

# 2020-12-17 R&S 2.0 Notes

## Attendees

- Heather Flanagan
- Nicole Harris
- Christos Kanellopoulos
- Hannah Short
- Jens Jensen
- Pål Axelsson
- David St Pierre Bantz
- Andrew Morgan
- David Groep
- Jiri Pavlik
- Alex Stuart
- Alan Buxey
- Michelle Williams
- Scott Cantor
- Miroslav Milinovi
- Licia Florio
- Marina Adomeit
- Michelle Williams

## Agenda

1. Poll: eduPersonScopedAffiliation as a required vs optional attribute
2. Identifier issue
  - a. One of the reasons R&S supports ePPN and ePTID 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.
      - **Based on the responses from the SPOG list, SPs do not handle identifier reassignment in any standardized manner. The level of automation in responding to this seems to depend entirely on the size of the SP and how big their IT budget is.**
3. Privacy Statements
  - a. Should R&S require privacy statements?
4. eduPersonAssurance
  - a. Should R&S encourage the release of eduPersonAssurance as a "SHOULD" value, in support of REFEDS Assurance Framework
5. Administrative involvement
  - a. How to be clearer about "Without administrative involvement"
  - b. How to be clearer that the campus does have control regarding what population they should release information about (e.g., whole campus? other?)
  - c. Should we write a framework for Federation Operators: [Requirements for Federations Operators Assessing R&S](#).
6. R&S as it relates to CoCo

## Notes

1. Poll: eduPersonScopedAffiliation as a required vs optional attribute
  - a. 41% Yes ; 24% No ; 35% Need more info (17 responses)
    - i. For Need more info, would like to know more about possible constraints and use cases. Would also like to know more about what the R&S SPs think of this.
    - ii. Is ePSA a useful attribute at all? Are optional attributes useful at all, or should we go purely towards required/not-required? Optional has been useful when trying to create information when information is missing otherwise. Worth noting that entitlement just isn't as commonly used as affiliation.
    - iii. For one of the R&S SPs represented on the call (CERN), they have no use of attributes that support authorization; they rely on IdPs for authentication only.
    - iv. Note that the assurance framework might also impact this, as affiliation is one of the only elements that provides "freshness" and it's the only thing the university can do for their users. They are the owners of that information.
    - v. The Scoped attribute offers an opportunity for a much more granular definition of the attribute.
    - vi. What about any potential burden on the IdP to generate this value? This will vary depending on the policies of the IdP in question, and how the IdP defines terms. The question of support burden if access fails and who the denied individual complains to is an open question.
    - vii. What if the values that would be required were restricted? If it were member vs not-member, that might result in a different answer regarding whether ePSA should be required. Definition of "member" might still be too vague (e.g., is a contractor a member? That's going to be up to the IdP)
  - b. Second poll: 81% yes, 6% No, 13% Need more info (16 responses)

2. Identifier issue - **postponed until we have more time**

- a. One of the reasons R&S supports ePPN and ePTID 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.
  - **Based on the responses from the SPOG list, SPs do not handle identifier reassignment in any standardized manner. The level of automation in responding to this seems to depend entirely on the size of the SP and how big their IT budget is.**

3. Privacy Statements

- a. Should R&S require privacy statements of SPs?
- b. 82% Yes; 6% No; 12% Need more info (17 responses)
  - i. What is the motivation to ask for this? Would it turn away SPs? Evidence so far is that it does to turn away SPs because about 95% of SPs in R&S already do this. Instead, this might encourage IdPs to support R&S because they might have greater trust in the SPs.
  - ii. Note we do have a good template, but we shouldn't make any requirements about content of a privacy statement

4. eduPersonAssurance

- a. Should R&S encourage the release of eduPersonAssurance as a "SHOULD" value, in support of REFEDS Assurance Framework?
- b. Value of "no assurance" would have to be include
- c. 31% Yes; 6% No; 38% Optional is bogus; require it or leave it out; 25% Need more info
  - i. Perhaps go back to this Assurance with how to indicate no value; it can't be required if it doesn't exist
  - ii. For the "No" vote, because it will massively reduce the number of IdPs that can/will release R&S as defined in 2.0
  - iii. General input is that this would be nice to have, but not MUST have to make decisions on their side; note that the NIH and other SPs are starting to require this information
  - iv. Assurance does imply liability, which may also complicate matters

5. Administrative involvement

- a. How to be clearer about "Without administrative involvement"
- b. How to be clearer that the campus does have control regarding what population they should release information about (e.g., whole campus? other?)
- c. Should we write a framework for Federation Operators: [Requirements for Federations Operators Assessing R&S](#).

6. R&S as it relates to CoCo