Identity and Access Management

- Manages
  - Users, identities and attributes
  - VOs, groups and registrations
  - Access control for services
  - Provisioning / deprovisioning
- Designed to fit in existing infrastructure
- Doesn’t do
  - Authentication, proxy
  - Credential storage
About Perun

- Developed by CESNET and Masaryk University
- Designed as a generic IAM tool
- Stable development and operations team
  - 9 core members + students
  - Other collaborators mainly for services connectors
- Open source - available on github
  - https://github.com/CESNET/perun/
- Can be used as a component or a service
Main deployments

- CESNET
  - National e-infrastructure
- Masaryk university
  - Over 40,000 users
- EGI
- ELIXIR
- BBMRI
- Westlife
- ...
VO management

- Custom registration flow
  - Including enrolments to groups
  - Invitations
  - Custom notification
  - Branding
- Automatic imports from other systems (LDAP, DB,...)
- User life-cycle
- Privileges delegation
Users management

- Users owns their data
- Account linking
  - Various supported identity types (eduGAIN, social, X.509, ORCID, ...)
  - Support for local accounts
- Self-service
  - Enrollments to VO
  - User profile
Services/access management

- Delegation of access management to VOs
  - Service manager configure basic rules and limitations
  - VOs have to manage access for individual users
- Configuration options are specific for each service
- Configuration done in Perun will be provisioned to services
Provisioning

- Push mechanism
- Simple connector for each service
- Using standard protocols
- Mapping from Perun entities to service internals
- Privacy preserving
  - Service gets only relevant data
- Administrator of service have full control
- Endpoints to query data as an alternative
  - LDAP, Perun API
Additional features

- API access
- Mini applications
  - Custom, minimalistic one purpose application
- LDAP interface
- Attributes framework
- Integration with security teams
- Notifications
- Internationalization
- ...

Perun in EOSC-hub AAI

- Integrated with EGI check-in
  - Manages about 25 communities
- Integrated with GÉANT eduTEAMS
  - One of 3 options for membership management service
- One of the component of Life Science AAI Pilot (candidate for being operated by EOSC-hub)
Thank you for attention

http://perun.cesnet.cz
perun@cesnet.cz
Slávek Licehammer
slavek@ics.muni.cz