Identity and Access Management System (IAM)

Soňa Mastráková
mastrakova@mail.muni.cz
Perun is an application for group management, access management and identity management.
Features
Various interfaces support

- LDAP
- SAML2 Attribute Authority
- VOOT
- SCIM (in progress)
Propagation mechanism

- PUSH mechanism
- services are always available
- independent on Perun accessibility
- scalability
- need only small connector to the service
Privileges delegation

2 separated manager roles:

- administrative manager
  - access control
- technical manager
  - manages services
Self-registration

- application form creation even on group level
- approval: manual vs. automatic
- user redirection to another system
- account expiration
Mini applications

- designed for one specific use-case
- fully customizable
- web based
- typically aimed to end users

- user profile
- simplified group management
Security teams

- security teams create and manage blacklists of users

- blacklisted users are not propagated to managed services
Successful stories
Challenge:

- services provided to academical environment
- distributed group management
- synchronization with existing groups and identities
Challenge:

- centralized access management at MU
- huge amount of users (students, employees, guests, service accounts)
Challenge:

- university access management
- heterogeneous systems at university
ELIXIR

Challenge:

- access management to sensitive data
- levels of assurance
- reliable authentication of researchers
Challenge:

- access management to grid infrastructure in South African Republic
- access to unreliable infrastructure
More about development
Development team

- team leader
- developers
- support
- Masaryk University cooperating (contributing students)
- service connectors development with other people from CESNET and MU
Development process

Agile development:
- iterative development
- extreme programming
- task/feature driven development
Development process

Version control system:

- Git (https://github.com/CESNET/perun)
- code reviews

Automated testing:

- Jenkins
Technologies

- Java, Spring, Maven, Tomcat
- Bash, Perl
- GWT, JavaScript, Bootstrap
- Jenkins
- Git
- Redmine