2023-Aug-22 CTAB Public Minutes

CTAB Call August 22, 2023

Attending

Warren Anderson, LIGO
Pål Axelsson, SUNET
David Bantz, University of Alaska (chair)
Richard Frovarp, North Dakota State
Eric Goodman, UCOP - InCommon TAC Representative to CTAB
Johnny Lasker, Internet2
Kyle Lewis, Research Data and Communication Technologies
Jon Miner, University of Wisc - Madison (co-chair)
Andy Morgan, Oregon State University
Kevin Morooney, Internet2
Rick Wagner, UCSD
Albert Wu, Internet2

Regrets

Tom Barton, Internet2, ex-officio
Matt Eisenberg, NIAID
Ercan Elibol, Florida Polytechnic University
Scott Green, Eastern Washington U
Meshna Koren, Elsevier
Andrew Scott, Internet2
Ann West, Internet2
Emily Eisbruch, Independent, scribe,

Mike Grady, Unicon

Discussion

- Internet2 Intellectual Property reminder

Working Group updates

- Update from Research Assurance Framework consultation (Kyle)
    - RAF 2.0 Public Consultation completed 15 August
    - https://wiki.refeds.org/display/CON/Consultation%3A+REFEDS+Assurance+Framework+%28RAF%29+v2.0
    - Research Assurance Framework Working Group has reconvened and is going through comments
        - stretch goal for release: prior to TechEX in September; if not, then soon after
    - Many editorial inputs, positive feedback
    - Preparing an Orientation to RAF 2.0 presentation for TechEX

- SIRTFI Exercise Working Group (Kyle)
    - Call for Participation for tabletop exercise is out on the street, closing Sep. 29, 2023.
    - Two signups so far, in addition to those participating in the Working Group
    - Will do more outreach at TechEx

- CTAB Recruitment has opened
    - CTAB has 4 members whose terms are finished at end of 2023.
    - Using a form from Monday.com tool for nominations
    - Hope to use TechEx as recruiting opportunity for InCommon Committees

- CACTI (Richard)
    - Approval of the Linking SSO Systems Working Group draft report
    - https://spaces.at.internet2.edu/display/TI/TI.171.1
    -
    - Discussion surrounding security and privacy in eduroam
        - A question of if they should have a baseline expectation for eduroam. Decided it is too early for that, but if that path is examined in the future they should work with CTAB.
    - Discussion about next steps with NIST.
        - Interest in NIST, EU shared terminology for verifiable credentials
        - Question as to if we have heard anything back about our 800-63 feedback?
        - Engaging NIST about our trust model.

- InCommon TAC
    - Discussion of Cross-committees chairs discussion
        - CTAB also discussed at our last meeting
    - Draft Charter for Federation Proxies working group
        - This is the output of the “Federation Middlethings/Proxy Workgroup”
        - Proposes a workgroup to propose formally practice/policy updates to Baseline Expectations/ Participant Operating Practices (POP)/Ts&Cs to address Proxy expectations, improve documentation around same, and potentially other changes.
        - Charter was accepted (at least as draft) within TAC. Will be shared with InCommon Steering. Will be shared with CTAB in the future.
    - SAML2Int deployment guide report out
        - Document providing guidance focused around the three new attribute bundles (anonymous, pseudonymous, personalized).
        - Speculation: these bundles may represent a long term replacement for what today is managed as R&S. Or maybe elements of Baseline Expectations? This is related to maturing the InCommon Federation.

Report from the Entitlements Discussion

- Following the Aug 8, 2023 CTAB call, Albert coordinated a group to discuss entitlements
- Scott Cantor, Kyle, Andrew, Jon M, Albert, David, Richard joined that meeting on Entitlements
- Use case:
    - David discussed that there’s a direction that SAML is used just as a password verifier (i.e., vendors do access management internally, rather than relying on SAML attributes/information).
    - Integration with a cloud service provider
    - Making different levels of their service available
    - The SP said “you just need to verify the password”
    - Shibboleth is a heavy lift for a credential relay
    - Current trend of requirements from an SP: All we want is a nameID , everything else will require custom programming to do an extract
    - This approach is a lose lose proposition, we ought to be able to leverage the tools we have to provide better more robust trusted access for the institution
- Albert: Need to continue to scope the topic, much interest, many different perspectives on what this “entitlement” thing involves, we need to clarify what we are tackling
- Authentication versus Authorization as a value add
- Refeds working group also has discussed this
- White paper by Scott Cantor may be relevant https://wiki.refeds.org/display/FBP/Federated+Authorization+Best+Practices
- Difference between how the research community wants to deal with these issues versus the campus applications need to deal with this.
- Which party is responsible for making the authorization decisions
    - Research centers have responsibilities for making authorizations (often delegated to the PI) so the IDP doesn’t have a decision making role, more a support role
    - But for campus application integration, campus IAM team often must manage authorization decisions in a bilateral situation
    - In multilateral case, the org responsible for safeguarding the resource has more responsibility for authZ decision
- **A working group could potentially define these patterns and integrations,** goal could be to identify, describe and clarify the scenarios. Naming the patterns is an accomplishable thing we could provide.
- Hope to discuss this with REFEDs at upcoming meeting in Stockholm
- There is much adoption of SAAS solutions. It’s not a greenfield.
- Getting a collection of schools doing same thing in interaction with vendors can be challenging
- Eric’s side comments: OAuth/OIDC separates out the AuthZ and AuthN more explicitly than SAML. E.g., typically in SAML we send attributes from the IdP to the SP, and the SP uses those attributes to both identify and authorize the user. In OIDC/OAuth, typically OIDC will authenticate the user, and then some application-adjacent OAuth OP will provide authorization tokens to the user. This (separating AuthN and AuthZ) might work better as a model….

Upcoming Meetings

- CTAB activities / topics at TechEx
    - We are less than 30 days away from TechEx
CTAB Session: Tuesday, Sept. 19, 2023, 12:30 to 1:30pm
    - https://internet2.edu/2023-internet2-technology-exchange/program/abstracts/#communitytrustassuranceboard
    - ACAMP - preview of the proposed CommEx session?
    - Call for participation on the “entitlements…” work?
    - Combined presentation with InCommon TAC: Scalable Trusted Federation, Wed, Sept 20, 2023 at 11:20am
    - CTAB Dinner
- Proposal for Community Exchange March 4-7, 2024 in Chicago
  “Foster Community and Collaboration at Your institution”
  CTAB Session Proposal for 2024 Community Exchange

- InCommon TAC’s work on Access entity category - not discussed on this call
- This Old House - discuss at next CTAB call

Next CTAB Call: Tuesday, September 5, 2023