# 2022-Sept-6 CTAB Public Minutes

## CTAB Minutes for Sept. 6, 2022

**Attending**

- David Bantz, University of Alaska (chair)
- Jon Miner, University of Wisc - Madison (co-chair)
- Pål Axelsson, SUNET
- Richard Frovarp,  North Dakota State
- Mike Grady, Liaison from CACTI to CTAB
- Eric Goodman, UCOP - InCommon TAC Representative to CTAB
- Andy Morgan, Oregon State University
- Rick Wagner, UCSD
- Robert Zybeck, Portland Community College
- Johnny Lasker, Internet2
- Albert Wu, Internet2
- Emily Eisbruch, Internet2

**Regrets**

- Sarah Borland, University of Nebraska
- Ercan Elibol, Florida Polytechnic University
- Dave Robinson, Grinnell College in Iowa, InCommon Steering Rep, ex-officio
- Meshna Koren, Elsevier
- Chris Whalen, Research Data and Communication Technologies
- Jule Ziegler,  Leibniz Supercomputing Centre
- Tom Barton, Internet2, ex-officio
- Kevin Morooney, Internet2
- Ann West, Internet2

## Discussion

- Intellectual Property reminder

**Working group updates**

- Entity Categories Working Group (R&S 2.0)
  - Next meeting is Thursday 9/8
- InCommon TAC - Did not meet
- SIRTFI Exercise Working Group
  - About 12 institutions will participate in the upcoming exercise
- CACTI
  - Components Architecture Group is working on a new charter.
  - Strategic investments for the future discussion with Steve Z.

Internet2 Technology Exchange

- Dec 5-9, 2022 in Denver
- Identity and Access Management Sessions
- InCommon  "Increasing Trust and Assurance" session, Wed Dec 7 at 8am

**Federation Challenges and Futures Discussion**

Looking ahead in the Federation's immediate future, what do you, as a "federation insider", need to solve?

What are the "pain points" of providing scalable trusted access to information resources?
What are SP, IdP, and Federation Standards exigencies?

Comments:

- Services we are proving through InCommon, Federation and Trusted Access Platform are challenged by changes at the institutions
- Executives are often looking to find a commercially vended solution
- That excludes InCommon Trusted Access Platform (TAP) software and sidelines the  InCommon Federation
- RFP for Identity Governance and IGA solution is vendor selected at Oregon State University.
  - Goal is to replace homegrown Perl scripts, etc.
  - Might still run Grouper on top of the chosen solution, thanks to Grouper's features (set math).
  - Ability to manage groups for which there is not  a data source from HR.
  - Will switch to Azure SSO, will run Federation adapter format.
  - Still intend to participate in federation.

  - Does not make sense to run SSO and Shiboleth.
  - Will contract with  Cirrus Identity for gateway.
  - Hope to centralize access policy.
  - Could be accomplished with InCommon Trusted Access Platform (TAP), but that requires staffing and knowledge.
- Unicon has found that some clients are open to the InCommon Trusted Access Platform (TAP)  and others are not.
  - Unicorn works with  institutions of various sizes.
  - For many institutions research is not a big driver.
  - Hard to get all SPs to join InCommon (this would make metadata management easier).
- Albert:  regional networks are interested in the federation model. They want to leverage federal funding  to access regional resources ( interschool shared courses).
- Comment: hosted and out of box IDM and SSO  and gateway are probably more likely as we look to the future, especially for smaller and non-research institutions.  They want turn-key
- How to make it simple for institutions to participate in InCommon federation?
  - Smaller institutions and many departments at various institutions have lost staff.
  - IDP as a service can be helpful
- Challenge in the North Dakota system with multiple colleges.
- NDSU has adopted InCommon Trusted Access Platform (TAP) since the staff can customize it to meet needs.
- Comment:  Getting a campus (or group) all under one identity umbrella can encourage a push towards commercial vendors because it allows a single, internally managed transition. There are discussions on a UC system-wide IDM system, but if InCommon federation was more seamless, would we need a single IAM system?
- Lack of (useful) common profile information is a blocker beyond just the technical integration layer.
  - Different campuses populate “standard” eduperson attributes differently. In the end,  email address, name and an identifier are frequently all that are reliable.
  - (Aside) Makes Azure look like (arguably) as good a solution as InCommon-based fed, since our InCommon-based federation isn’t making good use of InCommon/SAML-style federation’s flexibility.  We need to solve for organizations that are more tightly bound together than a Virtual Organization but less monolithic than a single IDP.
- If we had common naming, and we did not have the evolution of the identifiers, then InCommon could curate Shibboleth UI . There is limited use of eduperson attributes. At the edges you run into problems.
- More baseline expectations may not be the answer for increasing trust. More “you must” will not get broader adoptions
- Comment:  worked previously at EDUCAUSE.  There was no designated IAM staff. There were struggles with SSO. Partnering with Cirrus Identity was very helpful
- there are different ways the federation is used, such as
- 1) Multilateral and
- 2) Convenient way to exchange bilateral metadata.
- Pal: cannot use American cloud services in Europe due to legislation
  - Commercial providers must surrender user info if American authorities demand it
  - Some are moving out of the cloud.  Denmark example: it’s illegal to use any cloud service in the USA
  - K12 use case,  Europeans must not use Google productivity applications. A European cloud service would be acceptable.
  - Movement toward Microsoft solutions
- Seeing more and more “killer” services being used

**Baseline Expectation v2 update**

- Albert getting ready to send out notices to commercial SPs that no one has “picked up” for additional outreach.

**Next CTAB call**: Tuesday, Sept. 20, 2022, (Jon will chair that meeting)