InCommon TAC Meeting 2022-10-20

Minutes

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

With (Also Starring): David Bantz, IJ Kim, Johnny Lasker, Albert Wu, Les LaCroix (CACTI), Pål Axelsson (CTAB), Steve Zoppi, David Walker, Kevin Morooney **Guest stars:** Kerri Lemoie, Demitri Zagidulin, James Chartrand

Regrets: Heather Flanagan, Ann West, Matthew Economou,

Scribes: Johnny, Judith B

Status Updates - Q&A

Usual disclaimer about minutes and agenda; invitation for questions regarding the emailed reports. Invitation to approve minutes.

Reminder that we are in nominations which close TOMORROW (Oct 21). Please provide any nominations you are working on soon.

Nicole: Community request for supporting multiple logos, appropriate for different views and sizes (Eg horizontal, vertical, small, large with detail). Would be a change to the Federation Manager UI and the entity's xml; adding more logo records effectively.

Digital Wallets part II

Kerri with Digital Credentials Consortium (DCC) at MIT. She's had a chance to review Niels' presentation and discussion.Dimitri lead architect, James also engineer, working with universities. Kerri's dissertation was on adoption of Self-sovereign identities, new to universities.

[SLIDES: mission, principals, vision, global institutional membership]

"Trust: credentials can be verified without consulting original issuer"

12 founding institutional members across the globe

[grab URLs for white paper from chat later]

Everything starts with the Learner

Issuers can be entities or self

Identity : DID-key (maybe https://github.com/w3c-ccg/did-method-key)

VC-api credentials community group

Need a more consistent way to do authentication across multiple identities/wallets

Judith: You mentioned your wallet code and that it can be forked, another piece that comes to mind is that you may be working on a wallet that embodies the values you mentioned before. Your focus on this domain of credentialing, it's one sort of model of one party saying something about another. There are other types of models where things may be more transient. Your library card may be a much more transient assertion about you, more of an authorization for you to use. Would you imagine that one wallet would support various models vs. separate wallets for different purposes? This wallet proves I paid a membership fee, this is my library card, this is my university diploma, etc.

Kerri: Library card is a great use case. We don't need to have multiple wallets for multiple things. One of the purpose of education credentials is that they all can be used together. If you were applying for a loan, the proof you qualify could all be bundled together.

Judith: One is an assertion about a person. This library is authorizing this individual to access things.

Dmitri: Yes, we see wallets in general evolving towards supporting all use cases. We term those bearer credentials (library card, ticket to the state fair). If you have it, you can go in. An airplane ticket is different, it lets you in but also identifies you. We did a pilot for gym access. Because the bearer and the identity bound require a cryptographic element. Key management is very hard. The data model is very open, these could be statements about anything.

Eric: I would assume that the library credential is more likely to be a short term credential that expires vs. something about you that is forever.

Dmitri: yeah, and the expiration mechanism is built right into VCs

Eric: Do you have a sense how big vendors (Microsoft etc.) are putting hooks in place to support this?

Nicole: UMA does this and is used by your medical chart provider to interop with other medical chart providers

Dmitri: Microsoft has jumped in both feet to VC. They have a presence. There still is dynamic tension, but actively participating in the standards. Some of the UMA board are active in the VC space. One item of tension is not only the data model but the protocols used to exchange VC.

What is the current thinking in the InCommon community regarding SAML2 and OpenID Connect?

Nicole: It feels like we're going to get our toes in using proxies.

Eric: You were talking about building OIDC into the app, what endpoint is being authenticated and when you talk about passing the identity back, is the application doing the OIDC?

Dmitri: We're passing the email claim so the issuer can look up the student in the database.

Eric: The OIDC is to get the DID from the identity provider?

Dmitri: Technically the wallet is the identity provider.

Eric: The wallet is saying to the institution, tie this identifier to this email address. Some places can consume directly without needing an email address 'assist'

Dmitri: Ideally, we can built in support for InCommon in DCC

Keith: What you just articulated is the fascinating role that InCommon and other R&E organizations could play with DCC so they don't have to go door-to-door individually

Nicole: There is a global picture because of eduGAIN, ~5K identity providers. We are much more SAML2 than OIDC. The trust model, you're basically using a giant xml phone book signed by a trust oracle. All the metadata within is used to build a discovery service to pick which IdP you want to use. You go authenticate and get a SAML assertion. The claims that go into that wallet could be a flavor of assertions, an entity category. When the user authenticates, the wallet attributes come along for the ride. There are so many dependencies to reconcile.

Judith: The piece of the scalability isn't just, oh I have one place to get it, I as an IdP am incredibly protective of my student's info and I'm not going to pass these claims to just anyone. Either you do a pairwise approach or join a federation. You provide assertions about how well you are willing to play along with the community expectations. That's the ideal trust model.

REFERENCES:

- W3C standards: VC-EDU, CCG
  - https://w3c-ccg.github.io/vc-ed/
  - https://www.w3.org/community/credentials/
- 1EdTech
  - OpenBadges v3
  - Comprehensive Learner Record
- https://github.com/digitalcredentials
- Revocation: Status list 2021: https://w3c-ccg.github.io/vc-status-list-2021/
- Someone in the CCG community wrote this email on VCs & UMA: https://turing.kantarainitiative.org/pipermail/wg-uma/2018-October/005641.html
- MET

Email Updates

CACTI Updates

From Steven Premeau:

- Brief discussion of 2H22 Windows 11, CredentialGuard, and impacts on eduroam
- Discussion of the TAP Reference Architecture
- W3C Browser Privacy Update

Next Call November 3, 2022