

CACTI Public Meeting Notes of 7-July-2020

CACTI Call July 7, 2020

Attending

Members

- Tom Jordan, University of Wisc - Madison (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 Moroney
- Ann West
- Steve Zoppi
- Nick Roy
- Jessica Fink
- Emily Eisbruch
- Mike Zawacki

Regrets

- Jill Gemmill, Clemson (vice chair)
- Marina Adomeit, SUNET
- Nathan Dors, U Washington
- Margaret Cullen, Painless Security
- Christos Kanellopoulos, GEANT

Action Items from this call

- Al Jessica will share the glossary with CACTI when it's ready. CACTI will discuss after BaseCAMP

Older Action item

- Al Jessica - help coordinate a quarterly update from CACTI to community on best practices, trends and directions (coordinate with other InCommon governance groups)

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

DISCUSSION

Trust and Identity Glossary

- Jessica reported that with InCommon [BaseCAMP](#) coming up July 20-24, 2020, there is a need for an updated Trust and Identity Glossary, with common definitions for terms like IdP, SP, etc.
- There have been several glossaries developed over the years including:
 - [IAM Functional Model and IAM Glossary](#)
 - <http://doi.org/10.26869/TI.3.2> (see page 17)
- A new updated Trust and Identity Glossary is now being created
- Once developed the new glossary will need curation ongoing for consistency
- Would CACTI want to take charge of ongoing glossary curation?
- question: Where will this glossary live? Canvas? Google doc linked from Canvas? Wiki?
- answer: not sure yet, but it should be public for easy linking
- Suggestion to work with REFEDs on the glossary. Could help in connecting w IDPro and others
 - It was noted that sometimes terminology is solution specific
 - Midpoint, Grouper, etc. may use terms differently (privileges, permissions, groups, roles etc.)
 - Makes most sense to produce an InCommon trust and identity glossary, and offer it to others
- Suggestion not to overthink this, scope the glossary to the BaseCAMP audience
- Perhaps assign an editor so there will be a person moderating
- Al Jessica will share the glossary with CACTI when it's ready. CACTI will discuss after BaseCAMP

Update on IDPro Academic Profile work

- ChrisP: Heather Flanagan has added a section in the IDPro Body of Knowledge for Academic IAM
- <https://github.com/IDPros/bok-toc/commit/e353c765e409b0b63e5a1774df7a1965f4313a9f>
- Creating top level categories
- Need to determine what is meaningful to add
- Nick suggested focus on research identity (FIM4R)
- Any effort we apply to the IDPro effort will nudge things in the favor of Higher Ed
- Positive efforts but the road is long
- It was noted that Keith Hazelton is arranging a meeting around branding for Trusted Access Platform components, to address negative connotations that may exist in some quarters around adopting open source software

Packaging - CACTI / Component architects discussion on community requirements for packaging

- This is follow up to the CACTI discussion of June 23, 2020. See [CACTI Public Meeting Notes of 23-June-2020](#)
- TomJ spoke w Keith Hazelton around the [software integration working group](#) and packaging.
- TomJ will meet with the group this week around the principals they're using for packaging.
- will bring learnings back to CACTI for a future discussion.

Review of updated HE registry-aaS prospectus and next steps

- Following up on May 26, 2020 discussion with UCSD. See [CACTI Public Meeting Notes of 26-May-2020](#)
- TomJ has revised the **HE registry-aaS prospectus** document.
- How much is viable for US Higher Ed to do in the registry area without the framework that exists in Europe?
- Which parts can we tackle and which parts might be outside of our power?
- Identity registry for Higher Ed, can we pull this off?
- It was noted that all HE institutions have developed some identity registry inside their own spaces
- Question: what is so different / harder about a **cross institutional registry**?
- Comment: it's a technical challenge and there are regulatory issues
- New legal agreement will be required for InCommon
- Europe has general citizen registry
- There are many pieces we must fill in
- Comment: future would be fraught with state level changes in privacy laws
- Les and Bill: Don't think a cross institutional registry is feasible without significant and sustained top-down priority and funding at the national level.
 - Needs serious top down priority and funding
- Outsourcing identity proofing and authentication could be a viable service in our current context.
- Yet it's a big lift given technical challenges and existing solutions at each institution
- Question: Is there a partner to engage to navigate the bigger project?
 - It was noted partnering w federal govt can lead to different priorities in new administrations
- For identity proofing and authentication, we can look at hosting COnmanage and CI logon as examples
- Around authentication and identity proofing, there are questions of how to track it, need references to documents, devils in details
- For authentication, aspects that are federation specific but challenging to support
- Issues with implementing SAML
- Integrations of Microsoft campuses is a challenge
 - ADFS orgs cannot fully participate in federation without local modifications
- Difficult for the long tail, the group we want to attract to federation
- Suggestion that we should focus on offering services like those that proxies offer for SPs, but we might do it for IDPs
- We would contract with vendors to do the needed customization (filters, identifiers)
- This project is better "low hanging fruit"
- Each state has some different requirements
- Having something central provides standards
- Suggestion that we should focus on standards for deep and broad interoperability
 - let regionals run the infrastructure to help conform to state level policies and laws
- Distributed ORCID ID
- Operating with common standards and practices
- Work for broad adoption
- Eduroam program hints this is needed at state level for K12 eduroam
- Is there a business proposition at the state level?
- Suggestion to be more participatory in the ORCID space
- ORCID already has the framework
 - Comment: ORCID is a player but different from what we are talking about
- It was noted that if the framework is operated at a state level, it will be necessary to handle individuals operating in multiple states
- Matching and match algorithms will be important
- Operating a service like this is a big deal, there is crush traffic on certain days
- Verification step-up service experience showed a separate federation may be needed
- Subscriptions needed apart from InCommon membership
- How much of what UCSD requested could we achieve from identity cross matching, use a persistent identifier, less operational lift, more driven by the user, user would provide info to help with linking two or more identities
- There is the challenge of identity assurance in places where you can't get strong legal findings to link identities.
 - 25 years ago looked at directory synchronization issues.
 - Attribute authority interface.
 - Build tooling that lets organizations pull info about users.
 - Develop interface standard.
 - Here's how we agree to format this data.

- Agree to export data in a certain format. That might be enough
- HIPPA-Like approach, make the collaboration easier
- Ann: question of what we are not doing
- Internet2 is a community asset
- Helps the community do things that are tough to do alone
- Is this the right thing to be doing?
- Suggestion that we should be looking at user interfaces
- User enrollment is hard
- Perhaps do a user interface analysis?
- Focus on the UX issue versus the data sharing
- Making the enrollment process better for scientific collaborations
- Getting users onboarded in a better way
- Concern about phishing users, need to get identifiers
- Should be simple to email someone to get them registered
- Scientists should be able to kick off the enrollment flow
- **NEXT STEPS**
 - Look at the original problems from UCSD
 - clarify the problem we are trying to solve

Parking Lot

1. (From June 9, 2020 call) TomJ - Add as an agenda item for a future CACTI call: Operationalizing containers

Next CACTI Meeting: Tuesday, July 21st, 2020