InCommon TAC Meeting 2019-01-31

Minutes

Attending: Heather Flanagan, Matthew Economou, Matt Brookover, Mike Grady, Jessica Coltrin, Keith Wessel, Eric Kool-Brown, Janemarie Duh, Eric Goodman, Judith Bush,

With: Dean Woodbeck, Shannon Roddy, IJ Kim, Nick Roy, Ann West, Albert Wu, Dave Shafer, David Walker, James Babb, Ian Young, Steve Zoppi

Intellectual Property Reminder - All Internet2 activities are governed by the Internet2 Intellectual Property Framework

Public Content Notice - TAC minutes are public documents, please let the TAC and note taker know if you plan to discuss something of a sensitive nature.

Trust & Identity + InCommon Ops Update

Fee change feedback - Presentation done January 16. The goal of the change is to pay for support and development of the TIER program, which InCommon will continue to steward (as the InCommon Trusted Access Platform). Fee change would be effective January 1, 2020. We had one office hour with a few logistical-type questions (e.g. does this affect the cert service)

BaseCAMP - This idea comes out of a couple of working groups, which had recommended providing information/training on the basics (onboarding, operating in the federation, software, etc). The new BaseCAMP meeting is part of a new education program for the community and is focused on those new to identity and/or software and/or federation. The intent is for this to attract a different audience. August 13-15, 2019, in Milwaukee, Wisconsin (Hyatt Regency). A planning committee is working on the program.

MDQ update - The IAM Online was held last week. One question was whether we would distribute key shards to those outside of the organization. With the new model, you would need to

Internet2 Collaboration Platform - This involves using Shib, Grouper, etc., to manage collaboration tools at Internet2 (already in use for Confluence; under development for JIRA and Sympa).

International Update

PiDapalooza in Dublin last week focusing on identifiers. Federation presence wasn’t there. Heather mentioned this on the REFEDS list and did a blog post.

Working Groups

- **OIDC** - No meeting this week.
- **Deployment Profile** - Discussed some very small items today. But a review also discovered that some things are not quite finished. Those should be completed via email and then need to pass the report along to InCommon TAC and Steering.
- **REFEDS Federation 2.0** - Have had the first meeting. Next meeting is February 6 (11 am ET - https://internet2.zoom.us/j/8853848902). Discussing interviews and questionnaires to gather information.

Global Summit 2019

- No TAC F2F meeting this year

RA21 Update

View the slides from Heather's presentation.

- RA21 has roots from 2015 - corporate librarians concerned about IP address models, and wanted to explore something better, and someone suggested looking at federation. Pharma Documentation Ring (PDR) folks looked at this concept.
- Transitioned to something bigger with RA21 coordinating
- Strong support from the research community for federated IdM (see FIM4R), which should help
- Stumbling block has turned out to be the discovery interface. SPs implement it differently, which makes it tough on users.
- Also privacy concerns - and the privacy preserving nature of federation is a big win.
- RA21 goals
  - Provide best practice guidelines on discovery interface, security, and privacy
  - Test and improve solutions via pilots (completed)
  - Identify potential parties to operate any necessary centralized infrastructure
- User Experience - three building blocks
  - Consistent visual cue and call to action
  - Flexible and smart search (institution name, abbreviation, email). Type-ahead matching and URL.
  - Remember institution on next access
- Operations and Governance
  - Key - have one common method of WAYF persistence (storing choice of IdP)
  - Services will want their own customized discovery
- Persistence service means hosting a javascript and static HTML pages. Maybe some DNS magic for the backend (to make the persistence ubiquitous)
- InCommon should talk about the discovery default

AI for TAC - review Heather’s slides before the next meeting

AI - Heather - Demo at the next TAC meeting

MDQ Service Key Signing

Link to doc

- With rollout of MDQ, want to retire the signing key
- Move to 3072 bit
- Key generation to be done on a device not connected to any network and at a time that is not announced
- Would be encrypted in storage
- Introducing a technical solution for the two-person requirement
- Secure process to get the key into the HSM
- Recoverable key stored in two places and one is a physical copy in a safe deposit box, still with security requiring a quorum of people to use the key
- Plan to do the key retirement and new key in mid-March. Will have an audit trail.

2019 Working Groups

- **IdP as a Service** - Mary McKee is the TAC sponsor. Need to include some additional goals in the charter to accommodate additional use cases discussed via email. Will need to understand what capabilities organizations have, document what they want, and then determine if a proxy is the right solution. Motivation is another issue - someone may just not want to run an IdP, which is different than not having the capability to run one.
- **SAML Proxy** - Will not charter this group. The IdPaaS group needs to complete its work before considering this.

Next Meeting - February 14, 2019 - 1 pm ET