LDAP CA Authorization management

Conrad Steenberg

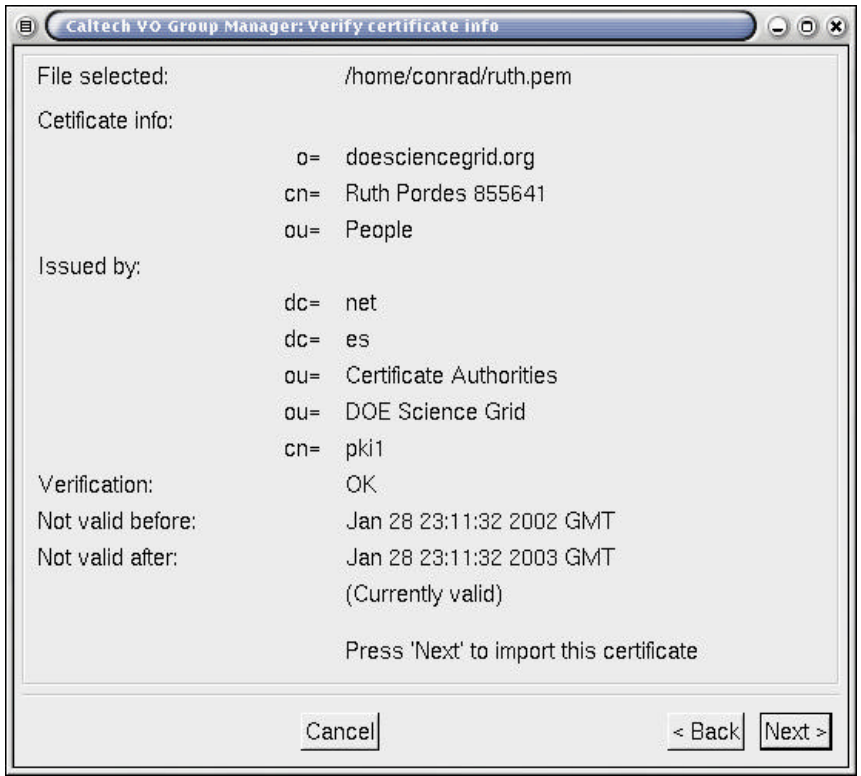
Caltech/CMS/PPDG

May 22, 2002

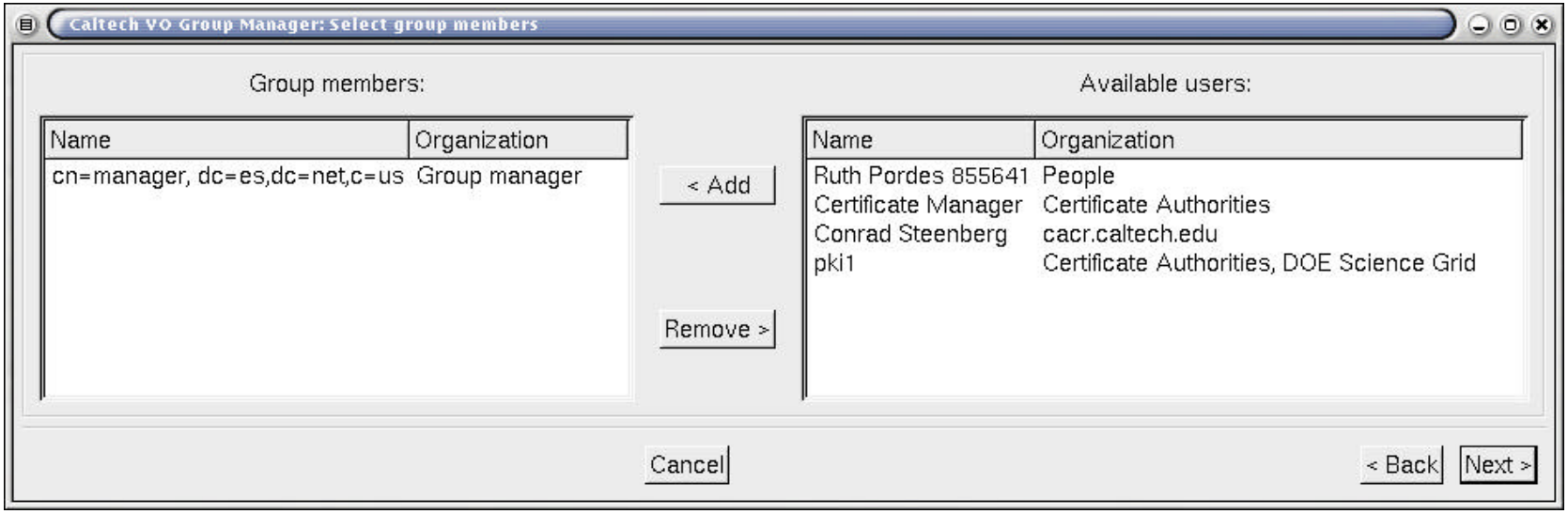
- Authorization management needed at Grid resource sites (CPU/storage) as Grid scales
- This eliminates the need to require that all users to have accounts at all sites
- A Virtual Organization (VO) is a way of distributing authorization management while maintaining:
  - Individual sites' control over authorization
  - The ability to grant authorization to users based upon a Grid identity established by the user's home institute
- This is accomplished by defining groups of users based on certificates issued by a Certificate Authority (CA)
- At a Grid site, these groups are mapped to users on the local system via a gridmap file (similar to an ACL)
- The person can log onto the Grid once, and be granted access to systems where the group has access

- In order to manage the VOs that are being set up, an infrastructure is being developed
  - A Certificate Authority (ESnet) - done
  - A group database (CA LDAP)
  - Group database administration (GroupMan, INFN scripts)
  - Gridmap file creation tools (EDG mkgridmap)

- Maintains a replica of certificates, which can be remotely accessed
- INFN CA LDAP uses a list of pem-encoded certificates to construct the database
- Or use a replica from a central LDAP server
- Caltech GroupMan script eases certificate management in this database



- GroupMan GUI interface to manage groups
  - Initialized empty database
  - Create/delete groups
  - Add/delete users from groups
  - Stores the results in a world-readable LDAP database



This is arguably the most important set of tools:

- Generates gridmap authorization files used by Globus for access to resources
- Uses a text configuration file *mkgridmap.conf* to bind group/user information from the LDAP directory to resources
- *A script creates gridmap files either automatically or manually after changes to the LDAP directory or the configuration file*

```
/C=US/O=Globus/O=California Institute of Technology/CN=Asad Samar globus
/C=US/O=Globus/O=California Institute of Technology/CN=Koen Holtman koen
/O=Grid/O=Globus/OU=cacr.caltech.edu/CN=Suresh M. Singh suresh
```

- The tools are available, needs to be deployed
- Central LDAP server for group database must be created and populated - ESnet an ideal candidate
- Designated site representatives should be able to modify their group lists - gentleman's agreement since LDAP doesn't allow fine-grained access control