2020-04-20 REFEDS R&S Entity Category Discusssion

Date

20 Apr 2020 at 16:00 CEST

VC details are in event invitation.

Attendees (35 at 10:08 am)

- Nicole Harris
- Pål Axelsson
- Alan Buxey
- Judith Bush
- Albert Wu
- Christos Kanellopoulos
- Kevin Morooney
- Arnout Terpstra
- Scott Cantor
- Maarten Kremers
- Heather Flanagan
- Wolfgang Pempe
- Alex Stuart
- Jule Ziegler
- David Groep
- David Kelsey
- Davide Vaghetti
- Guy Halse

Goals

- Discuss issues raised with the REFEDS R&S Entity Category and whether we should fix:
    - More supporting material for R&S (FO checklist / audits).
    - Minor issues withe current specification (e.g. issues with wording).
    - Major issues and a new release (changing attributes, adding new requirements).

Discussion items

1. Hey, I didn't know REFEDS did an annual R&S survey! What's that about?
2. Could we get a validator for R&S? (Spoiler, eduGAIN OT are working on it)
3. Should R&S require Privacy Statement URL?
4. Are FOs forbidden from filtering SPs that are tagged anywhere with R&S?
5. Can we have a more specific set of "rules" for FOs supporting R&S?
6. Do we plan to "fix" the identifier issue in R&S?
7. Your questions here...

Notes

InCommon

- 27 institutions in the US have started adopting R&S. Have heard 3 office hours to answer questions and help. The adoption was more dramatic in the first week (all 27 adopted in that first week). Last Friday, Kevin sent out a follow up message to the CIO list, so we're hoping to see another wave of adoption this week.
- On the documentation front, the InCommon wiki has been updated with documentation, and a dashboard added to show rate of adoption.
- Also now working to get the 77 institutions that were still tagging with the InCommon R&S category over to REFEDS R&S.
- Also reaching out to those institutions that have asked to be hidden from Discovery and from eduGAIN to reconsider their choices.

eduGAIN stats

- There are now 65 more institutions supporting R&S
- One new federation has started supporting R&S
- In doing this, reaching out to federations to understand what the barriers to adoption might be
    - How much can we trust decisions put in to R&S (didn't know there was an annual review of R&S)
    - Want a validator for R&S - there's nothing that automatically checks technical compliance
        - eduGAIN is adding that now
    - If R&S requires release of attributes, shouldn't it also require privacy statements?
    - Question re: wording - that IdP that must release attributes to all SPs, but they can't if the SP is in another federation, or if there are other issues that prevent doing this
    - Are the identifiers in the bundle the 'correct' identifiers? Or should we make a dramatic change and use a more appropriate identifier

Other issues?

- GEANT have been working with many SPs to integrate, but there have been very consistent comments from implementors:
    - Identifiers must be clarified and brought up to date. What's the point of having both ePPN *and* ePTID?
    - Scoped affiliation - the spec is vague. Is the release of scoped affiliation mandatory or not? What if the IdP doesn't actually have that value recorded?
    - How to handle R&S with Data Protection Code of Conduct? They seem to be in conflict - one saying you have to release a specific set, the other saying you must only release what's absolutely necessary and specifically requested
- Difficulty in explaining to a non-identity audience. The language has a great deal of meaning to us, but almost no meaning to people outside our sphere
    - Would like to start writing from the persona of the people who we are trying to influence to make a change, and then work back to the technical realities.
    - No federations on the call have created local materials to fill this gap. This would be useful, but REFEDS is probably too close to really write this.
    - Some of the problem starts with the term "entity category" - that makes sense in a SAML context, but if you try to explain this without the SAML context and understanding, it creates a gap.
    - Note that R&S is an attribute release agreement. Other entity categories are not that at all.
    - If we focus on trusted attribute release, maybe we call this as "controlled privacy"? Something to spin this appropriately for different audiences. The information you're talking about will be uniquely described based on your local nomenclature.
    - Before we get everyone on board with the right message, are we asking for the right thing to enable research collaboration? Federations are not interested in making a huge push until we are certain that R&S is in order. If there will be an R&S v2, then we need to finish that before we push farther (outside the COVID push)
    - Action: Nicole to take some of the language and talk through it with marketing people that would end up looking more like what we need for a broader audience
- Do people feel that the supporting documentation for fed ops is good enough?
    - The moment we give a specification freedom on choice, we should explain the options more clearly. "I support R&S and this is what I"m doing"
    - There is a difficulty in understanding what supporting R&S means. Also a difficulty in understanding each other's governing laws. In particular, R&S in areas not governed by GDPR. A blind "ok" to everyone causes concern.
        - Note that with institutions like The Ohio State, it is illegal to be under any legal jurisdiction (i.e., GDPR) outside of Ohio
    - Sometimes R&S is perceived as a blind agreement; that's not actually the case but perhaps the group we're covering is still too broad to understand that there are limitations? This is an exchange of trust between identity federations. Maybe we need to explain how this exchange of trust is happening?
    - The GDPR aspect is perhaps why R&S isn't as highly adopted as we like. If an SP is going to collaborate with a European researcher, then GDPR applies, which means there are the requirements to understand exactly what's being exchanged between the IdP and SP and why. That takes this outside of what something like R&S can solve.
    - What we've failed to express to the IdP is that it's not about you release attributes, it's about helping your researchers who are already at an SP use a more privacy preserving, secure model.
- Should the privacy statement be a requirement?
    - Of the SPs reviewed in the annual survey (about a quarter so far) only one is missing a privacy statement.
- Are there any issues with wording in the document itself?
    - The issue of affiliation has always been optional; if there's any ambiguity about that, that must be fixed.
    - If you're going to release affiliation, being consistent re: scoped affiliation vs affiliation would be helpful. There's confusion in the field.
        - Scoped affiliation is what gives us impersonation control; SAML was never intended to share just affiliation
    - Since R&S was created several years ago, we've created more things but have no way to use them in the spec. Example: assurance framework
        - In SAML, assurance is created to authN context and is orthogonal to attribute release
    - "Without administrative involvement" is being interpreted by some as meaning not ok to filter out these entities
    - Local campuses may not understand the implications of releasing R&S to a global community
    - The R&S specs don't explain the population you should release information about; is it the whole campus? The fact that there is more control here is lost in the spec.
- Identifiers may be the biggest driver towards a 2.0 version of the spec
    - One of the reasons R&S is what it is is that it was targeting applications that were broken because they only allow for a single identifier to identify an individual (the "one field for everything" approach). That's why ePPN was the chosen identifier, because it was traditionally a user-friendly identifier and so suitable for the one-size-fits-all use case, as long as you ignore reassignment. ePTID was added to address reassignment. Those applications failed miserably if they only had ePTID. Is this still an issue? Do we still need to support the one-size-fits-all approach? If we can chose a common, opaque identifier, with an understanding that you want the additional personalization, we can do that.
        - One opinion: time is right to do this, and R&S is the right place to do this first.
        - Second opinion: this is a question for the SP. Are they ready for R&S to move to a more opaque identifier? There's no incentive for an IdP to make their identifier better unless there's a demand by the SPs
        - Question: does all the IdP software support the new opaque identifiers?

Summary

- There is definitely enough interest to kick the entity category working group back into gear, with a mailing list, regular calls, etc.

Action items

- [x] Nicole Harris to start a document proposing some "jargon free" text for promoting R&S and some design work for a flyer. See: https://docs.google.com/document/d/13WtoZBZttepHXRbz4oYACI4AxlEO-W4T.
- [x] Heather Flanagan to create an editable version of the current spec so people can start proposing changes. See: https://docs.google.com/document/d/13G6aDjaeHD9SYB_er8cc_FOqbt7MD7cJZnxLqkG25P8/edit#heading=h.gi0bm8pkd4wl.
- [x] Nicole Harris to look into a proposal for more formal process for Federation Operators. See: Requirements for Federations Operators Assessing R&S.
- [x] Heather Flanagan to set up a mailing list for the R&S discussion and schedule the next call for the group. Subscribe at: https://lists.refeds.org/sympa/subscribe/rands.