Entity Category Consultation: Authentication Only

This Consultation is now CLOSED.

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.

Change Log

<table>
<thead>
<tr>
<th>Line Number / Reference</th>
<th>Proposed Change or Query</th>
<th>Proposer Affiliation</th>
<th>Action / Decision (please leave blank)</th>
</tr>
</thead>
<tbody>
<tr>
<td>01 general</td>
<td>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 entityID’s 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. <em>@univie.ac.at</em>, without tying this to one specific entityID (or managing the entityID’s 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.</td>
<td>Peter Schober, ACOnet</td>
<td></td>
</tr>
<tr>
<td>02 general</td>
<td>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.)</td>
<td>Peter Schober, ACOnet</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Nicola Harris, GÉANT</td>
<td></td>
</tr>
</tbody>
</table>
general note that none of the 3 specs mentions NameIDs which are not attributes (and so do not fall under the local -- and somewhat circular -- 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.

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.

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 "provide 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.

To make this specification scalable, clear and unambiguous, I think all the references to "bilateral agreements" should be removed.

Niels van Dijk, SURF.