CACTI Public Meeting Notes of 26-May-2020

CACTI Call May 26, 2020

Attending

Members

- Tom Jordan, University of Wisc - Madison (chair)
- Jill Gemmill, Clemson (vice chair)
- Rob Carter, Duke
- Margaret Cullen, Painless Security
- Matthew Economou, InCommon TAC Representative to CACTI
- Michael Grady, Unicon
- Karen Herrington, Virginia Tech
- Christos Kanellopoulos, GEANT
- Les LaCroix, Carleton College
- Chris Phillips, CANARIE
- Mike Corn, UCSD (Guest)
- David Hutches, UCSD (Guest)

Internet2

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

Regrets

- Marina Adomeit, SUNET
- Nathan Dors, U Washington
- Bill Thompson, Lafayette College

Action Item from this call

- AI TomJ - start documentation around the effort to outsource parts of Identity and Access Management

Discussion

Announcements

- OPENID foundation virtual workshop was May 21, 2020.
- Featured speed dating format, lightning talks
- Presentations: https://openid.net/workshops/oidf-virtual-workshop-may-21-2020/

Identity and Access Management - fully-outsourcing to InCommon?

(Mike Corn CISO at UCSD, with identity in portfolio and David Hutches, Enterprise Architect at UCSD)

- UCSD asks CACTI/InCommon to consider handling aspects of IAM (beyond identity proofing) for campuses
- Background: UCSD has 20 or 30 year old infrastructure
- Two sets of credentials; Not one authoritative person registry
- Want to change the identity ecosystem along lines of ITAP reference architecture
- Rely on COmanage to de-duplicate; Will feed info to Grouper and AD
- Will use legacy system (Racf) for another 3 years until student info system is replaced
- Much work and figuring out to consume records and build an identity record
- Identity proofing should likely be done by each campus
- Beyond identity proofing, why are individual campuses doing this identity work?
- Would like InCommon to “solve the problem”

- Don’t trust the private sector to manage this
- Waiting for government to handle identity is not a solution

- There can be merit to digital wallet and badging efforts for providing transcripts
- A platform with tokens representing each person's degrees and certifications would be helpful

- Regarding **Identity Proofing**:
  - Verification of all identities is a complex task
  - Would need a level of flexibility to handle exceptions
  - Each institution has different notion of affiliates
  - Health system affiliations can be complex, issues around health provider certifications
  - Question of who is an affiliate

        - What about people who park on campus and provide some identity info in order to pay for parking?
        - What about people who are summer interns?
        - These questions belong to the campuses

- Beyond identity proofing, it would be helpful if InCommon can handle the identity token/record management
- TomJ: What should be the demarcation in the handoff between campus and the central infrastructure provider?
- Mike: Campus must deal with access to resources based on affiliation type

- UW Madison looking at consumer identity in access management model
- Looking at demarcation between self registration, identity proofing,
    - once identity is established you moved into IGA territory and provisioning decisions
- MidPoint is focused on IGA
- Maintaining identities is big operational challenge
- UW Madison researching external solutions, their conclusion is that keeping it in higher ed family is likely important

- **Progressive profiling**, tracking all online interactions with the organization, eventually a higher level of identity proofing is required. Following NIST standards.
- Sometimes a self asserted identity is fine
- Beneficial to track identity over time
- For degree program, identity proofing is important
- NIST 863 framework for identity proofing does not provide higher level identity proofing requirements
- Nick: must be able to assert info the org understands, must be able to delegate to others for maintaining and injecting attributes
    - OPENID connect is the technology that provides this
    - but not broadly implemented to date
    - In the EU there is an identity assurance working group, working on ability to inject identity claims into other streams
- In worrisome scenario, financial services firms could end up as identity providers
- In EU the privacy regulations are strong
- UCSD: looking for a few identifiers, parallel to the ORCID ID concept

- Restatement of what the desired identity service might do:
    - Identity proofing probably not in scope
    - Identity registration and identity matching components of the ITAP architecture
    - register an identity and make it available to downstream
    - maintain the identity record with a unique identifier and the infrastructure around that

- What's the difference in trust between handing that off to InCommon versus a commercial entity?
- More trust in a consortium versus a commercial party that can leave the business

- Christos noted that In Europe the direction is to link academic identity with citizen ID provided by government
- Each country looking at who are the identity providers
- Some countries debating (or tried and backed off from) using identity data provided by banks
- Will move part of the academic identity to AARC infrastructure

- Thinking of demise of United ID as a way of bootstrapping IDs for people
- Provide SAML authentication, and replace what United ID is doing

- In the Federation space there is a need for a persistent high quality form of authentication, something people don't forget about.
- Use Web Authentication? But there are issues if person loses their phone

- CANARIE looked at a prototype / proof of concept for managing identities
- Leveraging a consortium is a good idea, versus a commercial model
- EID https://www.idemia.com/electronic-id-eid in Europe, Other approach in Sweden
- Lead adopters can fund the effort in the beginning
- What are the expectations for operations?
- Bootstrapping is one challenge, but maintaining the records is a big deal
- Like a networking protocol, the solution should be deep and highly distributable and high performance
- Integration ability at each institution is thin. How to adapt your onsite process to a new approach?
- At what point would organizations be ready to shift the risk?
- Host the PII necessary for the identity record.
- What is the **legal risk to InCommon** to take on running such a service. **Data protection** is key

Additional comments

- **user benefit** : identity owned by HE consortium means my identity is not being sold.
- it's disruptive to need a new identity when I change institutions.
- Valuable to have one identity. But don't want Google to control everything.
- Something rooted in a trusted group is valuable.
- Connecting certifications to the identity has value
    - Wisconsin state education department has some interest in this type of approach
- ORCID for things other than research
- Some friction around technology, SAML, openID Connect, etc.
- companies like Apple who want to verify student-ness, could be interested in helping with funding
    - Must be careful to not "resell" people's info

Kevin

- This idea comes up often, very interested in CACTI's input and thoughts on this
- Regarding funding such an effort,

- Can do things in our environment for free, create dependency, then make a business case and create the revenue to sustain it
- or
- Get some institutions to pay for the work, up to a point. Then ask for broader funding

Next Step: articulate this more crisply, sharpen the description, problem statement, value proposition, list related efforts

AI TomJ will start documentation around the effort discussed to outsource parts of Identity and Access Management

------

Recruiting and Hiring Working Group (Jessica)

1. Gauging interest/readiness to spin up the Working Group
2. Prep for surveying the community and/or announcing this at the June 10, 2020 IAM Online "Hiring for IAM"
3. Start an email list and promote it at end of the June webinar?
4. Agree to solicit for participation in the proposed working group on the June 10, 2020 IAM Online

Parking Lot

Next Meeting: Tuesday, June 9th, 2020