LCG User registration issues

Maria Dimou - Ian Neilson (CERN/IT/GD) DRAFT

Material:

These are notes/actions deriving the 2003/12/15-17 workshop held at CERN.
Workshop agenda with links to the talks:
http://agenda.cern.ch/fullAgenda.php?ida=a036363

Design issues:

The following issues may apply to larger communities (HEP, EGEE, other Grids) but are written here with only the LCG in mind.

- **Registration Database** will be called, further on in this document, the part of user information that corresponds to his/her personal data.
- **User Registration** process means:
    - Acceptance by the user of the Guidelines (Usage Rules),
    - Verification of the user's information. This is done by the VO manager contacting the Institute Representative (Registration Authority, RA) and
    - Entry (sensitive personal data involved here) in the Registration Database.

  This is the Authentication part of the process. The VOX architecture provides VOMRS to handle this.

- **VO database** will be called, further on in this document, the part of the information that contains user's access rights on data stored at the resource (Group/Role in VOMS terms). This is the Authorization (AuthZ) part of the process.

The workshop suggested to propose to the GDB keeping the Registration database separate from the VO database but decentralise it, i.e. instead of one place for the whole community, (today's situation, interface: http://lcg-registrar.cern.ch) host it at the level of each VO and trust the VO managers will only admit new users once their identity is checked and the Guidelines are accepted.

Points to discuss at the GDB 2004/01/13 meeting:

An update of the, GDB-approved, Registration document (https://edms.cern.ch/file/428034/1/LCG_User_Registration.pdf) is necessary to re-iterate the set of required data and clarify the policy on their validity check:

- "Institute":
    - The field must be present in the Registration database, because it is used, indirectly, to check the user's eligibility to be included in a VO. The tool(s) should provide a scroll-down menu of Institutes associated with the VO.

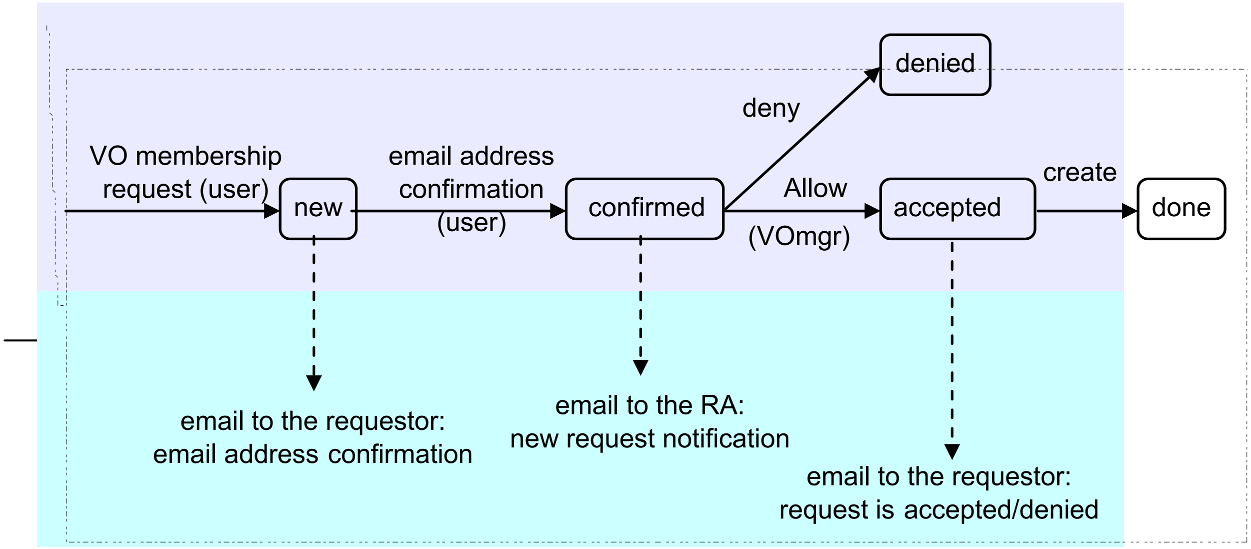
  - The user must select his/her Institute for the registration process to complete successfully. If it is not present in the list, (s)he must be able to enter his/her Institute's name in the registration request and leave the VO manager to check whether it should be, from now on, associated with the VO.
- "Institute Representative":
  - The VO manager must have a list of official RAs per Institute and follow a procedure, which could be offline, i.e. by email to obtain, from the relevant RA taking responsibility for the user, the approval of this new member in the VO. This step is mandatory for the Authentication part of the process, before deciding whether to admit a new member in the VO database.
- Sites' notification on new member registration:
  It is suggested to change the Registration document (section 3, note f) to a "site subscription model", where a site interested in (new) VO member(s) information will have to query the VO database, provided the tool(s) offer this functionality. Today, the VO managers must inform all LCG sites about the acceptance of new member but the community believes this procedure is not useful.

Once the above are defined, the community has to decide on the tools which map closely to the agreed procedures.

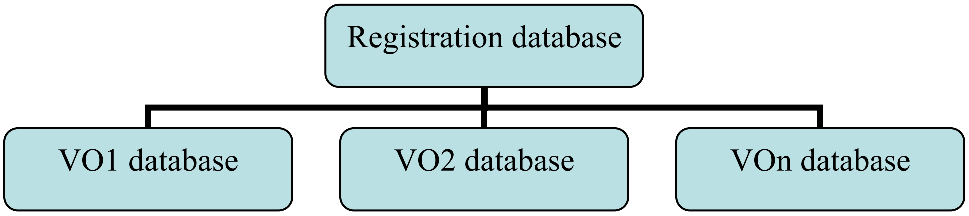
Technical points to be decided within LCG (which body?):

Registration issues:
There is a need for the presence of the "Institute" field in whichever tool we'll be using, before the VO managers can agree to admit new users in the VO. This information exists in today's LDAP-based tool (it has to be typed by the user) and VOX/VOMRS but not in VOMS).
The inclusion of the "Institute Representative" (RA) field has practical advantages especially if it is implemented with the relevant software support, i.e. if the approval request to the RA is automatically generated. The RA field exists in VOMRS but not in LDAP or VOMS.

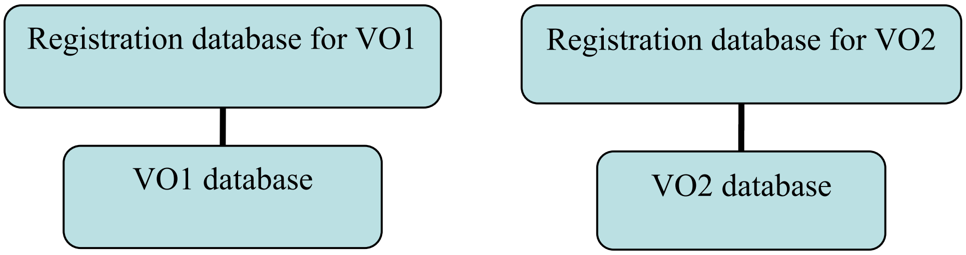
The following figure, based on an original by A.Frohner, contains a sequence diagram of registration process.


VO membership request (user)
new
email address confirmation (user)
confirmed
deny
denied
Allow
(VOmgr)
accepted
create
done
email to the requestor: email address confirmation
email to the RA: new request notification
email to the requestor: request is accepted/denied

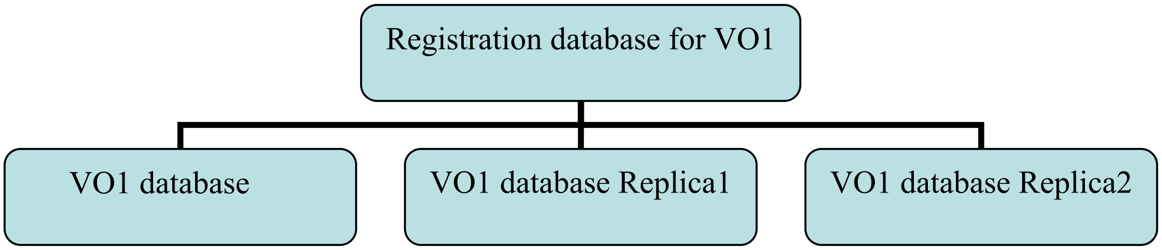
The following figure describes today's situation in LCG, based on LDAP, using servers lcg-registrar.cern.ch (Guidelines' database), lcg-vo.cern.ch (DTEAM VO) and grid-vo.nikhef.nl (LHC experiments' VOs):

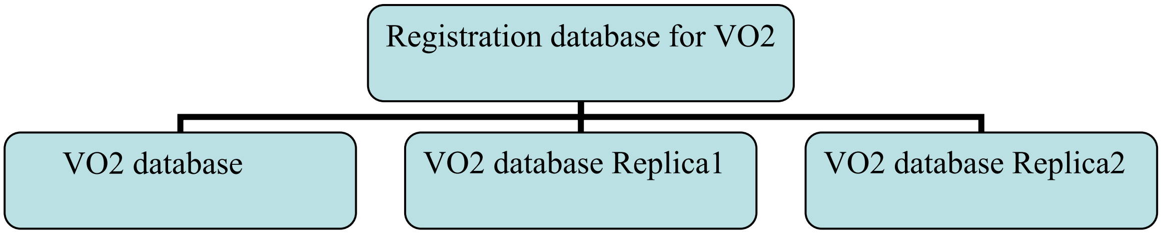


The following figures describe the "decentralised" model to be suggested to GDB:



Data replication issues (both databases):
It is, probably, harmless to keep replicas of the VO database at each site for performance reasons but not desirable to keep replicas of the Guidelines' database due to security and privacy issues. The following figures demonstrate this.
Action: LCG Security Group to publish this policy.


Registration database for VO1
VO1 database
VO1 database Replica1
VO1 database Replica2


Registration database for VO2
VO2 database
VO2 database Replica1
VO2 database Replica2