InCommon TAC Meeting 2022-03-24

Date, Time, and Location

Thursday, March 24, 2022
1:00pm ET | 12:00pm CT | 11:00am MT | 10:00am PT

Minutes

Attending: Judith Bush, Eric Goodman, Keith Wessel, Mark Rank, , Matt Brookover, Joanne Boomer, Steven Premeau, Heather Flanagan, Matt Porter

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

Regrets: Matthew Economou

Agenda Bash + request for notable working and advisory group updates

- CACTI update sent,
- CTAB was primarily focused on the work plan. CTAB spent facetime on the issue of supporting the board's role of increasing trust in the federation other than more baseline. "Optional" instructions regarding MFA becomes "nice to have" by implementers.
- No updates from Heather, will come: see an announcement re REFEDS community chat regarding browser "stuff"
- Keith shared InCommon TAC accomplishments report with Steering

Status Updates - Q&A

- Teaser: IdP as a service program is being picked up again
- OPS no updates, steady state

Update regarding IdP Discovery Document (Albert)

1. Can SPs limit the IdPs? Yes, that is on the roadmap for the standard implementation. As well as bringing in IdPs that are needed by the SP but not in the federation.
2. Latest document https://docs.google.com/document/d/1AMlIsqnU2vB01HTzGmp6uRE6fHe8GGsbr3MSY4XDm5U/edit
3. TAC consents for this to be sent to Steering
4. Just before sending to Steering, InCommon heard from SWITCH that they ARE maintaining their discovery code. More of an FYI as authors believe this does not change the recommendations given other issues.

Overview of emerging issues affecting federation evolution (discussion continues)

1. Proxies can mean different things. Here, consider a service provider component:
    a. SAML -> other protocol
    b. SAML aggregation point -> other resources
    c. Additional processing such as account linking, etc before user reaches resource
2. See
    a. CI Login, does all above
    b. NIH login is a gateway to all NIH resources
    c. EDUCAUSE
    d. Many many resources use this pattern
3. This is treated as a local matter in current documentation.
    a. Consider SAML to an OAuth2 that gives indefinite refresh token
    b. "We can have reasonable arguments about which party should have this control?"
        i. LIGO might make a decision independent of the org
        ii. An institution that have contracted access to a SP and wants to control who is affiliated
    a. Does the SP attesting via entity categories decrease friction? EG: if "R&S" is asserted, does it really reduce the friction?
    b. This points to a principle that everything behind the proxy MUST have the same requirements
    c. Is the entity that placed the proxy in place responsible for everything behind the proxy?
    a. How To & Policy (trust issue)
    b. Example SessionNotOnOrAfter
    c. Example "What is going on behind the proxy that i do not know about?" How can i trust the proxy? (But is that just general trust issue with SPs?)
    d. Technical or organizational trust?
    e. An SP is not literally an application, but is a policy point. With a proxy, that policy point passes on to descendants which can make other policy decisions. *POINT NOT BOUNDARY*
    f. Compare to how you have to deal with HIPAA agreements
    g. Is the eventual SP a member of the Fed? Is the behavior of the contract?
    h. Judith explains OCLC's proxy behavior (contractual). Eric explains UC's and notes of others who run proxies to simplify onboarding (one entity ID gets releases and why should i go through that pain again)

i. Propose TAC make a position paper before ACAMP for a jumping off place instead of the perennial discussion.

a. EG:
   i. UCTrust attestation on the InCommon members who are UC members.
   ii. Pixie Dust
   iii. IdP filtering - Seamless tagging that an IdP is preferred for a type of SP (library resources)
   iv. R&S certifier?
b. InCommon prohibits the augmentation by another organization
c. SAML Metadata has an affiliation group.
   i. Have a UCTrust affiliation group lists the SPs that are members
   ii. PROBLEM: would ANY other IdP software than shib have the release configuration functionality
d. Are these patterns similar enough to discuss one solution? Federation would need to adjust policies.
   i. Yes, 20% technical, 80% policy
e. We will continue the next meeting….
f. Setting Context: Making Federation Easier... What's missing
g. RECAP: last meeting, role of SP and cloud SAS service changes
h. … the context is - Albert is providing a set of observations of trends for us to consider whether the trends point to adjustments needed in the federation model. In keeping the goal “Making Federation Easier” let’s look at these trends and consider whether there are changes we should be making.
i. Next topic: Proxies (aka Middle Things)
j. NEXT: third party attestation on a party’s metadata.

2. Thanks to Albert for framing up this discussion!

Email Updates

CACTI Updates

Subject: CACTI Update
From: Steven Premeau
Sent On: Thur, March 24, 2022

Short update today:

- The Linking SSO working group has schedules it's first meeting (for April 6, 2022)

- Continued discussion of 2022 CACTI Themes.