InCommon TAC Meeting 2022-03-10

Minutes

Attending:

Judith Bush, Matt Porter, Heather Flanagan, Matthew Brookover, Steven Premeau, Keith Wessel, Kevin Morooney, Eric Goodman, Ann West, Steve Zoppi, Albert Wu, David Walker,

With (Also Starring): David St. Pierre Bantz (CTAB), Les LaCroix (CACTI)

Regrets: Mark Rank, Joanne Boomer

Status Updates - Q&A (10 minutes)

1. Heather's via email (Multiple topics)
2. Steve's via email
3. CTAB
    a. Developing work plan along the lines of the TAC work plan
    b. How can we enhance interop beyond something like a BE3?
    c. In the long tail of the BE2 cleanup. "Last" round of notifications went out last week. Uncovered lots of bad contact information through this process.
4. InCommon / T&I Updates
    a. https://www.ala.org/core/member-center/sections/technology/federated-authentication-committee
    b. There's also a recommendation there for the use of Seamless Access as part of discovery.
    c. Ann will reach out to the team to offer to assist with coordination/info/whatnot.
    a. In about 5 weeks I2 will be holding a leadership event.
    b. Needs a short (e.g. 3 item) bullet list to call out what TAC is
    c. All TAC members should consider what should go into that bullet list.
    a. Minor Federation Manager update went out last week. No changes to UI.
    b. American Library Association has started a federated access group.
    c. From Kevin
    d. Ops

Overview of emerging issues affecting federation evolution (discussion)

1. Background at https://docs.google.com/document/d/1PCQ2FvBWzHUKigW-UQ2KeJ4p45svsPt10KWhAaiER94/edit
2. Current doc is a "thought document". Not requirements, not solution, more identifying concerns and asking for directions.
3. The InCommon wiki has a number of recommendations developed from previous discussions.
4. SaaS solutions and IAM frequently work differently than we used to consider and don't necessarily align with previous models:
    a. Atlassian (IdP's pay to federated, but once federated allow authentication to all sites via one SP)
    b. Zoom (Registers individual SPs per client)
5. Calling out a perceived difference in how SPs and IdPs are expected to interact.
    a. But we want the big vendor to register if they want to provide access to the whole community
6. There are different relationships and roles, and it's probably more than just IdPO and SPO. E.g., the difference between a SaaS provider (hidden) behind a service being rolled out by a university vs. a third party like MS or LIGO that wants to directly offer services to end users from arbitrary IdPs.
7. Also looking at how several SPs are themselves federations. E.g., Azure/O365, Google, Zoom, Box, Atlassian - once authenticated to the SP, cross-institution federation is not controlled at the IdP or the SP. (Once I authenticate to Box via my IdP, the owner of a Box folder outside of my org does not have any direct control over how I authenticate when accessing their service. E.g., "we want to require MFA for logins that access my folder" cannot be done at the SP level with Zoom.)
8. Matthew E worked directly with Box to configure/rearchitect their SP to give them more control and make it look more like a "normal" InCommon SP.
9. Do we want to spell out expectations like this and have some InCommon wide agreement/petition to have vendors support them?
10. Is CASB another avenue to pursue? E.g., have CASB communicate some of the authentication information we think of sending via a SAML assertion, and then work with vendors to tie the SAML assertion info into the CASB info.
    a. **"Cloud access security broker**: A cloud access security broker (CASB) is a service that applies institutional security policies, such as authentication and authorization rules, to cloud-based resources. A CASB extends institutional information security policies and practices to the cloud-based services that the institution uses."
    b. https://en.wikipedia.org/wiki/Cloud_access_security_broker
11. But the overall point is that these kinds of integrations may require us to rethink/expand our models for what we need/want from (especially SaaS) vendors out of federation.
12. Proxy issues (of hiding/abstracting the resources behind the proxy) are related to this.
    a. Attribute packages (data released to the proxy is the superset of required attributes)
    b. How do the policies (trust, security BE, etc) get "enforced" behind the Proxy.

Email Updates

CACTI Updates

Subject: CACTI Update - March 1, 2022
From: Steven Premeau
Sent On: Thur, March 10, 2022

- The Linking SSO Systems Working Group charter has been published with a DOI (http://doi.org/10.26869/TI.163.1). Rob will work with Netta to announce the group and solicit participants.

- Discussed TACs proposed subcommittee on subject identifier adoption
    - Good discussion.
    - Received two volunteers during the meeting (Chris Phillips & Kevin Hickey)
    - Anyone that might be interested was directed to email Les or me. *(I have received nothing additional.)*

- Discussion of the themes that appeared during a survey of CACTI membership about thoughts and priorities for 2022.

- Final approval of the "Wallets and Federation" Working Group charter was not reached due to lack of time.
    - Rob was seeking final confirmation from Heather that all feedback has been received and the document has reached its final state.

International, SeamlessAccess, Browsers, and Wallet updates

Subject: International, SeamlessAccess, Browsers, and Wallet updates
From: Heather Flanagan
Sent On: Thur, March 10, 2022

International Update
REFEDS

- The recording from the REFEDS Community Chat is available on the new REFEDS YouTube channel:
- https://youtu.be/RiYJ3X-A6so
- Registration for TNC22 and the REFEDS side meeting is available. There will be proper support for remote participation (a first for REFEDS) and if you're attending in person, note that registration for the REFEDS meeting will be required to be allowed into the venue that day.
    - TNC22 registration: https://tnc22.geant.org/register/
    - REFEDS registration: https://tnc22.geant.org/information-on-all-passes/#side_meeting_pass

SeamlessAccess
The product roadmap is always available to the public: https://seamlessaccess.org/services/

The Contract Language Working Group has completed its Model Contract and expects it to be published in March 2022.

The WAYF Entry Disambiguation Working Group has finished its first draft of the recommendations that complement the problem description paper (https://seamlessaccess.org/learning-center/challenges-federated-wayf/). The WG is looking for friendly reviewers to offer feedback before publishing to the broader community.

Browser Interactions
OpenAthens is hosting their annual Access Lab meeting (https://www.openathens.net/events/access-lab-2022/). Heather Flanagan and Adam Snook will be presenting on the browser changes and how they will impact the user journey around access to online content.

The Federated Identity Community Group is working on a community group report that will capture the state of work in the group. The group is also starting to open up discussion on the issues surrounding link decoration and bounce tracking. While third-party cookies have been a comparatively tractable problem, the W3C community is struggling with how to address the tracking behavior supported by link decoration and bounce tracking. The Privacy CG is considering the following and the FedID CG will be asking the authors of that proposal to come speak about the implications for federated authentication: https://privacycg.github.io/nav-tracking-mitigations/

There will be an active set of sessions on the proposed browser changes at the upcoming Internet Identity Workshop, being held in person April 26-28 in Mountain View, CA.

Wallets and Federation
Heather Flanagan is sorting out the last of the charter questions with Rob Carter and Chris Phillips (representing CACTI). The next step will be to find chairs for the group.