

2021-05-27 R&S 2.0 Notes

Attendees

- [Nicole Harris](#)
- [Pål Axelsson](#)
- [David St Pierre Bantz](#)
- [Jens Jensen - STFC UKRI](#)
- [Alex Stuart](#)
- [Björn Mattsson](#)
- [Christos Kanellopoulos](#)
- [Jii Pavlik](#)
- [Maarten Kremers](#)
- [Miroslav Milinovi](#)
- [Mischa Salle](#)
- [Andrew Morgan](#)
- [Nicolas Liampotis](#)
- [Scott Cantor](#)
- [Heather Flanagan](#)

Working Draft

- [Draft spec for R&S 2.0](#)

Agenda

1. Recap of consensus so far - **note that all changes will need to be validated via the consultation process**
 - a. The FAQ will be revised to offer clarity on the term "affiliation" (see [Research and Scholarship FAQ](#)) and editorial changes made to the spec to make it more clear (see new draft spec for updated structure)
 - b. eduPersonScopedAffiliation will become a required value
 - c. R&S will require privacy statements
 - d. subject-id should be listed as the new identifier
 - e. R&S 1.3 and R&S 2.0 can co-exist; no migration detail will be included in the spec itself.
 - f. ePPN and targeted ID to both be removed from R&S 2.0
 - g. Information on OIDC requirements will be moved to R&S 2.1 (after the OIDF OIDCre working group has formal documentation in this space)
 - h. eduPersonAssurance will be required, RAF recommended
 - i. We'll resolve the need for information on the origin organization by adding guidance for the use for eduPersonScopedAffiliation
 - j. DisplayName and Given/SN are required
2. Definition Statement for R&S.
3. Discussion of subject-id as source for origin organization (if not resolved on the list)
4. Solicitation of volunteers to focus on supporting documentation

Definition Statement for R&S

Problem statement: the current definition of who can be tagged with R&S ("Candidates for the Research and Scholarship (R&S) Category are Service Providers that are operated for the purpose of supporting research and scholarship interaction, collaboration or management, at least in part.") is being interpreted differently by different groups. Requirements that are not specifically in the specification are being applied by federations, creating an uneven use of the specification.

Areas questioned	Potential issues
Is R&S focused on the requirements of the service or the organisational type	Issues with not having a definition of an R&S / R&E organisation and the fact that most organisations have business arms to R&E structure
Should "commercial" services be allowed	No way to distinguish the nuance in commercial vs paid for
Should services that are contracted be allowed	Contracts are paid for things like collaborative wikis, having a contract does nothing to help the IdP administrator formulate an attribute release policy
Should "management" be dropped from the definition statement	
Is this about translation of real world trust (need to collaborate with other humans) into the spec	
Should services that are "operated for" IdPs be allowed (e.g. cloud infrastructure - geant.altassian.com vs wiki.geant.org)	Who is registering the entity, which challenges are there with registering cloud entities, how do you determine the difference between a private / community based approach vs just having an account in a commercial environment

Problem of only calling out e-journals in the existing spec	Better phrased as something like "Service Provider MUST be able to prove that it has a legitimate need for the personal data in the attribute bundle." (positive rather than negative entry requirement).
---	---

Notes

1. Recap of consensus so far - **note that all changes will need to be validated via the consultation process**
 - a. The FAQ will be revised to offer clarity on the term "affiliation" (see [Research and Scholarship FAQ](#)) and editorial changes made to the spec to make it more clear (see new draft spec for updated structure)
 - b. eduPersonScopedAffiliation will become a required value
 - c. R&S will require privacy statements
 - d. subject-id should be listed as the new identifier
 - e. R&S 1.3 and R&S 2.0 can co-exist; no migration detail will be included in the spec itself.
 - f. ePPN and targeted ID to both be removed from R&S 2.0
 - g. Information on OIDC requirements will be moved to R&S 2.1 (after the OIDF OIDCre working group has formal documentation in this space)
 - h. eduPersonAssurance will be required, RAF recommended
 - i. We'll resolve the need for information on the origin organization by adding guidance for the use for eduPersonScopedAffiliation
 - j. DisplayName and Given/SN are required
2. Definition Statement for R&S.
 - a. There is disagreement about the definition of R&S; the table captures some of the questions that have been posted about questions re: "Commercial", "Management, etc. We should be making positive statements about what should be included, not focus on what should be excluded.
 - b. One comment - do not want to have normative text in examples (which is something done in the second paragraph of the definition)
 - c. Focusing on the word "Commercial" - does this need to be relevant to the spec? We don't have a clear way to distinguish "commercial" from "academic". If GEANT buys a service from someone else for use by the GEANT community, is that a commercial service? What if the platform is used both by obvious 'commercial' entities (e.g., Oracle) and non-commercial entities (e.g., GEANT).
 - i. What are we trying to preserve by restricting who gets into R&S? attribute release of name, email, affiliation, non-targetedID. InCommon is considering requiring this for all participants. That may not meet the EU use cases.
 - ii. Coming back to why 'commercial' is a problem - is it because they make money off of secondary use of identities? Nominally, they shouldn't be doing that anyway, but we are assuming there are greater protections or something in place with R&S-qualifying entities. Could we include a statement just to that effect, that this data won't be used for any other purposes. "These won't be used outside of R&S space". But we shouldn't write what should be legally binding anyway.
 - iii. We're making R&S not about the service but about the organization. We're saying the organization must have some R&S-type characteristics, but we have no definition for that. Attempts to define "academia" have already failed a few times.
 - iv. Commercial was viewed as a problem because we were trying to soothe people's concerns that information would be released to bad actors, and by restricting it to our community would lessen the risk of bad actors. Also, the centrality of contracts - R&S was for those entities that did NOT require a contract. If there is a contract in place for the party releasing attributes, then any question of attribute release should be dealt with that way. R&S is about ad hoc federation.
 - v. There is a growing trend of getting services under contract that are not necessarily for just the campus users, but also apply to individuals outside the specific organization.
 - vi. What we want to do is release basic profile information - historically, we are comfortable doing that within the R&S community. After so much time, maybe the level of comfort has changed and expanded. Maybe we don't need to limit this to just the one community of interest. Let the fed op make the determination re: what their local community is comfortable with.
 - vii. Given the original definition, we were explicit about e-journals. What was the basic reasoning? You shouldn't need PII to authenticate to a publisher; they shouldn't need to know who the user is.
 - viii. This is about establishing a trust relationship with entities that legitimately need this bundle.
 - ix. Could this be alleviated by definition about what the SP is allowed to do with the data? e.g., "Only for the purposes for the R&S service involved". There will always be some subjective consideration for trust.
 - x. Hearing two things 1) strengthen saying how you can use the data and 2) strengthen the language around the federation must prove that the SP needs the data.
 - xi. Is R&S still necessary? It may be time to retire it entirely and just say this is the standard bundle to release. It could be a collaboration bundle and not targeted to R&S.
 - xii. Poll: Should we retire the term R&S in favor of a collaboration bundle? (Thus retiring the issue of defining what is research and scholarship) - Yes, 29%; No, 21%, Need more info, 50%
 1. This introduces a marketing problem; people are familiar with the term R&S
 2. Note that R&S 1.3 will stay, so we're introducing something of a new name regardless
 - xiii. Where is the implied trust here? on the IdP side, or on the SP side
 - xiv. Looking at the list of SPs currently tagged with R&S, it seems 10% are test entities.
 - xv. We need to work on this more, and make the trust model explicit. Is this basically bringing in aspects of CoCo?
 - xvi. R&S has always been different because it requires the fed ops to do something. Is that where we need to do more work, not in the spec itself?
 - xvii. Next steps: Heather and Nicole will work on some proposals, noting that there is work needed both on guidance for fed ops, and there is work to consider a radical rewrite.
 - d. **Note: the definition of "organizational attributes" differs between the Pseudonymous Entity Category and the R&S Entity Category. This will need to be addressed.**
3. Discussion of subject-id as source for origin organization (if not resolved on the list)
4. Solicitation of volunteers to focus on supporting documentation