MetaCentrum

CESNET

Perun—Future Generation Identity Management

M. Procházka, Z. Sebestianová, S. Licehammer, P. Zlámal, V. Mach, M. Šťava, et al.

CESNET, a. l. e., Prague,
Masaryk University, Brno

User Management Challenges

Centralized solutions introduce single points of failure. Management of large infrastructures requires a single place to define all the characteristics of the environment. Such arrangements, however may lead to decreased performance and introduce single points of failure. We need to seek better ways how to allow administrators to manage the information centrally yet retain a sufficient level of fault-tolerance.

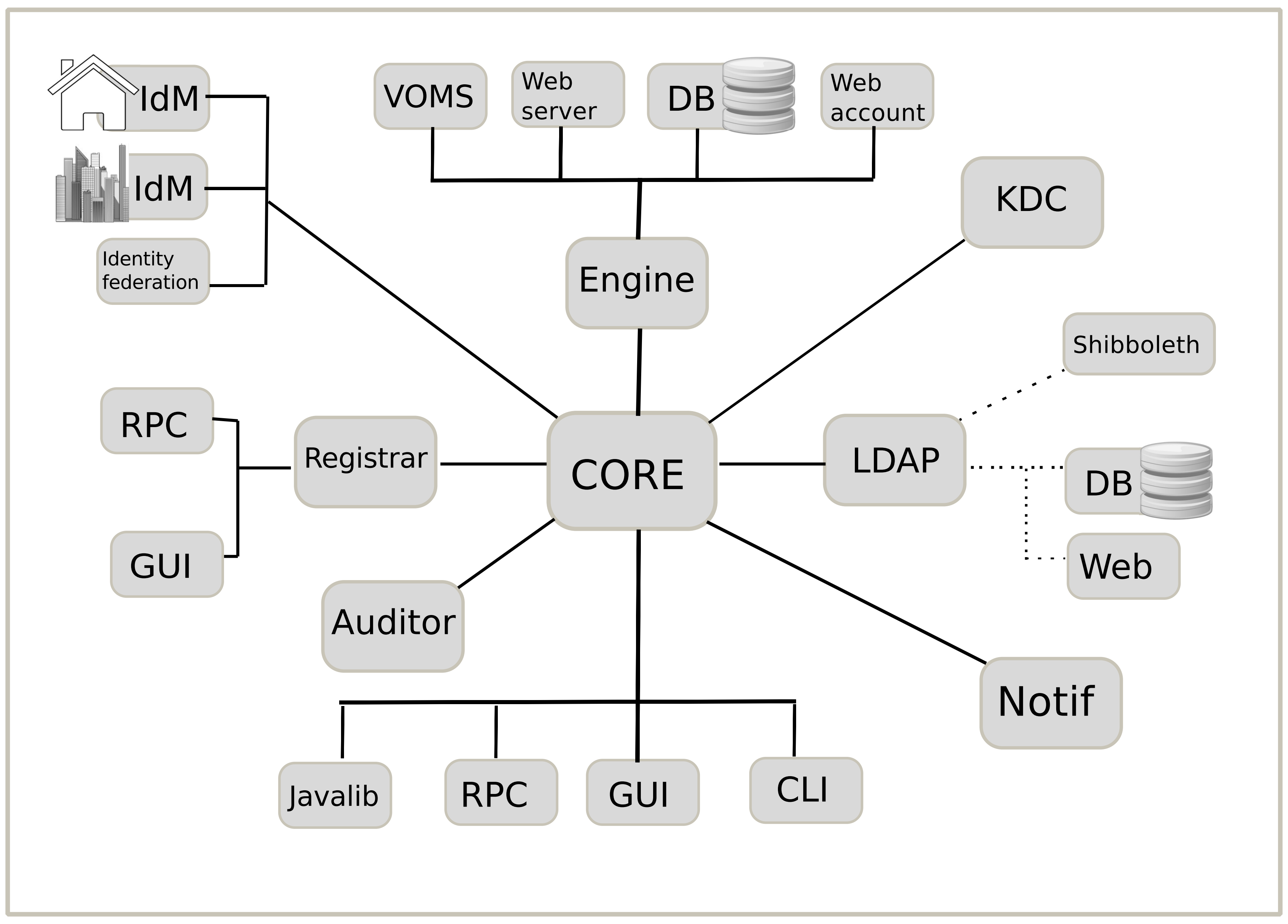
Users need to utilize multiple identities/credentials. Current users often have multiple identities that they want to combine while accessing end services. A common example is possession of multiple X.509 certificates combined with an account in an identity federation.

Difficult service integration. Integration of identity management services requires changes on the side of the end services and/or introducing new services to provide additional support. For instance, when management Unix accounts is moved to LDAP, every single machine in the infrastructure has to be reconfigured properly, which is quite expensive.

Missing for management for virtual organization. The concept of virtual organizations become an inherent part of current Grid environments. However, only few identity management systems today make it possible for users to define and maintain their VOs that are composed of users registered with the identity management system. In order to provide full support for VO it is also inevitable to mediate other features, like negotiations with resource/infrastructure providers.

Identity Management in Czech NGI

In order to manage users in the Czech NGI we have been developing own solution for user management called *Perun*. The system was designed to address the challenges of current user management systems and provide scalable way to maintain identities across thousands machines and services. The Perun system is deployed as a technical pilot in the the Czech NGI.



Perun architecture

Current deployment

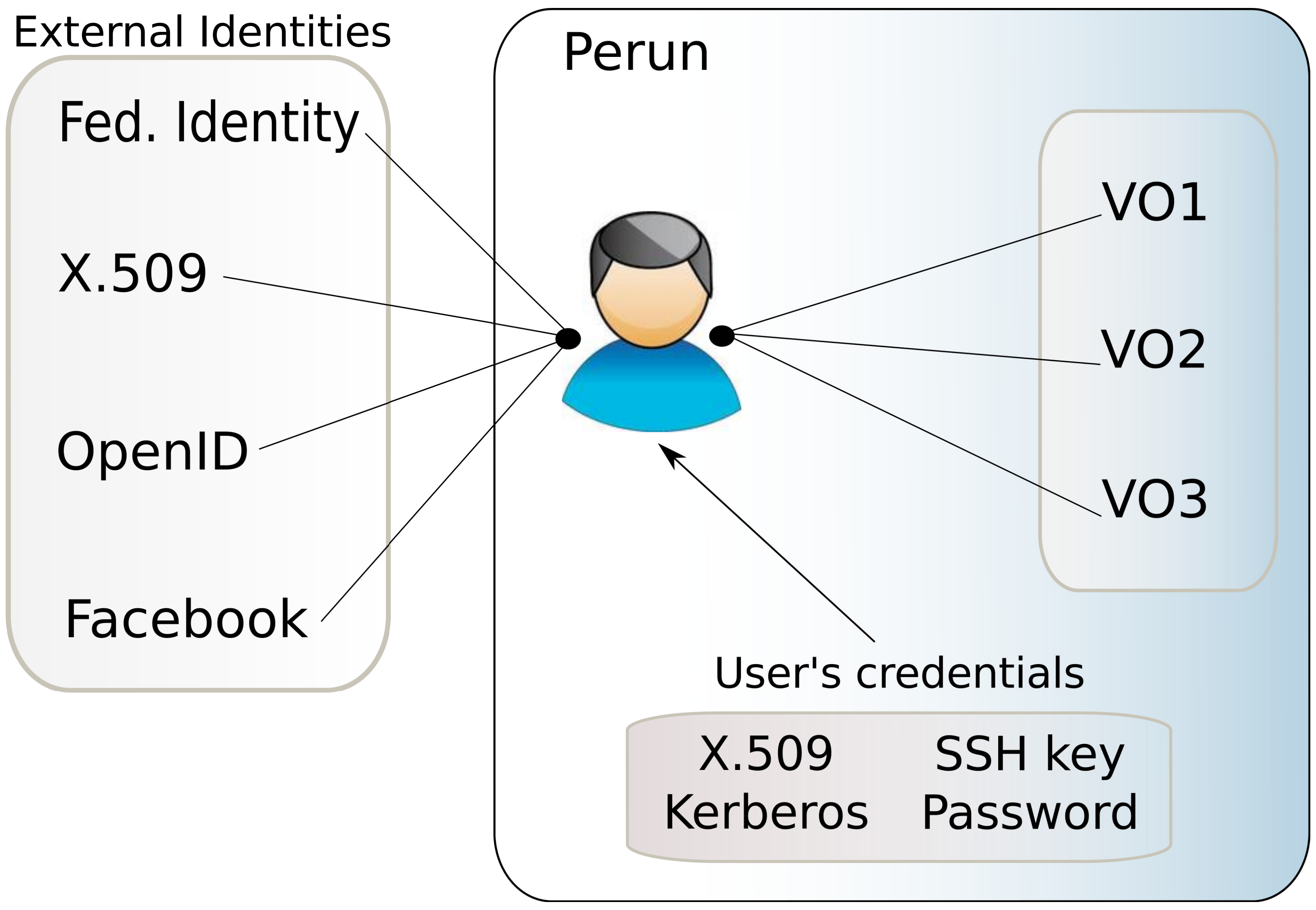
- Major part of Czech NGI switched to Perun, including management of computing clusters, storage facilities and other services (i.e. videoconferencing).
- Managing **158** different facilities, **1135** hosts, **1838** users and **14** VOs (including EGI ones).
- Several interfaces available, including Web GUI, REST, CLI, Perl and Java libraries, and LDAP.

Basic Principles of Perun

- Perun introduces no on-line dependency on centralized servers. Information about users is delivered to the end services which make all decisions locally.
- Perun is flexible enough to provide configurations for any end services (i.e. passwd files, LDAP ldif files, VOMS admin recipes, . . .). Therefore, it is easy to integrate any new service with Perun.
- The end services are only contacted by Perun on changes, i.e. when something changed in the users' information. Perun utilizes a push model to deliver the information.
- Only simple connectors are needed to be deployed on the end services, which provide the interface to Perun.

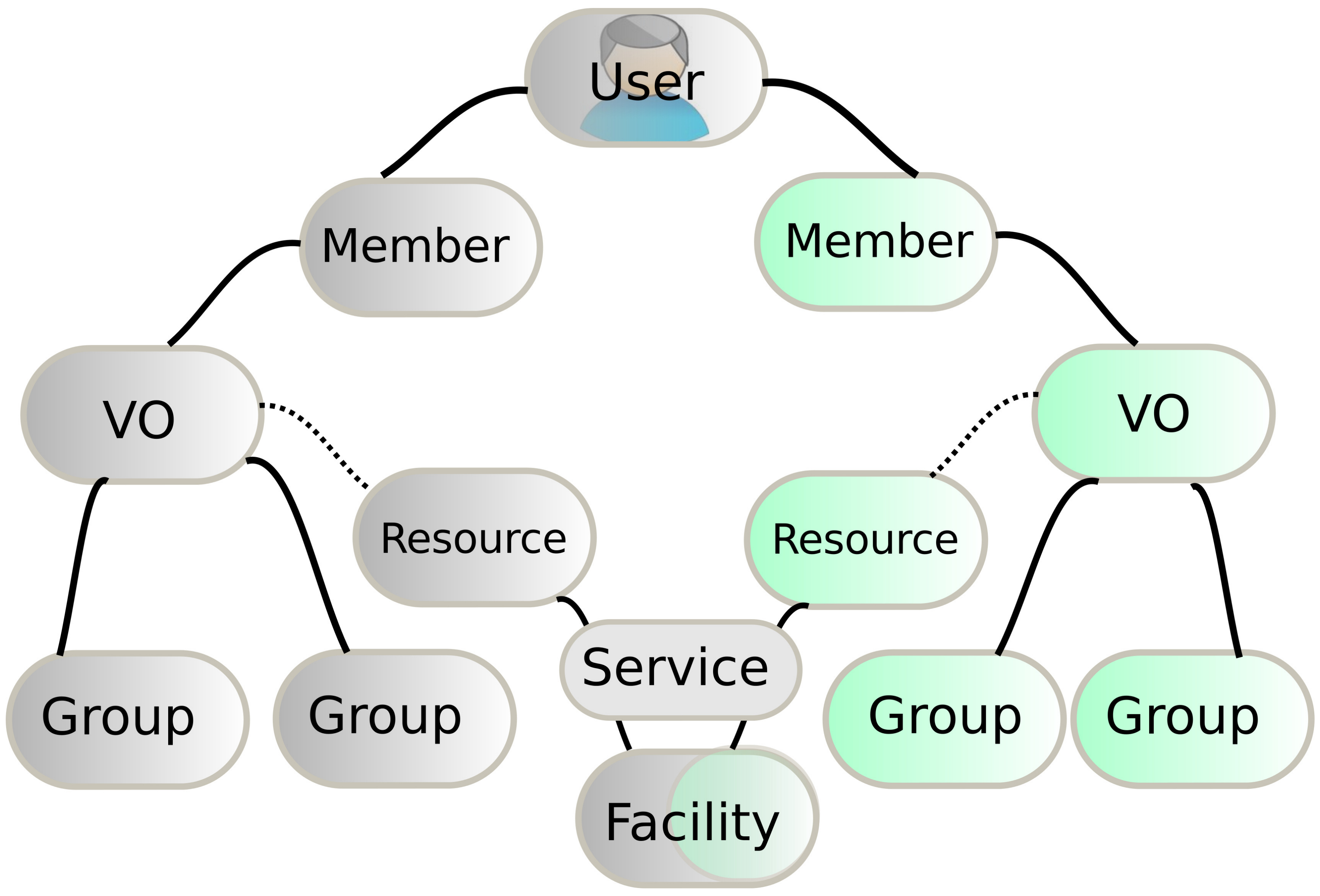
Multiple Identities

Various user's external identities can be mapped to the user in the Perun database. The design of Perun foresees users possessing and using multiple credentials based on the type of the end services.



VO Management

Management of virtual services is an inherent part of Perun design. Users can establish their virtual organizations and maintain users' membership. Perun also provides methods how service providers and VO operators can establish mutual *contracts*.



http://metacentrum.cz
meta@cesnet.cz

MetaCentrum project is supported by research intent "Optical Network of National Research and Its New Applications" (MŠM 6383917201) and partially by project "Vzdělávání akademických pracovníků v oblasti eInfrastruktur (CZ.1.07/2.3.00/09.0074)"