Identity management beyond a simple VO management

EGI Conference 2021

Slávek Licehammer
slavek@ics.muni.cz

AAI

- Access management
  - IdP/SP proxy
- **Identity management**
  - **Perun IdM** 
  - COmanage

Perun

- Set of tools for Identity and access management
- Developed by CESNET and Masaryk University
  - https://perun-aai.org/
- Designed for academic distributed environment
- Customizable, focus on integration options
- Perun IdM is part of EGI Check-in service
- Perun in also deployed in ELIXIR AAI, BBMRI-ERIC AAI, GEANT eduTEAMS, Czech national e-infrastructure, ...

IdM in general

- Users
- Entitlements (VO, groups, ...)
- Attributes
- Services
  - Access control
  - Provisioning and deprovisioning
- Policies (life-cycles, attribute value policies)
- Privilege delegation
- Centralized view on identity data

Typical use-cases for IdM

- VO management
  - Registration
  - Group management
- Account linking
- User-profile
- Providing data for access management

Advanced use-cases with Perun

Account linking

- User can possess multiple identities
- Perun is able to link/unlink those identities
  - Interactive process
- Heuristic search during registration
- User can access Perun with any of linked identity
- Identities can be transferred to end services
- Levels of assurance can be derived from identities

Provisioning

- Providing identity-related data to services based on rules in IdM
  - Deprovisioning
- Necessity for some services
  - Persistent data, service without direct user interaction, services requiring up-to-date user info
- Focus on data consistency
- Perun support custom provisioning engine
- Privacy preserving design

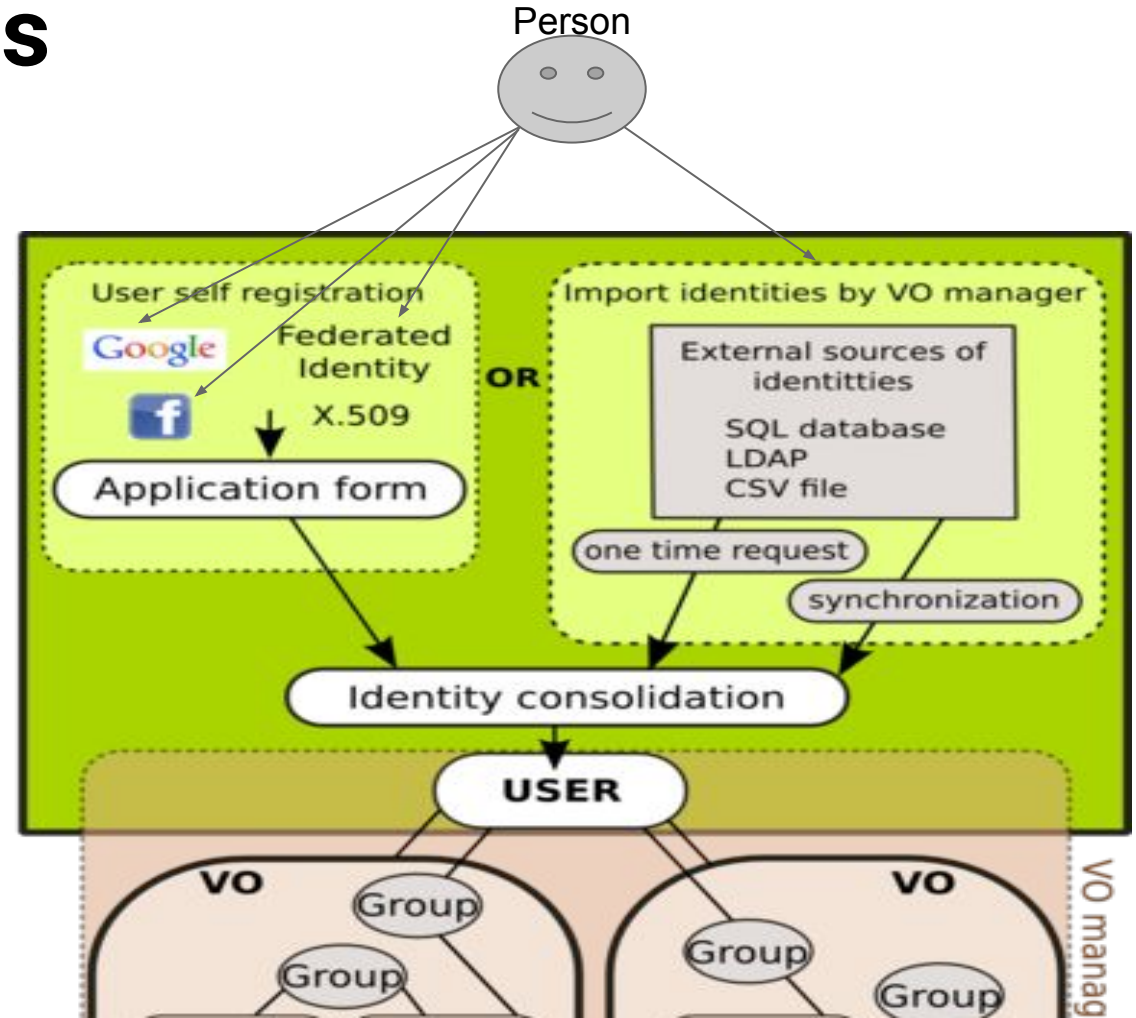
Registrations

- Customizable registration forms
- Part of life-cycle (registration, expiration, renewal)
- Customizable notifications
- Group registration
  - Can be part of service access request
- Approval by designated manager

Synchronization

- Users import from existing source system
- Periodic or one-time
- Mapping rules between Perun and external source
- Various protocols supported
  - LDAP, SQL, XML, CSV, AD, …
- Automatic account-linking based on defined rules
- It’s possible to synchronize groups as well

Entities


Person
User self registration
Google
Federated Identity
X.509
Application form
OR
Import identities by VO manager
External sources of identitties
SQL database
LDAP
CSV file
one time request
synchronization
Identity consolidation
USER
VO
Group
Group
VO
Group
Group
VO manag

Combining features

- Building an infrastructure
- Automation
- Delegation
- Consistency and reliability
- Integration with access management necessary
- Unified view on identities and accesses
    - Potential for building other service (catalog, helpdesk, …)

Thank you for attention

EGI Conference 2021

Slávek Licehammer
slavek@ics.muni.cz