Entity Category Consultation: Research and Scholarship 2

Background

The Research and Scholarship Entity Category has been in place for a number of years. It has become evident that there have been different implementation approaches to R&S within federations, which points to issues within the specification that need clarification. This issue has been discussed on various e-mail threads on the REFEDS mailing list and in a dedicated VC (2016-05-23 Attribute Coordination Call) on the issue.

In response to these issues, some proposed amendments to the current R&S text have been made and a new version is available at: R&S Clarification Proposal Clean Copy . These amendments are intended to be clarifications and should not represent any significant changes to the current meaning of the text. As such, REFEDS proposes that this be issued as V1.3 of R&S, rather than a new v2, which would require a separate category. The work in progress can be tracked at: R&S Clarification Proposal.

REFEDS Participants and the wider community are invited to consider the proposed amendments, make appropriate changes / challenges to the propose text and confirm that they are happy the amendments are a clarification and do not introduce new or different requirements.

Overview

This consultation was open from: **Tuesday 7th June 2016 - 17:00 CEST, 19th July 2016** and is now CLOSED.

Participants are invited to:

- to consider the proposed amendments,
- make appropriate changes / challenges to the propose text, and
- confirm that they are happy the amendments are a clarification and do not introduce new or different requirements.

The proposed text for the consultation is available at R&S Clarification Proposal Clean Copy. All comments should be made on: consultations@lists.refeds.org. The deadline for comments is 17:00 CEST 19th July 2016.

Changes Introduced

The table below captures the changes introduced in the new proposal in the broadest sense. Please review the full wording of the change proposal as well as considering this high level summary.

Section	Proposed Changes
Overview	No changes.
1.Definition	Added ways in which Identity Providers can support the entity category - this was previously silent.
2. Syntax	No changes.
3. Semantics	Minor wording improvements for clarity.
4. Registration Criteria	4.2 better definition of current publication practices. REMOVAL of 4.3.5 - requirement for requested attributes.
5. Attribute Bundle	Completely new section added to provide clarity on expectations around attribute release. PLEASE READ CAREFULLY. Potential to add non-SAML approaches added (but not expanded at this stage).
6. Service Provider Requirements	Expands on old section 6, splitting Identity Provider and Service Provider requirements, explaining in more detail and adding the SP example to this section. Provides clarity on support multiple different identifiers and name attributes as introduced in new section 5.
7. Identity Provider Requirements	Expands on old section 6, splitting Identity Provider and Service Provider requirements, explaining in more detail and adding the IdP example to this section. Provides clarity on support multiple different identifiers and name attributes as introduced in new section 5.
References	Two relevant references added - eduPerson and MACE-Dir SAML Attribute Profiles.

Responses

Please indicate your support or not for these changes and the following questions as indicated.

Name	Do you support this update to R&S?	Do you believe the text proposed is a clarification (v1 change) or represents a new version (v2)?
Nick Roy (Internet2)	Yes	Yes, it's a clarification
James Alan Basney	Yes	Yes
Lukas Hämmerle (SWITCH)	Yes	Yes, it is.
Rhys Smith (Jisc)	Yes	Clarification.
Kristof Bajnok (NIIF.hu)	Yes	A v2 would cause more practical problems than the ones the change might introduce, therefore I support keeping it v1.
Thomas Lenggenhager (SWITCH)	Yes	v1, it's a clarification
Scott Koranda (LIGO)	Yes	Clarification
Chris Phillips (CANARIE)	Yes	It's a clarification
Heath Marks (AAF)	Yes	Clarification
Peter Schober (Aconet)	Yes	Clarification
Jan Oppolzer (eduid.cz)	Yes	Clarification
Pål Axelsson (SWAMID)	Yes	Clarification
Maja Gorecka-Wolniewicz (PIONIER.Id)	Yes	Yes, it is.
Tom Scavo (Internet2)	Yes	It is a clarification
Ioannis Kakavas (GRNET)	Yes	Clarification
Arnout Terpstra (SURFnet)	Yes	Clarification
Maarten Kremers (SURFnet)	Yes	Clarification
Laura Paglione (ORCID)	Yes	Clarification
Wolfgang Pempe (DFN)	Yes	I agree with Kristof. Since 4.3.5 has been dropped (with good reason btw.) we have to modify our R&S compliance check for SPs

Change Proposals

Number	Current Text	Proposed Text / Query	Proposer	Action (please leave this column blank)
1	Section 7: ...release all required attributes in the bundle defined in Section 5 to all R&S Service Providers without administrative involvement by any party, either automatically or subject to user consent.	...release all required attributes in the bundle defined in Section 5 to all R&S Service Providers, either automatically or subject to user consent **or notification**, without administrative involvement by any party.	Thomas Lenggenhager	Clarity and should be accepted as a change. Add consent "or notification". ACTION: implement clarification as shown below. *"...release all required attributes in the bundle defined in Section 5 to all R&S Service Providers, either automatically or subject to user consent **or notification**, without administrative involvement by any party."*

2	1. Definition .. Example Service Providers may include (but are not limited to) collaborative tools and services such as wikis, blogs, project and grant management tools that require some personal information about users to work effectively. This Entity Category should not be used for access to licensed content such as e-journals.	1. Definition .. "Example Service Providers may include (but are not limited to) collaborative tools and services such as wikis, blogs, project, research portals, compute resources, data sets and grant management tools that require some personal information about users to work effectively. This Entity Category must not be used for access to any services where a fee or licence for access to the service is required (e.g. licensed content and fee for service such as: e-journals, commercial research services, commercial data sets, SaaS providers, cloud services)" OR This Entity Category must not be applied to any service where a subscription or other fee is charged directly to the end user for access to the service (e.g. e-journals, commercial research services, commercial data sets and cloud services not purchased and managed by an organization on behalf of its researchers and scholars).	Heath Marks (AAF)	This was intended to be about contract / non-contract and not to do with whether money changes hand. It was also supposed to protect people from people getting identity information where they need it. Charging out of scope. Clarify "this is not intended to be used by services where PII is NOT required" - this is quite tautological so perhaps not relevant. NO CHANGE PROPOSED.
3	1. Definition "Identity Providers may indicate support for Service Providers in this category (typically through self-assertion, though this is not required)"	"Identity Providers may" already states it is not required to indicate support. What is added by stating "typically through self-assertion, though this is not required". Is it relevant how an IdP got to announce its support?	Niels van Dijk	Parentheses are about the self-assertion not the may part, minor wording changes to make this clear. ACTION: implement clarification as shown below. *"Identity Providers may indicate support for Service Providers in this category (self-assertion is the typical approach used but this is not the only acceptable method)"*
4	4.1 The service enhances the research and scholarship activities of some subset of the registrar's user community.	If I read 4.1 to the letter, a service must serve at least 1 institution within its own federation. Does the home institution count? If not: what about an SP that only serves SPs outside of the home federation? This could be true for an SP that is setup only for the purpose of collaboration with institutions outside of the own federation (but within the VO) Possibly pre-eduGAIN text - may need some work	Niels van Dijk Scott Cantor	Remove the word "registrar" here. Does this put too much on the registering federation? Does this limit this if an IdP wants to flag this for an SP that is their own? ACTION: implement clarification as shown below: *"The service enhances the research and scholarship activities of some subset of the user community."*
5	5. Attribute Bundle "where shared user identifier is a persistent, non-reassigned, non-targeted identifier defined to be either of the following..."	By stating "either" is allowed (and having read section 6), an SP using #2 and NOT using #1 is allowed within R&S, right? Section 5 (Attribute Bundle) still isn't as clear as it could be. This section should be a pure definition of the R&S attribute bundle with no hint of what might or might not be required. The latter should be left to later sections. So, for example, when it says "required data elements" or "one optional data element" or "either (or both)", it is contaminating the definition with attribute release requirements (non-normative, no less), which should be relegated to section 7.	Niels van Dijk Tom Scavo	This is the ORCID use case. This is correct, yes. There is some work to be done here for v2. This could be changed, but it was felt that having the differences highlighted early in the text was better for comprehension. The EPPN issue will always call people problems - if a Dean / CEO demands a change...it is likely that this will happen. Is "in good faith" good enough for now. NO CHANGES PROPOSED.

6	7. An Identity Provider indicates support for the R&S Category by exhibiting the R&S entity attribute in its metadata. Such an Identity Provider MUST, for a significant subset of its user population, release all required attributes in the bundle defined in Section 5 to all R&S Service Providers without administrative involvement by any party, either automatically or subject to user consent.	Clarification needed that user consent is permitted. This currently implies user consent not allowed if read in a certain way	Thomas Lenggenhager	merge with point 1. Does consent then imply that the user has per-attribute consent and will still have access? Would notification be a better word? No, a user can be offered consent but they would have to accept that by refusing to release they may break something. it doesn't raise the bar for interoperability but this is the current scenario. There are known scenarios where the data simply doesn't exist in the IDM system. See June 12th thread on the consultation list. Perhaps add something to the FAQ on this issue that clarifies that we cannot guarantee you will get what you want. ACTION: implement an update to the FAQ.
7	Section 5 Attribute Bundles	In "5. Attribute Bundle" I note all attributes are worded as being single valued. Clearly this is not the case for some of these, for example for person name, email and affiliation. In an R&S scenario, a user may for example choose to use both their institutional email, as well as some private email, so releasing both would make sense.	Niels van Dijk	It was not felt that the text implied this. Grammatically, this cannot be added to the things that are definite attribute names as this is NOT what they are called, even where multi-values are possible. There may be scenarios where SPs do expect single-values but this is more of a general issue. Add this to the FAQ. ACTION: Implement an update to the FAQ.
8	Section 5 Attribute Bundle where *shared user identifier* is a persistent, non-reassigned, non-targeted identifier defined to be either of the following: 1. `eduPersonPrincipalName` (if non-reassigned) 2. `eduPersonPrincipalName` + `eduPersonTargetedID`	This can be read as if you release "eduPersonPrincipalName + eduPersonTargetedID" you have a reassignable eduPersonPrincipalName. Within SWAMID eduPersonTargetedID is a recommended minimal release and therefore every Service Provider get it. At the same time there is in SWAMID Assurance Profiles a policy that says that eduPersonPrincipalName is non-reassignable. I want to add a parenthesis in the second row that defines remove false interpretations. You can't use an available eduPersonTargetedID to interpret that this Identity Provider has reassingable eduPersonPrincipalName . *"2. `eduPersonPrincipalName` + `eduPersonTargetedID` (if reassigned or non-reassigned)"*	Pål Axelsson	This is not in the spec - it says you can do one or the other but if you reassign you can ONLY do 2. The FAQ already recommends sending both. ACTION: Implement an update to the FAQ.

9	4.3.3 The Service Provider provides an mdui: DisplayName and mdui:InformationURL in metadata	Should include: an english language version (xml:lang="en") mdui: InformationURL element MUST be provided in metadata (Why is this a URL and not a description? - probably a 2.0 thing to consider).	Tom Scavo	Is this an absolute requirement? If the use case doesn't require English then why force them. The content should be in the language of its target audience. Is English first a good thing to predict future scenarios where you do open up your needs? Makes more sense for DisplayName than InformationURL. ACTION: add wording clarification that english language is strongly recommended. *4.3.3 The Service Provider provides an mdui:DisplayName and mdui:InformationURL in metadata (an english language version xml: lang="en" is strongly recommended).*
10	Referring to 2 by Heath	We fully support the explicit notion of not having commercial SPs in this category, however we wonder whether non-commercial SPs that require a fee to cover their expenses should be allowed. Otherwise it will be very hard for some services to sustain themselves. Point for discussion?	Niels van Dijk Arnout Terpstra	See point 2 above.
11	Concerning comments 2 & 10,	I see no relationship between whether a service is pay-for and whether it's low (privacy) risk. Or, actually, I'd be **more** concerned about a service that had no visible means of financial support - "if you're not the customer, you're the product" and all that. In any case, this change could invalidate existing R&S entities, so is a v2 at best.	Andrew Cormack	See point 2 above.
12	"In possessing the Entity Category Attribute with the above value, a Service Provider claims that it will not use attributes for purposes that fall outside of the service definition."	What does "service definition" mean? Could this be clarified? (NH: it is intended to limited the use of the attributes to the parameters of the service presented to the registrar for assessment). (ANC: "service definition" is the definition of the service that the service provider provides. Would putting a capital on "Service" make it clearer that it's the same service we're talking about? And since IIRC the registrar isn't assessing the Service in any sense, I'd see it being the definition of the Service as presented to the users of the Service that matters. But I can't imagine that not being the same thing as what the registrar sees) In possessing the Entity Category Attribute with the above value, a Service Provider claims that it will not use attributes for purposes that fall outside of the service definition, *as presented at the time of registration to its users and referred to in metadata.*	Mikael Linden	ACTION: add wording clarification *"In possessing the Entity Category Attribute with the above value, a Service Provider claims that it will not use attributes for purposes that fall outside of the service definition, *as presented at the time of registration to its users and referred to in metadata.*"*

it i