WIKI Link https://spaces.at.internet2.edu/x/o4VQDw

# Advance CAMP FRI. Sept 22, 2023

## Room - V

## Session Title: Moving from eptid to subject-id/pairwise-id

CONVENER: Jon Agland & Matthew Slowe

MAIN SCRIBE(S): Matthew Slowe (foo)

ADDITIONAL CONTRIBUTORS: Scott Cantor, Tommy Doan, Matthew Economou, Colin McCarthy, Albert Wu, Vlad (NZ)

# of ATTENDEES: ~20

## DISCUSSION:

Jon Agland: Presenting pre-existing paper describing the problems for Federation Operators and members. Understand different federations have different problems.

UK Federation predominantly uses eptid as a attribute NameID (rather than Subject) and sometimes also eppn as a privacy preserving facet (most use cases are library resources etc).

RequestedAttributes not a very good indicator of behaviour for ukfed.

Note that “email” is not a good identifier for persistence 

Subject-id roughly eppn, but pairwise-id harder to get to despite apparent simplicity.

Scott Cantor: Reiterating that other SAML implementations unable to generate an eptid flavour fo attribute (eg Okta) so moving away from it is a **good** thing. Compatibility is key, migration is hard. Things that *can* consume the eptid can *probably* consume the simpler pairwise-id syntax.

Similar problem to changing your (signing) keys… it can result in a massive bi-lateral 1-N test loop to realise. Consider enabling *impersonation* to test.

Jon Agland: Case sensitivity problem of older deployments employing BASE64 and unable to seamlessly move to a BASE32 value without big-bang dependent SP work. Could use it as a fresh-start for the IdP operator anyway… we have many cases of bad choices of ComputedID source attribute (eg objectGUID) and could use this as a time to

Matthew Economou?: It's (now?) possible to migrate objectSID to a new domain. But this is poorly used.

Chris Philips: objectGUID is a *really* bad attribute to use as if you end up in a DR situation then all the GUIDs can be regenerated.

foo: If an AD attribute is used then SID is probably better than GUID 🙂

P1 Q: In Azure AD is objectGUID good enough?

Chris: ImmutableID might be better in AAD as it's deployer controllable.

Noting that if one chooses a *directory centric* attribute to source this then you're entirely at the mercy of the software platform on what you can do with this.

P1: We're working with deployers and they're asking about what attributes to use as source and need while also considering the re-use of username etc (batting up against eduPersonAssurance).

Matthew E: Maturity model thing… must be rigorous about how you handle the source attribute definitions. If you have deployers who can't make the jump to the assurance requirements then that should be a learning point for the deployer.

Scott: This is *Maturity Level 1* and anything below this is *Level 0*. It needs to be addressed somewhere by the organisation. Important that we try to collect the implementation knowledge that people have about these things (eg. Global Catalog everywhere problem).

Chris: Microsoft have advice on the GUID/SID migration problem (link?)

Matthew E: *The Ghost of Scott Cantor* says identifiers that we think are stable **are not**. Things change… so what? If an upstream-idp changes things then how do I as a downstream service handle that?

Scott: Is that too much to ask of RPs? The thing you expect to be stable/immutable is not… how do we advise on this in a way that people don't run for the hills?

Matthew E: We have a process to re-authorise/re-link accounts annually. Are we overthinking this? Do we just wait for a user to hit a problem then do a re-link manually? We have out-of-band processes for doing this already as we have other relationships with users though.

Chris: *Duty Of Care* - with whom does the responsibility rest to manage this? It's probably the IdP's job and the downstream RP relies on that. We ask "do you reassign identifiers?" and use that in decision making. Reassignment is bad and makes us sad but there are ways around this.

Scott: Reassignment and re-keying (re-encoding) not quite the same.

Chris: Rekeying

P1: With eduroam CAT we suggested all IdPs to switch from eptid to subject-id and it fell flat!

Chris: ORCiD also uses eptid but also does some automatic deduplication / relinking based on R&S. In UK Fed there are **many** RPs to handle and that's where the DoC appears.

Alan Buxey: Dedup based on other attributes can go wrong. Out of band relinking (via email address?) isn't reliable either.

Chris: Must come up with possible steps to relink out of band.

Scott: We need RPs to come up with a process to *rename* Persistent Identifiers. We should ask vendors (on deployment) "can we rename accounts?" by some means… those who say "No" we go with anyway (rightly-or-wrongly) but at least we know in advance.

Albert Wu: re Account Linking we have operators who have been doing this that it would be good to get documented in the open… whether or not the vendor does it… CI Logon, ORCiD, eduGAIN.

Jon Agland: On eduroam CAT there's an out of band process involving the eduroam Operator.

Chris: Should probably follow the "Account recovery" process (link)

Albert: Is this a Baseline Expectations problem?

Scott: Maybe but it's firstly important to understand the extent of the problem before tackling BE.

Jon: Noting Maturity of IAM is one aspect of the problem but also binary attributes (GUID) are also difficult to handle. Pairwise-id you need "something" (used to be upstream student number etc but currently thinking an IAM defined immutable attribute linked to the upstream system's PID).

Scott: Don't be beholden to the organisational system's view of the world.

Joanne: Can we "just" create a static attribute linked back to the organisational attribute for subject-id?

Scott: Yes that's a really good idea. But get the IAM system to do it if possible. IdP *could* do this (using StoredID) but it's better to do this upstream as it's not really a long-term solution.

Joanne: Should that be the primary recommendation?

Scott: Absolutely yes. Subject-id *should* be generated in this way. But this not well understood/communicated.

Chris: It's been called many things over time and some places don't have the capacity/ability to handle this.

Tommy: Person Registry should handle this (referenced elsewhere?)

Chris: Sounds like violent agreement! 🙂

P3: This sounds very like a maturity thing… the breadth of deployments makes this hard for some places.

Albert: This entirely depends on the deployer's *maturity* and it can be very hard.

Chris: We use the term "speaker of truth" for the IAM system but is data based elsewhere.

Jon: We've only tackled the IdP problem…

Scott: but it's incumbent on the IdP to make the SP's job easier

Jon: How do we reassign? How do we educate RPs?

Alan: It's often not the IdP's *fault* as they're reliant on upstream data.

Scott: It *is* the IdP operator's organisation's problem!

Jon: RequestedAttributes is a brittle tool. Require vs Desire semantics are not up to the job. Some IdPs support multiple scopes. Existing identifier based on EntityID but new one based on scope… this has challenges! How do you systematically map the entityID to scope?

Matthew E: Why not just use identifier + entityid?

Scott: Length, ugly, poorly implemented. Intent is to provide portability when entityid *must* change. OpenID has the same problem if not worse with location values baked into identifiers.
Jon: Coordination required between IdP and SP if remapping. UK Fed will be baking migration-test accounts into the Test IdP for SP operators to test migrations.

Scott: Worried that subject-id will not be used correctly… also should be portable into the "sub" claim in OpenID (ref REFEDS document?)

Chris: Likely to have many hundreds of RPs to deal with as a fed-op. Entity Categories are a tool but the problem rests with the IdP-SP relationship. Possibly use "common dates" to migrated (based on entity category too?). Some many not move.

Matthew E: On the RP side, in Satosa, there's a Primary ID plugin to handle this sort of migration.

Albert: InCommon need to deal with this too. As a community we're bad at sunsetting things and we need to change this. The kicker is Security Breaches and functional breaking of services.

## ARTIFACTS / LINKS

1. Action: Collect the implementation knowledge that people have about these things
2. Microsoft docs about GUID/SID: https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/plan-connect-design-concepts
3. Can we get the Jon's Presentation link ?
    a. https://www.slideshare.net/JonAgland/20230922-acamp-session-on-moving-from-edupersontargetedid-to-subject-identifierpptx (was edit'd within about 20minutes before the ACAMP session)
    b. Previous UK federation webinar session on this (which slides are based on)
        i. https://www.ukfederation.org.uk/library/uploads/News/20210525-Subject-Identifiers-in-the-UK-federation.pdf
        ii. https://youtu.be/wPxTA9EHxWY?si=eNFlvy6dk2F3fEDb
4. IDPro Account Recovery article https://bok.idpro.org/article/id/64/