



Perun

Perun Description

Michal Procházka

Perun Days, CESNET, Prague, 16. 3. 2017

Outline



10:00 - 11:00 What Perun can do

11:00 - 12:00 VO manager training

12:00 - 12:30 Lunch

12:30 - 13:30 How to manage access to your service

13:30 - 15:00 Thematic discussions

What is it? (Shortly)



- IAM - Identity and Access Management
- Grab user identity -> categorize -> assign services -> let them use the services
- Support user life-cycle

Motivation



- Manage users from different institutions
- Manage different service providers
- User enrollment is needed
 - Users already have some digital identity
- Delegation of the rights to manage entities
- Configuration of access rights to the services
- Global view on access control

Perun Manages



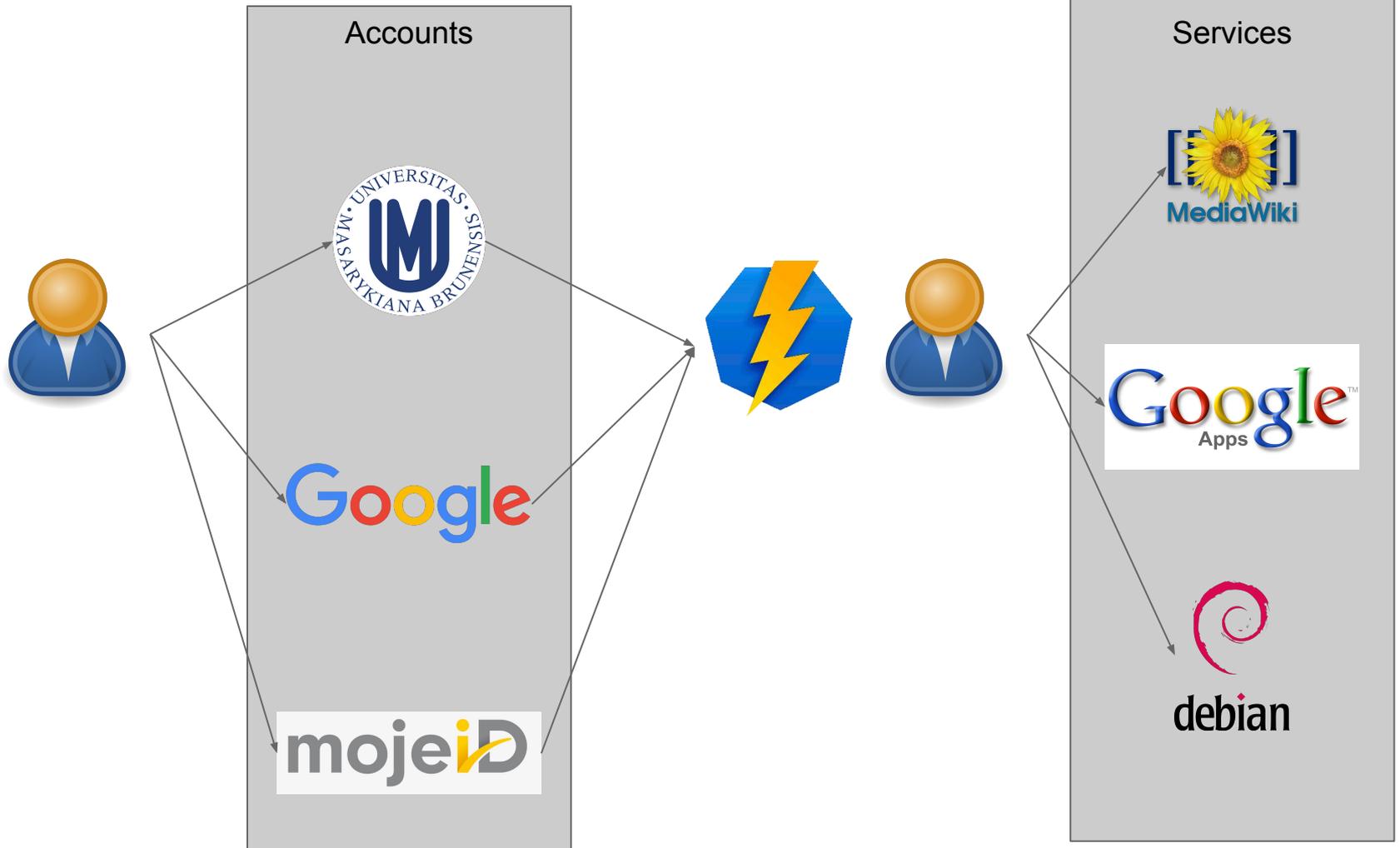
- Virtual organizations
- Users
- Groups
- Resources
- Services
- Application forms
- Attributes, ...

Example #1



- Organisation operates set of services
 - Not only local users want to use those services
- Single place for access control
- Support for user life cycle

Example #1

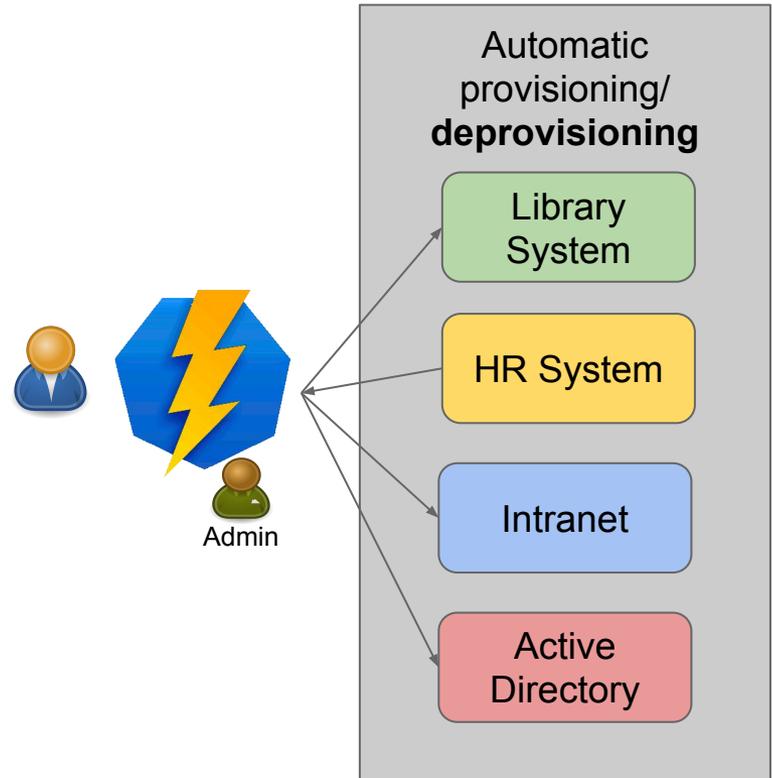
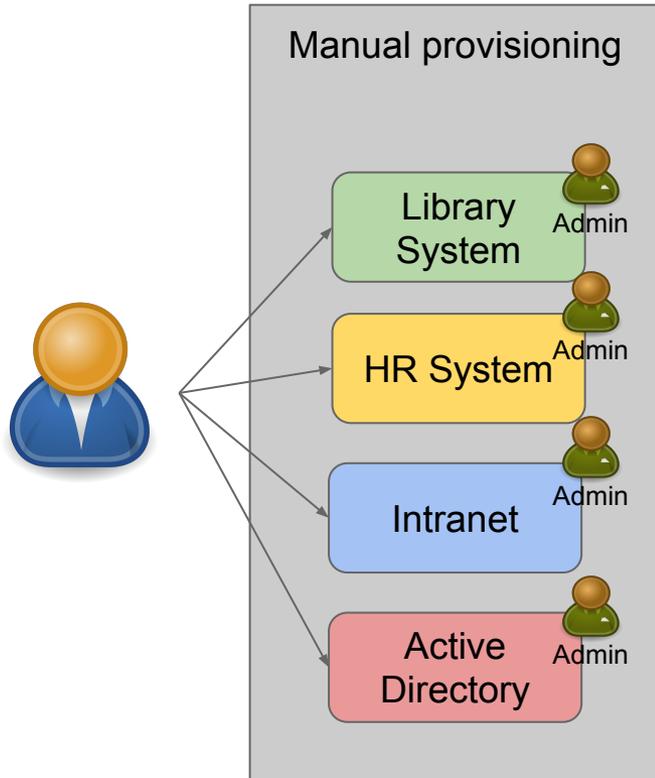


Example #2



- Organisation has several systems with dedicated user management
 - Problematic synchronization among them
- Problematic user life cycle support
- Service's support overhead

Example #2



Perun at Masaryk University



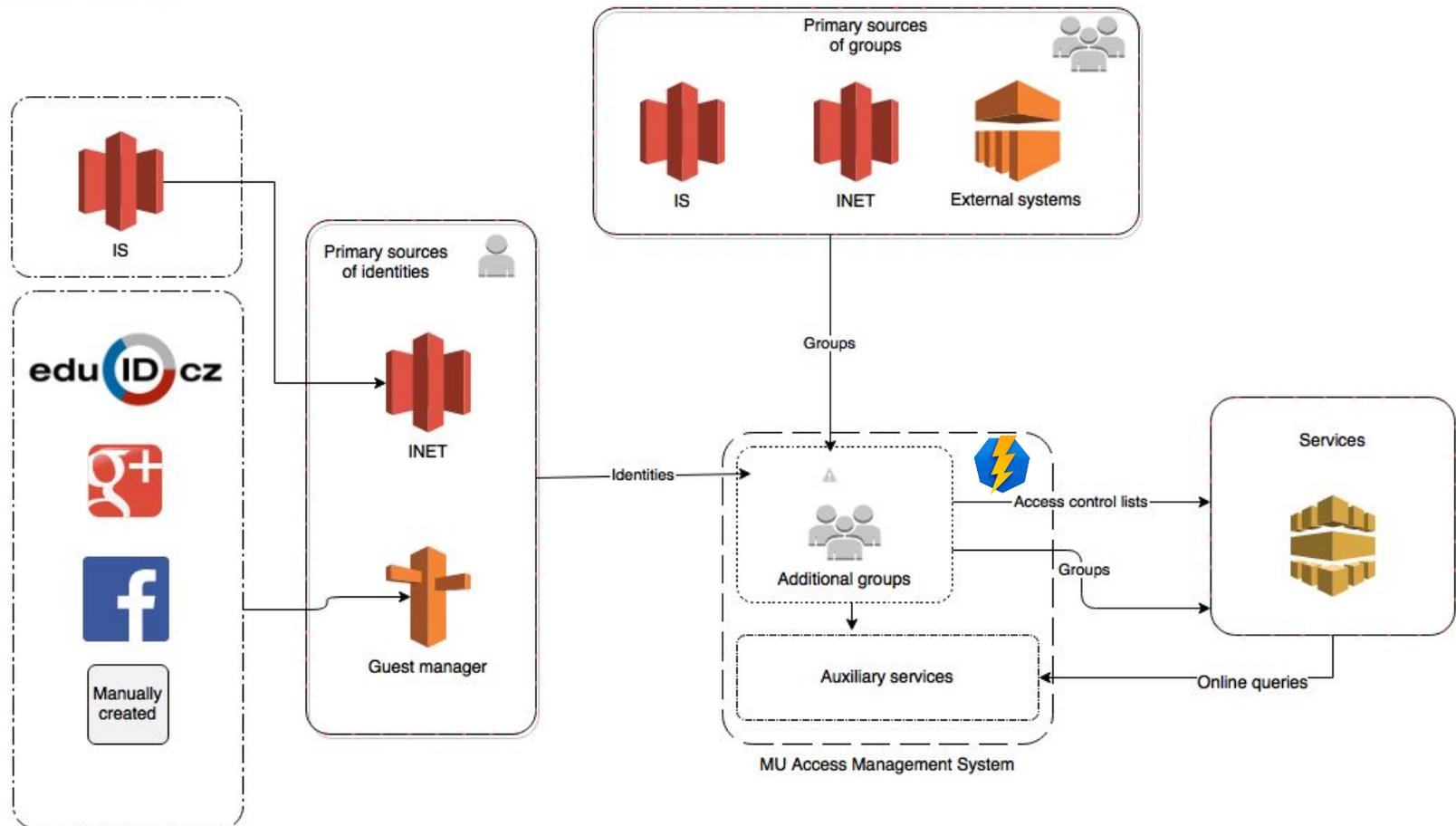
- Central component for user and group aggregation
- Single entry point for authorization for services
 - Groups, group memberships
 - User's attributes

Perun at MU



Mandragora

Architecture of identity and access management for MU



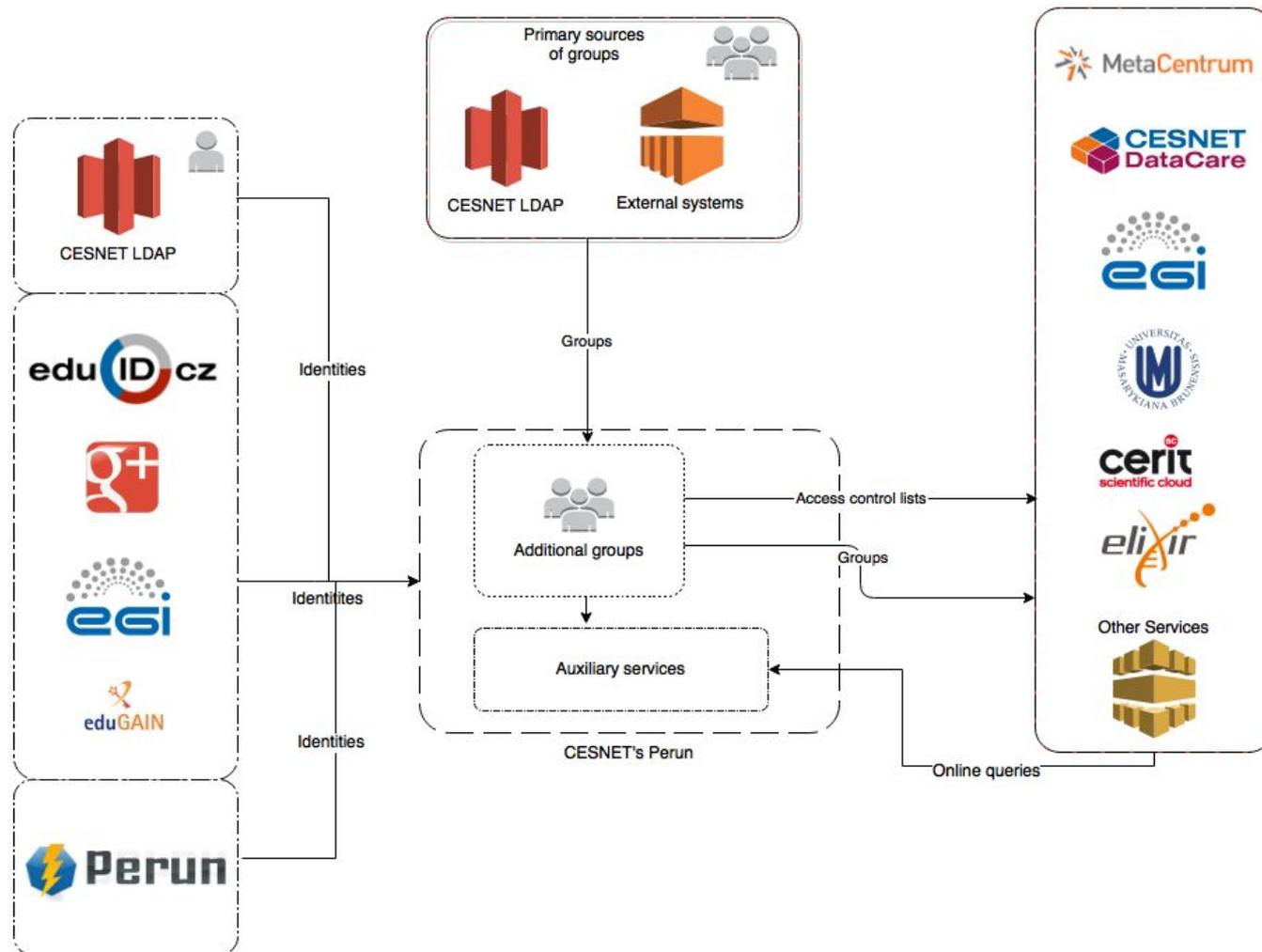
Perun at CESNET



- Multi-tenant deployment
- Manages and aggregates data from various sources
- Manages access to various types of services



CESNET's Perun



Perun at CESNET



-  MetaCentrum
 - User self registration → Approval (MetaCentrum staff) → Use of computational resources
-  CESNET DataCare
 - Representative registration → User registration → Approval (Representative) → Use of storage resources
-  EGI
 - User aggregation from external sources → Use of EGI cloud resources
 - User self registration → Distributed Approval → Use of EGI cloud resources
-  elixir
 - Users from different Perun → Use of EGI cloud resources

Aggregator



- Perun is able to aggregate data from various sources
 - Directories (LDAP/AD)
 - Databases (SQL)
 - APIs (XML, CSV, SCIM, ...)
- Configurable import rules for mapping external data into Perun

Disseminator



- Perun disseminates authorization data to the end services via
 - PUSH mechanism
 - Online queries (LDAP, API)

Features



- Selected features
 - Auditer
 - API/Mini applications
 - Service users
 - Security teams

Auditer



- Every successful operation is audited
- Auditer produces audit logs
 - Textual representation of operation and entities involved
- Audit log can be read by external applications

API/Mini applications



- Perun integration
 - REST-like interface over HTTPs
 - Command Line Interface (CLI)
 - Perl and PHP binding
- Mini applications
 - Dedicated web based applications
 - JavaScript library

Mini application example

The screenshot shows the 'eInfrastructure User Profile' page for RNDr. Michal Procházka Ph.D. The page has a dark grey navigation bar at the top with links for 'e-infrastruktura CESNET', 'Network', 'Computing', 'Data storage', 'Cooperation', 'Multimedia', 'Security', and 'AAI'. Below this is a light grey header with the 'Perun' logo and the title 'eInfrastructure User Profile'. A left sidebar contains a 'MENU' section with options: 'My Profile', 'Virtual Organizations', 'My Identities', 'My Alternative Passwords', and 'Password reset'. The main content area displays the user's name in teal, followed by a list of profile details: 'Login' (michalp), 'Organization' (Masarykova univerzita), 'E-mail' (michalp@ics.muni.cz with a 'change' button), 'Phone' (549 49 6141), 'Preferred language' (cs with a dropdown arrow), and 'Your timezone' (Europe/Prague with a dropdown arrow).

e-infrastruktura
CESNET

Network Computing Data storage Cooperation Multimedia Security AAI

Perun eInfrastructure User Profile

▼ MENU

- My Profile
- Virtual Organizations
- My Identities
- My Alternative Passwords
- Password reset ↻

RNDr. Michal Procházka Ph.D.

Login michalp
Organization Masarykova univerzita
E-mail michalp@ics.muni.cz [change](#)
Phone 549 49 6141
Preferred language cs ▼
Your timezone Europe/Prague ▼

Service Users



- Used for automatic systems identification
 - backups, monitoring, etc.
- Normal Users are assigned to this Service User
 - Have rights to work with it, use it
 - Have responsibility for this service User

Security Teams



- Support for CSIRT/CERT teams
- Suspension of the user across the services
- Suspended users are:
 - not propagated to the services
 - or marked there as suspended

Team Development



- CESNET and Masaryk University cooperation
- Core team developers and students from Masaryk University and ČVUT
- Sharing responsibilities
- Service development with external people

Technical Development



- Open GitHub repository
 - <https://github.com/CESNET/Perun>
- Everyone can contribute
 - Validated by Perun core team
- Every change is tested

Documentation



- <https://perun.cesnet.cz/web/documentation.shtml>
 - Global overview
 - Basic and advanced use cases description
 - API
- <https://wiki.metacentrum.cz/wiki/Kategorie:Perun>
 - User documentation

Thematic discussions



- Integration with O365 and Google Apps
- Integration with AD/LDAP/389 Directory
- Integration with social identity providers
- Advanced group management
- Import/export from other IdM systems



<http://perun.cesnet.cz>

perun@cesnet.cz