

2021-March-9 CTAB Public Minutes

CTAB call Tuesday, March 9, 2021

Attending

- David Bantz, University of Alaska (chair)
- Pål Axelsson, SUNET
- Rachana Ananthakrishnan, Globus, University of Chicago
- Tom Barton, University Chicago and Internet2, ex-officio
- Ercan Elibol, Florida Polytechnic University
- Richard Frovarp, North Dakota State
- Eric Goodman, UCOP - InCommon TAC Representative to CTAB
- Meshna Koren, Elsevier
- John Pfeifer, University of Maryland
- Dave Robinson, Grinnell College in Iowa, InCommon Steering Rep, ex-officio
- Chris Whalen, Research Data and Communication Technologies
- Jule Ziegler, Leibniz Supercomputing Centre
- Robert Zybeck, Portland Community College
- Johnny Lasker, Internet2
- Kevin Morooney, Internet2
- Albert Wu, Internet2
- Emily Eisbruch, Internet2

Regrets

- Brett Bieber, University of Nebraska (vice chair)
- Jon Miner, University of Wisc - Madison
- Andy Morgan, Oregon State University
- Ann West, Internet2

Action Items

- AI - TomB will take issue of a standard to tell the SP what they can report back to IDP when abuse is detected to SIRTfI working group and report back to CTAB
- [Intellectual Property reminder](#)

Discussion

Potential Gap in SIRTfI

- Meshna noted that it would be helpful to have a standard around what SP's can/should report back to the IDP when they detect abuse,
- when there is a security incident related to a credential
- to help the IDP find and handle the situation around the compromised credential.
- TomB: (chairs the [REFEDs SIRTfI working group](#)), yes this is likely a gap in SIRTfI.
- There is a handbook, not yet circulated, that will reference templates and other materials
- AI, Tom will take issue a standard to tell the SP what they can report back to IDP when abuse is detected to SIRTfI working group and report back to CTAB

Around the community

- **Trust and Identity Operations Update**
 - Johnny is readying a release for tomorrow, with bug fixes
 - Ruby upgrade for the Federation Manager
 - Outreach around Baseline Expectations v2 will start this week
 - Finalizing communications for BEv2
 - Will do biweekly communications (to site admins first)
 - Reports for baseline are in a google share drive
 - Have not announced BEv2 yet; therefore the data is flat
 - ShannonR is working on automation of testing TLS
- **InCommon TAC updates**
 - InCommon TAC is finishing 2021 workplan development
 - Forming a recommendation on what InCommon should do around the SAML deployment profile,
 - <https://docs.kantarainitiative.org/fi/rec-saml2-Deployment-profile-for-fedinterop.html>
 - Profile does not include pushing for subject ID adoption this year

- For CTAB next year, it may be relevant to look at whether the elements in the SAML deployment profile are useful for guidance around baseline
- Work with Google and privacy initiatives, looking at same site cookies on steroids
 - Nicole Roy is participating, want to ensure we don't "break" SAML
 - This is a serious issue, if Google left alone could have bad consequences
- There is a new InCommon TAC working group spinning up to look at issues around testing environments
- InCommon TAC is looking at the work of [Seamless Access](#) and also tracking CTAB's work around assurance
- **REFEDs Working Groups** (Assurance WG; Baseline Expectations WG; R&S 2.0 WG)
 - [REFEDs Assurance WG](#)
 - There is a subgroup forming for topics related to MFA
 - Jule will give presentation at next R&S v2.0 working group call on the eduperson assurance attribute
 - [REFEDs Baseline Expectations WG](#)
 - [Consultation](#) closed, updates made, there is now a final draft
 - Will be sent to REFEDs Steering Committee
 - Then determine next steps

Assured Access Working Group Updates

- [Assured Access Working Group](#) is making good progress
- At last meeting, the working group
 - discussed local enterprise, laid out proposed structure of draft report
 - BE allows every InCommon participant operating in IDP to assert claim for wide swath of users
 - Brett shared draft of recommendations, will be filled in during coming weeks
 - Albert will likely work on creating a decision tree

Updates on NIH happenings

- Albert building a timeline around what's happening at NIH around requirements
- Things are still shifting to some extent; some segments of NIH are still developing timeframe for logon requirements
- [eRA](#) is requiring MFA and R&S by Sept 15, 2021 by single sign-on or [logon.gov](#)
- [PubMed](#) blog announces transition to federated credentials for 2021
- Albert creating a set of wiki pages
- https://docs.google.com/document/d/1lealFqLesBToPi96BV_fjLBYu6hw6Hs0gl7skY2cVu4/edit **DO NOT SHARE IN PUBLIC NOTES**
- Hope to provide a timeline sharing what we know
- InCommon office hours are scheduled for Wed. March 10 where we can be to answer questions the community may have
- Ann West sent email to schools with eRA grants, received a few responses
 - There is potential confusion between what NIH announced as being required (MFA, R&S and identity assurance) and recent communication about requirements for eRA (MFA and R&S)
- Cooperation between InCommon and NIH has been going well in working out the requirements and steps needed.

Framing BEv3

- We are sort of in a race; researcher / researcher community wants richer/safer/easier ways to interact, or they'll seek alternatives
 - we need to go fast
- Bringing along orgs not focused on research takes time
 - we need to go slow
- How do we balance?
- Want to be sure that InCommon scales to make it possible for institutions to have the resources/access they need
- **Require Research and Scholarship Entity Category (R&S) in BEv3?**
- There is value to including R&S in baseline expectations
- But we need to be careful not to make it too high a burden to be in the InCommon federation
- ChrisW: was very concerned about making the burden too high, when CTAB worked on BEv1
- But the number of organizations that dropped out of InCommon was very small. They were organizations that were not using InCommon federation anyhow
- BEv1 was relatively easy to comply with
- Including R&S in BE can challenge organizations' technology choices
- There are other use cases besides research
- Some organizations join InCommon for commercial use cases
- Should we have baseline expectations plus, where requirements are set based on the nature of the collaboration?
- Comment: We should be careful in partitioning the federation
- When CTAB discusses R&S, common topics are:
 - technology challenges, and [IDP as a Service](#) as potential mitigation for that, and
 - attribute release and privacy issues
- Suggestion that CTAB do in depth look at potential mitigations, to address the issues that stall our discussions
- Reminder: InCommon TAC is implementing some of the recommendations of the [IDP as a Service](#) working group
- **MFA is another issue as CTAB considers BEv3**
- Agreed supporting MFA is good and necessary
- We get stuck on how an SP and IDP communication around MFA
- We want to use REFEDs MFA profile <https://refeds.org/profile/mfa>
- How do we help schools that use products that don't support the REFEDs MFA approach?
- Azure or ADFS users may not be willing to add another layer of technology, they see more technology and more risk
- There are sometimes bilateral relationships with institutions and researchers when an institution cannot assert MFA
- But there are dangers to bilateral relationships

- There are business choices, risk based choices
- SP perspective: use case of Elsevier, students needing to reach articles,
 - MFA becomes a burden
- Many SPs will not require all IDPs to support MFA
- Signaling support of MFA or not makes most sense
- Globus supports different levels
- Ability to signal how you perform authentication is important
- Ability to signal MFA may be part of certain profiles
- **Summary:**
 - Makes sense to create a subgroup or working group to lay out the considerations
 - Create a map to understand what is fundamental and what is specific to certain cohort
 - Start a working group to put move this discussion ahead, frame the questions
 - Hope Rachana might take the lead
 - Discuss at next CTAB call

Next CTAB call: Tuesday, March 23, 2019 [Summer or Daylight Time will have begun in U.S.]