2023-April-4 CTAB Public Minutes

CTAB Call Tuesday April 4, 2023

Attending

Warren Anderson, LIGO
Pål Axelsson, SUNET
David Bantz, University of Alaska (chair)
Tom Barton, Internet2, ex-officio
Matt Eisenberg, NIAID
Richard Frovarp, North Dakota State
Eric Goodman, UCOP - InCommon TAC Representative to CTAB
Mike Grady, Unicon
Scott Green, Eastern Washington U
Johnny Lasker, Internet2
Kyle Lewis, Research Data and Communication Technologies
Jon Miner, University of Wisc - Madison (co-chair)
Andy Morgan, Oregon State University
Andrew Scott, Internet2
Rick Wagner, UCSD
Kevin Morooney, Internet2
Ann West, Internet2
Nicole Roy, Internet2 (guest)

Emily Eisbruch, Independent, scribe

Regrets

Ercan Elibol, Florida Polytechnic University
Meshna Koren, Elsevier
Albert Wu, Internet2

Resources / Pre-watch

- **REFEDS Community Chat: Federated Identity and Browsers – Update** (23 March 2023) – YouTube (or https://refeds.org/community-chats to see all REFEDS Community Chat recordings)
- NIST Digital Identity Guidelines Webinar Series - https://www.nccoe.nist.gov/digital-identity-guidelines-webinar-series

DISCUSSION

- Internet2 Intellectual Property Reminder: https://internet2.edu/community/about-us/policies/internet2-intellectual-property-policy/
- Disclaimer: The meeting proceedings (minutes) are published. If you wish to discuss items that you do not wish to be included in the published notes, please mention it so the scribe can note the exception.
- Agenda Bash

Working Group updates

- NIST 800-63-4 review (Tom B)

    - Completed, waiting on any remaining feedback through April 6, then will post feedback to NIST.
    - 78 feedback items
    - Tom will submit them to NIST on April 7
    - Tom will produce a report on the work for InCommon
    - Highlights: most comments were in 63C around federation
    - There were some things there not specification worthy (informative or opinion text in sections marked normative)

- REFEDS Assurance (Kyle)
    - Completed editorial pass; ready for final Working Group review prior to public consultation

- SIRTFI Exercise (Kyle)
    - Developing a 'how to Sirtfi" presentation (near final) for IAM Online webinar or ad hoc presentation
    - Developing a survey for community to poll what community wants from Sirtfi/cybersecurity training opportunities
    - Will eventually develop a scenario script for fall
    - Submitted a TechEx proposal

- InCommon TAC (Eric)
  - TechEx planning
    - Note: No REFEDS side meeting this time.
    - Potentially joint session with CTAB and other committees
    - Browser changes item
    - Entity Categories (multiple types) discussion
  - Workplan
    - Theme and focus
    - A bit of a deep dive on SAML2Int/SubjectID and related EntityCategory.
    - Future Proofing federation is theme
    - Saml2int and subject ID, and various entity categories being looked at

- CACTI (Richard)
  - FedCM report - work is ongoing. Demonstrations are being created.
  - Further discussion on digital wallets and verifiable credentials. Looking for use cases in higher education.

- InCommon Steering
  - draft report on InCommon accomplishments
    Shout-out to CTAB: "The InCommon Federation infrastructure got better last year. The federation is of higher quality, more trustworthy, and more secure. Baseline Expectations and the SIRTFI tabletop exercise were major contributors to these improvements."

FedCM Hackathon Q&A - Nicole Roy

  - See REFEDS workplan for some background on FedCM: https://wiki.refeds.org/display/WOR/2023+Work+Plan+Preparation
  - CACTI sponsored Next Generation Working Group is being planned
  - Today Nicole Roy representing the InCommon technology platform, also flywheel for CACTI
  - The browser vendors (Chrome, Safari, Firefox, etc) are looking at privacy preservation strategies,
  - This work came to our community's notice in Fall 2019
  - Goal is to prevent unknown tracking of user around the web
  - From example, Intelligent Tracking Protection, looking at cookies
  - Chrome limiting support for 3rd party cookies
  - No immediate threat to SAML, and InCommon federation
  - But this is only a first step
  - Will get more encompassing
  - This will eventually get to a point where it affects the SAML protocol as tracking prevention starts to get into the body of HTTP POSTs, etc.
  - At 2022 TechEx, a group led by Heather Flanagan discussed this.
  - Decision to get together with Chrome people and Firefox people
  - (would be nice to have Apple involved, but there are barriers on Apple's side)
  - And representatives from international organizations and publishers
  - There was a Hackathon in early March
  - Goal to educate the browser people about how the items on their roadmap will break single sign on, including OPENIDConnect and OAUTH
  - The browser people were enthusiastic about the trust mechanisms our community has developed and adopted
  - Suggestion that the browser people provide an API call for browser to pop up something for user that says "do you want to continue with interaction between IDP and SP"
  - Some concern about another barrier/ popup
  - Some don't understand we have thousands of IDPs, we need to education that this is part of the privacy preservation
  - Solution must be protocol agnostic
  - Suggestion the browser use Federation metadata (but this would be hard to support)
  - Hope to get a proposal for community comment
  - Then develop a proof of concept
  - There is a REFEDS working group looking at the issues
  - Still early, but Nicole is cautiously optimistic
  - Good to see that there can be a chance to connect with big organizations like Google and influence key issues of impact to our community
  - Question: is OIDC community aware of these changes?
  -   Answer: Yes
  - Possible approach: Combine trust allow list and modal, to learn about the things not to be trusted
  - Comment: An allow list would let us (or the browsers) know who is going where, these IDPs go to these SPs, build up a network map. There are privacy violation issues.
  - We get some version of this from Metadata
  - Question: is this work the browsers are doing about privacy or about locking out other browsers and ad revenue?
  - Long term approach: verifiable credential and wallets, but it will take time to get there

  - Next meeting of key players: **Internet Identity workshop** in Mountainview, CA in mid April
    - Nicole and Johnny will attend IIW in April
    - Would be helpful if more of our R&E community attend   https://internetidentityworkshop.com/about/
    - It's like a giant cross sector Advanced CAMP unconference
    - Should we consider incentives, support for R&E people to attend IIW?
    - OpenID Connect meetings are co-located

- Operationalizing Baseline Expectations Group discussions (Warren / Albert)
  - Tom, Andy, Albert, David, Johnny met last week
  - Reviewed spreadsheet
  - Talked about cadence of communication with the community
  - Hope to have an annual email loop (with InCommon admins?) to confirm details of participation with InCommon, confirm roles
  - Hope to help people keep their eyes on the road

TechEx 2023 proposal

- **Joint CTAB & TAC TechEx session**
- Draft Abstract (David, Jon, Albert, Keith Wessel):
  The InCommon Community Trust & Assurance Board (CTAB) and the InCommon Technical Advisory Committee (TAC) have been working this year on several important initiatives to increase trusted interoperability among InCommon participants. First part of this session will describe the progress in these areas to date and how it will benefit scalable federation, including:
  - better user identifiers
  - new entity categories
  - completion of Baseline Expectations v2
  - operationalizing baseline expectations,
  Second portion of this session will invite broad input on potential next directions to increase levels of assurance, interoperability, security, and streamline integration of relying parties.
  Come to be part of current and future enhancements of the InCommon federation.

  Above for CTAB endorsement/approval; additional presenters to add to proposal

- Comment: it would be helpful to have a CTAB lunch after this session
- REFEDs will not meet at TechEx in 2023. REFEDs will meet in Stockholm

Next CTAB Call: Wed. April 18, 2023