Authorization Group Report

Authorization Group
(presented by Luciano Gaido, INFN Torino)

DataGRID WP6 Meeting
2 September 2002, Budapest

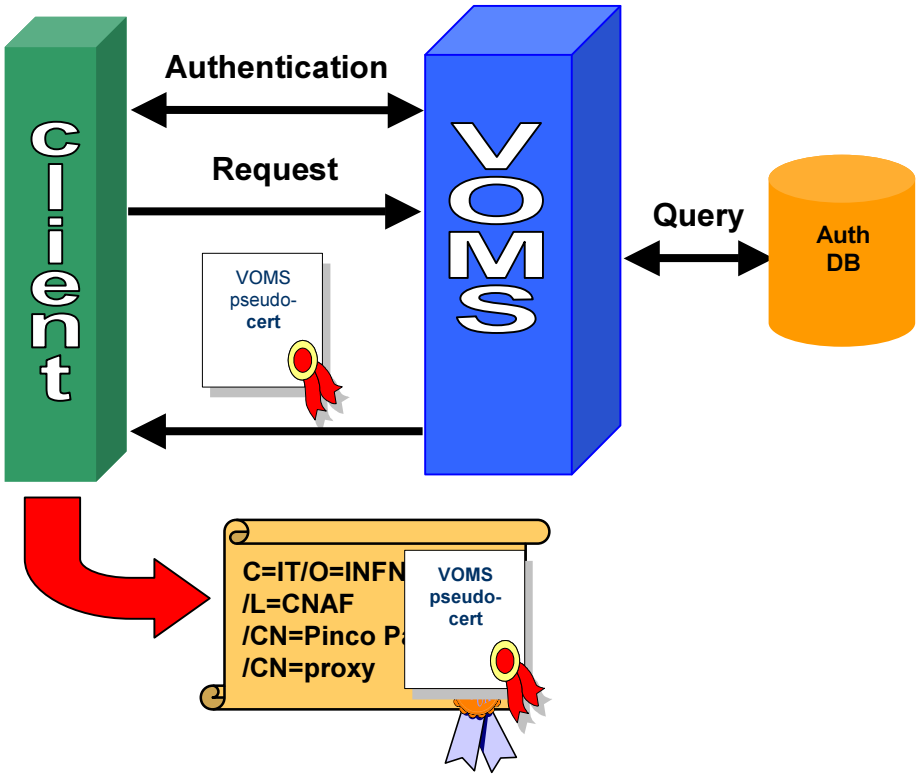
EDG Authorization System

- current implementation (VO LDAP)
  - support for multiple VO's
- future implementation
  - Virtual Organization Membership Service (VOMS)

current implementation (LDAP)

- Support for users belonging to more than one VO
  - **-vo** option to **grid-proxy-init** command;
  - the VO name is inserted in the Subject of the proxy certificate (**D** field);
  - requires a patch to Globus code (and a change to **mkgridmap**);
  - under test the interaction with RB;
  - availability: 30 September '02.

VO Membership Service



1. Client and server authenticate themselves and establish a secure communication channel using standard Globus API.
2. The Client sends the request to the Server.
3. The Server checks the request and sends back the required info (signed by itself).
4. The Client checks the validity of the info received.
5. Steps 1—4 are repeated for each Server the Client wants to contact.
6. The Client creates a proxy certificate with an extension (non critical) containing all the info received from the contacted VOMS Servers.

VOMS implementation

- In collaboration with CERN (Akos Frohner)
  - administration interface (API & GUI).
- Features:
  - uses a RDBMS (currently MySQL);
  - users can belong to groups (no subgroups) and can have roles;
  - replicas & traceability
    - it is always possible to roll-back the updates;
  - multiple administrators (controlled by ACL's).
- The "VOMS-enabled" proxy requires special handling at the local site (e.g. LCAS plugin).
- More info on:
  - **http://cvs.infn.it/VOMS/**
  - **http://ppewww.ph.gla.ac.uk/cgi-bin/cvsweb.cgi/edg-security-voms/**

VOMS availability

- user client (new command **voms-proxy-init**): available (interaction with RB to be tested);
- migration tools from VO LDAP servers: available;
- server: available;
- API & admin: 30 September '02.