



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)



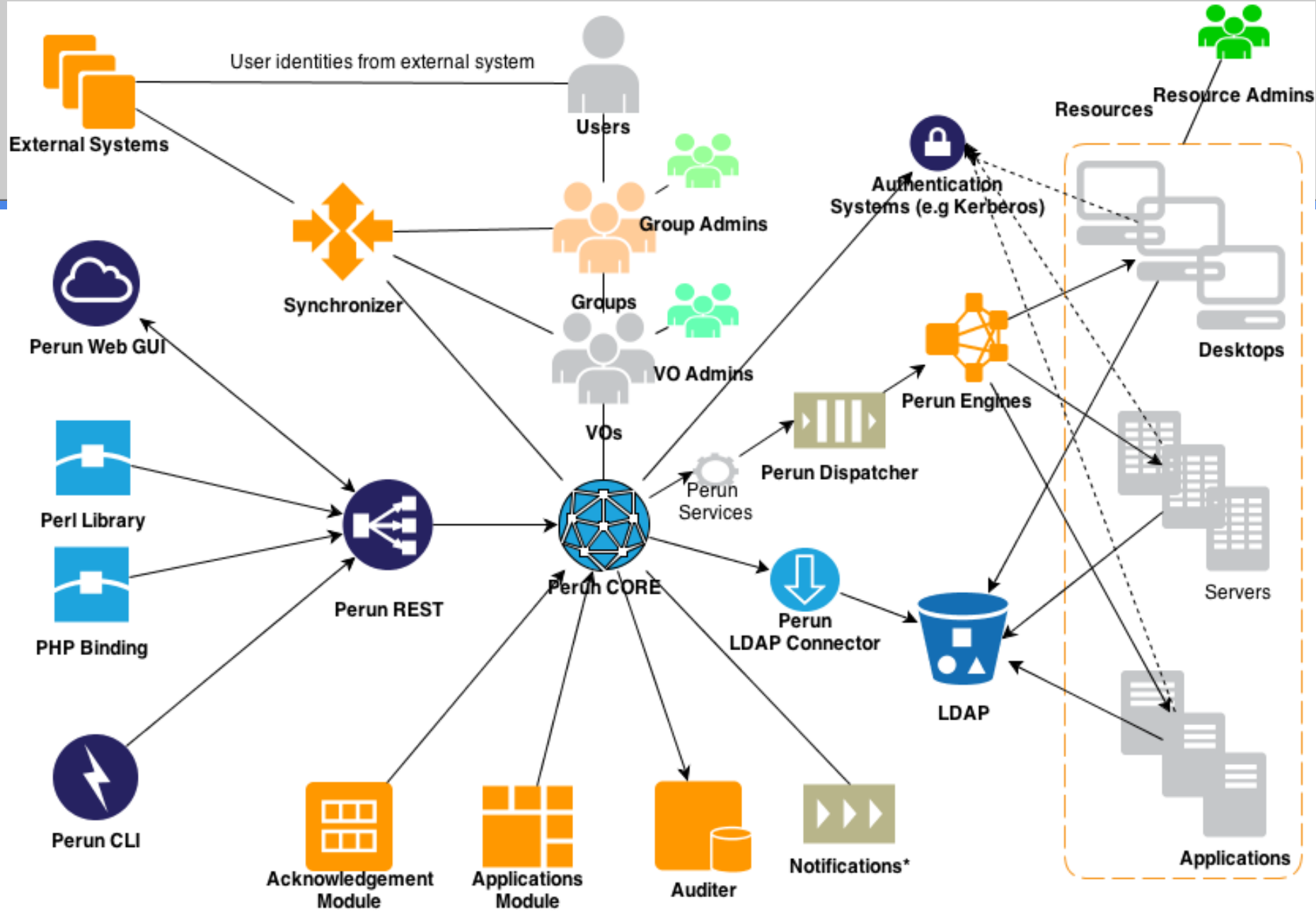
Solution #3

- 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



* 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

https://perun.metacentrum.cz/perun-gui-krb/#usr/users;usr/detail?id=3354&active=1

Perun Now managing: voms2.grid.cesnet.cz Recently used: KYPO voms1.egee.cesnet.cz No active requests Name: Michal Procházka (change) Roles: SELF, PERUNADMIN Logout

Perun admin

Users x Michal Procházka: Full Details x

Information overview Vos, Groups, Accounts Resources Facilities External identity Publications Certificates, Logins, Passwords Service identities

+ Add - Remove

<input type="checkbox"/>	UES ID	External source name	ID in external source	Level of as	Count: 19
<input type="checkbox"/>	3414	PERUNPEOPLE	michalp	0	
<input type="checkbox"/>	4976	PERUNPEOPLE	6699	0	
<input type="checkbox"/>	5732	META	michalp@META	0	
<input type="checkbox"/>	6247	LDAPMU	39700	0	
<input type="checkbox"/>	6551	https://idp2.ics.muni.cz/idp/shibboleth	39700@muni.cz	2	
<input type="checkbox"/>	7350	EINFRA	michalp@EINFRA	0	
<input type="checkbox"/>	14221	LDAPCESNET	xprocha7	0	
<input type="checkbox"/>	18102	/C=NL/O=TERENA/CN=TERENA Personal CA	/C=CZ/O=Masarykova univerzita/CN=Michal Procházka/unstructuredName=39700	2	
<input type="checkbox"/>	18103	/C=NL/O=TERENA/CN=TERENA eScience Personal CA	/DC=org/DC=terena/DC=tcs/C=CZ/O=Masaryk University/CN=Michal Prochazka 39700	2	
<input type="checkbox"/>	18104	/C=NL/O=TERENA/CN=TERENA Personal CA	/C=CZ/O=CESNET/CN=Michal Prochazka/unstructuredName=8497	2	
<input type="checkbox"/>	20545	EGI	michalp@EGI	0	
<input type="checkbox"/>	23055	PERUNEGI	michalp	0	
<input type="checkbox"/>	23121	/C=NL/O=TERENA/CN=TERENA eScience Personal CA	/DC=org/DC=terena/DC=tcs/C=CZ/O=CESNET/CN=Michal Prochazka 8497	0	
<input type="checkbox"/>	23287	https://login.ics.muni.cz/idp/shibboleth	michalp@meta.cesnet.cz	0	
<input type="checkbox"/>	24254	PERUNSIOLA	tauceti	0	
<input type="checkbox"/>	24255	PERUNPEOPLE	6444	0	
<input type="checkbox"/>	24256	SITOLA.FI.MUNI.CZ	tauceti@SITOLA.FI.MUNI.CZ	0	
<input type="checkbox"/>	26992	PERUN	3354	0	
<input type="checkbox"/>	30054	https://whoami.cesnet.cz/idp/shibboleth	xprocha7@cesnet.cz	2	

Web: Perun Web Mail: perun@cesnet.cz © CESNET, CERIT 2011 - 2013 Settings



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