Perun

User and Resource Management System

Michal Procházka

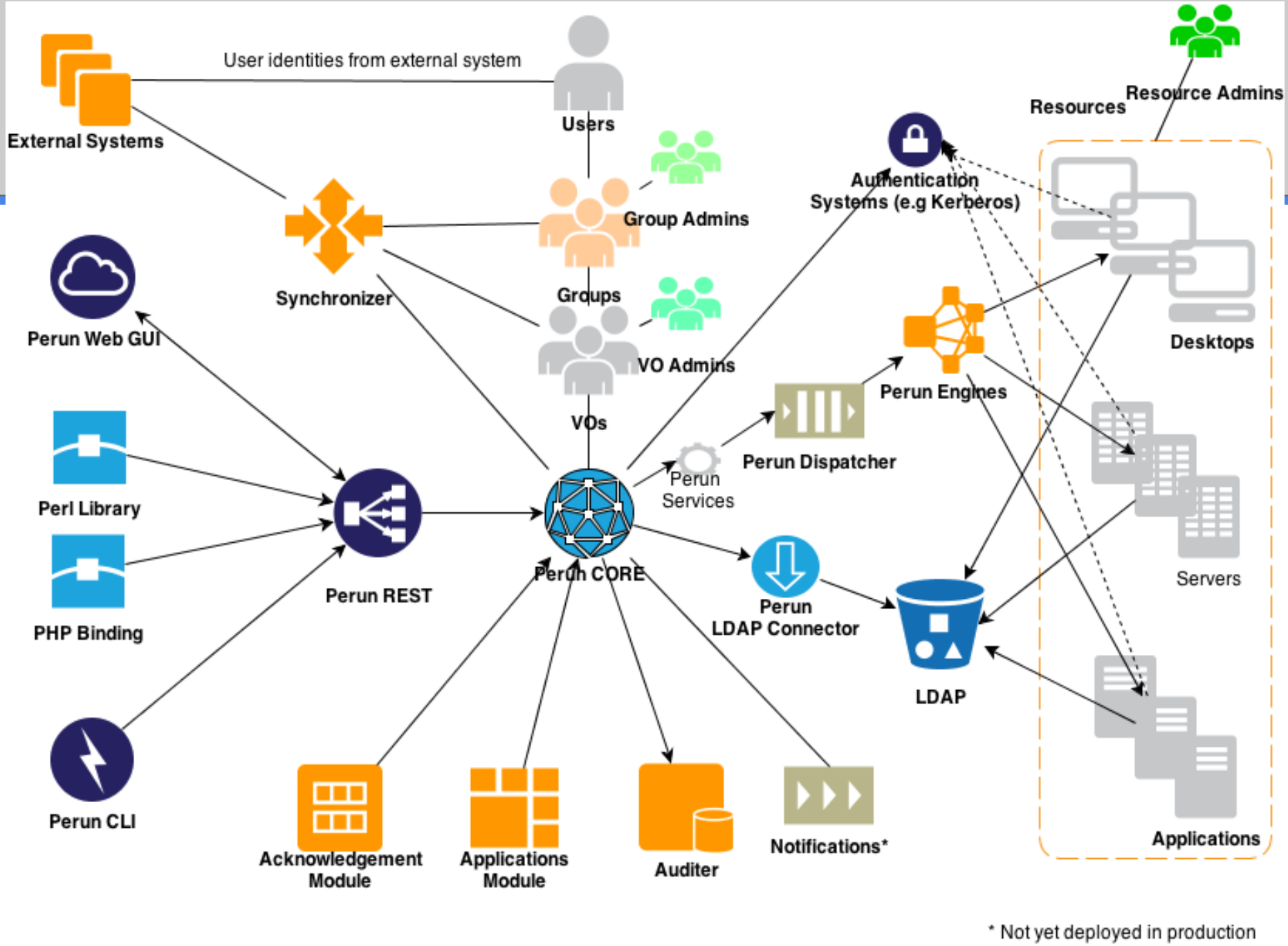
CESNET, Institute of Computer Science Masaryk University

Motivation

- National Grid infrastructure
  - Users from different institutions
  - Different resource providers
- Difficult to manage such different entities
- User registration is needed
- Users already have some digital identity
- Delegation of the right to manage entities
- Configuration of the access rights
- Fill the gap between IF and end services

History

- Perun v 1 (1996-2002)
  - Managed access to the super computers at Masaryk University
- Perun v 2 (2002-2012)
  - Support for Grid resources across whole country
- Perun v 3 (2012-)
  - Support for virtual organizations and rights delegation
  - Written from scratch


User identities from external system
External Systems
Users
Resources
Resource Admins
Authentication Systems (e.g Kerberos)
Group Admins
Synchronizer
Groups
Perun Web GUI
VO Admins
VOs
Desktops
Perun Engines
Perun Dispatcher
Perun Services
Perl Library
Perun REST
Perun CORE
Servers
PHP Binding
Perun LDAP Connector
LDAP
Perun CLI
Acknowledgement Module
Applications Module
Auditer
Notifications*
Applications
* Not yet deployed in production

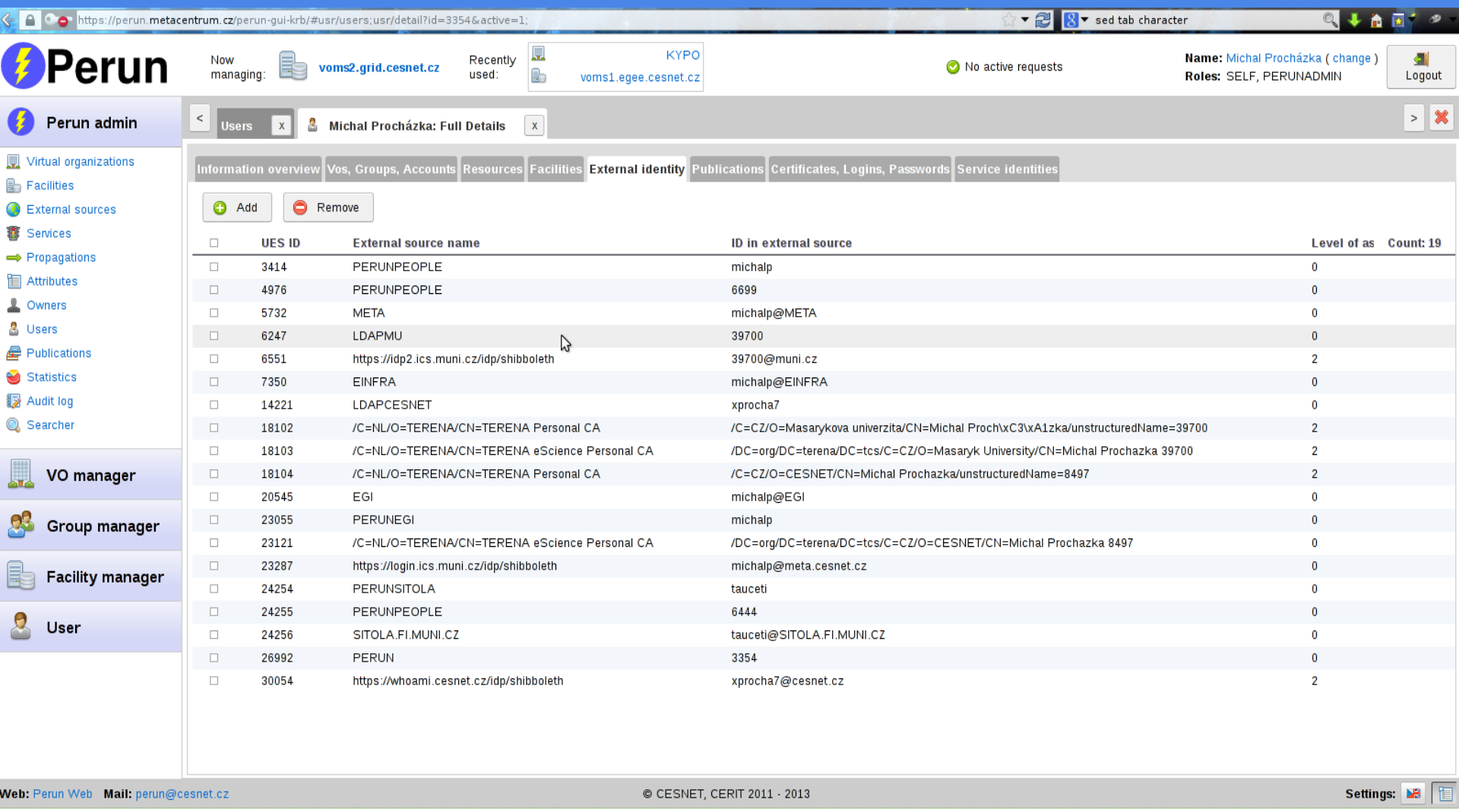
Perun manages

- Virtual organizations
- Users
- Groups
- Resources
- Services
- Application forms

User Management

- User can have assigned several external identities
  - Federated identities, X.509 certificates, social identities, SSH keys, Kerberos principals, ...
  - Identity consolidation
- Application forms
  - Each VO can define its own application form with various requirements on applicant
  - Prefilled information from external authN system

External Identities



VO and Group Management

- Build-in support for virtual organizations
  - Configurable application form
    - Initial and extension application type
  - VO manager role
    - Delegation of rights to the end users
  - Resource management
- Group management
  - Group manager role
  - Automatic synchronization with external systems
  - Support for VOOT protocol is under development

Resource Management

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

LDAP and Attribute Authority

- Nearly real time synchronization with Perun Core DB
  - Reacts on each change in Perun (new member, change in group membership, ...)
- Attribute Authority can be connected to Perun LDAP

Attributes Management

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

Application Interfaces

- Complete set of functions of each Perun component is available through API
- REST with JSON
- Perl and Java library
- PHP binding

Statistics

- In production since autumn 2012
- >2000 users
- >1800 machines
- 39 virtual organizations
  - national and also international VOs

Conclusion

- System for managing virtual organizations, groups and users
- Consolidate different user's identities
- User registrations
- Do the ACL configurations for services
- Additional value for IF
  - Group management
  - Attribute authority

Thank you for your attention

http://perun.metacentrum.cz

CESNET, Institute of Computer Science Masaryk University