

2021-March-23 CTAB Public Minutes

CTAB call Tuesday, March 23, 2021

Attending

- David Bantz, University of Alaska (chair)
- Brett Bieber, University of Nebraska (vice 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
- Jon Miner, University of Wisc - Madison
- Andy Morgan, Oregon State University
- John Pfeifer, University of Maryland
- Dave Robinson, Grinnell College in Iowa, InCommon Steering Rep, ex-officio
- Chris Whalen, Research Data and Communication Technologies
- Johnny Lasker, Internet2
- Kevin Morooney, Internet2
- Ann West, Internet2
- Albert Wu, Internet2
- Emily Eisbruch, Internet2

Regrets

- Jule Ziegler, Leibniz Supercomputing Centre
- Robert Zybeck, Portland Community College

Intellectual Property reminder

New Action Items

- AI - Rachana and Andy will report back with proposed charter and name for the working group to look at issues around R&S
- AI - Andy, David, Albert will discuss issues around the community's endpoint requirement concerns before next BEv2 office hours

Older Action Item

- 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

DISCUSSION

Update on Federation Operations / Baseline Expectations v2

- Targeted alerts for BEv2 were sent out to InCommon site admins last week.
- See blog <https://incommon.org/news/federation-site-admins-receive-baseline-expectations-notice/>
- Albert has begun plotting progress <https://spaces.at.internet2.edu/display/be>
- The data we have looks promising
- Note: The measurement we have is for SIRTFI and ERROR URL, not endpoints
 - 55 orgs met BEv2 in January 2021
 - 103 orgs as of last Friday
 - 35 orgs updated in the last week since the targeted email announcement
- There have been questions around "what do I need to do meet the requirement for SIRTFI?"
 - Answer is "go into Federation manager and check the **Complies with SIRTFI** box"
 - See [page 7 here](#)
- There have been questions about TLS Scoring, and why grade of A is being required
 - **TO DO:** CTAB should put out a statement on why we are requiring a TLS Scoring grade of A
 - Some orgs have legacy apps that don't support TLSv1.2, they must support old browsers on campus
 - There are cases where application server is incapable of current TLS
 - Suggestion: CTAB should produce best practices, recommendation on how to handle use cases for supporting legacy apps
 - e.g. Limit use of browsers in those application settings, install a 2nd browser
- There have been questions on ERROR URL, and what should the page look like

- Examples:
 - https://errorurl-sp-demo.swamid.se/demo/idp-support-example.php?code=ERRORURL_CODE
 - <https://refeds.org/specifications/saml-v2-0-metadata-deployment-profile-for-errorurl-version-1-0>
 - Some community members would like something more than these examples provide
 - Suggestions: Provide sample pages for IdPs to use as reference/copy from
- **Implementation Guide**
 - There is an [implementation guide](#) for BEv2, but not many have read it.
 - Albert has taken the implementation guide (from the Trust and Identity Document Repository) and made it into wiki pages, and there will also be an FAQ.
 - these wiki pages has been published along with NIH support materials
 - [meet-baseline-expectations](#)
 - [get-nih-ready](#)
 - Should we direct people to FAQ or to implementation guide?
 - Albert: direct people to the cover page with links for both FAQ and implementation guide. Implementation guide is primary
- **Preparing Responses to Common Questions around BEv2**
 - Before the next BEv2 office hours, CTAB should get together and discuss issues, such as around support for older apps, or around logging, browser and app limitations
 - We can encourage community members to reach out to CTAB before office hours
 - Our messaging should emphasize "Let's talk, we will help you find solutions"
 - Possibly on org can still get grade of A with TLS 1 if careful about encryption suites
- **AI - Andy, David, Albert will discuss issues around the community's endpoint requirement concerns before next BEv2 office hours**

Scheduling next BEv2 Office Hours

- Next CTAB BEv2 Office Hours could be at slot of one of the upcoming CTAB calls
- Would be helpful to have the [Qualys SSL labs scanning](#) in place before we address the issues related to endpoints
- Shannon R and Johnny will discuss issues around Qualys SSL labs scanning tomorrow
- It's not always completely straightforward
 - There are business logic issues
 - For example, how to handle cases of unreachable, scan can't complete etc.
 - Suggestion to be reasonably forgiving
- Not yet ready to schedule office hours
- There will be an **NIH Office hour** on Thursday April 1
 - InCommon has scheduled a second open office hour with representatives from InCommon and the National Institutes of Health to discuss the coming changes to the NIH electronic Research Administration (eRA) modules.
 - The office hour will take place Thursday, April 1, at 4 pm ET, 3 pm CT, 2 pm MT, 1 pm PT
- Aim for CTAB BEv2 office hours 4 weeks from today?

REFEDS R&S Working Group

- <https://wiki.refeds.org/display/GROUPS/Entity+Categories+Development+Working+Group>
- There has been discussion about whether `eduPersonAssurance` and REFEDs assurance framework should be added to R&S v2
- Some concern about lack of fit
- Heather F is trying to guide to consensus
- What does it take to seamlessly collaborate? It takes more than entity categories
- NIH is asking for a good sampling of the things needed to bundle together for a collaboration to work
- Includes authentication and identity assurance
- R&S Entity Category can signal support for **attribute release**
- Should it signal more?
- **Authentication assurance** and **identity assurance** are needed in many cases for collaboration
- If scope is not big enough to encompass minimum things that research orgs need to interoperate, then more is needed
- The more problems we try to solve with same tool, the more complex things get
- Some think of R&S as an attribute release mechanism
- In absence of specifying Research Assurance Framework as signaling, then what will work?
- Need to standardize on a means of signaling.
- How to get R&S more widely adopted within InCommon Federation?

Proposed new working group to tackle issues around MFA and R&S as part of BEv3

- Suggestion that Rachana lead a group to tackle the issues round MFA and R&S as part of BEv3
- Andy will co-chair this working group
- Hope for recommendations from this group
- They would liaise with [REFEDs R&S working group](#) regarding R&S
- Revising the R&S spec should happen in the REFEDS R&S working group
- **AI Rachana and Andy will report back with proposed charter and name for the proposed working group to look at issues around MFA and R&S as part of BEv3**

For Future CTAB call

- Next steps around R&S / MFA / SA attribute bundles (related, new REFEDS entity categories)
 - What about IdP products that are not "R&E" friendly, ala Azure AD, Okta, etc
 - Recipes on how to configure specific/popular IdP products to do xyz
 - Where does consent flow fit in this?

- Working groups for detailed discussion, digesting, recommending on these topics?
- Would a "recipe book" for BE2 be useful?

Next CTAB Call: Tuesday, April 6, 2021