Contribution ID: **23** Type: **Presentation short (15 min)**

Identity management beyond a simple VO management

Tuesday, 19 October 2021 11:30 (15 minutes)

Federated authentication and authorization management represented by AARC Blueprint Architecture is naturally stressing out the importance of the part represented by the proxy component. Indeed, the proxy component has an essential role because it handles the connection to the home IdP or other authentication sources and processes all the attributes, which are consequently passed downstream.

Another crucial part of AARC Blueprint Architecture is an identity management system (IdM). Its role is sometimes perceived only as a tool for managing virtual organizations (VO) and groups. That is a logical first step when building new authentication and authorization infrastructure (AAI). Having the option to enrol new users and manage them in VOs and groups is often enough to support basic use-cases for AAI. But in reality, the role of IdM is much broader and utilizing its whole range enables pushing capabilities of AAI to an entirely new level.

The role of IdM is to provide storage and a centralized view of all identity-related data. It can also ensure that relevant data is provisioned (and deprovisioned) to any services that need them. Proxy is only one from many components that are governed by the IdM system. There are other systems and services where user accounts have to be created and maintained even though they do not access them using federated authentication through proxy. Good examples are directories services or mailing lists.

IdM is not only about provisioning but also about importing data from other sources. Therefore the IdM system can be used as a central component that gathers data from all relevant authorities, including data self-provided by users (e.g. during registration), processes them, applies policies, and then is able to provision them to targets. Furthermore, it maintains consistency among all the connected systems during the whole user-life cycle.

Except for the automated processes described before, IdM enables managing attributes, groups, roles and other entitlements. People having the manager role can decide who will be authorized to which service and configure other attributes to fine-tune authorization rules and properties of managed accounts. Then the automatic process of IdM takes over and makes sure the configuration is provisioned to proper targets.

This presentation will demonstrate a wide range of IdM features using the IdM system Perun, which is quite a known tool for federated identity management. The features will be explained on real-world use-cases gathered from existing instances of Perun and communities using it, like EGI, ELIXIR, BBMRI-ERIC or Czech national e-Infrastructure.

Speaker info: https://www.muni.cz/en/people/255920-slavek-licehammer

Most suitable track

Collaborating across boundaries

By submitting my abstract, I agree that my personal data is being stored in accordance to conference Privacy Policy

Primary author: LICEHAMMER, Slavek (CESNET)

Presenter: LICEHAMMER, Slavek (CESNET)

Session Classification: Collaboration Accross Boundaries - Presentations

Track Classification: Collaboration Accross Boundaries