InCommon TAC Meeting 2020-05-21

Minutes - May 21, 2020

Attending: Eric Goodman, Heather Flanagan, Matt Brookover, Keith Wessel, Mary McKee, Janemarie Duh, Mizuki Karasawa, Eric Kool-Brown, Matthew Economou

With: David Walker, Ian Young, Nick Roy, Albert Wu, Les LaCroix, David Bantz

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.

Action Items

(AI) Albert Wu - put entity category and attribute release discussion on next call agenda

Federation manager release

InCommon operations released a major update to the Federation Manager last week. There were a couple of minor regressions, but overall everything went smoothly.

International Update

IDPro has been working on developing a higher education profile. That profile seeks to define and document which areas of IAM have aspects unique to higher education. Several members of CACTI are helping to brainstorm and figure out what needs to be on the list. There will be other profiles, including workforce/enterprise, consumer IAM, health care, and possibly others.

REFEDS has not made a determination yet on what we might do in place of this year's face-to-face meetings, both of which are now cancelled. We do know that a full-day webinar won't work, and we're trying to decide if and how to conduct shorter sessions to help the community stay together.

SeamlessAccess Update

SeamlessAccess has several different areas of effort right now.

- A subcommittee of the governance committee is working on the Terms of Service for the beta phase, and we hope to make that publicly available in the next few weeks.
- The technical steering committee has been focused on the future issue of browser changes that would negatively impact how federated identity currently works. There is a webinar scheduled to talk about this on 26 May, hosted by NISO. See https://www.niso.org/events/2020/05/browser-changes-and-identity-federation-impact-identity-flows to sign up.
- The Entity Categories and Attribute Bundles Working Group has finished the bulk of the work for the three proposed entity categories: Authorization Only, Anonymous, and Pseudonymous. The current expectation is that these will go through the REFEDS consultation process; there may be some NISO involvement as well in the form of a formal endorsement. That is still under discussion.
- Once the entity categories are out for public review, a new committee that will focus on contract language will kick off. The goal of this group is to help librarians develop common contract language that will require publishers stick to known attribute release activities, as defined by the three entity categories in question.
- The outreach committee is creating a set of videos to try and explain some of the concepts of federated identity and SeamlessAccess to people new to the space. The first draft of the videos are done, and are currently being reviewed by the Advisory Committee.
- IAMOnline held a webinar earlier this month to bring people up to speed on what SeamlessAccess is, and to talk about how the terms commonly used by the federation space are used differently in other sectors (such as the scholarly publishing and library communities). If you were unable to attend, the slides and recording are on the IAMOnline website.
- If you would like more detail on exactly how user data flows through SeamlessAccess, a new document is available on the SeamlessAccess website: https://seamlessaccess.org/work/SA_User-DataFlow.pdf. This is linked to from the Getting Started Step 2 and Step 3 pages.
- Last but not least, the beta phase has been formally extended to run through the end of this calendar year. Some of our criteria for success in terms of adoption has been delayed because of a recent change in technical priorities for many of the target service providers

Contract Language Working Group - InCommon probably doesn't want to get involved with that, but it is a useful discussion to have. How do you get people to recognize an entity category, for example. This working group about getting people to put this into contracts is very useful. It motivates people to learn about the issue at hand.

What segment of R&S do we need to get ahead of next re: federated access?

This discussion kicked off with a summary of a question from Kevin Morooney, wondering what fall would look like on campus, and where the data (COVID-related) reside that would affect how schools make decisions. How will people manage access to that data? How do we get involved in those discussions to provide support?

Mary McKee - Duke has had conversations about survey tools related to reopening and COVID-19 tracking. The intention is to use Shibboleth to make sure the login experience is seamless and persistent. There is also discussion about using Grouper for managing target audiences.

Heather Flanagan - I wonder if we might be looking at disruption the wrong way. What are campus groups doing, like with WebAuthn or OAuth, that work around federation that will disrupt us? Do we need to decide how to evolve with that? Web AuthN is a big part of that - how will federations support that? What problems might people get into that they don't know about when they do device-based authorization models?

Eric Goodman - The people I talk to about federation are mostly worried about their role as an IdP rather than an SP. For the most part, there is only one central group that cares about discovery services. Even though UCLA has hundreds or thousands of applications, people all authenticate at the UCLA IdP. The focus also is on the business apps, and the federation part is there, but it tends to look more bilateral. I've been refused projects related to things like improving discovery services, because centrally it isn't high priority.

Mary McKee - The challenges with federation, and IAM team structure in general, is that you need to make the "tragedy of commons" case, where we are all stronger together and stronger with standards, that there are problems with WebAuthn when it doesn't go through the central institutional hub. Duke has open-sourced its WebAuthn to Shibboleth code. We hope this will help get ahead of the problem and make sure people do this in a way that doesn't undercut. We need to make sure using the IdP is the easiest and best thing to happen.

Tim McGeary, the Duke librarian, is active in the Seamless Access Entity Categories in Attribute Bundles working group. He contends that the service provider must never directly ask a user for information. All user information must go through the campus because the campus owns the relationship and the campus owns the data exchange. This was news to the publishers. Their perspective is that they have their own privacy policies and if they get called to account, they have to answer, so we have to go to the user and ask for consent.

Mary McKee - Thinking in terms of supporting reopening efforts (COVID-19) is helping people understand the difference between a system of record and IDM systems. There is a need for a comprehensive inventory of the people at your organization. That's easy for people to understand. They likely don't know that there is already infrastructure in place that has done the de-duping and normalizing of the data. We make the case to not do things piecemeal, but make sure anything we offer goes through these enterprise IAM teams.

David Bantz - One challenge is the desire to have a "master control panel" where an institution can control all access from a single point. That's an attractive draw. But this is, in some ways, fundamentally at odds with federated access. Look at direct SSO access to academic journals or researchers finding resources. With federation, IT doesn't have to do anything in terms of granting access. We facilitate that by having reliable trusted information about their affiliation. Some IT staff find this threatening.

Nick Roy - Storytelling is how to solve that problem. Educating CIOs so they can talk to their staff about how you folks are facilitating the mission of the university by getting out of the way. But some IT staff have been told for years to be the gatekeeper; need to update that mindset.

Mary McKee - If this helps advance academia and we're not giving away anything proprietary or sensitive about the person, why should we be getting in the way? I'm curious about the entity categories discussions and would love if there were some entity categories like "give me if nothing sensitive is at stake.

(AI) Albert Wu - put entity category and attribute release discussion on next call agenda

Deployment Profile survey response

There was discussion about how to present the implementation profile and deployment profile to the community. Should InCommon publicize the profiles in their entirety and also have general statements about how a participant should approach the profiles? Should we provide guidance, such as turning these into best practices, requirements, and/or recommendations? Perhaps also guidance on which statements will likely take longer to implement than others? The implementation profile, for example, is almost a perfect set of requirements for IdP as a Service. If you were starting today, these are the things you should do. If you already are in the federation, how to you maintain backward compatibility while moving to support these practices?

Communication is a key concern. People are unlikely to read a technical profile, so we need a way to give it to them in bite-sized chunks. We can provide the profile and talk about the various parts and suggest priorities. This will be a longer-term marketing/outreach campaign.

Albert's recommendation is to publicize our adoption of these two profiles and have a discussion about sequencing. Might portions of the profiles, for instance, lend themselves to badges (say for federation readiness, software deployment, etc.). Perhaps create a simple grading system to prioritize what we want people to implement first.

TAC will continue to discuss the individual items from the survey, determine what will be involved with each and who will be tasked with action items. The discussion can include which to address first. The experience with Baseline Expectations provides a consensus-building process that we might leverage.

Next Meeting - Thursday, June 4, 2020