Identity and Access Management System for Virtual Organizations/Research Communities

EGI-GEANT Symposium
25.9.2014

Michal Procházka
CESNET, Institute of Computer Science Masaryk University
Motivation

- Single Sign-On for services within the project
- Reuse existing users' identities
  - Federated identity
  - Social identity
- Provide an identity for "homeless" users
- Support grouping of such identities
  - Use existing user’s groups
- Delegation of the rights to manage the entities
- Expose data to the federated services
Perun manages

- Virtual organizations
- Users
- Groups
- Resources
- Attributes
VO and Group Management

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

● Group management
  ○ Configurable application form
  ○ Group manager role
  ○ Automatic synchronization with external systems
  ○ Support for VOOT protocol
User Management

● User can have several existing 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
  ○ Pre-filled information from external authN system

● Service users
  ○ Represents services
Access Management

- Resources are assigned to the VOs
  - Generally non-web/SAML incompatible services
- Configuration of the access to the services
  - E.g. unix accounts, access to NFS, radius ACLs, mailing lists, ACLs for web applications, OpenNebula
- Push mechanism
  - omit online queries
  - push only on change (ideal for clouds)
- Alternatively publish data through the LDAP
- SAML based Attribute authority
Attributes Management

- Every entity and also relationship can have assigned the 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
Attribute Authority

- Attribute Authority is just another resource from Perun’s point of view
  - AA per VO
- Deployed at CESNET eInfrastructure
  - Provides information of vo/group membership within the Czech eInfrastructure
Cooperation projects

- Cooperation with HEXAA and Surfnet
  - Finding processes and protocols for AA interoperability
- Elixir project
  - Cooperation with REMS system
  - Providing user management for Elixir
Selected deployments

- **EGI core service**
  - Manages user access to the EGI federated cloud infrastructure
  - Connected with VOMS service

- **EBI**
  - Manages access to the AppDB applications
  - Pilot installation

- **Czech Elixir node**
  - Manages access to the whole back office and computational/storage resources

- **SAGRID**
  - Production installation for the NGI management
EGI fedcloud case

Management using Perun

Management using VOMS utilizing Perun
EBI case
Elixir case
Statistics

- CESNET’s Perun instance
- In production since autumn 2012
- 152 VOs national/international
- >3900 users
- Manages access to services on ~1800 machines
Thank you for your attention

http://perun.cesnet.cz

http://github.com/CESNET/perun