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 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

<table>
<thead>
<tr>
<th>UES ID</th>
<th>External source name</th>
<th>ID in external source</th>
<th>Level of access</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>4976</td>
<td>PERUNPEOPLE</td>
<td>6699</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>LDAPMÚ</td>
<td>39700</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6551</td>
<td><a href="https://idp2.ics.muni.cz/idp/shibboleth">https://idp2.ics.muni.cz/idp/shibboleth</a></td>
<td><a href="mailto:39700@muni.cz">39700@muni.cz</a></td>
<td>2</td>
<td>2</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>18103</td>
<td>/CN=NL0=TERENA/CN=TERENA Personal CA /DC=cz/O=Masarykova universita/CN=Michal Prochazka</td>
<td>89700</td>
<td>Michal Prochazka 89700</td>
<td>2</td>
</tr>
<tr>
<td>18104</td>
<td>/CN=NL0=TERENA/CN=TERENA eScience Personal CA /DC=org/DC=terena/DC=tcs/C=cz/O=Masarykova University/CN=Michal Prochazka 39700</td>
<td>39700</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>20545</td>
<td>EGI</td>
<td>michalp@EGI</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>23055</td>
<td>PERUNEGI</td>
<td>michalp</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>23121</td>
<td>/CN=NL0=TERENA/CN=TERENA eScience Personal CA /DC=org/DC=terena/DC=tcs/C=cz/O=CESNET/CN=Michal Prochazka 89497</td>
<td>89497</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>23287</td>
<td><a href="https://login.ics.muni.cz/idp/shibboleth">https://login.ics.muni.cz/idp/shibboleth</a></td>
<td><a href="mailto:michalp@mata.cesnet.cz">michalp@mata.cesnet.cz</a></td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
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