: Thursday, May 5

The REFEDS steering has not found consensus on the latest version of the Fed2.0 report: <https://wiki.refeds.org/download/attachments/44958215/Federation2Report.pdf?version=1&modificationDate=1651162971694&api=v2>

The working group has decided to continue the process by taking the offer of a 45 min session in the June REFEDS meeting in Trieste to present the challenges facing how federations work together to create a global service and discuss the recommendations, before kicking off another consultation period. We plan for the TAC to discuss this report and how the TAC will continue to engage with the strategic direction questions in our May 19th meeting. Alternative ways to engage with strategic direction might be through EduGAIN Futures (<https://wiki.geant.org/display/eduGAIN/eduGAIN+Futures+Working+Group+Charter>)

## CACTI update

Subject: CACTI update (4/12 & 4/26 meetings combined)

From: Steven Premeau  
Date: Thursday, May 5, 2022

- Query on the status of the Subject Identifier sub-group (Les & my reply: "should be starting soon")
- Mention that several NIST standard draft revisions will be out for public comment sometime this year
  - 800-63 rev 4, 800-217, 800-157 rev 1
- Discussion around the Digital Credentials for Europe (DC4EU) consortium (<https://dc4eu.eu>).
- Continued discussion of CACTI Themes

Steve.

H3. Federation testing WG update

Subject: Federation testing WG update

From: Matthew X. Economou

The federation testing working group reviewed the SAML 2.0 Deployment Profile and created a framework to define unit tests from the perspective of a federation operator (compliance), vendor (interoperability), or deployer (correctness). An analysis of certain SAML 2.0 interactions lead to the conclusion that not all behaviors or failure modes have machine-readable test results, so a SAML conformance test suite similar to the Qualys SSL Labs may not be possible in all cases (or may require out-of-band analysis by the testee and self-reporting of the results).

Current action items include a draft of an SP test suite (so whether it handles different IdP behaviors correctly).

## CTAB update

Subject: CTAB update 5/5/2022

From: Eric Goodman  
Date: Thursday, May 5, 2022

Most of the last meeting was focused on the continued development of the workplan and the details of the items therein.

The meat of the discussion was around how to make "Baseline Expectations" an ongoing process rather than a once every X year event. E.g., how to we help organizations stay in line/on track with Baseline Expectations in general? How do we detect when people are out of compliance and help when there hasn't just been a revision to BE, etc.? Also discussion of the role of the CTAB vs. the role of uncommon staff in supporting these efforts.

Both the REFEDS MFA subgroup and the SIRTfI exercise working group are expecting outputs in the near future. REFEDS MFA expecting to send a draft to the REFEDS Assurance group soon, SIRTfI group is planning their first exercise later this month.