Entity Category Consultation Authentication Only

This Consultation is now CLOSED. A post-consultation version of the 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: "Authentication Only". 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	Authentication Only: Seems to me such a category would be proliferating an anti-pattern, which would be actively harmful: Authentication at /any/ IDP at all, combined with no attributes and no user identity, doesn't mean anything and I'd question whether such services actually (should) exist. While some site licenses may be phrased in such a way (that anyone who can authenticate at the org's IDP is also considered authorised) the SP still performs authorisation based on the asserting IDP's entityID (lacking anything else to identify the "site" from) -- which is a clear anti-pattern: Organisations and SAML entityIDs do not map cleanly onto each other, i.e., certainly not 1:1. Some organisations have multiple IDPs (e.g. one per campus), in some regions a single IDP serves multiple, fully independent organisations (e.g. central IDP-style federations). Which is of course why scoped attributes have been created/used for such use-cases, so that you can authorise based on an (still not personally identifying) attribute's scope, e.g. *@univie.ac.at, without tying this to one specific entityID (or managing the entityIDs allow to assert that at each SP; instead the allowed scopes are managed in trustworthy federation metadata). Furthermore, the claim "to support completely anonymous, privacy-preserving single sign-on" is unattainable in SAML, IMO, as SAML protocol messages *always* contain technical identifiers of some sort that allow tracking of the subject in cooperation with the IDP. So this spec simply *cannot* promise "complete anonymity" as it cannot prevent the SP and IDP from collaborating in identifying the subject. (Only where that's impossible by design could one make such claims, but not with SAML today.) Based on the fact that "completely anonymous" is not possible with SAML (only pseudonymous), the names of the three proposed categories may also need to be reconsidered ("Authentication Only", "Anonymous Authorization", "Pseudonymous Authorization") since all three offer pseudonymity at most.	Peter Schober, ACOnet	
02	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.)	Peter Schober, ACOnet. Nicole Harris, GÉANT	

03	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.	
04	general	Entity categories are intended to facilitate scalable and preferably automated attribute release. To be able to do so, the specification must be clear and unambiguous, so the implementation, impact and risk of implementing/using an entity category is clear and unambiguous. This specification on one hand tries to signal limited exchange of attributes is requested, described by as its goal in lines 30 to 34. Yet at the same time the same specification consistently adds the statement that "bilateral agreements" may be in place to have broader release of attributes, like e.g. in lines 43-45. I would argue that scenarios where a bilateral agreement is in place always exist and hence does not need mentioning here. Taking that further, the addition of the statements on "bilateral agreements" throughout the specification in my option undermine the whole purpose of the entity category: Firstly, there is no way technical way to signal the difference between the "default configuration" and a broader set, other then to request additional attributes, which is rightfully prohibited by section 4 and 5 of this specification itself. How is the use of additional attributes intended to be signaled? If that actually means the IdP will have to negotiate with the SP, the scalability purpose of the entity category is defeated. How can the actual attributes being used be presented in a machine readable way? Also SPs claiming this entity category may be interpreted as 'privacy preserving' and 'GDPR friendly'. However with the addition of "bilateral agreements", this may actually be a false promise. Secondly if you are entering into a bilateral agreements anyway, you have no need for scalable attribute release as you are already, by definition, agreeing to specific attribute release on an per entity basis. More importantly, you have also gone beyond the purpose of this entity category as described in 30-34, as now you are clearly no longer want to "provide a completely privacy-preserving experience and do not require any user attributes". There is no possible way to both live up to the specification goal of a service wanting to "provid[e] a completely privacy-preserving experience and do not require any user attributes" and yet at the same requesting additional attributes in a bilateral agreement. Doing so breaks the fundamental premise of this entity category. If you do need additional attributes beyond the ones agreed upon in this specification, use another entity category, or agree on bilateral exchange without declaring this category, which is already a possibility today. To make this specification scalable, clear and unambiguous, I think all the references to "bilateral agreements" should be removed.	Niels van Dijk, SURF	
05	Line 54	Which "agreement" is being referred to here?	Niels van Dijk, SURF Nicole Harris, GÉANT	
06	Line 80-85	This statement (MUST NOT) is not consistent with lines 117 - 123 (SHOULD NOT). Please explain which is leading. 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	
07	Line 122	"Doing so sends conflicting messages" - I fully agree with that statement, and hence I do not understand how having this entity category but allowing "bilateral agreements" is not considered conflicting, whereas supporting multiple attribute categories is. Both result in unwanted attribute exchange and impact the usability and credibility of the entity category in a similar way.	Niels van Dijk, SURF	
08	Line 76	"when supported by their federation assert this in metadata" is that a MUST also? or perhaps a SHOULD?	Niels van Dijk, SURF	
09	Line 21	"RAEC" - I wouldn't create new terminology and specifically just new acronyms that will confuse people. Just call them entity categories - the "resource access" part doesn't add anything	Nicole Harris, GÉANT	
10	Line 72-74	it is not possible to use CoCo in scenarios where personal data is not being exchanged via attributes. If you really want something like this, require a privacy notice	Nicole Harris, GÉANT	
11	Annexes	Split annexes out of the specification document and add as supporting documents on wiki	Nicole Harris, GÉANT	
12	General	From an European GDPR perspective the goal of this entity category should be the default behaviour of an European IdP, i.e. no attributes should as standard be released if not defined by other entity categories, bilateral agreements or other agreed models. This entity category is otiose as this should be the default behaviour.	Pål Axelsson, Sunet	