Link to 2025 ACAMP Wiki

Advance CAMP Thu. Dec 11, 2025

Room - 1

Session Title: Implementing subject identifiers in REFEDS Entity Categories

CONVENER: Joanne Boomer

MAIN SCRIBE(S): Chris Hubing, Gabor Eszes, Jon Miner (filling in with more errors)

ADDITIONAL CONTRIBUTORS:

# of ATTENDEES: 22

ARTIFACTS / LINKS

- WG: https://spaces.at.internet2.edu/spaces/inctac/pages/295339346/subject-id-deployment-guide-wg
- Subject Identifiers spec: https://docs.oasis-open.org/security/saml-subject-id-attr/v1.0/saml-subject-id-attr-v1.0.pdf
- Deployment Guidance for REFEDS Access Entity Categories - **http://doi.org/10.26869/TI.178.1**
- Deployment Guidance for Subject Identifiers - **http://doi.org/10.26869/TI.182.1**

DISCUSSION:

- Intro by Joanne
    - This relates to the InCommon Deployment Guidance for the REFEDS Access Entity Categories and the Subject Identifiers
    - REFEDS Access Entity Categories

        - Personalized
        - Pseudonymous
        - Anonymous
    - Subject Identifiers:
        - Subject-id
        - Pairwise-id
- VT implemented subject, has not had anyone use it, yet
- Hannah: how should attrib release work? Is it sent because of what's in the SAML metadata or is there some other channel?
    - Scott: there's a specific method also, defined in the same spec as the one that defines subject-id and pairwise-id, but adoption is spotty. You can use other methods also.
- Gabor: intro for subject identifiers
    - Pair-wise id: Promise not to release same value for same user to different SP (unique to SP)
    - REFEDS Access Entity Categories - Anonymous (affiliation only), Pseudonymous (pairwise-id, affiliation), Personalized (subject-id, PII and the like)
- Albert: requested attributes come from SP, but IDP does not have to release the attribute. Would prefer in InCommon to rely more on attribute bundles
- Albert: As compared to the prior art "Research & Scholarship Attribute Bundle" (R&S), there is a notion that somebody certifies it as compliant.
- Albert: It helps to think of these REFEDS Access Entity Categories as attribute bundles instead of requiring attribute release.
- Albert & Mike Grady: The REFEDS spec requires automatic attribute release to SPs that are registered with the corresponding Access Entity Categories, and that's probably a loaded controversial question.
- Amanda - does the Federation want us to trigger automatic attribute release or are we satisied with the attribute bundles for now?
- Albert - I personally would like to see these three attribute bundles as the default bundles for InCommon attribute release
- Gabor - Now that we have guidance for Subject Entity IDs and Access Entity Categories … What are we missing?
    - Dalia (AAF) - How are we going to communicate these changes to the service providers? Because they're all still using the old attribs like eduPersonPrincipalName and eduPersonTargetedID.

- Amanda - An SP's work is not done when they start accepting these attributes and mapping functions to them… they also (probably – some may be OK without it) need to map their legacy attributes to the new ones so that continuity can be maintained for end users. If the IdPs collectively said that they want to do this, I could build a business case for my bosses to put work into supporting it.
- Albert - from a federation perspective, this is what we're talking about when we talk about Federation Expectations. Exactly the sort of thing we're looking to formalize for interoperability purposes.
    - First, we say that for Federation transactions you will use these attributes if these attributes cover your use-case. Other attribs are fine if they're not covered by these use-cases.
    - If you join the federation these are the attributes your expected to use
- Scott - w.r.t. How IdP operators feel, re: email address, I'm starting to get more pushback from SPs when I point out that email is not appropriate for a user identifier.
    - Used to be "OK I get it", now it's "you're wrong"
    - Assuming that they're getting pressure from users.
- Scott (spec author for subject-id and pairwise-id): one of the things we were trying to do with these was to create an opportunity to start over, and this needs IdPs to support it.
    - Were not intending to force on all RPs/SPs. Especially not SaaS vendors who insist it's emali or nothing.
    - Saas apps tend to want email or the don't really care.
    - I had been getting feedback that the built-in scope in subject-id and pairwise-id is useful to SPs.
- Shannon: a lot of SaaS apps do discovery via email.
- Shannon: IDPro Body of Knowledge (https://idpro.org/body-of-knowledge/) does say that email is not a user identifier (https://bok.idpro.org/article/id/16/) so that's one other place you can point to to make the case that they shouldn't do that.
- Gabor: the SaaS apps don't really care about the properties of the identifier because it's the IdP's organization that has to fix it if it gets changed/reassigned.
- Albert: important to remember that Expectations only apply to transactions happening through InCommon between members, does not apply to bilateral transactions, unfortunately.
- Shannon: the OpenID Foundation's IPSIE Working Group (https://openid.net/wg/ipsie/), where Shannon sits and tries to represent our

community, is looking at a somewhat similar topic regarding interop but they're focused on OIDC. Nonetheless Shannon is trying to advocate for SAML specs like saml2int instead of reinventing the wheel or going elsewhere

- Albert: for REFEDS Access Entity Categories authors, especially w.r.t. Personalized, … whether it is appropriate to use the 'email' attribute for purposes beyond the strict "routable email only" usage. Consensus is that it's okay, to, e.g. show in a UI to help locate the user. But of course, these are only as valid as the assertion's timestamp – it's not guaranteed it won't change later. Support the user using various attributes to find the right entry, they're temporarily correct, but not long-term.

- Gabor - Stepping back … we have guidance, what do we really need to get the community to move on this?
  - Shannon - you can get a big or relevant SP to require it. at Berkeley they used employee ID scoped for subject-id
  - Gabor - can we have Federation Manager require Personalized?
  - Albert - we need the community to assert that this is the standard, which we don't have yet. We need to agree and publish that as the standard.
  - Albert - simultaneously, we should work with major SPs to get them to request it, eg, Elsever is requesting that IdPs release pairwise-id. But the major SPs/RPs have a major lift to move.
  - Albert - you tell me if you all are willing to ratify a Federation Expectation that says that beyond a certain date we will not admit members that do not support a standard attribute bundle(s)
  - Amanda - has this worked out before? What has happened?
    - Albert - we did lose some IdPs in BE, but they were already dead.
  - Hannah - as an SP i have a hierarchy of identifiers and I choose the best one. After this transition, will it be the case that only subject-id will remain?
    - Amanda - I have bilateral integrations too who are unlikely to adopt subject-id, but for the Federation use-case perhaps.
  - Albert - we can articulate that in the US Higher Ed / Research community these are the attributes we make available
  - Scott - we can't force everybody to do something, so SPs will have to remain flexible, since they'll need to interact with a lot of different IdPs in different federations.
  - Scott - when I worked on the subject-id spec, part of the design intent was to make a value that was suitable for OIDC also (in the 'sub' claim).

    - Jim Basney - would like to see somewhere on the timeline that we update eduPerson to deprecate eduPersonPrincipalName (and epTID).
        - Albert - related, did anybody else notice that this is a SAML-specific thing? It's right in the name
        - Gabor - that's semantics, this is about the values and usage, not SAML-specifc
        - Scott - abstracting was a historical anachronism, it seems to have been a mistake to abstract the attributes anyway.
        - Gabor - we can still move forward and we can debate that later, i.e. in the schema board
    -
- Gabor - So now we have Federation Expectations… It's going to start up soon and we'll have opportunities yearly to add more. Question is, do we roll this in the first set or is it later?
    - Albert - we've been working on what we'll do for first options Right now we have the concrete use case from NIH pushing (MFA, Assurance). We don't have the big concrete use case here that we know of yet.
    - Shannon - we'll be doing this soon for Elsevere
    - David - Is NAIR a use case?
    - Albert - we could push on NIH to go to Personalized, but that's a big lift and change.
    - Cory - I'm working on American science cloud folk to find
    - Albert - my holy grail would be we have a "Research Ready" set, Personalized, MFA, Assurance, Attrib release / affiliation (we'll workshop with Albert to make sure this is accurate. Great branding through).
    - Hannah: I'm considering (...) but it's different from the SIRTFI scenario because here we don't know if an IdP is ready to release subject-id
    - Bjorn: There is Entity Category signalling for IdPs too, not just SPs.
    - Albert: so we package it together into a single "expectation" that these are the things that the IdP has to / will provide
        - And Elsevier and ESBCO are the two biggest publishers, we work on something like "library ready" to have a similar push.
    - Scott - finding that library resources switching to federation, vendors are silently attempting to switch to getting PII and de-anonymizing access, brings it up with the library and they are unaware.

        - Potentially because they are trying to track for security reasons. They are usually wrong.
    - Albert - Expectations will need to come with explanation.
-
-
-
-
-
-
-
- .
-