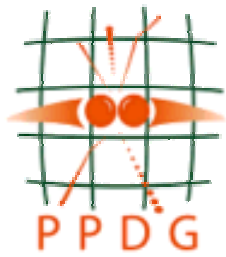


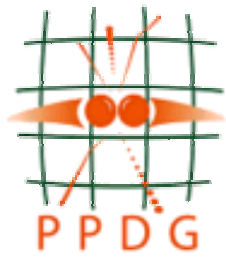
Certificates, Authorization activity in US

D. Olson, LBNL
21 Jul 2002
HICB meeting
Edinburgh

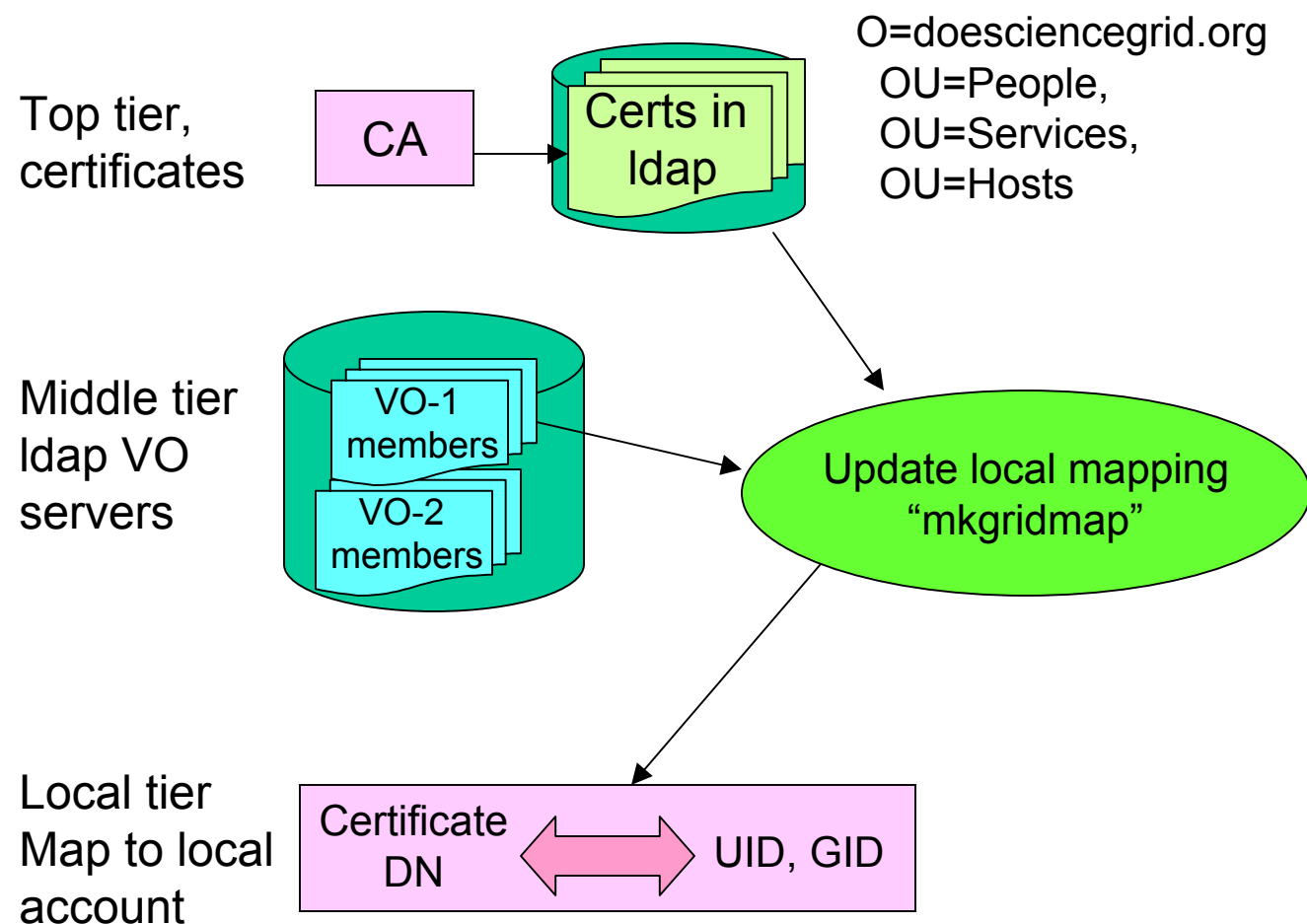


Contents

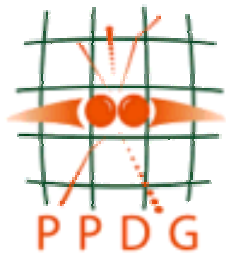
- 3 level architecture
- Certificates
- Authorization
- Near future
 - BOF at GGF5 on grid - site facilities issues
 - Looking at lcas/lcmaps, CAS alphaR2



3-tier implementation architecture

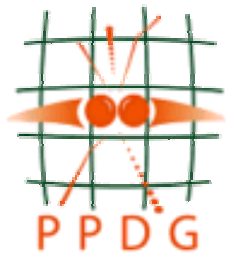


Many open issues:
 technical solutions in progress
 AUP, user registration for multi-site access is next big issue



CA status

- DOE Science Grid CA very successful
 - Many RA's, including iVDGL
 - Moved entry point to doegrids.org domain
 - To distinguish from DOE Science Grid Collaboratory Pilot SciDAC project
- DOE and EDG CA signing certificates being included in VDT



DOEGrids Certificate Service - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print Mail

Address <http://www.doe grids.org/> Go Links

Google Search Web Search Site PageRank Page Info Up Highlight

DOEGrids Certificate Service

DOEGrids is funded by the DOE MICS program and operated by ESnet

REGISTRATION AUTHORITIES

- PPDG
- FusionGRID
- VDGL
- NERSC
- PNNL
- ANL
- LBNL
- ORNL
- DOESG
- ESG Application**

PEER CERTIFICATE AUTHORITIES

- European Data Grid
- Cross Grid CA

A 3D illustration of a classical building with four columns and a pediment. A spiral of binary code (0s and 1s) winds around the columns. Several small human figures are standing on the steps and around the base of the building. One figure in the foreground is holding a large red ribbon.

SERVICE LINKS

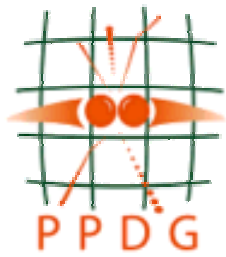
- How to Request Certificates
- Policy Management Authority
- Certificate Service
- Directory Service

SERVICE DOCUMENTS

- CP/CPS
- CRLs
- CA Certificates
- Certificate Request Workflow

Welcome

Internet

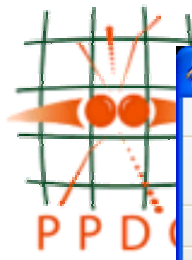


VO GroupMan

Conrad Steenberg

<http://heppc22.cithep.caltech.edu/groupman/index.php4?intro>

- Python program
 - Create ldap directory using INFN structure and schema for inetorgperson, pkiuser.
 - Load names from ldap certificate publishing directory
 - Minor format issue (, vs. / in DN string)
 - Create group for VO (I.e., USCMS)
 - Edit group membership
- Run edg-mkgridmap for multiple VO servers to create full grid-mapfile
 - Tested using servers in EU, US



Caltech Virtual Organization Group Manager : Information : News - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Refresh Print Mail Stop

Address <http://heppc22.cithep.caltech.edu/groupman/index.php4?intro+news> Go Links

Google pgp freeware Search Web Search Site PageRank Page Info Up Highlight pgp freeware

GroupMan

Information
> News
Screenshots
Download

News

Jul 15, 2002

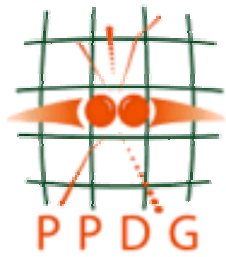
New release 0.3.0.

This is the result of a week's hacking at FNAL. Thanks to Yujun and Scott for more testing!

Changelog

- The internal organization of the LDAP directory was changed to match the EDG setup. Thanks to Roberto Cecchini for his help to get this right. The edg-mkgridmap tool can now be used to create grid-map files from directories created by VGroup, as well as the INFN VO scripts.
- All downloads are now asynchronous, with plenty of feedback during the downloads. Hopefully this should mostly eliminate the 'blank wizard window' effect seen when downloading data from slow sites.
- Fixed a bug where the application would crash when no ~/VOgrouprc file
- User information can now be downloaded from multiple CAs, and stored in the same directory as the group information. was found.

Internet



"This version has been tested to work with the DOE Science Grid and several EDG CAs, and it is now possible to build groups consisting of users from any of these CAs irrespective of certificate origin." - C.S.

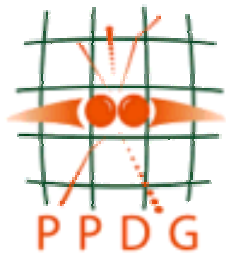
A screenshot of the LDAP Browser/Editor v2.8.2 application window. The title bar shows the path [ldap://hepgrid1.caltech.edu/dc=es,dc=net,c=us]. The interface includes a menu bar (File, Edit, View, LDIF, Help) and a toolbar. On the left, a tree view shows the directory structure: dc=es,dc=net,c=us > cn=manager > ou=People. The main pane displays a table of LDAP attributes for the selected entry: ou=People.

Attribute	Value
dc	People
ou	People
objectClass	top

A screenshot of the 'Caltech VO Group Manager: Select group members' dialog box. It is used to manage the members of a group named 'uscms'. The dialog is split into two panes: 'Members of group 'uscms':' and 'Available users:'. The 'Members' pane contains a table of current group members, and the 'Available users' pane contains a list of potential members. Buttons for '< Add', 'Remove >', and 'Cancel' are visible. At the bottom right, there are '< Back' and 'Next >' navigation buttons.

Name	Organization
Chip Watson 312066	
Douglas L Olson	
Jiewei Lin 373105	
Joshua Boverhof 654400	
Ruth Pordes 855641	
Von S Welch 574014	
cn=manager, dc=es,dc=net,c=us	Group manager

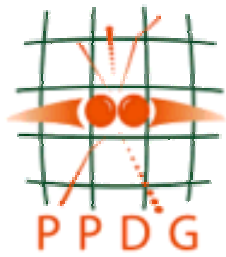
Name	Organization
David Paul 163033	
Michael Hand 734934	
Stephen Y. Chan 704134	
David Cowley 237197	
Paul M Eugenio 931582	
Peter F. Couvares 483376	
mary TDC 385323	
Shane Canon 940695	
Keith R. Jackson 719270	
Shreyas Cholia 493998	
Kasidit Chanchio 887070	
Timur Perelmutov 141265	
Patrick T. McGuigan 843935	



PPDG Site-AAA

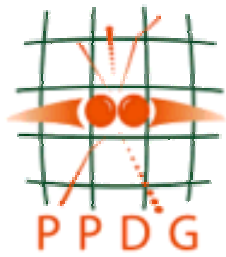
(authentication, authorization, accounting)

- Working on the authentication/authorization part
- Becoming aware of LCAS/LCMAPS (VoMS?)
- Caltech (Conrad) - VO server (GroupMan)
- FNAL - KCA/KX509
- BNL - "automated" local account creation for VO users
- Jlab - integrated GSI with data access/replication
- SLAC - starting on KCA/KX509
- LBNL/NERSC - ldap authentication



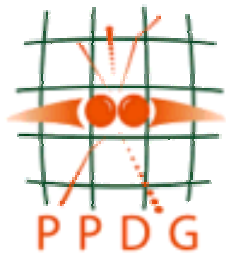
FNAL

- Have working KCA which generates proxy X509 certificate from Kerberos credentials
- Addresses private key management issues
- Can use existing user registration and Kerberos infrastructure to provide GSI credentials
- Looking at how to deal with CA signing certificate chain
 - I.e., does DOESG CA sign FNAL KCA?



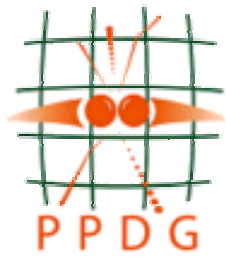
BNL

- Some sites require individual accounts for users
- Planning to develop procedures and mechanism to collect user information so accounts can be created at several sites without user applying independently for several accounts
- Leads to many issues of local policy



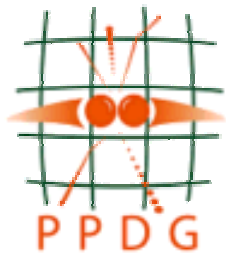
LBNL

- Testing INFN VO server in NERSC environment, integration with user database
- Looking at ldap authentication to generating proxy certificate (like myproxy), for private key management issues



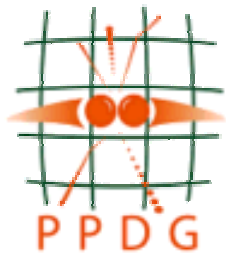
SLAC

- Recently hired person to address AAA issues
- Planning KCA/KX509 usage like FNAL



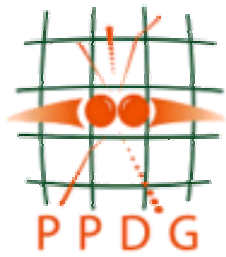
Jlab

- Have integrated GSI with data access services
- Integrating GridFTP with storage system, testing with FSU site
- Looking at globus/firewall issues



CAS / LCAS

- Recently started looking at LCAS/LCMAPS, VoMS
- Initial view looks good, similar to ideas discussed with Von Welch for putting PAM-like interface in gatekeeper
- Globus CAS alphaR2 modifications resulting from discussions in April/May
 - Due to be released soon
 - Will look at detailed issues when available for test



BOF at GGF5

- Move to formation of research group
- Address AAA issues of production computing sites integrating with grid, not just testbeds
- Welcome participation of European site/facilities personnel
- Tuesday evening