2024-06-11 WG meeting

Present

- Alex Stuart
- Björn Mattsson
- Zacharias Törnblom
- Albert Wu
- Pål Axelsson

Notes

This was an ad hoc meeting convened during TNC24. We started by recapping the discussion at REFEDS with Leif. The original spec in the google doc is a thought experiment about how discovery could work more generally, with different trust profiles for applications that allow certain IdPs to provision admin users, other IdPs to provision regular users etc. However, we're now trying to focus on a smaller problem, mainly focussed around SeamlessAccess' requirements.

We discussed having a small controlled vocabulary of values for md_source. INCOMMON, SWAMID, eduGAIN... so that it's no implementation-specific. However, no consensus was reached on who would manage that vocabulary (REFEDS WG, REFEDS Steering Committee, a third party).

Q: are we back to only defining profiles?

A: No. Zacharias gave us a steer that he would not consider this work done until there was full filtering mechanism, which included the facility to exclude specific IdPs (by entityID) which were known not to work.

There was confirmation that we would look at filter on the 4 in the original google doc:

1. entityID
2. registrationAuthority (There was some concern that SP operators would not recognise registrationAuthority. However, the group noted that SP operators would typically be writing rules in collaboration with the federation operator or Seamless, so would get support on this)
3. md_source (with the caveats above)
4. entity category

The discussion turned to defining the behaviour of metadata consumers:

- by default, display all
- if there is data in the entity attribute, hide all and each of the include rules adds entities to the list
- exclude rules happen later

TODO: check whether default behaviour of SeamlessAccess is to display all IdPs which do not have hide-from-discovery.

There was much discussion about semantics of "strict".

- if this keyword is present, then the include rules are the only entities which are show. No others are displayed.
- If this keyword is absent, then the include rules do not exclude IdPs. IdPs which are not selected are displayed with a warning box. For example, we did not discuss the effect of strict on exclude rules (presumably if the entity would have been given a warning by the rules, it would totally excluded by strict)

TODO: InCommon said prefer R&S, they would want IdPs which do not support R&S to be given the warning. However, IdPs show entity category support & therefor we need to expand the list of 4 filter categories to include entity category support.

Finally, we discussed SeamlessAccess' smart button, which allows the SP to integrate the login button and to specify rules. If this button is used, it would take precedence over metadata.

TODO: we did not discuss behaviour if the button is used without any filtering rules. Would it then take filtering rules from metadata?

Use cases

1. eduGAIN Access Check. This SP is used to check the attribute release from IdPs. The IdPs may still be in a testing phase and marked with hide-from-discovery so the SP wants to be able to specify that it wants to see IdPs with hide-from-discovery and without hide-from-discovery
2. An SP wishes to exclude IdPs by entityID that it knows has an interoperability issue (note: there must be a mechanism for the IdP to get back into the allow list)