

2022-July-28 CTAB Public Minutes

CTAB Call Tuesday June 28, 2022

Attending

- David Bantz, University of Alaska (chair)
- Jon Miner, University of Wisc - Madison (co-chair)
- Richard Frovarp, North Dakota State
- Eric Goodman, UCOP - InCommon TAC Representative to CTAB
- Mike Grady, Liaison from CACTI to CTAB
- Andy Morgan, Oregon State University
- Rick Wagner, UCSD
- Chris Whalen, Research Data and Communication Technologies
- Tom Barton, Internet2, ex-officio
- Johnny Lasker, Internet2
- Kevin Morooney, Internet2
- Ann West, Internet2
- Albert Wu, Internet2
- Emily Eisbruch, Internet2

Regrets

- Pål Axelsson, SUNET
- Sarah Borland, University of Nebraska
- Ercan Elibol, Florida Polytech Institute
- Dave Robinson, Grinnell College in Iowa, InCommon Steering Rep, ex-officio
- Meshna Koren, Elsevier
- Jule Ziegler, Leibniz Supercomputing Centre
- Robert Zybeck, Portland Community College

Discussion

- [Intellectual Property reminder](#)
- Welcome Mike Grady, Liaison from CACTI to CTAB
- Note: CTAB work plan now public on wiki [InCommon CTAB 2022 Work Plan](#)

Working Group Updates

- InCommon TAC Update
 - Behind on publishing minutes
 - Discussion of entityID validation rules (potential change in InCommon policy/practice)
 - Currently you must be owner of URL or URN you are publishing. Causes issues w/ e.g., Amazon and Okta entities.
 - Amazon uses URN:amazon for its SP entityIDs even though urn:amazon is not valid/registered
 - Okta uses something like <http://org.okta.com> for IdP entityIDs).
 - The organization registering the entity does not own the URN/domain, so even ignoring that Amazon's is invalid, the registrant cannot do any form of domain validation.
 - Discussion of message level encryption (expectations) change.
 - What are encryption level expectations? Some vendor SPs don't support encryption of certificates, but the Fed Manager requires that SPs publish them. So some SPs publish dummy certs (and tell IdPs to override encryption). Should we ease the requirement and make it possible to register without encryption? Should we disallow these SPs from registering? Etc.
 - Related to the TLS requirements/expectations discussion going on in CTAB.
- SIRTFI Exercise Working Group <https://spaces.at.internet2.edu/x/KoKQD>
 - On hiatus for a few weeks, as a call of participation will go out soon
- [TNC Meeting](#) recap: REFEDS Meetings; others
 - Ann, Chris, Albert, Kevin attended, June 13-17 in Italy
 - Albert gave update on NIH implementation, it was well received
 - There was discussion of how many federations must change because of NIH requirements
 - Some federations had not yet supported MFA profile, as required to meet NIH requirements
- Tom: Recently had a discussion with a European colleague on the trend at research universities to downsize IT departments and rely on commodity/commercial solutions for IAM. IDP as a service becomes even more important

Continued: [Discussion: Should InCommon Federation remove message level encryption requirement, and what are its implications?](#)

- Is it safe enough to relax the message level encryption?
- If it is, how do we communicate this change, who decides?
- If it is not, we are not enforcing it, how do we enforce it?

Chapter II: TLS encryption next steps from Andy/Richard/Tom

- Did some rewrites based on feedback received, draft #3
- Andy sent draft #3 to CTAB list
- The proposal is fairly solid now, need to figure out next steps
- We will have a detailed discussion on that at next CTAB call
- **All CTAB members review the TLS encryption next steps**

Beyond (Impossible if that is your preferred brand) BE3 Update (if available)

- Naming Suggestions: Baseline Expectations vs Advanced Expectations vs **R&S Expectations**
 - CTAB previously discussed a “service catalog” which ideally would:
 - Be a discovery vehicle for researchers to identify resources of interest to which they have access via federation;
 - Document the scope and value of InC and eduGAIN in fostering access to resources for R&E
 - Provide enough information about the SPs need for additional user attributes for IdPs to readily integrate, and perhaps
 - Provide sufficient information to enable fully automated IdP integration with appropriate attributes released.
 - Plan to ask European colleagues for their input
 - Issue of how to make a service catalog well known to the community who could use it
 - Intent is not a comprehensive catalog, but self-selected for those SPs welcoming discovery and seamless integration with IdPs.
 - What are the issues that **R&S Expectations** would try to address?
 - Have gotten feedback from smaller schools that emphasis on Research and access to NIH does not resonate , is not compelling for them, smaller schools are interested in consortium issues
 - David has found in terms of day to day operations, saying “this is a need for researchers” is not compelling to the average staff and faculty
 - Ann: not sure Research and Scholarship (and the term R&S Expectations) is the right term today.
 - Leave out the word research?
 - Research is the tail that leads
 - Rick: At the next CTAB meeting, we should clarify what we are trying to do.
 - Richard F: Northern Tier meeting just finished. Many tribal colleges are engaged on the network side, but less interested in eduroam and InCommon.
 - We may have two different markets to target
 - What do we focus on for NOT BE3?
 - A one pager is being vetted
 - Needs to emphasize collaborative access among higher ed, and others; emphasis on access to vendors is likely less pertinent
 - Eric: a lot of what InCommon has provided over time has been software oriented (Shib, SimpleSAMLPHP). But now vendors can fill that portion
 - The model of how to integrate is the key that InCommon should provide
 - Some orgs using OKTA as a proxy
 - How does that fit into federation participation?
- Kevin M. and Klaas Wierenga (of GEANT) will be presenting to Global CEO Forum in a few weeks.
 - To prepare, Kevin has been reading the edugain futures report and FED 2.0 paper.
 - It's clear we need a different way to present our value.

Next CTAB Call: Tuesday, July 12, 2022