REFEDS Working Meeting @ TIIME, 29 January 2024

Promoting Adoption of REFEDS Specifications (Heather Flanagan)

- Baseline Expectations is an example of success - did the work to get in touch with everybody and ask for a very specific thing (adopt BE). Had to re-establish all the executive contacts (who signs things and pays the bills; those contacts hadn’t been maintained). It wasn’t all done by federation staff; members of the advisory boards also stepped up to help.
- R&S is a moderate success because a major funding agency essentially mandated.
- SIRTFI works well in SURF because they required it. SIRTFI also had a major agency (CERN) require it.
- CIOs practically don’t have the time to think about this. They need something more direct and easy to delegate (e.g., have the federation send out a name-and-shame email as to who is and is not doing the right thing)
- Where we do have success, we have control over the specs we promote. That’s not always going to work. Identity Assurance is an example of that. The Wallet space is going to be another.
- Most of our institutions are incapable of doing anything now because they no longer run their own software stack.
- SUNET created a test suite for entity categories and reported the results at annual meetings. They created Shibboleth and ADFS toolkits to help get them running. Once they got the IdP running, they had more leverage to push the SP.
- Why aren’t entity categories being adopted? Maybe we didn’t ask the right questions of what stakeholders actually needed.
  - The Wallet architecture moves the risk away from the IdP. Entity categories tried to touch on that.
  - Maybe people have stopped complaining because we solved their problems?
- Do the smaller federations feel they can tell their members what to do and require certain specifications?
  - Big federations can do this. Small federations are also more flexible. Middle federations are the ones that struggle most to have the resources to drive change.
  - If we focus on federation operators, they are the ones that can push this out.
- It would also help if we had key services that also force matters.
- What we’re talking about is a capacity for change, and that’s what’s the actual struggle.
- Erasmus+ is driving a significant increase in IdPs in eduGAIN. We should expect SPs to decrease as things get cleaned up.
  - You can hand-configure Erasmus and be done
- In the future, do a better analysis of what’s required and engage beyond the technical people to find out what’s needed and get commitment to adoption

Evolving REFEDS specifications to work in an OpenID Federation and Wallet ecosystems (Niels van Dijk)

- for some, the specs are good enough that they can be adopted.
- You have to have something to write into the spec that exists in the other specifications. E.g., a detailed way to define contact points exists for the SAML specs, but its not native to OpenID
- MFA and RAF is not just specification that says “do this”; it’s also policy. We need a combined idea on how that works. For OpenID Federation, we have to define as a community how to take all its bits and pieces and build something.
- If you start thinking about Wallets, some of the specs are maybe useless. What does Hide from Discovery mean in a wallet ecosystem? If we think a spec doesn’t work in any other ecosystem, should that be an explicit decision?
- Suggest we start with the regular entity categories.
- MFA might not be as easy - what does MFA mean for a wallet? Is that something that the wallet itself needs to require? How?
  - One next step: register the authentication context class in OIDC in the IANA registry
- One suggestion: do this in two steps. Take the REFEDS steps, deciding what “appropriate” is, then describe the impact for OpenID Federation. It will be more complicated for Frameworks.
  - Spin up a WG within REFEDS to look at the Entity Categories
  - See [https://wiki.geant.org/pages/viewpage.action?pageId=694812853](https://wiki.geant.org/pages/viewpage.action?pageId=694812853) for a start on this work

Microsoft Multilateral Federation & SPs (Mary McKee)

- Conversation started at TNC23.
- Microsoft has published some guidelines, but they are all directed towards IdPs.
- The use case: I use M365 for collaboration, and I don’t want people to sign up for a more MS Guest account; I want them to use their federated identity.
- Seeing two use cases:
  - Lightweight collaboration (come in, come into a word doc, and collaborate, using a federation discovery to onboard a guest account)
  - Research where people want to closely manage the environment and have high assurance requirements.
- These are the biggest things that SURF and WAYF are dealing with. MS is the dominant technology, and the way the office suite is being connected is the dominant way of dealing with identity. MS is providing institutions with additional tooling which integrate in their ecosystem (which impacts the ability to govern our own data in our community). SURF’s way of combating this is extremely limited: talking to the EU; to making sure that for collaboration scenarios where its cross-institution collaboration for 100+ people trying to work together are considered; to raising issues with procurement. Even having eduIds for everyone is troublesome and provides a bad user experience. Do they want one Azure tenant for all of the Netherlands, or provide lightweight collaboration based on federated identity and the tooling that we’re used to and hope that cross-institution users will agree to use it rather than the Office stuff.
- Cirrus PoC has an architecture where they tried to be a protocol translator, but that didn’t work. Alternatively, abstract all the federation stuff through a proxy so that according to Microsoft it looks like just one IdP (rather than a whole federation)
- Since Microsoft’s platform seems to think that identifiers are emails, there are still challenges. But this might be a tightly-enough scoped problem that Microsoft would be willing to help.
- One thing that won’t work is trying to compete with Office products.
- There may be a way in via common frameworks.
- There are a lot of points where different regions are pushing for change, but within Microsoft they aren’t talking to each other.
- Some researchers just use Google, which goes against institutional (and GDPR) policy, but they do it to make their collaborations work.
- How to manage Microsoft
  - Competitive analysis (what has Google, Okta, others solved that MS hasn’t)
Getting someone within MS to submit bug reports

FedCM, FedID CG, FedID WG, and the WICG Identity Credential group

[See Heather’s latest slides]

SeamlessAccess Trust Extensions (Leif Johansson)

- a new WG within REFEDS that will make a standard on how to include reciprocal trust in metadata
  - E.g., reverse lookup
- this information would allow you to remotely configure SA to display only the IdPs you want or indicate what IdPs are likely not to work, and provide ways to fallback to other IdPs (e.g., fallback registration)
- We are going to run into this with verifiable credentials as well. A verifier may require a particular trust mark or combination of trust marks. So why isn’t this just a link to metadata? Because you want more semantics in there, to tell the users “you are being denied access because…”
- Would this just make metadata files bigger?
  - There aren’t that many policy combinations. So, like acr in SAML, you can do the full extension or reference someone else’s. So, for most SPs it will be just another URI.
  - If you use this a way for services to signal they are members of other organizations, that will grow metadata quite a bit.
- This may be a different problem for issuers of wallets.
- Seamless Access could be a migration tool from classical federation to wallet-based federation. Rather than use a cookie, persist the entry in the wallet. It’s a claim of affiliation.
- Could this thing take the place of federation management software? Or could the federation managers rewrite and post the information to the SeamlessAccess wallet?

Supporting Open Science through Attributes proposal (Niels van Dijk, Benn Oshrin)

- is there any relation here with EU initiatives?
- This came up at an I2 meeting about how to support researchers’ access to datasets based on a small handful of existing or new attributes.
- First step for the WG will be to scope the problem. It might lead to schema work.
- Suggest leveraging the GA4GH researcher credential. The bone fide researcher credential is fairly generic; granularity not required. There is also an ontology that describes the research area the researcher is asking for. That’s not an attribute of the researcher but instead of the research. It also maps the informed consent.
- It is the data that decides the requirement.
- Researchers also seem to be allergic to using other researcher’s ontology.
- Going back to the first topic of the day (adoption) - how do you get IdP operators to mint these attributes and configure their systems to use them?
  - Maybe a delegation model for the owners of the data running the approval process to get the attribute assigned to an individual? (Attribute Authorities FTW!)
  - You can’t move governance; you need to be able to trigger the existing governance process.
  - The entitlement model only works where the person that owns the resources also owns the identity. You can find who owns the resource, but the record is too broad.
  - Ultimately, there is no way to automate this process. At best, the committees have standardized information being fed into them. Don’t forget the legal process that is part of this when PII is involved.
- You don’t want the IdP operator to be in the critical path here. Could this instead be a group system?
- All this is part of the scope conversation the WG needs to have.
- Note this is in some respects what the Seamless Access Trust Extensions covered. Maybe use a similar model?
- Don’t think about this in terms of campuses; think about it in terms of professional disciplines. If it is a delegation mechanism that says who can get access, that can be queried.
- This may also be considered a redress process.