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
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

### Information overview

<table>
<thead>
<tr>
<th>User ID</th>
<th>External Source Name</th>
<th>ID in External Source</th>
<th>Level of Use</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>3414</td>
<td>PERUNPEOPLE</td>
<td>michalp</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4978</td>
<td>PERUNPEOPLE</td>
<td>6899</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5732</td>
<td>META</td>
<td>michalp@META</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6247</td>
<td>LDAPMUI</td>
<td>39700</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6551</td>
<td><a href="https://dp2.ics.muni.cz/dp2nhibboleth">https://dp2.ics.muni.cz/dp2nhibboleth</a></td>
<td><a href="mailto:39700@muni.cz">39700@muni.cz</a></td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>7350</td>
<td>EINFRA</td>
<td>michalp@EINFRA</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>14221</td>
<td>LDAPCESNET</td>
<td>xprocha7</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>18102</td>
<td>/C=NL/O=TERENA/CN=TERENA Personal CA</td>
<td>/C=NL/O=Masarykova univerzita/CN=Michal Procházk/3xAl.zka/unstructuredName=39700</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>18104</td>
<td>/C=NL/O=TERENA/CN=TERENA eScience Personal CA</td>
<td>/DC=org/DC=terena/DC=tcs/C=NL/O=Masaryk University/CN=Michal Procházk/39700</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>20545</td>
<td>EGI</td>
<td>michalp@EGI</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>23655</td>
<td>PERUNEGI</td>
<td>michalp</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>23121</td>
<td>/C=NL/O=TERENA/CN=TERENA eScience Personal CA</td>
<td>/DC=org/DC=terena/DC=tcs/C=NL/O=CESNET/CN=Michal Procházk/39700</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>23287</td>
<td><a href="https://login.ics.muni.cz/dp2nhibboleth">https://login.ics.muni.cz/dp2nhibboleth</a></td>
<td><a href="mailto:michalp@meta.cesnet.cz">michalp@meta.cesnet.cz</a></td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>24254</td>
<td>PERUNSITOLA</td>
<td>taucetb</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>24255</td>
<td>PERUNPEOPLE</td>
<td>6444</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>24256</td>
<td>SITOLA.FI.MUNI.CZ</td>
<td><a href="mailto:taucetb@SITOLA.FI.MUNI.CZ">taucetb@SITOLA.FI.MUNI.CZ</a></td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>26992</td>
<td>PERUN</td>
<td>3154</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>30054</td>
<td><a href="https://whoami.cesnet.cz/dp2nhibboleth">https://whoami.cesnet.cz/dp2nhibboleth</a></td>
<td><a href="mailto:xprocha7@cesnet.cz">xprocha7@cesnet.cz</a></td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

**Web:** Perun Web  | **Mail:** perun@cesnet.cz  
**© CESNET, CERT 2011 - 2013**  
2. 6. 2013 - REFEDS Meeting | CESNET, Institute of Computer Science Masaryk University, Czech Republic | Michal Procházká
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