Community tagging - GAP analysis

This short document will provide an initial consideration of the implemented Community Tagging Access tool, and discuss the potential future improvements of the tool.

Introduction

The initial work started as a there was a need identified that research communities have a need to express and potentially share certain trust marks on IdPs and SPs. These trust marks may differ from existing trust marks issued by identity federations, or may be put in to compliment existing ones, in case the federation operator does not support these, like e.g. in the case of SIRTFI.

In order to achieve this, a technical solution is necessary that matches the requirements as described by the SIRTFI community and investigates usability of the solution for research communities and the impact of the solution of Identity federations.

Requirements

The following are the minimal set of requirements:
- Web portal (web application)
- Able to handle metadata
- Capable to add entity category (self assertion of the entity's owner)
- Comprehensive logs of all actions taken

These requirements are met. The tool selected (i.e. two tools working in tandem) is capable of fulfilling these requirements. The tool consists of Jagger[1] and Access Check[2] working together.

Jagger is used for the following purposes:
- Metadata handling
- Actions based on user rights discrimination (user vs. admin)
- Managing entity categories (including creating and assigning)
- Exporting/importing/changing metadata

Access Check supports "Invitation flow", where entity owner can select its entity, which will subsequently create credentials to access Jagger.

---

[1] http://jagger.heanet.ie/
[2] https://access-check.edugain.org/

Additional requirements - GAP analysis

During the initial rounds of discussion regarding the desired features, some additional requirements were mentioned. These are:
- The tool is an SP in eduGAIN
- Excluding the Sirtfi capable federations
- Consuming eduGAIN metadata
- Extended "tagging" decision process
- Signing of the metadata

Not all of these requirements present a technical problems, because some of these requirements require organisational solutions (i.e. rules and agreements, or policies). The initial mandate of the work required a minimal viable product (MVP) that can later be extended, if necessary, to encompass the additional requirements. In the next paragraph, we will consider the additional requirements.
- The tool is an SP in eduGAIN - This depends on how the tool should be deployed and used, i.e. is it a general tool that is run on behalf of the academic community, or it is run by a particular community for their own needs. In the former case, there is a need to consider decision making process, i.e. how the tagging will be conducted. Also, the potential introduction of new entities will require an agreement on their meaning and usage. These considerations were outside of scope of the initial work.
- Excluding the Sirtfi capable federations - This requirement is related to the one above, i.e. whether the whole of eduGAIN will be considered or not. At the moment, there is no automated way of knowing whether the federation is Sirtfi capable or not. This would also be a consideration for other entity categories.
- Consuming eduGAIN metadata - See the first point
- Extended "tagging" decision process - This point considers how the tagging will be decided, i.e. who should execute the actual tagging. This could be the owner of the tool, or admin after the owner of the tool has initiated the process. Also, the decision making process may involve multiple people. This process must be transparent, but its structure and procedural steps were outside of scope for this phase of work.
- Signing of the metadata - This point involves both technical and procedural considerations. The actual signing using a key is supported by the tool (Jagger), however, the implications of signing were not considered. These include the decision processes described above, and the "key handling", i.e. what is the source of trust for this action ("who owns the key").

Conclusion

This work served to provide a solution for ad-hoc application of the entity categories. Currently, the desire was expressed to further help with the adoption of Sirtfi, and the work in this activity has set out to provide technical means to achieve so. As presented, the potential future work may consider the additional identified requirements, but the current version of the tool is not a hindrance for their successful implementation.