2023-Oct-17 CTAB Public Minutes

CTAB Call October 17, 2023

Attending

David Bantz, University of Alaska (chair)
Pål Axelsson, SUNET
Tom Barton, Internet2, ex-officio
Richard Frovarp, North Dakota State
Eric Goodman, UCOP - InCommon TAC Representative to CTAB
Mike Grady, Unicon Johnny Lasker, Internet2
Kyle Lewis, Research Data and Communication Technologies
Jon Miner, University of Wisc - Madison (co-chair)
Andrew Scott, Internet2
Rick Wagner, UCSD
Ann West, Internet2
Albert Wu, Internet2
Emily Eisbruch, Independent, scribe

 Regrets

 Warren Anderson, LIGO
Matt Eisenberg, NIAID
Ercan Elibol, Florida Polytechnic University
Scott Green, Eastern Washington U
Meshna Koren, Elsevier
Andy Morgan, Oregon State University
Kevin Morooney, Internet2

Discussion

- Internet2 Intellectual Property reminder
- Agenda Bash

Working Group updates

- CACTI
  - NISTIR-8481 feedback discussion
- InCommon TAC
  - Mostly a debrief from TechEx.
  - Call for (or maybe just invitation to) committee member participation in InCommon's Component Architecture group
  - Nomination administrivia
  - Federation Proxy Working Group prep
  - 2023 Workplan review
- RAF 2.0 (Kyle)
  - RAF 2.0 sent to REFEDS Steering Committee
  - Hope to finish by end of December 2023
- REFEDS MFA
  - Profile edits complete and submitted.
  - Now working on updating FAQ based on changes from 1.0 to 1.2 version of the profile.
- SIRTFI Exercise (Kyle)
  - Communications Test with participating organizations' security contacts in progress
  - representation from Australia and New Zealand!
  - training for organizations' exercise Point of Contact start next week
- Federation Operator updates
  - Demo of metadata health tab, not yet in production
  - Part of operationalizing Baseline Expectations
  - Results based on URLs (checking: is this URL responding?) and TLS endpoints we are checking
  - Will be possible for user to kick off a scan
  - Issuing a message, an entity check request
  - There is an entity check infrastructure, set up in AWS
  - Will pull from MDQ
  - Federation manager reconciles responses
  - Release in next few weeks
  - Suggestion for annual email to spur System Admins to do an annual check
  - Will fold in intelligent email validation
  - Painless Security did backend infrastructure
  - They are contracted to do some additional work on the emails

SUNET/eduGAIN/REFEDS Meeting (was in Stockholm, Oct 10-11, 2023)

- https://wiki.geant.org/display/eduGAIN/eduGAIN+and+REFEDS+Town+Hall+2023

Topics discussed included:

- Wallets, assurance, were major topics
- New working groups starting up, one looking at metadata configuring signaling
- A group will look at the "Who Moved my AuthZ Cheeze" topic, this group will look at what is communicated in federated single sign on. Authorization? Affiliation? Certification? Entitlements. Federal agencies are starting to look at this. Work is being done in the AARC world around tagging with certifications to provide access. Create a structure for managing this. What wallets will mean to federation is also in scope for this.
- Pal: A group may look at decorating federation part of metadata with contact info, etc, to make them easier to find edugain.
- Pal: EduIDs, national identity services, are popping up in Europe, there are at least 5 or 6 of them. There are discussions on creating a REFEDs operations group around those EduIDs.

Info From Ren-ISAC:

David B shared with CTAB via email: info from REN ISAC - CISA and NSA Release New Guidance on Identity and Access Management

- Interesting documents
- Brings up the question: is InCommon a SAML federation? Or independent of protocol?
- Nobody is actively working on SAML protocols.
- People are working on OIDC protocols

CTAB Recruitment / Election

- CTAB has 5 nominations
- There are 4 CTAB members whose terms end this year
- Noted: these 5 CTAB nominees represent identity providers, CTAB may be lacking representation from SPs and research groups
- It could be useful to tap subject matter experts to assist CTAB
- Mapping between REFEDs and NIST could be a work item moving forward
- Suggestion to reach out to current CTAB members who rarely attend CTAB calls

CTAB Workplan 2024 Ideas

- Chartering the "Who Moved my AuthZ Cheeze" Working Group
- Building Baseline Expectations v3
  - Require support for MDQ protocol? (to be discussed more at next CTAB call)
  - Define Subject Identifier migration roadmap
    Entity categories (go along with subject) - default, standard attribute bundles

  - (authz support stuff?)
    - How do we exchange authorization support information?
    - How do we manage/govern ongoing authz-support values?
  - About new federation "actors": federation proxies; attribute authority (that is not the IdP), etc
  - IAL / AAL signaling (in the REFEDS flavor)!
  - REFEDS Assurance (AAL or IAL? Level? MFA?) IAL "local enterprise" to start
  - How do we expand federation and federation tools to embrace wallets and strong authentication

- RAF 2.0 implementation guide (update of last year's assurance work by Brett Bieber and team)
- For Reference: Public CTAB Workplan 2023

Next CTAB Call: Tuesday, Oct. 31, 2023