Entity Category Consultation Anonymous Authorization

This Consultation is now CLOSED. A post consultation version of this proposal is now with the REFEDS Steering Committee for consideration.

Background

The Seamless Access Entity Categories and Attribute Bundles Working Group has approached REFEDS and asked if it will become the custodians of a proposed new Entity Category: "Anonymous Authorization". As per the REFEDS Consultations guidelines, the REFEDS Steering Committee has reviewed and accepted that this proposal meets the criteria for a REFEDS Consultation. We are therefore opening up a consultation period to invite comments and questions from the REFEDS Community.

Please note the proposed URI would be changed to a URI within the REFEDS domain space if this category is accepted.

Overview

This consultation was open from: **Monday 6th July 2020 at 17:00 CEST to Monday 31st August at 17:00 CEST**

Participants are invited to:

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

The document for the consultation is available as a Google doc in Suggestion mode or as a pdf attachment. All comments should be made on: consultations@lists.refeds.org, added to the google doc as a suggestion or added to the change log below. Comments posted to other lists will not be included in the consultation review.

Change Log

	Line Number / Reference	Proposed Change or Query	Proposer / Affiliation	Action / Decision (please leave blank)
01	general	As an editorial comment I'd suggest avoiding all the "For the purposes of this document" re-definitions or existing terms and instead referencing existing glossaries where possible. (No need to define what attributes, users, affiliations, etc. are here, IMO.) Supported in google doc comments	Peter Schober, ACOnet. Nicole Harris, GÉANT	Nicole Harris and Heather Flanagan will review the document and move the interpretive statements into supporting documents or an annex.
02	general	note that none of the 3 specs mentions NameIDs which are not attributes (and so do not fall under the local -- and somewhat circual -- definition of "user attributes": "a user attribute is *an* *attribute* that [...]"; my emphasis) but are personal data and suitable to identify the subject, in cooperation with the IDP, or even without, depending on the NameID format, nonetheless. So that seems like a significant omission	Peter Schober, ACOnet.	This may be resolved by removing the interpretive statements as noted in 01. Nicole Harris to verify with Peter Schober whether he wants an explicit statement or a removal of the definition of "user attribute."
03	lines 56, 57, general	As mentioned also with "Authentication Only" comment 04, I do not see the added value of bringing in bilateral agreements. It only weakens the spec, and there is no need because bilateral agreements can always be made.	Niels van Dijk, SURF	Given bilateral agreements can always happen, then specifying both bilateral and entity category is not helpful to either party. This should be removed.
04	line 85 - 87	"Organisation", especially if provided in the form of eduPersonScopedAffiliation, is in many cases already a very usefull and likely enough to manage authorization. What if the service has no need for additional roles/groups being provided via the currently required entitlement(s)? I would suggest to state either Organizational or Entitlement MUST be provided, where both MAY be provided	Niels van Dijk, SURF	Use cases outside common lib terms may find this useful. See also next item.

05	line 98-99	It is bad practice to send empty attribute statements, so how to combine the mandatory entitlement as per line 87 combined with the statement in these lines where it might be that no entitlement data is relevant to the SP? Also see above in (04)	Niels van Dijk, SURF	If there are no specific entitlements for an SP, then having entitlement as a requirement is a bad idea. Propose different text: The specification should note that the implementor should take care to only send entitlements that have a relationship to that SP. Use generic signaling where no specific entitlements are available.
06	line 96.3	Which schema does the memberOf attribute come from?	Niels van Dijk, SURF	Some directory services ship with this as part of the group of DNs; it is not a SAML attribute. It is something that could be passed as an entitlement. Suggest we add something to the supporting document about constructing an entitlement that may use memberOf or isMemberOf. Heather Flanagan to go back to the original group to get more detail on the use cases that resulted in these specific three items as examples. Why would common lib terms not serve the purpose of this entity category?
07	line 116	"when supported by their federation assert this in metadata" is that a MUST also? or perhaps a SHOULD?	Niels van Dijk, SURF	Suggest that instead we say that "any SP that uses this entity category must have a privacy statement URL." and point to an appropriate template.
08	line 155	Using normative wording in implementation guide conflics with normative wording in core document. I would suggest to remove RFC2119 wording from the implementation guide so it is clear that is not normative, but informative.	Niels van Dijk, SURF	Anything in the Annex should not contain normative wording.
09	line 34-35	do we have examples? i'm struggling to think of any collaboration tool that does not need personal data	Nicole Harris, GÉANT	Nicole and Heather to review this list.
10	line 42	use specification not document	Nicole Harris, GÉANT	Agreed.
11	line 39-41	the term user attribute is defined then only used in the definition. Why not use an existing term like personal data? I wouldn't associate user attribute with this definition	Nicole Harris, GÉANT	See comment 1.
12	Definitions section	for a clear and concise entity category, the definition section should only focus on the definition of the entity category itself. The many definitions are making the document quite lengthy. Why not simply refer to the definitions in eduPerson?	Nicole Harris, GÉANT	See comment 2.
13	General	either use the full terms for IdP or SP consistently or add these in brackets to the first instance then use the abbreviation consistently	Nicole Harris, GÉANT	Agreed.
14	General	why is this category styled as anonymous-authorization where as the pseudonymous one does not have the -authorization as part of the syntax?	Nicole Harris, GÉANT	Need to make sure the URIs are consistent.
15	line 67	don't use the word typically - i think this introduces lack of clarity as to how this gets tagged. It's either self asserted or not, and then there needs to be a process for not	Nicole Harris, GÉANT	Agreed.
16	line 71-72	i don't think this sentence is needed in a specification: ' They may need to consult with other departments within their organization to verify the relationship with the Service Provider." it doesn't have any bearing on the spec itself.	Nicole Harris, GÉANT	Agreed.
17	line 93-95	This is explanatory text that has no bearing on the specification itself, it is just a fact of identity approaches. Move as much explanatory text outside of the specification into supporting documents.	Nicole Harris, GÉANT	Agreed.
18	section 4 entitlement data	Entity categories are intended to facilitate scalable and preferably automated attribute release. eduPersonEntitlement, isMemberOf and MemberOf are attributes whose values should from a security perspective only should be presented to the intended services. Due to this the attribute release of these three attributes should be configured outside entity category release mechanism.	Pål Axelsson, Sunet	See response to comment 6.