Perun

User and Resource Management System for Virtual Organizations/Research Communities

Michal Procházka

CESNET, Institute of Computer Science Masaryk University

Use case

- Research community needs access to the protected external service
- They need
  - digital identity for each user, which is accepted by the external service
  - manage users fluctuation
  - propagate set of allowed users to the external service

Solution #1

- Every user will register at the service
- Pros
  - No activity is needed from user's organization, neither from research community
- Cons
  - Does not scale with increasing number of services
  - Users have yet another digital identity
  - Service needs to manage users accounts

Solution #2

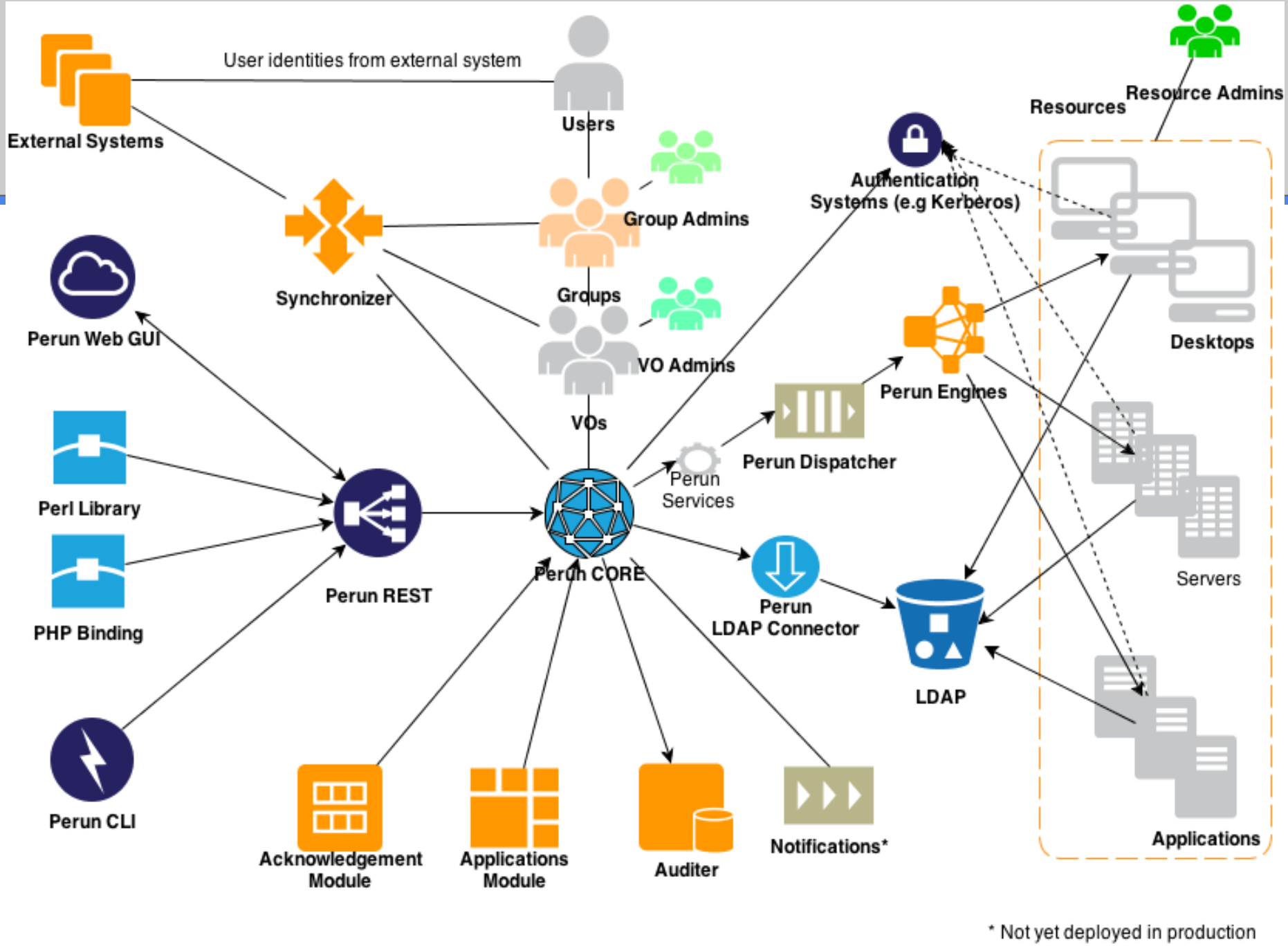
- Research community members have federated identity from well recognized organization and service is part of the IF
- Pros
  - Relatively easy to gain access
  - Without any action from end users, they logon as usual
- Cons
  - Strong requirements on existing IF
  - Needs some kind of agreement between IF and (eduGAIN or service)

Solution #3

- Research community will create VO in Perun
- Pros
  - Users only fills the application form for the VO
  - Perun will send list of allowed users to the service in its required format
  - Members are managed in Perun by research community itself
  - Perun can provide IdP interface
- Cons
  - Use of non in-house solution
  - Service configuration must be managed in Perun

Perun manages

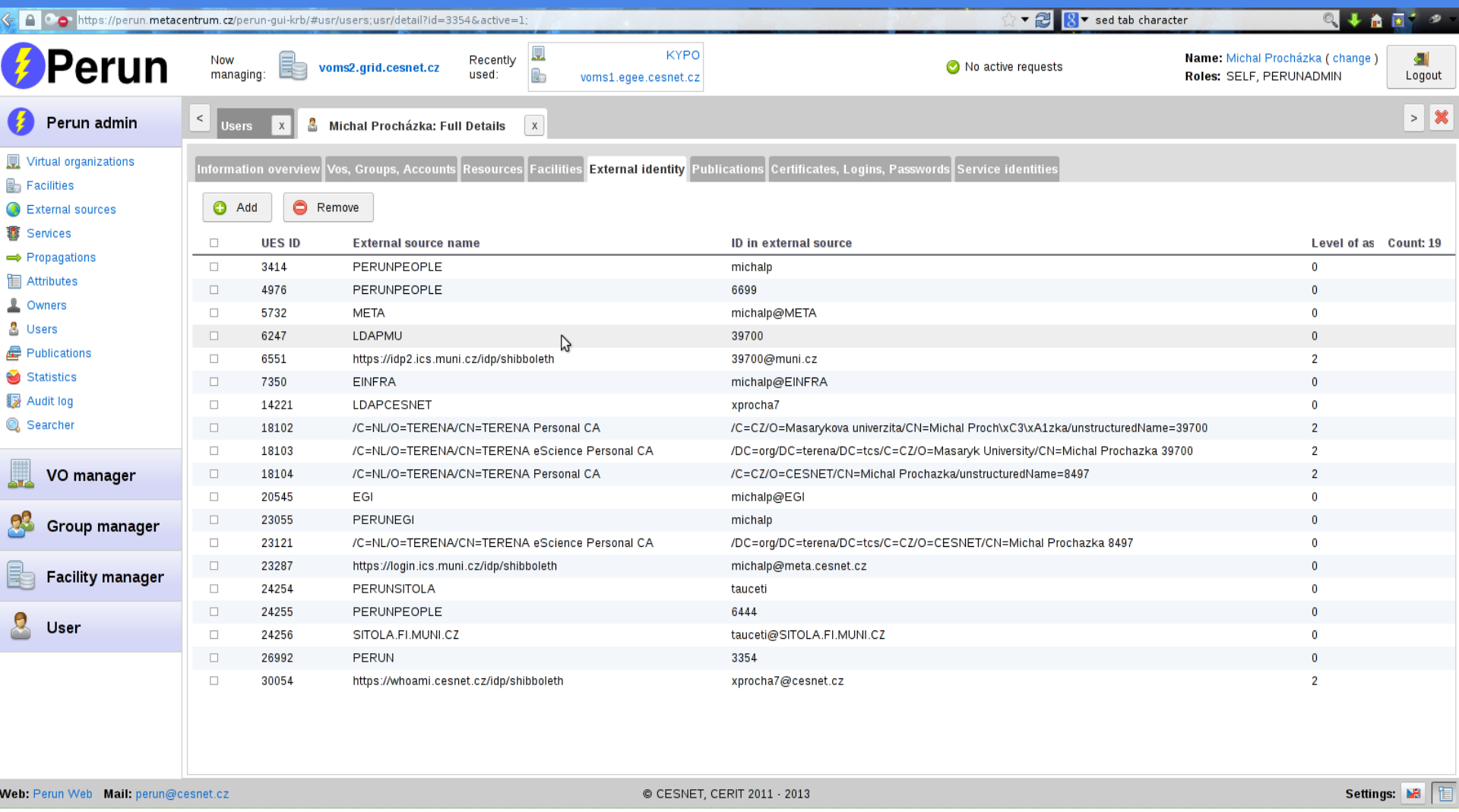
- Virtual organizations
- Users
- Groups
- Resources
- Services
- Enrollments


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

User Management

- Identity consolidation
  - Federated identities, X.509 certificates, social identities, SSH keys, Kerberos principals, ...
- Users' enrollments
  - Each VO can define its own application form with various requirements on applicant

External Identities



VO and Group Management

- Putting users from different organizations together
- Manage members of VO and groups in one place
- Delegation of rights - group manager role
- Group management
  - Automatic synchronization with external systems

Resource Management

- Perun can send predefined access control list to the service
- Examples of supported 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

Example

- Access to the Wiki
  - Service represents Wiki created in Perun
  - Service assigned to the VO
  - Setup service configuration
  - Selected groups are assigned to the service
  - Propagation of the data to the service
  - **User can access the service**

Application Interfaces

- Complete set of functions of each Perun component is available through API
- REST with JSON
- Perl and Java library
- PHP binding
- Perun can be integrated into existing user/group/resource management systems

Statistics

- In production since autumn 2012
- >2000 users
- >1800 machines
- 39 virtual organizations
  - national and also international VOs
  - VO representing research projects
  - VO representing school subjects with special requirements

Conclusion

- System for managing virtual organizations, groups and users
- Consolidate existing user's identities
- User enrollments
- 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