Modern Approach for User and Service Management

Michal Procházka

CESNET

Czech Republic

Motivation

- Users want to access valuable services
- Ideally using one digital identity

vs.

- Service providers need to know the user
  - Accounting
  - Restricted access

vs.

- Costs of maintaining users' digital identity

- Like Google services but in large heterogeneous area

Insert Org Logo
in Master slide

Approach

- Necessity: provide users with digital identity (IdM)

- Convince all service providers to use single authN/authZ framework (e.g. all have to accept Google users) – **this is not possible**

or

- Having a system which can manage
  - Users from different sources
  - Groups from different sources
  - Access to various services

Perun

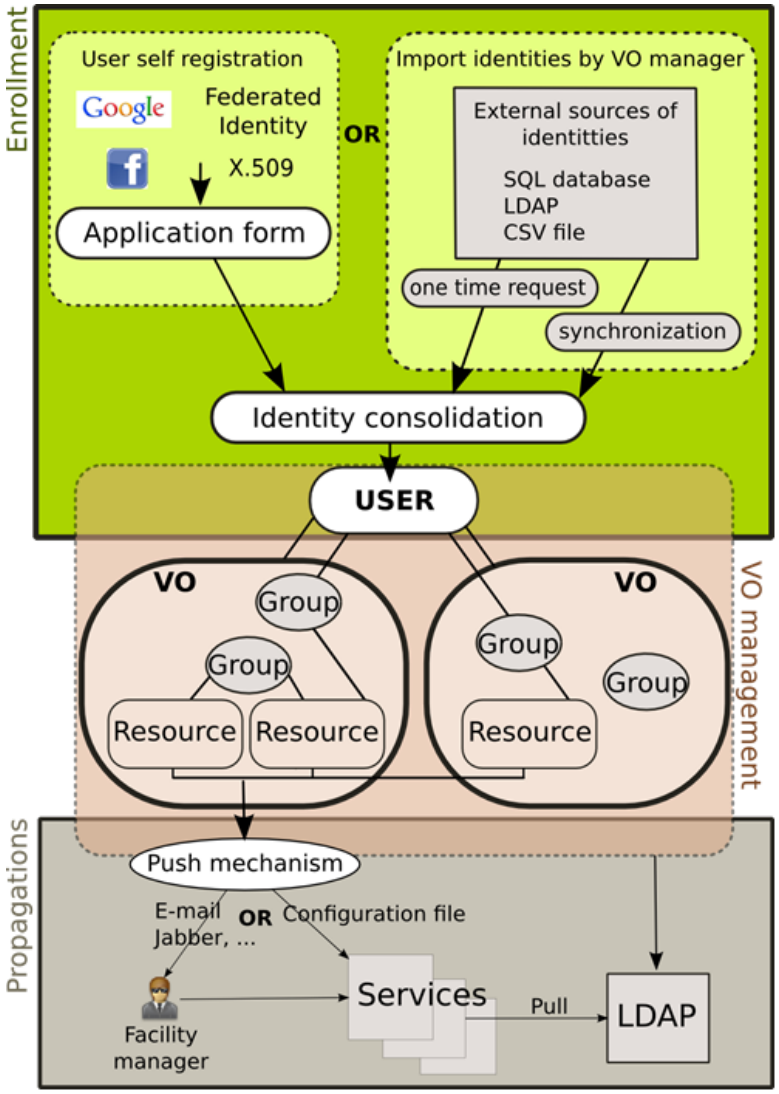
Insert Org Logo
in Master slide

What can be managed?

- Virtual organizations
- Users from different sources
- Local or external groups
- Resources
- Access to the services
- Application forms
- Attributes

Insert Org Logo
in Master slide

User flow schema



Insert Org Logo in Master slide

User management

- User can have several external identities
  - Federated identities, X.509 certificates, social identities (Google, Facebook, …), SSH keys, local accounts in DB/LDAP, …
  - Identity consolidation – connect external identities
  - Perun does not store users' passwords, private keys, ...
- Users' enrollments
  - Each VO can define its own application form with various requirements on the applicant
  - Pre-filled information from external identity management systems
- Service users

Insert Org Logo
in Master slide

VO and group management

- Built-in support for virtual organizations (VO)
  - Virtual organization = group with defined membership rules providing services to the users
  - Configurable application form
  - Delegation of rights to the end users
  - Access management for resources
- Group management
  - Configurable application form (special groups within the VO)
  - Group manager role
  - Automatic synchronization with external systems
  - Support for VOOT protocol (connect with other systems)

Insert Org Logo
in Master slide

Access management

- Resources are assigned to the VOs
- Configuration of access to the services
  - E.g. unix accounts, access to NFS storage systems, radius ACLs, mailing lists, ACLs for web applications (e.g. wikis)
- How they are technically configured?
  - Push mechanism
    - Omit online queries
    - Pushing only on change
    - Pushing in service required format
  - Various APIs
    - LDAP interface
    - REST JSON

Insert Org Logo
in Master slide

Current deployments

- South African National Grid Infrastructure (sagrid)
  - Management of the users and resources
- GARR's CloudIdP
  - User management
- Support for eduroam and identity federation in Malaysia
  - User and group management
- EGI fedCloud
  - User and group management
- Czech national e-Infrastructure
  - Manages whole Czech national grid infrastructure (users, resources)
  - Manages major part of the Czech e-Infrastructure

Insert Org Logo
in Master slide

Where we can help?

- eduroam deployment
  - Enable eduroam for institutions without proper IdM
  - All-in-one package
  - Minimal requirements on hardware and human resources
  - Does not require IT experts
- Identity federations
  - Provides identity provider for institution without proper IdM
  - Provides attribute authority for research projects
  - All-in-one package
  - IdP opens gates to the various services around the world (electronic books, Science Gateways, foodle, …)

Insert Org Logo
in Master slide

Economic benefits

- Reduce costs on IT infrastructure
  - Reasonable hardware requirements
  - All-in-one solution, no need to support several different systems
- Does not require a lot of IT experts
  - 1-2 persons who are Perun admins, all other management work is delegated to the end users
- Delegating rights to the end users => IT staff only do what they have to do
- Allows organization to connect to the international projects like eduroam, identity federation => valuable services for users, prestige for the organization

Insert Org Logo
in Master slide

Some statistics

- Perun instance at CESNET (Czech e-Infrastructure)
- In production since autumn 2012
- >3000 registered users from all around the World
- Manages access to ~1800 services
- >110 virtual organizations (national, international)

Insert Org Logo
in Master slide

Conclusion

- Perun is open source project hosted on GitHub http://github.com/CESNET/perun
- Maintained by CESNET and Institute of Computer Science Masaryk university
- Detailed information, manuals and use-cases available on web pages http://perun.cesnet.cz
- CHAIN-REDS can support local deployment for eduroam and identity federation needs
- For any questions just write to perun@cesnet.cz

Insert Org Logo
in Master slide

Thank you for your attention

http://perun.cesnet.cz

michalp@ics.muni.cz

Insert Org Logo
in Master slide

