BNL VO Management and Grid Mapfile Generation

Brookhaven National Lab

The packages I am using:

GroupMan:

http://heppc22.hep.caltech.edu/groupman/

VO server management tools

http://cvs.infn.it/cgi-bin/cvsweb.cgi/Auth/VO/sbin/

new edg-mkgridmap package

http://www.fis.unipr.it/pub/edg/repository/datagrid/

http://grid.sinp.msu.ru/distribution/datagrid/wp6/RPMS/

Advantages of project.

Help VO manager keep track of collaborators.

Provide a single-sign-on service for each user, Each user will be authenticated by VO manager once, he/she will be authorized to use the computing resource within organization.

Help site administrators to maintain grid-mapfile automatically. Avoid the hassle of constantly editting gridmapfile per individual request.

EDG Authorization Structure

Each VO Server uses CA server: an LDAP Directory with the issued certificates.

Each VO manages an LDAP Directory (o=atlas,dc=ppdg-datagrid,dc=org):

members (**ou=People**);

groups (e.g. **ou=us-atlas general, us-dc1, us-dc2**):

- each user **must** belong to server groups;

each user entry contains:

- the URI of the certificate on the CA LDAP server;
- the Subject of the users certificate.

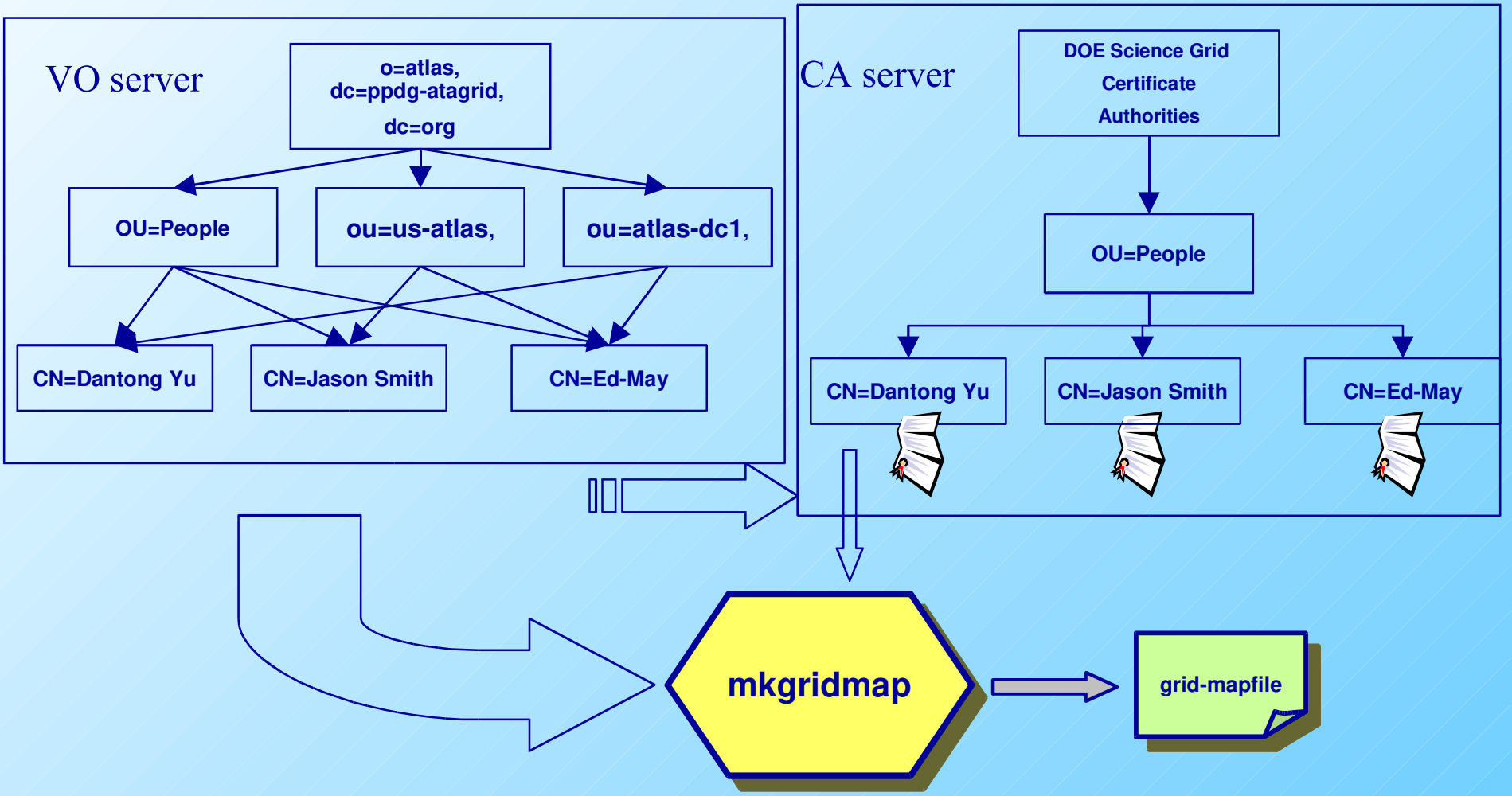
grid-mapfile**s are generated from the VO Directories:**

looking for the members of the groups;

according to users attributes (For example,the Certificate Subject);

with different local policies

grid-mapfile generation



PPDG

BROOKHAVEN NATIONAL LABORATORY

VO Manager

Insertion of users:

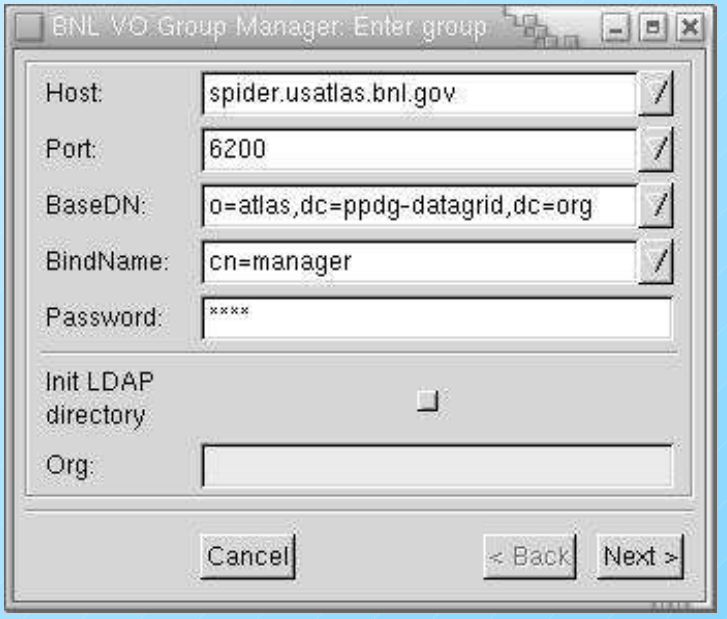
from CAs LDAP servers:

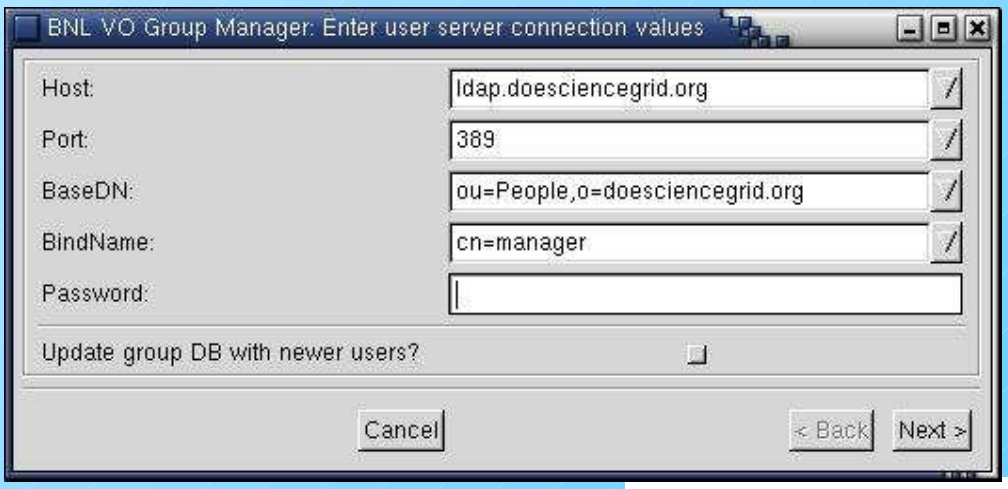
1. VO manager specifies CA and VO Directories
2. users entries are read from the specified CA Directory;
3. validity of users certificates is checked;
4. Selected users will be saved into VO server.

from certificate files: **cert2ldif.pl**

- reads user certificate;
- produces an LDIF file for the insertion of the user.

Consistency check between VO and CA Directories: Update VO server user information with CA user information.

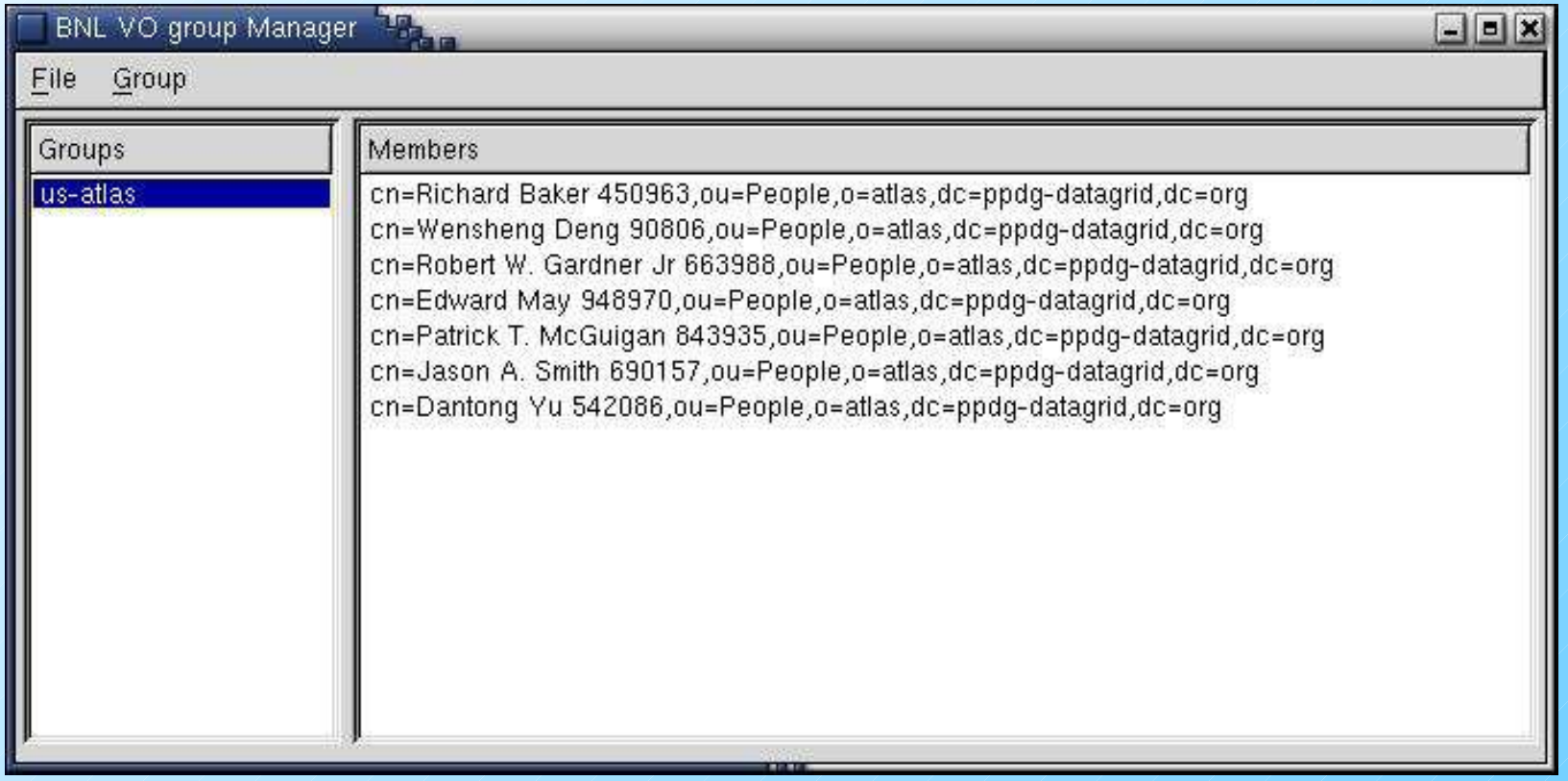




PPDG

BROOKHAVEN NATIONAL LABORATORY

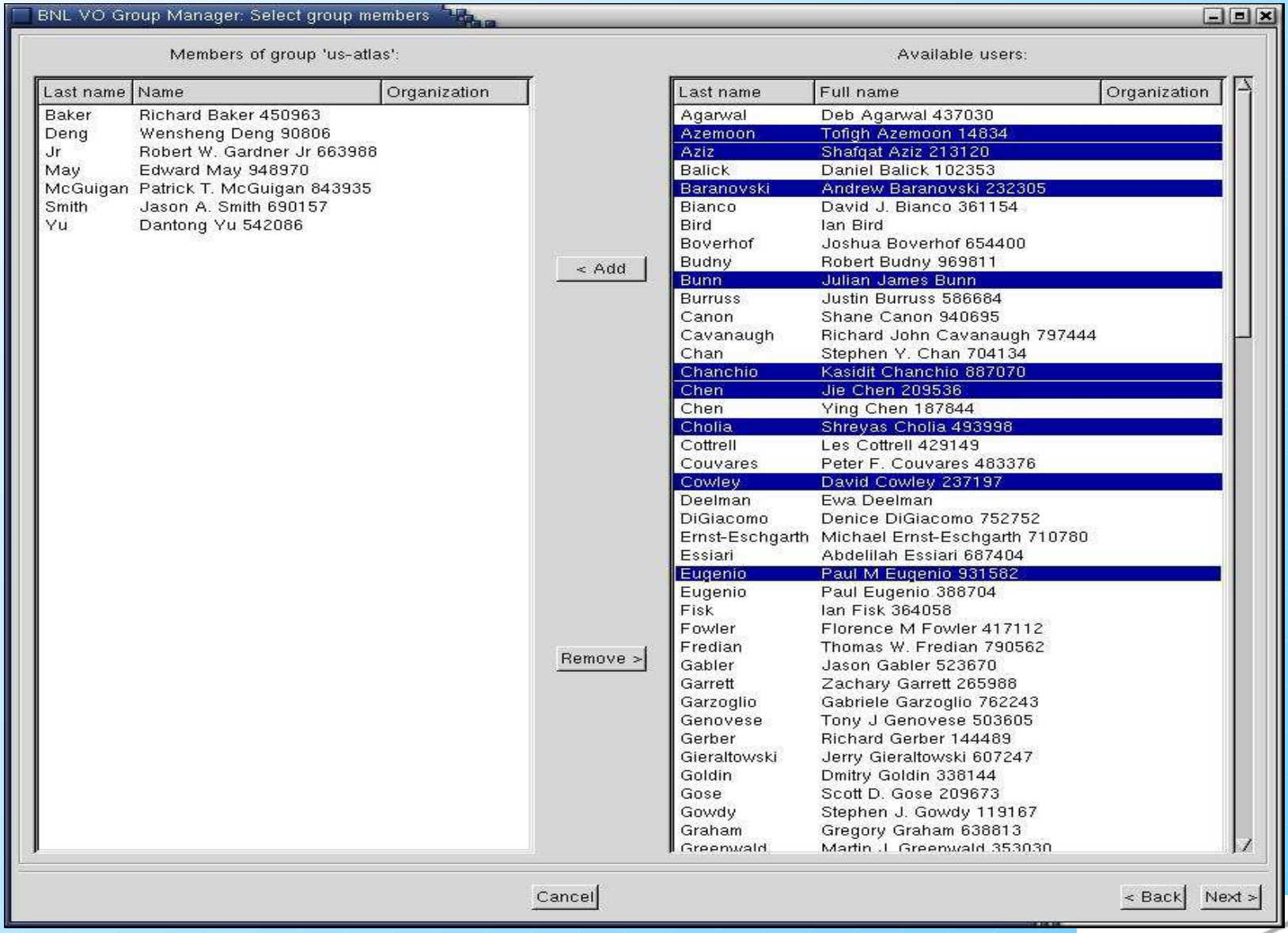
Group management



PPDG

BROOKHAVEN NATIONAL LABORATORY

Add Group Members



PPDG

BROOKHAVEN NATIONAL LABORATORY

Configure mkgridmap.conf

```
#### GROUP: group URI [lcluser]
group ldap://spider.usatlas.bnl.gov/ou=us-atlas,o=atlas,dc=ppdg-datagrid,dc=org AUTO atlas_grid_default
#group ldap://grid-vo.nikhef.nl/ou=testbed1,o=atlas,dc=eu-datagrid,dc=org
#group ldap://grid-vo.nikhef.nl/ou=testbed1,o=cms,dc=eu-datagrid,dc=org
#group ldap://grid-vo.nikhef.nl/ou=testbed1,o=lhcb,dc=eu-datagrid,dc=org
#group ldap://grid-vo.nikhef.nl/ou=testbed1,o=earthob,dc=eu-datagrid,dc=org

#### Optional - DEFAULT LOCAL USER: default_lcluser lcluser
default_lcluser AUTO
```

Grid-mapfile generated

"/O=doesciencegrid.org/OU=People/CN=Dantong Yu 542086" dtyu

"/O=doesciencegrid.org/OU=People/CN=David Adams 287950" dladams

"/O=doesciencegrid.org/OU=People/CN=Edward May 948970" enm

"/O=doesciencegrid.org/OU=People/CN=Frederick Luehring 26143" luehring

"/O=doesciencegrid.org/OU=People/CN=Iwona Sakrejda 302074" sakrejda

"/O=doesciencegrid.org/OU=People/CN=Jason A. Smith 690157" smithj4

"/O=doesciencegrid.org/OU=People/CN=Jerry Gieraltowski 607247" atlas_grid_default

"/O=doesciencegrid.org/OU=People/CN=Mark Sosebee 270653" atlas_grid_default

"/O=doesciencegrid.org/OU=People/CN=Patrick T. McGuigan 843935" atlas_grid_default

"/O=doesciencegrid.org/OU=People/CN=Pavel Nevski" nevski

"/O=doesciencegrid.org/OU=People/CN=Richard Baker 530597" rbaker

"/O=doesciencegrid.org/OU=People/CN=Robert W. Gardner Jr 663988" rwg

"/O=doesciencegrid.org/OU=People/CN=Shane Canon 940695" atlas_grid_default

"/O=doesciencegrid.org/OU=People/CN=Shawn McKee 83467" smckee

"/O=doesciencegrid.org/OU=People/CN=Thom Sulanke 1375" atlas_grid_default

"/O=doesciencegrid.org/OU=People/CN=Torre Wenaus 181507" wenaus

"/O=doesciencegrid.org/OU=People/CN=Wensheng Deng 90806" wdeng

Current Status

Set up VO server at BNL.

We worked with GroupMan Developer on certificate format which could by recognized by GateKeeper.

First version of Gridmap toolkits is created from EDG-GridMapfile Toolkits, with some enhancements which follows the local policy and requirements of each individual testbed site.

Created grid-mapfile pacman package, Eight US Atlas testbeds started to deploy it.

Most of US ATLAS do not have DOE certificates. We will encourage users to apply for the certificates.

Near Term Plan

- **Each Site needs to install several EU data grid signing policy files. Dantong will follow up a tar file for all EU data grid testbed: CERN, Czech Republic CESNET, France CNRS,France - CNRS Datagrid-fr, German Grid, Ireland - Grid-Ireland, Italy INFN, Netherlands NIKHEF, Nordic countries NorduGrid, Portugal LIP, Russia - Russian DataGRID, Spanish - DATAGRID-ES, United Kingdom GridPP, US - DOE Root CA, US - DOE Sub CA**

- **Each Site Periodically Downloads The User Lists From Each VO using the gridmap file management tools.**

- **The Combination Of Utilities And Manual Intervention Will Create And Manage A Set Of Local Accounts And A grid-mapfile**

- **BNL Will Continue to Design The Local Account Management As Much As Possible.**

Future Plans

Security Model Replaces the Password authentication

Support More for users attributes in the VO Directories;

Web Interface to Manage the VO server.

Develop Tool For Automatic Account Creation, Management And Mapping