



UVOS and VOMS differences

Krzysztof Benedyczak
ICM Warsaw University

Introduction

- By "VOMS" I mean either VOMS-Admin or VOMS common properties (like DB schema) - depending on context.
- Purpose: establish a complete list of differences between VOMS and UVOS.
 - This list will be an input for selection of critical/important/nice-to-have features which are needed in VOMS for replacing UVOS.
 - It is much more important to know what UVOS features are not in VOMS.
 - Feature counterparts and ideological differences must be also collected.

Conceptual differences

- In VOMS the role is a special concept (e.g. one can assign (generic) attributes to role owners). In UVOS all attributes are "equal". VOMS uses special generic attributes.
- In VOMS one VO is served per server, and each user registered in VOMS is automatically member of this VO. In UVOS VO==top-level group, one server can serve multiple VOs, users can be registered in database without assignment to any of the VOs.
- The VOMS-Admin is managed by a WWW application. UVOS doesn't offer such (except for users registration and web authentication) but provides a sophisticated standalone GUI manager (RCP - eclipse based).
- UVOS and VOMS internal authorization is solved in a different way but at first it seems that possibilities offered by both solutions are similar.

UVOS features not present in VOMS

- Notifications: UVOS administrator may configure UVOS to send (currently email) notifications when any of the management operations takes place. This is useful when multiple admins maintain the DB.
- UVOS supports multiple identities which can represent the same person (e.g. different certificates).
- UVOS supports email-type identity (note that this is not an attribute) along with password used for authentication.
- UVOS supports SAML Web-based authentication. This allows web portal to be very easily integrated with authentication based on UVOS. If user has email identity in UVOS this allows for logging with user & password.

UVOS features not present in VOMS

- UVOS registration forms are quite different to what VOMS offers.
 - TODO - what is offered by VOMS registration form? How it is managed?
 -
 - UVOS: administrator can configure registration form dynamically using UVOS client.
 - Name, description, agreement.
 - Supported identity formats including CSR (if UVOS is integrated with an on-line CA) - for tutorials/open infrastructures etc.
 - Mandatory: primary group/VO.
 - Possibility to apply for additional subgroup membership.
 - and attributes (e.g. role).
 - User must fill what the form requires and provide some additional info about herself (e.g. email, telephone).

UVOS features not present in VOMS

- UVOS supports 3rd party SAML queries (under work in VOMS Admin)
- Attribute scopes: in UVOS all attributes can be group-scoped. In VOMS only the role.
- Attributes inheritance: in UVOS attributes assigned in subgroup are also visible in the parent group (e.g. role=admin in assigned in /users/staff is also valid in /users).
- TODO - describe management UI differences. Might result in several points.
 - Possibility to access demo VOMS-Admin?

UVOS features not present in VOMS

- UVOS can be deployed with embedded (no-config) database and with PostgreSQL and MySQL databases. Support for the two first is missing in VOMS.
- UVOS records all DB management events, therefore admin can check what happened. E.g. what identity removal actions were done since a given date.
- UVOS provides possibility to go back in time and browse (of course in read only mode) a snapshot of the database at a given point in the past.
- UVOS supports filtering of attributes served by SAML interface.

VOMS features not present in UVOS

- *Note: title has been changed!*
- UVOS doesn't support AUP management (except of showing a VO agreement upon users registration).
- UVOS doesn't issue ACs (so what is done by VOMS, and not by VOMS-Admin).
- It is not possible to assign a specified attribute to all owners of other attribute. VOMS supports this for the Role attribute.