17-Oct-2017 Attributes WG Minutes (from TechEx in San Francisco)

Attributes for Collaboration and Federation Working Group
at TechEx in San Francisco
Oct. 17, 2017

Led by Tom Barton and Mark Scheible

Scribe: Mike Zawacki, Internet2

Objectives today:

1. Identify the problem we are trying to address
    a. Research & Scholarship attributes
    b. Not singlehandedly solve, but rather identify impediments in adoption of R&S.
        i. Ignorance of utility?
        ii. Process issues?
        iii. Etc.

- Nate: Research is not a part of what some schools do - our (Cal State) problem is more related to cloud services.
- David: Do we know which R1s are releasing R&S? Answer: A minority - 11%.

- Chris: Is it the best use of our time and energy to evangelize R&S?
- Seems like release of email address is a blocker. Do we just remove that?
    - Counterpoint: Would limit utility for some organizations.
- Tom: So do we focus on existing bundle and then refine after more use? We considered a baseline of elements when attribute was first formed /deployed.
- Question: Not every user/account has an email address. Is that required for everyone? Answer: No, just “a majority”.
- Idea is that you have a mechanism in place and you can use it to release needed attributes to everyone in that category. So are we changing that now?
    - Tom: Needs to be defined before moving on. Also (again) consider need to define audiences. I don’t think the issue is the nature of how the categories work.
- SP =[Andy Sanford, EBSCO - Mark S.] : Bundle name doesn’t speak to me as a Service Provider. We need uniqueID, name, and email address. If we don’t have those we will prompt the user to provide that info. Can’t do anything without those - audit concerns, etc.

- Scott: Original motivation of R&S bundle was that many services don’t work without things like email.
- Tom: So we’re hearing that there are required elements, that there are workarounds for lack of some of those, but not others.

    - Notion of targeted ID was that you aren’t giving away names, but allows SP some assurance that the user is the same user as they were last time they used the service.
        - Scott: Targeted IDs may be too restrictive, not work with some SPs [e.g. proxied Services - Mark S.]
- [Jill]: Is it understood that user info is only released when they’re trying to access something they want? It isn’t being released willy nilly to the internet
    - [Weak] Counterpoint: Consider that user may not understand what they’re accessing/think they’re accessing something else.

- ORCID didn’t go down the R&S path but did require uniqueID.

- Those institutions that don’t want to adopt R&S because of concerns around email address release, yet send email all the time. Also, if you only send a unique ID, what is your value proposition over ORCID and similar platforms.

- Opinion: Vast majority of InCommon IdP operators only want to work with the small number of Service Providers that they have standing with. That’s a major obstacle.
    - Posit: What if InCommon *was* the provider? Would that solve some of these cases?
    - Scott: Possible counter - if they have no business use case to contract with InCommon, why would they?
    - Paul: Consider risk concerns

- MaryD: We would rather release same attributes to everyone. One-offs are tedious and slow adoption. Our contract is with InCommon so there’s no passthrough agreement with our IdP and other SPs. We’ve addressed this with consent.
    - Is the implication there that you don’t have trust in what random SPs in the metadata does with trust structure between the various players?
    - Mary: Concerns are legal in nature.
- Nate: Could some of these conversations go better if we couched it in more accessible terms? Also, do we want more than one attribute bundle? I think “no” for sake of simplicity.
- Mark: Re - comment around email addresses and release.

    - In talking about problems there's been a lot of finger pointing at Registrars. Maybe look at how we're talking about attribute release, make people understand it's less scary than it sounds.
- Chris:
    - There is a binary on or off stratification of attribute sets (aka not enough entity categories) -- make a rich option and it will be easier. (ie we haven't reached a paradox of choice yet)
    - AAF has gone down this path with baseline expectations (https://aaf.edu.au/media/2016/04/auEduPerson_attribute_vocabulary_v02-1-0.pdf).
    - Tom: What is the stated mission of the AAF? To support research. Much more clear need case. Ours is less clearcut.
    - Chris: They've classified (page 5 of above link
      Classification: Category of the attribute, giving a general indication of how it is intended to be used. The categories listed below have been collected from the NSF Middleware Initiative HigherEducation Person survey [NMI]. The categories are as follows and are described in Appendix B of this document. • Personal characteristics • Contact / Location information • Student information • Employee information • Linkage identifiers / Foreign keys • Entry metadata / Administration information • Security attributes and keys • Confidentiality / Attribute release (visibility) • Authorisation, entitlements • Group-related attributes • Other attributes)
- Scott: Consider if the goal is to look at the institutions which aren't releasing appropriate attributes. If so, we seem to have some representatives in the room and can level set off them.
    - Tom: I'm not sure the question has been cued up appropriately from many/most of the institutions that aren't releasing. Important to do that.

1. Gather input and perspectives on:
    a. Circumstances that inhibit enabling federated collaboration with R&S
    b. Possible mitigations for those circumstances
        i. Start IAM working group on campuses
        ii. Leverage value of Shibboleth, stress benefits to password security
    c. Naming of [Working?] group: Identify audiences, motivations, challenges first.
        i. FERPA-defined Directory Data
            1. Would address concerns of/speak value to registrars
        ii. Need additional categories? Is "R&S" too narrow?
            1. Originated from R1s, so made sense in that context
        iii. Consider what data you're releasing, or political justification for release.
            1. "Hey, if that's what it takes"
            2. We understand needs that must be addressed… but is this the place for discussion of naming conventions & how they relate to broad spectrum of needs? Are we worried about use cases/needs outside of this group/community [Research, or InCommon]?
        iv. [Part of the] Charter of this group is to propose a default release attribute policy. So we should be talking about that default

1. Identify the more feasible approaches in 2.b.

Closing words from Ann:

- Some of us did mini attribute release trial. We agree that walking registrars through what release looks like, how it works, they get the value.
- One of the components could be enabling the CIOs to make the case to registrars.
- Other blocker is that IT teams on campus don't check logs, aren't aware of lack of access to resources that some users deal with.

Summary of F2F Meeting Key Points (by Mark Scheible)

- Working Group Deliverables
    - Not trying to single-handedly solve, but understand what the impediments are for IdPs (campuses) to release R&S
        - Some schools do not do "research" and don't feel the need to adopt R&S
        - Releasing email address might be an issue for some campuses
            - Can that requirement be removed?
            - Email address is a required attribute for some R&S SPs
        - The R&S attributes are not being released to every SP a user goes to, just those that are approved as R&S SPs and identify as such
        - Opinion: Vast majority of IdP operators only want to work with a small number of SPs they have contracts with - that's a major obstacle
        - Many organizations point the finger at Registrars, but when they're walked through the process, they have no problem with it (recent meeting with registrars at AACRAO conference)
            - Possibly just needs to be communicated more clearly than "attribute release"
        - (Chris) Currently just R&S or nothing, maybe having more granularity would be better received?
        - Focus on institutions that aren't currently releasing R&S
            - R1s? Or all participants?

- R&S SPs (Vendors, Research VOs, etc.)
    - "Bundles" don't mean that much to me as a vendor… Just need UniqueID, name, email address
        - If those aren't provided as attributes from the user, we'll prompt them
        - Can't do much without those attributes
    - As far as R&S attributes, there are some that might have workarounds (specific identifiers maybe?), but others that are required.
    - ORCHID didn't go down the R&S path, but did require a UniqueID

- eduPersonTargetedID

  - Idea was that it was privacy preserving, but provided a way to recognize returning users to a specific SP (unique, hashed identifier for a user accessing one SP resource from a unique IdP)
  - However, this won't work for VOs that are using a proxy SP to get to multiple service

- Individual Comments on R&S release:
    - MaryD (VT) - Advocating for R&S release by IdPs, "We would rather release same attributes to everyone. One-offs are tedious and slow adoption."

  - Contract is with InCommon, not IdPs or SPs
  - We've addressed any VT legal concerns with Consent

  - R&S Attribute "Bundle"

  - For and against comments on a single bundle vs. more granularity