Entity Category Consultation - Personalized Entity Category

This consultation **is closed as of Monday 18 October at 17:00 CEST**

Background

As part of the evolution of the Research & Scholarship Entity Category, the Entity Category Working Group offers a new entity category that focuses on the attributes being released rather than the type of organization requesting the attributes. This stands in place of developing an "R&S 2.0" specification. For more background and a detailed history of the discussions that lead to this draft, please see the Working Group wiki pages.

Overview

This consultation will be open from **Monday 20th September 2021 at 18:00 CEST to Monday 18 October at 17:00 CEST**

Participants are invited to:

- to consider the proposed entity category
- propose appropriate changes / challenges to the proposed text, and
- confirm that they are happy that this should be considered as a REFEDS Entity Category.

We would particularly look for feedback on the proposed attributes associated with a person's name. Given the known challenges in supporting naming conventions that are respectful to differing global standards we would seek to ensure that proposed attributes in this area serve the best possible outcome.

The document for the consultation is available as a pdf attachment. All comments should be made on: consultations@lists.refeds.org or added to the changelog below. Comments posted to other lists will not be included in the consultation review.

Change Log

comment #	Line /Reference #	Proposed Change or Query	Proposer / Affiliation	Action / Decision (please leave blank)
1	15 & elsewhere	I'm struggling to understand the use cases where there would be a "need" for personalization. Most of the time I hear about personalization to be a useability/user interface feature - we want to greet this individual by name once they have signed in. Would it be enough to say "I need my users to have a good experience, and personalizing their experience is a key component so I need these attributes"? I could even see an organization showing data that users respond better to being addressed by name. (a demonstration of the need?) I agree that a specific reason needs to be provided with specific information about how the attributes will be used. But, restricting this to "need" seems to me to be very much in the eyes of the beholder and a potential source of conflict.	Laura Paglione / SCG	One use case would be where there is a need for some (low) level of assurance that the person logging in is who they say they are. Also, where applications that require more information might want to get this from federation data rather than having to build more IAM infrastructure to collect this information directly. There are also use cases for non-pairwise identifiers that this will resolve. No change to the spec. There will be more about appropriate use cases in the supporting documentation.
2	29, 149, and elsewhere	Maybe I am not making the connection. Use of "personalized" seems like it could lead to confusion. The category is not a personalized attribute bundle, but is used to indicate a standard attribute bundle for personalization (line 122). Would suggest use of "personalization" (or something else) in the entity category definition instead of "personalized".	Mark Rank / Cirrus Identity	Personalization suggests only one of the use cases that this would support. We did consider "Onymous Entity Category" but it was poorly received by the organizer.
3	38-41	These lines require an SP to present the service definition to the users at the time they register with the service and that the service definition is referred to in metadata, I guess it is meant to part of `<mdui:InformationURL>`. However, these two requirements are not explicitly listed in the following chapter 'Registration Criteria'.	Thomas Lenggenhager / SWITCH	Text has been changed to: By asserting this Entity Category Attribute, 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 and will support this statement within their published Privacy Statement.
4	15, 49	The term "proven" concerns me a little. It seems to imply some kind of test or thorough process, and I'm not sure what that would look like. I'd suggest "justifiable" instead. Additionally, do you need to "prove" that you need all of the attributes in the bundle, or does one suffice?	Hannah Short / CERN	"Proven" is the term used by the GDPR. No change to the spec.

5	90, 89	Propose to move line 90 after line 81 as lines 82 - 89 solely refer to assurance whereas line 90 again applies to the whole attribute bundle. I do also wonder what "specific conditions" are. Are there examples? Double punctuation in line 89. Reference "REFEDSAF" (line 82) not in reference section. Do we need an (informative) statement, that the authentication assurance (SFA/MFA) is not covered by the EC?	Jule Ziegler / LRZ	Line 90 has been moved. We will add examples re: specific conditions in the supporting material. Double punctuation fixed. Will add the RAF reference. Adding a negative (stating what we do NOT do) in the spec is not good practice; we can add something to the supporting material if this becomes a frequent question.
6	Section 4.3 or 5.1.1	The entity category spec does not explicitly state that SPs must include the signalling defined in [SAML2SubjId] to indicate requirement for subject-id. It might make it easier for deployers if this were mentioned in either section 4.3 or 5.1.1 (alternatively it could go in the FAQ).	Alex Stuart / Jisc	If an SP requests pairwise in addition to subject-id, they are going to be in unspecified territory. No change to the spec.
7	49-52 and 98-101	Understanding the term 'data minimisation' in the sense of GDPR, we as federation operators would have to check whether the Service Provider actually needs an identifier (in SAML: subject-id) that enables global user tracking. As for our constituency, only a small number (<10) of initiatives or projects would fit into that category. For the overwhelming majority of Service Providers pairwise-id would be sufficient. So why don't leave it to the Service Providers to indicate the required identifier attribute via the Entity Attribute provided for this purpose?	Wolfgang Pempe / DFN	We agree that a small subset of SPs will actually need this entity category. If an SP wants personalized attributes and pairwise, that is not a logical requirement. No change to the spec.
8	53-61	Why not making a security contact mandatory - as a trust-buldling measure?	Wolfgang Pempe / DFN	This is outside the scope of this entity category. Requiring security contact is more appropriate as an eduGAIN policy or part of Baseline Expectations. No change to the spec.
9	68-70	Since some IdPs release attributes based on the Requested Attributes listed in SP metadata (rather than ECs), it might be helpful to **recommend** that Service Providers also tag the required attributes in their metadata, especially if an SP requires additional attributes .	Wolfgang Pempe / DFN	This is out of scope for the spec.
10	75, 98	"shared user identifier" Shared by whom? I think "user identifier" would suffice.	Meshna Koren / Elsevier	Agreed. Changed to "user identifier"
11				