Motivation

● Missing IdM and access management
● User registration is needed
  ○ Users already have some digital identity

● Delegation of the rights to manage entities
● Configuration of the access rights
● Attribute authority for SAML based services
Perun manages

- Virtual organizations
- Users
- Groups
- Resources
- Services
- Application forms
- Attributes
VO and Group Management

- **Built-in support for virtual organizations**
  - Configurable application form
  - Delegation of rights to the end users
  - Access management for resources

- **Group management**
  - Configurable application form
  - Group manager role
  - Automatic synchronization with external systems
  - Support for VOOT protocol (server/client) will be deployed in a few weeks
User Management

- User can have several external identities
  - Federated identities, X.509 certificates, social identities, SSH keys, Kerberos principals, ...
  - Identity consolidation
  - Perun doesn’t store user’s password, private keys, ...

- Users' enrollments
  - Each VO can define its own application form with various requirements on the applicant
  - Pre-filled information from external authN system

- Service users
Access Management

- Resources are assigned to the VOs
  - Resource tagging
- Configuration of services
  - E.g. unix accounts, access to NFS storage systems, radius ACLs, mailing lists, ACLs for web applications
  - Service packages
- Push mechanism
  - omit online queries
  - pushing only on change
- Alternatively publish data through the LDAP
Attribute Authority

- Attribute Authority is another resource from Perun’s point of view
  - Perun fills the LDAP
  - AA per VO
- Deployed at CESNET - DocuWiki
  - Authorization based on the group membership
Attributes Management

- Every entity and also relationship can have assigned attributes
- Different value types: string, number, list, array
- Access rights on attribute values
- Attribute modules
  - check proper value of the attribute
  - fill default values
  - check value of dependant attributes
Statistics

- In production since autumn 2012 (CESNET)
- >2900 users, ~1800 machines, 96 VOs
- Other deployments as virtual appliance
  - GARR - CloudIdP + Perun test
  - sagrid - pilot installation in NGI management
- Cooperation with HEXAA project
Thank you for your attention

http://perun.cesnet.cz
http://github.com/CESNET/perun