CACTI Public Meeting Notes of 9-June-2020

CACTI Call June 9, 2020

Attending

Members

- Tom Jordan, University of Wisc - Madison (chair)
- Jill Gemmill, Clemson (vice chair)
- Rob Carter, Duke
- Matthew Economou, InCommon TAC Representative to CACTI
- Michael Grady, Unicon
- Karen Herrington, Virginia Tech
- Les LaCroix, Carleton College
- Chris Phillips, CANARIE
- Bill Thompson, Lafayette College

Internet2

- Kevin Morooney
- Ann West
- Steve Zoppi
- Nick Roy
- Jessica Fink
- Emily Eisbruch
- Mike Zawacki

Regrets

- Christos Kanellopoulos, GEANT
- Margaret Cullen, Painless Security
- Nathan Dors, U Washington
- Marina Adomeit, SUNET

Action Items from this call

AI Jessica - help coordinate a quarterly update from CACTI to community on best practices, trends and directions

AI TomJ - Add as an agenda item for a future CACTI call: Operationalizing containers

AI TomJ - Revise identity service prospectus with

- Model for individual institution
- Model for HE identity registry
- Federation brokering service to endorse assertions

Discussion

- Intellectual Property reminder https://www.internet2.edu/policies/intellectual-property-framework/

- Agenda bash
  - Survey of interest for the Recruiting & Developing IAM Resources WG - https://tinyurl.com/resources-wg
  - AI TomJ Operations should be agenda item for a future meeting)
  - Update from InCommon TAC - Les
  - Reminder of Hiring for IAM webinar tomorrow June 10, 2020
  - Posted as of June 12:
    - Download the slides (PDF)
    - View the recording (You Tube)

Update from InCommon TAC - Les

- Last few InCommon TAC meetings have included discussion of Seamless Access and Entity categories and attribute bundles Working Group and new proposed deployment profile
- Three entity categories are being proposed
  - Authentication only
  - Anonymous Authorization
  - Pseudonymous Authorization
- Use of new OASIS user identifiers, there is a bit of a chicken/egg situation:
- SPs haven't been asking for them because IdP operators haven't largely implemented them yet
- Uptake is slow for IdP operators, though, because SPs haven't been asking for them

- There was a suggestion to make the new OASIS user identifiers part of profile and require them for InCommon
- Does CACTI have a role in moving the new entity categories and user identifiers forward?
- SUBJECT ID is recommended for orgs w ADFS implementations
- EdupersontargetedID does not work well in ADFS
- See info from the Australian Access federation around NON targeted ID https://aaf.edu.au/support/resources.html#aaf-core-attributes
- CACTI might offer advocacy and best practices for adoption and reference implementations
- Cover operational considerations, including need for extra schema

- There is likely a gap in how CACTI interfaces with the community
- Baseline Expectations provides coordination and guidance community around expectations.
- But CACTI should be calling the community's attention to best practices and trends and directions.
- Suggestion for a periodic blog post from CACTI about trends and things to be aware of
- Perhaps CACTI should commit to providing a quarterly update
- **AI Jessica - help coordinate a quarterly update from CACTI to community on best practices, trends and directions**
- Important to coordinate with InCommon TAC on the quarterly updates
- CACTI's interaction with IDPro fits in here also
- Could be helpful to provide a one-pager on why subjectID is important, to provide a broader perspective

Identity and Access Management - registration service prospectus/next steps (Tom)

- TomJ created a draft prospectus as follow up to the discussion with UCSD about an identity and access management service at the May 267, 2020 CACTI call.
- Good to have Pal or others share their EDU ID story https://eduid.se/en/
- Comment: A service is a compelling idea, especially if adoption scenario is straightforward.
- It would be attractive if campuses could offload digital identity management but still preserve the student experience and manage the security boundary
- There are Interesting architecture questions

- **Learning from other efforts:**
  - Question: What did we learn from InCommon Bronze and Silver Assurance efforts that we could apply to this?
  - Previous efforts that CACTI should learn from include:
    - PESC and National Student Clearinghouse, and COMMIT
    - Issue was around lack of funding model
    - There was discussion about 5 years ago on a notary service, some of those notes might be relevant. Central database for identity proofing.
    - AnnW: National Student Clearinghouse is doing similar things to what this prospective is discussing. Doing this with AA CRAO. Query NSC database for matching attributes if there are none then an identifier is created, for longitudinal data thru the clearing house See National Learner Record Index info here
  - For connecting identity proofing back to risk, understanding what requires higher levels for identity proofing, NIST has useful guidance

- **Further refining the vision:**
  - Some use cases only require self assertion, some require stronger identity proofing
  - Risk calculation issue could be spelled out better in the prospectus
  - Intrinsic and extrinsic attributes could be explained in the prospectus
  - Carleton relies on HR and admissions departments to do identity proofing
  - U Wisconsin uses I9 for employees, there is value in making that vetting visible to other business processes, and same for other vetting that is done
  - BillT: the vetting is tightly coupled w institutional business process
  - Is the proposal for an entity registry service or for a national HE entity registry?
  - Use as authentication and profile management for whatever institution I go to?
  - I access services thru my home institution's IDP, but still maintain my profile in a registry for all of HE
  - Scoping is important
  - Self sovereign identity record? IRMA? Info card idea? https://privacybydesign.foundation/en/.
  - Self managed identity
  - In ORCID, much is self attested
  - LINKEDIN for higher ed, put the user in control
  - Allow the user to make a claim they have gotten a degree and provide a way to verify
  - Subject attribute proxy
  - Takes time to achieve buy in and big view
  - Like X509, needs maintenance
  - Plan for self sovereign
  - Suggestion to Loop in Phil W to this discussion
  - Is the info opaque to the operator of the institution?
  - Risk is real if info is not opaque to operator
    - But some of the significant use cases require that some data is NOT opaque

- Two different things: depending on whether this is for all of Higher Ed or not
- Could write the prospectus in two different ways and assess the interest
- **Next steps**
  AI Tom J Revise prospectus with
  Model for individual institution
  Model for HE identity registry
  Federation brokering service to endorse assertions

Next Meeting: Tuesday, June 23rd, 2020