Membership Management Services in eduTEAMS

Mihály Héder, SZTAKI
Slávek Licehammer, CESNET
MMS-es in eduTEAMS

- A Membership Management Service
  - Virtual Organizations
  - Groups
  - Roles
  - Entitlements

- Provide interface for user enrollment

- Assign rights and permissions to people through roles, groups, etc.

- Management is delegated to Principal Investigator or Community manager
  - Can be delegated further
What is an MMS

euGAIN

euTEAMS
Membership Management Service

AA

eduTEAMS Proxy

eduTEAMS Identity Hub

eduTEAMS DS

eduTEAMS MDS

GEANT Step-Up Authentication Service

SP

SP

SP

SP
The eduTEAMS MMS-es

- **COmanage**
  - Developed by Internet2
  - Several deployments mainly in the US

- **HEXAA**
  - Developed by MTA SZTAKI/NIIF
  - Runs in Hungarian Federation

- **PERUN**
  - Developed by CESNET and Masaryk University
  - Several deployments for European research projects and in Czechia
Supporting multiple MMS-es

● Different options for different communities
  ○ Complexity of the tool
  ○ User interface
  ○ Management of organizational structure
  ○ Data provisioning and intake
  ○ User enrollment

● Offering tools which communities are familiar with

● Equivalent functionality for all MMSes on eduTEAMS service (shared)
  ○ Different look & feel and workflows

● Unlock full MMS potential on eduTEAMS dedicated
## MMS in eduTEAMS: high-level comparison

<table>
<thead>
<tr>
<th></th>
<th>COmanage</th>
<th>HEXAA</th>
<th>Perun</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>User profile limited to collaborative organization</td>
<td>User profile is platform wide</td>
<td>User profile is platform wide</td>
</tr>
<tr>
<td></td>
<td>Services limited to collaborative organization</td>
<td>Services are platform wide</td>
<td>Services are platform wide</td>
</tr>
<tr>
<td></td>
<td>Partial functionality available through API</td>
<td>All functionality available through API</td>
<td>All functionality available through API</td>
</tr>
<tr>
<td></td>
<td>Complex functionality supported, long learning curve</td>
<td>Lightweight, short learning curve</td>
<td>Complex functionality supported, long learning curve</td>
</tr>
<tr>
<td></td>
<td>Development team part of eduTEAMS</td>
<td>Development team part of eduTEAMS</td>
<td>Development team part of eduTEAMS</td>
</tr>
</tbody>
</table>
COmanage in eduTEAMS: main highlights

- Provisioning targets
  - LDAP and other, custom-written

- Fully customizable enrollments
  - Separate enrollment flows for COUs (Organizational Units)

- Various ways to take users in

- High-powered collaboration admins
Configuration for COmanage

- CO Settings
- Attribute Enumerations
- Authenticators
- CO Navigation Links
- COUs
- Dashboards
- Enrollment Flows
- Expiration Policies
- Extended Attributes
- Extended Types
- Identifier Assignments
- Identifier Validators
- Localizations
- Message Templates
- Organizational Identity Sources
- Pipelines
- Provisioning Targets
- Self Service Permissions
- Services
- Terms and Conditions
- Themes
CAMS at GEANT

- Manages access to GEANT-internal applications
  - Mailing list
  - SW catalog
  - gitlab
  - etc

- Based on the COU concept of COmanage

- Leverages enrollment functionality of COmanage
CAMS at GEANT (design)
HEXAA in eduTEAMS: main highlights

- Simple interface for Role-Based Access Control
  - Wizards
- Two enrollment modes
  - Pre-defined number of seats via link
  - Email
- Full transparency with event log
### Managers

<table>
<thead>
<tr>
<th>Name</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Almáš Tamás</td>
<td><a href="mailto:almastamas@example.com">almastamas@example.com</a></td>
</tr>
<tr>
<td>Kis Tamás</td>
<td><a href="mailto:kistamas@example.com">kistamas@example.com</a></td>
</tr>
<tr>
<td>Nagy Tamás</td>
<td><a href="mailto:nagytamas@example.com">nagytamas@example.com</a></td>
</tr>
<tr>
<td>Szabó Tamás</td>
<td><a href="mailto:szabotamas@example.com">szabotamas@example.com</a></td>
</tr>
<tr>
<td>Szűcs Tamás</td>
<td><a href="mailto:szucstamas@example.com">szucstamas@example.com</a></td>
</tr>
<tr>
<td>Vas Tamás</td>
<td><a href="mailto:vastamas@example.com">vastamas@example.com</a></td>
</tr>
</tbody>
</table>

### Users

<table>
<thead>
<tr>
<th>Name</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Almáš Tamás</td>
<td><a href="mailto:almastamas@example.com">almastamas@example.com</a></td>
</tr>
<tr>
<td>Almáš Tamás</td>
<td><a href="mailto:almastamas@example.com">almastamas@example.com</a></td>
</tr>
</tbody>
</table>
HEXAA at Hungarian Researcher Support

- Takes care of OpenStack authorization
  - Provisioning of OpenStack projects
- Custom UI for HPC
- Auxiliary tools
  - drupal site
  - ticketing
  - etc.
HEXAA at C4E and MTA Cloud
Perun in eduTEAMS: main highlights

● Integration with other systems
  ○ (De-)provisioning
  ○ Import capabilities
  ○ Full API support

● Account linking

● Privilege delegations

● Attribute framework

● Branding of user-facing components

● Stable development team
  ○ 8 core members + students
Name: Mgr. Slávek Licehammer
Role: PERUN / SECURITY ADMIN

Overview | Groups | Resources | Applications | Settings | Service identities | Sponsored users

Personal:
- Organization: Masarykova univerzita
- Workplace: FI
- Research group: MetaCentrum staff
- Preferred mail: slavek@ics.muni.cz
- Mail: slavek@ics.muni.cz
- Phone: +420 724 062 225
- Address: N/A
- Preferred language: en
- Local: 2 (verified identity)
- EDU person affiliation: N/A

Membership:
- Status: VALID
- Status change
- Expiration: never
- Member type: Person
- Sponsored by: N/A
- Member ID: 19179
- User ID: 3255
- Password reset: Send password reset request...
Perun example use-case

Building up eduTEAMS on top of existing AAI

- Case with existing active directory server and services connected to it
- Enhancing VO management capabilities
- Connecting services to eduTEAMS infrastructure
Conclusions

- With 3 MMS options we can cover all use-cases
  - Customization for dedicated and bespoke offering
  - Incorporating into existing environment
  - Data migration

- Consultation to select best MMS for particular user-case

- All MMS are available for tryout
  - https://www.eduteams.org
  - support@eduteams.org
Thank you

https://www.eduteams.org

support@eduteams.org