Contribution ID: **72** Type: **Full presentation: long (25 mins.)**

Efficient AAI for research communities using the IdP/SP Proxy

Tuesday, 3 November 2020 11:35 (20 minutes)

Lots of Authentication the Authorization Infrastructures (AAI) are adopting AARC blueprint architecture which relies heavily on the IdP/SP Proxy. This model was verified in the real deployments and surely there are no doubts about its technical feasibility. Main advantages like attributes harmonization, protocol translation or providing a single identifier regardless of authentication method are well known and used in most Proxies. Over the time of operating a proxy solution, we have realized the proxy concept offers much more. Therefore, we have tried to develop additional features on top of this standard set to either make the whole AAI more efficient or to improve end-user experience with the AAI workflows.

Examples of such features are:

"Automatic account validity extension"
On every user access Proxy updates the "last access"timestamp of corresponding digital identity of the user in the backend IAM system. Users can have registered multiple identities, therefore the IAM system knows which digital identity is used by the user and can do automatic account validity extension based on that information.

"Delegated authorization"
Proprietary software or software which is not capable to do the authorization can delegate it to the Proxy. Proxy checks every access to the service and compares it with data stored in the IAM system to determine whether the user is allowed to access the service. If the user is denied Proxy shows information on how the user can get access.

"Acceptable Usage Policy management"
When the user accesses the service through the Proxy the check-in the backend IAM system is done to verify whether the user accepted the latest version of AUP. If not, then the user needs to accept the current version which is presented by Proxy.

"Multi-factor authentication"
Some services can be in need to have the user reliably authenticated. Proxy can request multi-factor authentication from upstream IdP or can provide it itself in case the upstream IdP is not able to. All the data about the authentication can be delivered to the service, which can decide if the used mechanism satisfies given needs.

"Manually assigned affiliations"
External sources often do not provide all the information service might use. For these purposes, Proxy is able to generate this additional information based on the data in the IAM system. Usually, there is a trusted user who is providing the missing data. For example a trusted representative of an organization can manually assign affiliation related to the organization to any user.

"Identity provider enforcement requested by services"
Sometimes, a service might require having an account in a specific organization or can be offered only to users coming from a specific identity provider. Proxy has a mechanism using which the service can enforce an user to use the specific identity provider for login.

In our presentation, we will explain in detail how the features work and what is their added value. The use-cases for the individual feature demonstration will be taken from production environments of ELIXIR, BBMRI and CESNET AAIs, where the features are already deployed and used.

Primary authors: LICEHAMMER, Slavek (CESNET); BUCIK, Dominik Frantisek (Masaryk University); PROCHAZKA, Michal (CESNET)

Presenter: LICEHAMMER, Slavek (CESNET)

Session Classification: Authentication-Authorisation solutions - Part 1