Managing Virtual Organizations (VO) at DESY using LDAP

Karen Mkoyan

Yerevan State University, Armenia
E-mail: karen.mkoyan@yerphi.am
August/September 2004
DESY, Hamburg

While participating in the DESY Summer Student Program in the IT group, an administration tool to manage Virtual Organizations (VO) at DESY was developed. It exploits LDAP. The central DESY LDAP server holds sensitive information like e-mail addresses which should not be exposed. Hence, a separate LDAP server would hold only grid specific information (Name, Subject of user certificate, the institution, etc). It should be managed in a way, that every VO (Virtual Organization) should have a possibility to be administered by a separate administrator, the VO Admin. The server should be located on the demilitarized zone (DMZ) of the network to guarantee the highest security. Additional task(s) also included developing of script based mechanism of creating grid map files querying the LDAP server, and deploy other scripts in order to serve VOs in a more efficient way.

1 Introduction

DESY has started Grid Activities beginning of 2003. Since 2004 the DESY Grid Testbed2 is in operation, exploiting middleware of the LHC Computing Grid (LCG-2). In this context DESY has become an official LCG-2-site in the so-called LCG TestZone. The LCG-2 activities are carried out in the context of the EU-project Enabling Grids for E-science in Europe (EGEE) which started on April 1st, 2004. DESY is one of 70 partners, aiming on installing and operating a Grid infrastructure for e-science. DESY is also founding partner of a German-wide initiative to exploit Grids for e-science called D-GRID.
Currently a production-grade Grid infrastructure is being prepared at DESY to enable DESY groups and HERA-experiments to use Grids for data processing, e.g. *Monte Carlo* production.

2 The Virtual Organizations (VO)

Grid experts argue that the Grid will be fully exploited only when people will have the means to quickly and conveniently build Virtual Organizations (VO). What are they talking about?

Consider a group of people that, for any reason, share a common "computationally demanding" or "data-intensive" goal. These different groups share the same needs. To achieve their goal, they need to perform several types of demanding calculations which can not be handled with the resources belonging to just one of participants. Otherwise they would need to access each others' databases in a well-defined and secure way.

The VO is used in the implementation of the authorization phase of user task. Basically, VOs are used to organize the credentials (certificate subject lines) of sets of users into different subgroups. When a user submits a task request, the user's certificate information is compared with a file which is populated by information from the various VOs.
A user who is the member of 'zeus' VO, has strong restrictions, and can work within that VO only.

On the other hand for the person/VO mapping the database is needed. For the implementation of that database LDAP was chosen, see below “What is LDAP”.
The question of LDAP administration and fast access are described below in “VO administration tools” part.

Below are the figures of grid-vo.desy.de LDAP server:

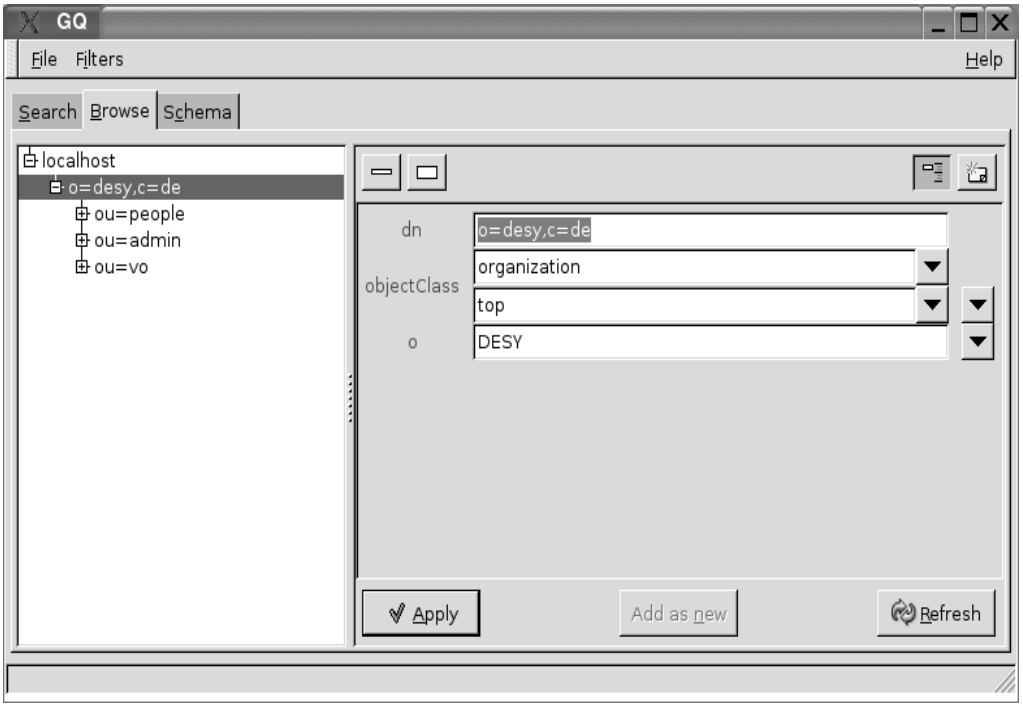

Figure 1: The LDAP server has 3 sub-trees, 'people', 'admins' and 'vo'

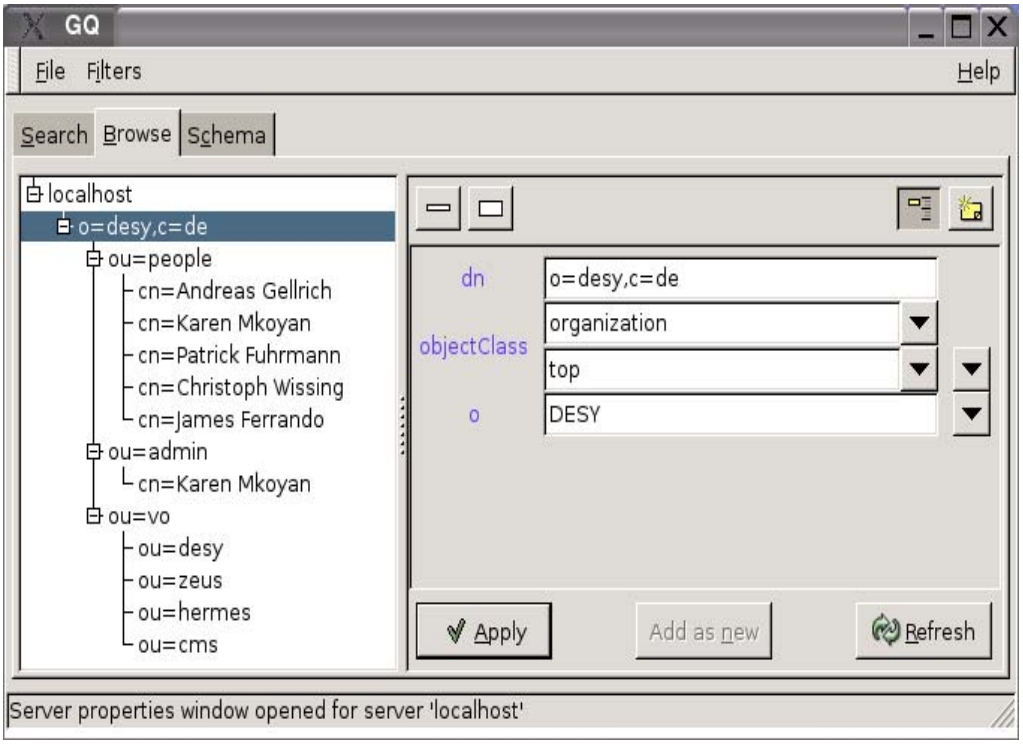

Figure 2: All trees are expanded.

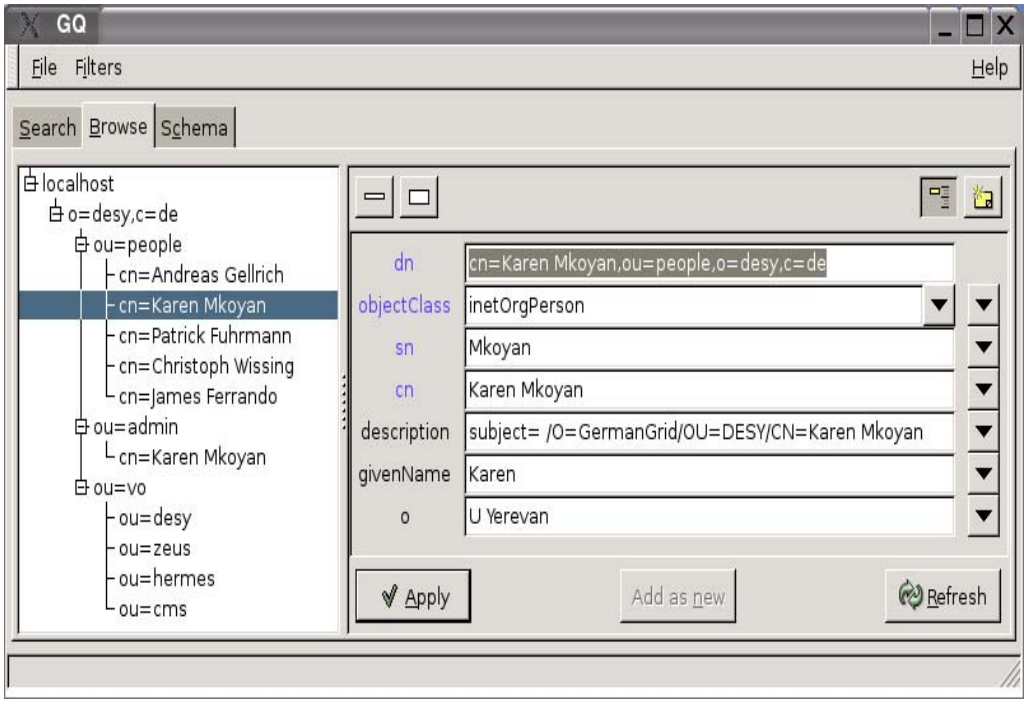

Figure 3: Person 'Karen Mkoyan' expanded, viewing details.

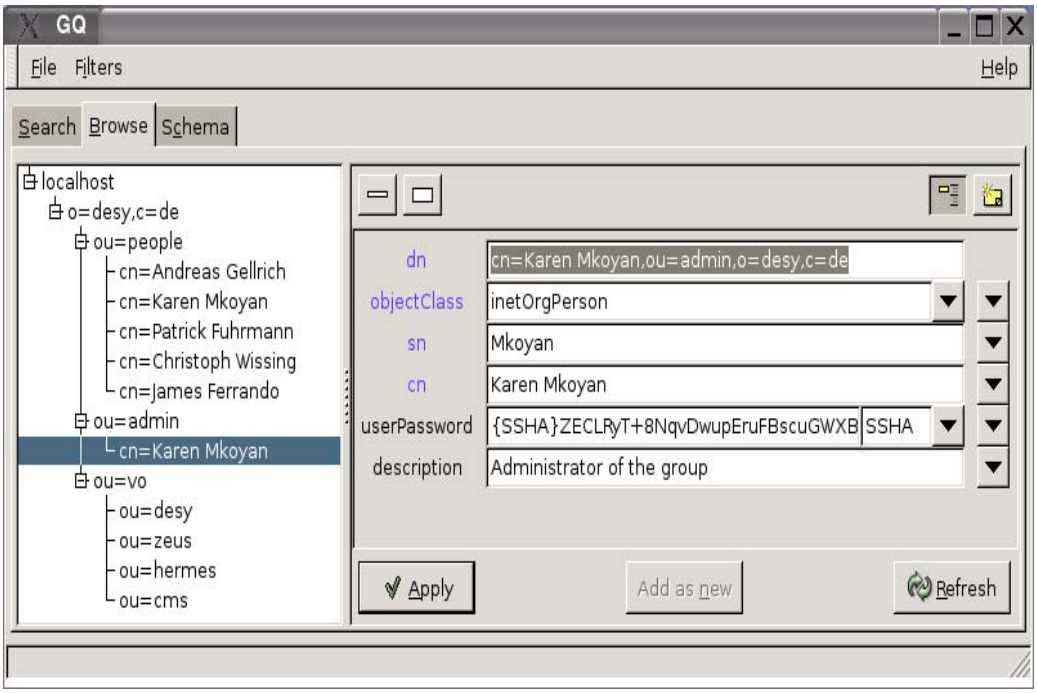

Figure 4: Group Administrator 'Karen Mkoyan' expanded, viewing details.

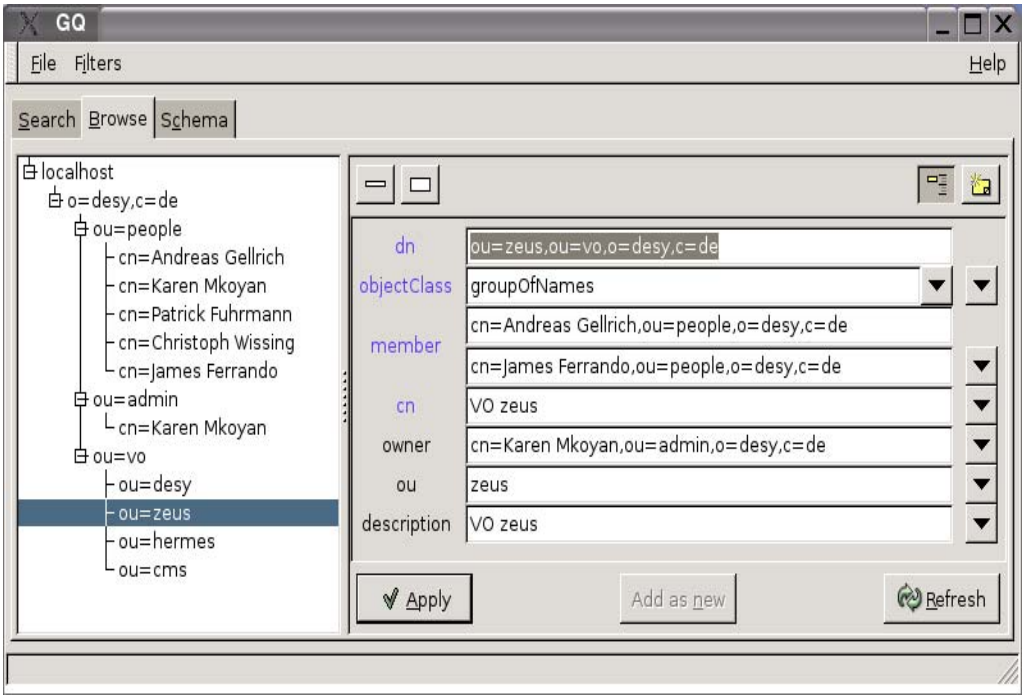

Figure 5: Group Administrator 'Karen Mkoyan' is the owner of VO 'zeus'.

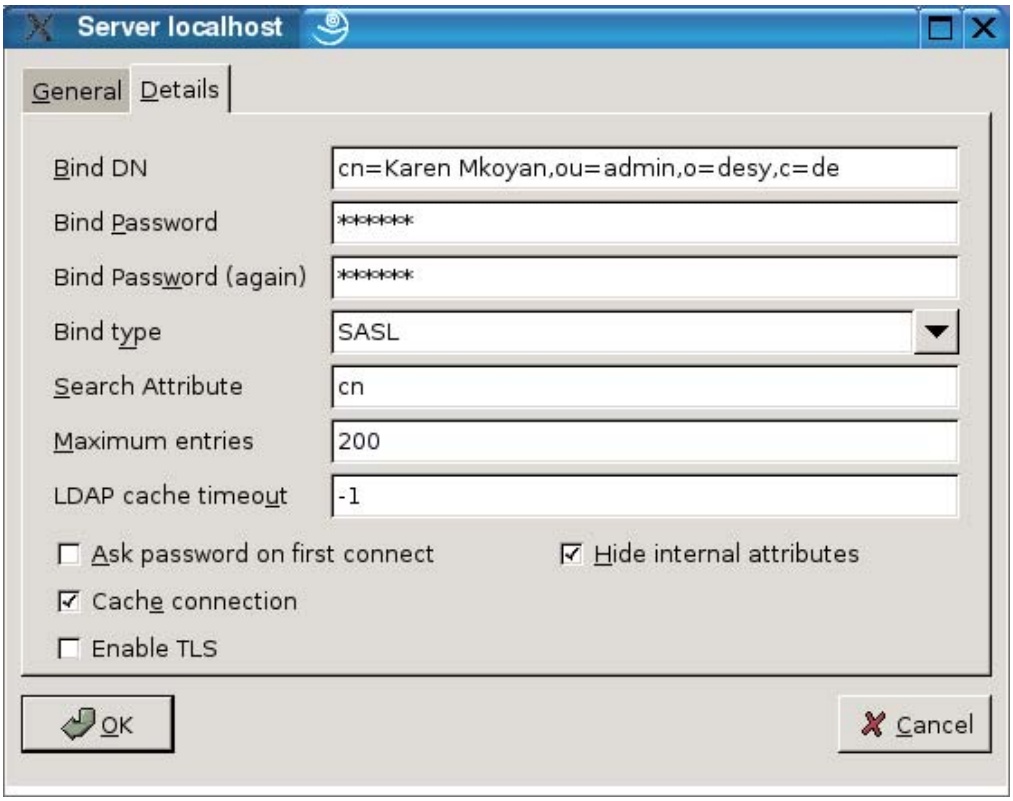

Figure 6: The DN to bind with to the LDAP server.

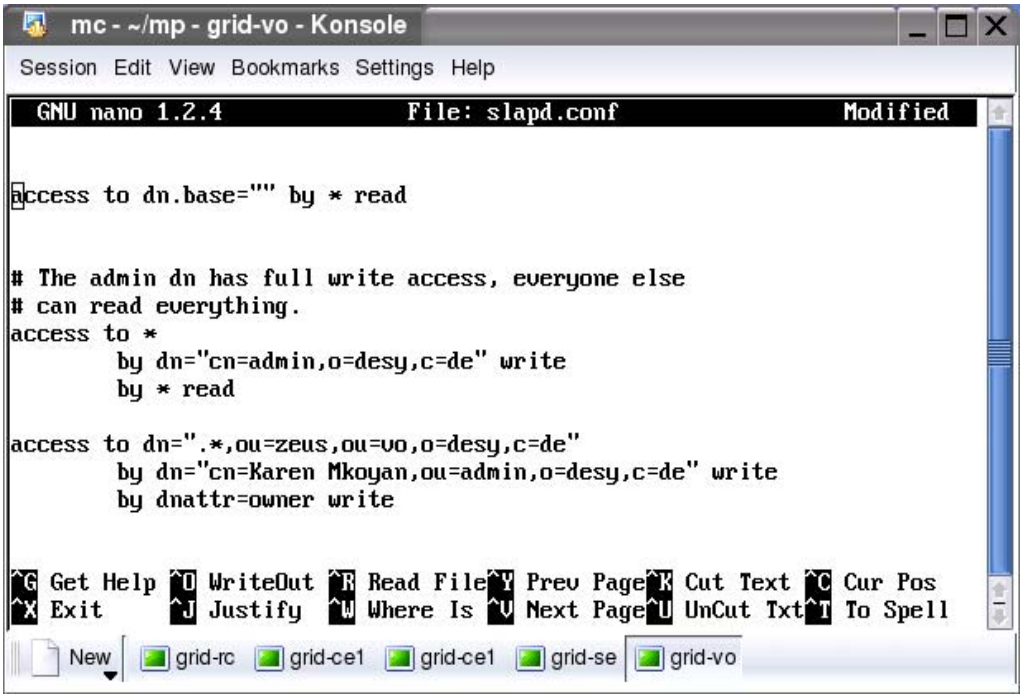

Figure 7: A part of the LDAP server configuration file, 'Karen Mkoyan' is VO 'zeus' admin.

3 What is LDAP?

LDAP (Lightweight Directory Access Protocol) is a directory service which allows to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet. LDAP is a "lightweight" (smaller amount of code) version of Directory Access Protocol (DAP), a standard for directory services in a network. LDAP originated at the University of Michigan and has been endorsed by at least 40 companies.

In a network, a directory tells you where in the network something is located. On TCP/IP networks (including the Internet), the domain name system (DNS) is the directory system used to relate the domain name to a specific network address (a unique location on the network). However, you may not know the domain name. LDAP allows you to search for an individual without knowing where they're located (although additional information will help with the search).

An LDAP directory is organized in a simple "tree" hierarchy

consisting of the following levels:

- The root directory (the starting place or the source of the tree), which branches out to:
- Countries, each of which branches out to:
- Organizations, which branch out to:
- Organizational units (divisions, departments, and so forth), which branches out to (includes an entry for):
- Individuals (which includes people, files, and shared resources such as printers)

An LDAP directory can be distributed among many servers. Each server can have a replicated version of the total directory that is synchronized periodically.

4 Understanding DMZ

In computer networks, a DMZ (*demilitarized zone*) is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data. (The term comes from the geographic buffer zone that was set up between North Korea and South Korea following the UN "police action" in the early 1950s.) A DMZ is an optional and more secure approach to a firewall and effectively acts as a proxy server as well.

In a typical DMZ configuration for a small company, a separate computer (or host in network terms) receives requests from users within the private network for access to Web sites or other companies accessible on the public network. The DMZ host then initiates sessions for these requests on the public network. However, the DMZ host is not able to initiate a session back into the private network. It can only forward packets that have already been requested.

Users of the public network outside the company can access only the DMZ host. The DMZ may typically also have the company's Web pages, in this practical example it holds LDAP Database. These could be served to the outside world. However, the DMZ provides access to no other company data.

5 VO administration tools

There are several graphical tools for LDAP server administration, see below:

Kldap is a graphical LDAP client written for KDE. Kldap has a nice interface and is able to show all the information tree stored on your Directory. Some screen shots of the application and downloads are available at: http://www.mountpoint.ch/oliver/kldap/

KDirAdm is a management tool written for the KDE. It aims to provide all of the functionality of most commercial directory management tools: http://www.carillonis.com/kdiradm/

Directory Administrator is the most widely used GNOME application for managing UNIX users and groups on LDAP directory servers. Directory administrator allows you to create and delete users and groups, and manage your users associated address book information, per-server access controls and sendmail mail routing: http://diradmin.open-it.org/index.php

GQ is another graphical LDAP client with a simpler interface. It was written for GNOME. It also runs under KDE, the same way Kldap runs under GNOME. The address for downloading and getting more information is: http://biot.com/gq/

Within the framework of this project two scripts was developed. DESY LCG account request analyzer, and DESY VO/USERS administration tool, which are described below. Cert2ldif.pl script is also widely used, originally written in NIKHEF, it contains some minor DESY specific changes. It converts user certificate (or LCG account request) to LDIF file, which can be easily imported to LDAP database.

cert2ldif.pl Certificate to LDIF Converter
This script reads the files on the command line (or from standard input), which should contain certificates in pem format, and writes to the standard output the LDIF records suitable for insertion in the VO directory by ldapadd.

request.sh DESY LCG account requests analyzer

With the help of this script you can:

- Find out if the user already made an LCG account request
- Find out in which VO the user should be
- Find out if the VO exists in the LDAP server
- Find out if the user exists in the LDAP server

It also gives some smart tips and hits.

This script is good way to handle users requests.

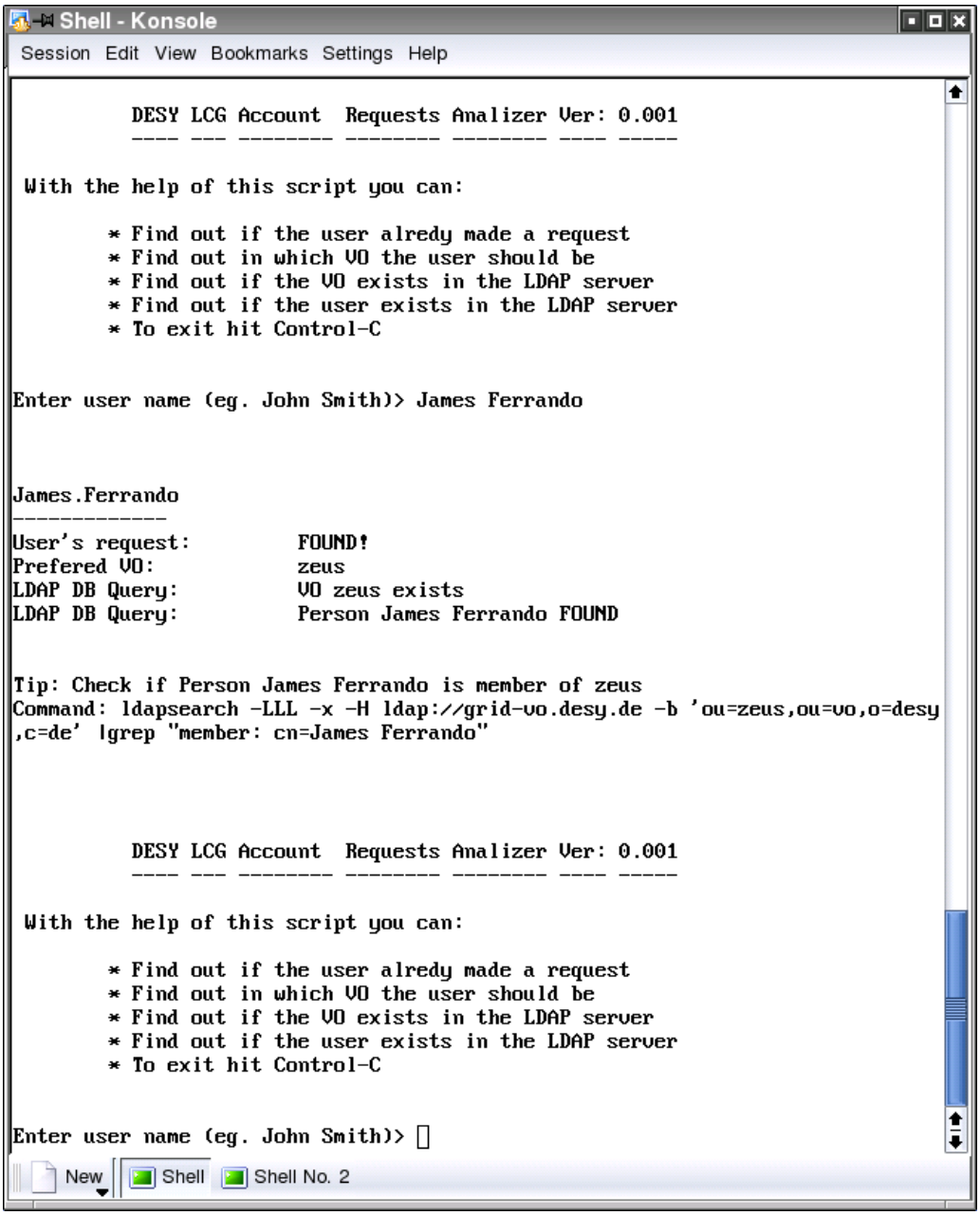

Figure 8: User made a request, preferred VO is 'zeus', Person exists in LDAP Database. Check whether the user included in his preferred VO.

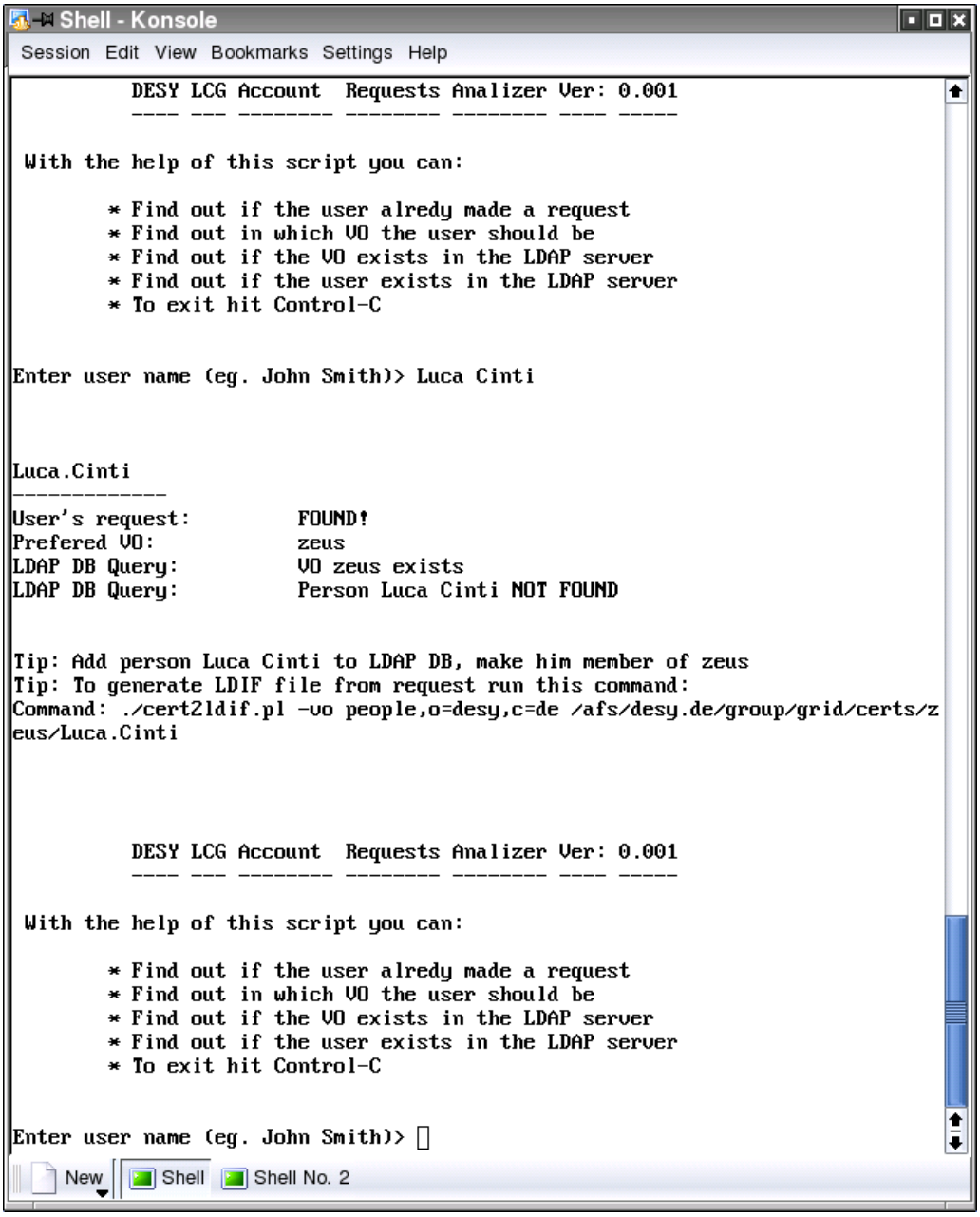

Figure 9: Another User made a request, again preferred VO is 'zeus', but this time person not found in LDAP database. This means that VO administrator need to add the person the database. There are several ways to do that.
To use cert2ldif.pl external script and convert user's request to LDIF file, than import the LDIF file to the database.
Note: LDIF stands for (Lightweight Directory Interchange Format). It is an ASCII file format used to exchange data and enable the synchronization of that data between LDAP servers. This is the actual data you wish to store in the LDAP database. It follows an object model (data schema) defined in either a pre-existing object definition or in an object model definition you have defined in a slapd.conf include file.

admin.sh DESY VO and LCG USERS Administration Tool

This is a script for the administration of VO and Users.
Using the script VO administrator can do the following:

- List all VOs
- List a single VO
- Create VO in 2 steps
  (just entering VO name, the owner, and a member).
- Delete VO
- Import an LDIF file
- List all users
- List a single user
- Create User in 4 steps
  (entering user name, user's institution, subject line of user certificate, and preferred VO).
- Delete user

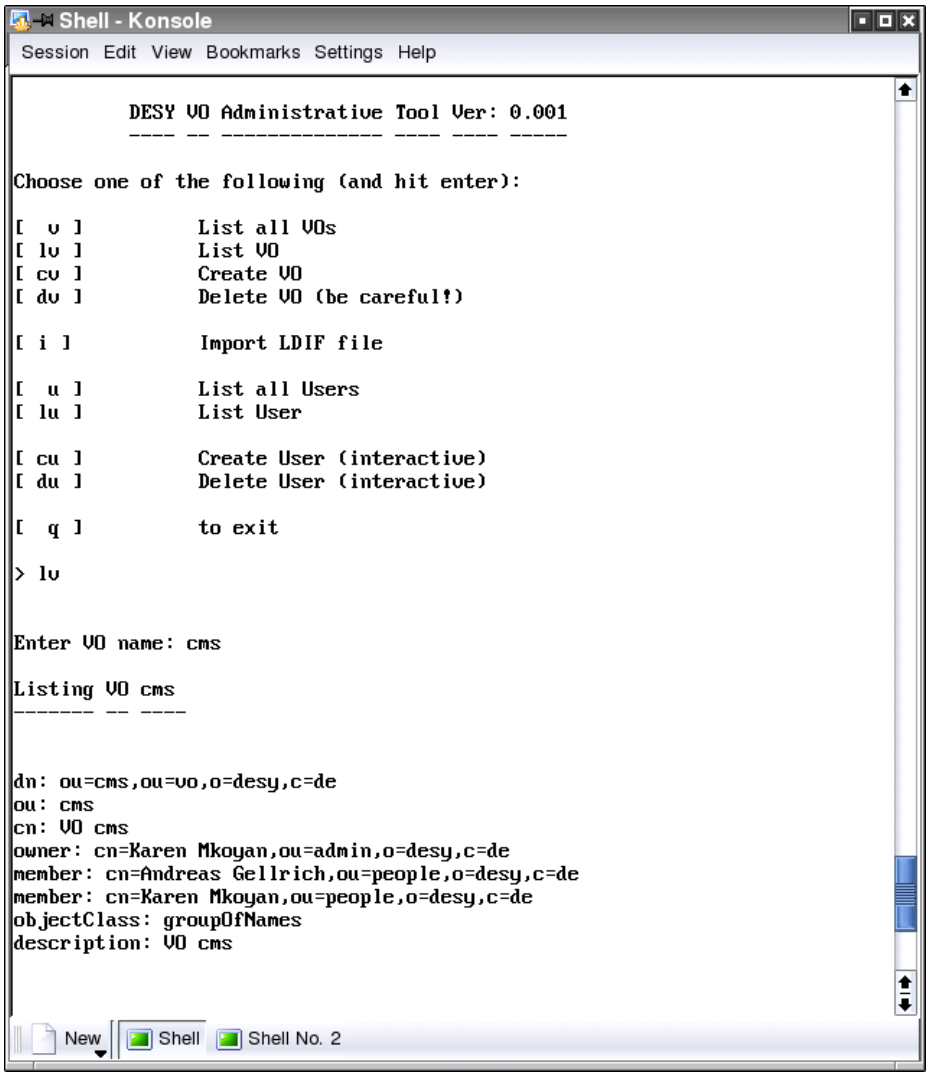

Figure 10:Listing VO 'cms' using DESY VO and LCG USERS Admin. Tool

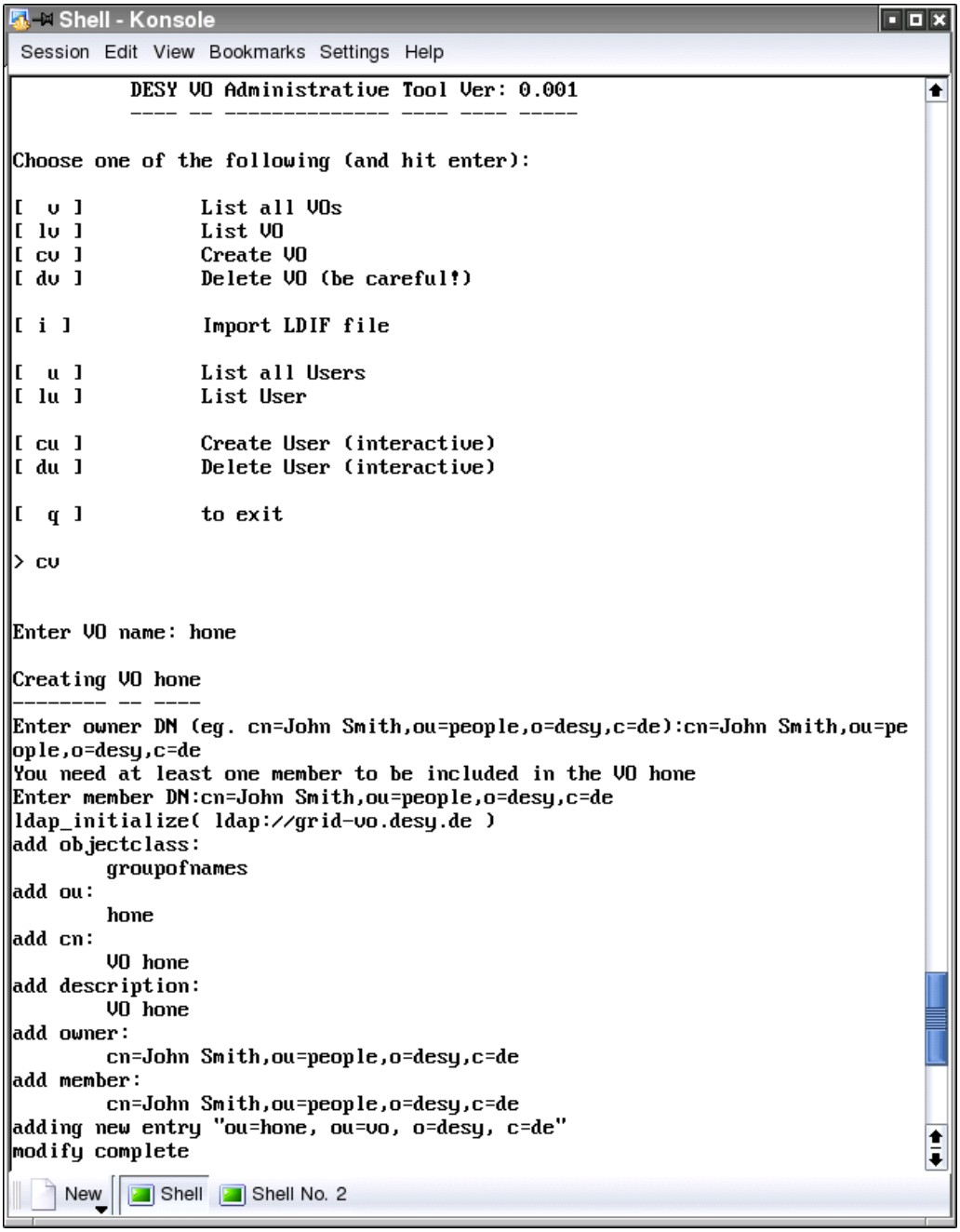

Figure 11: Adding VO 'hone' to LDAP database. It requires a VO owner who will administer that VO latter. At least one member needs to be included, and this is a good idea to include the owner as a member too.

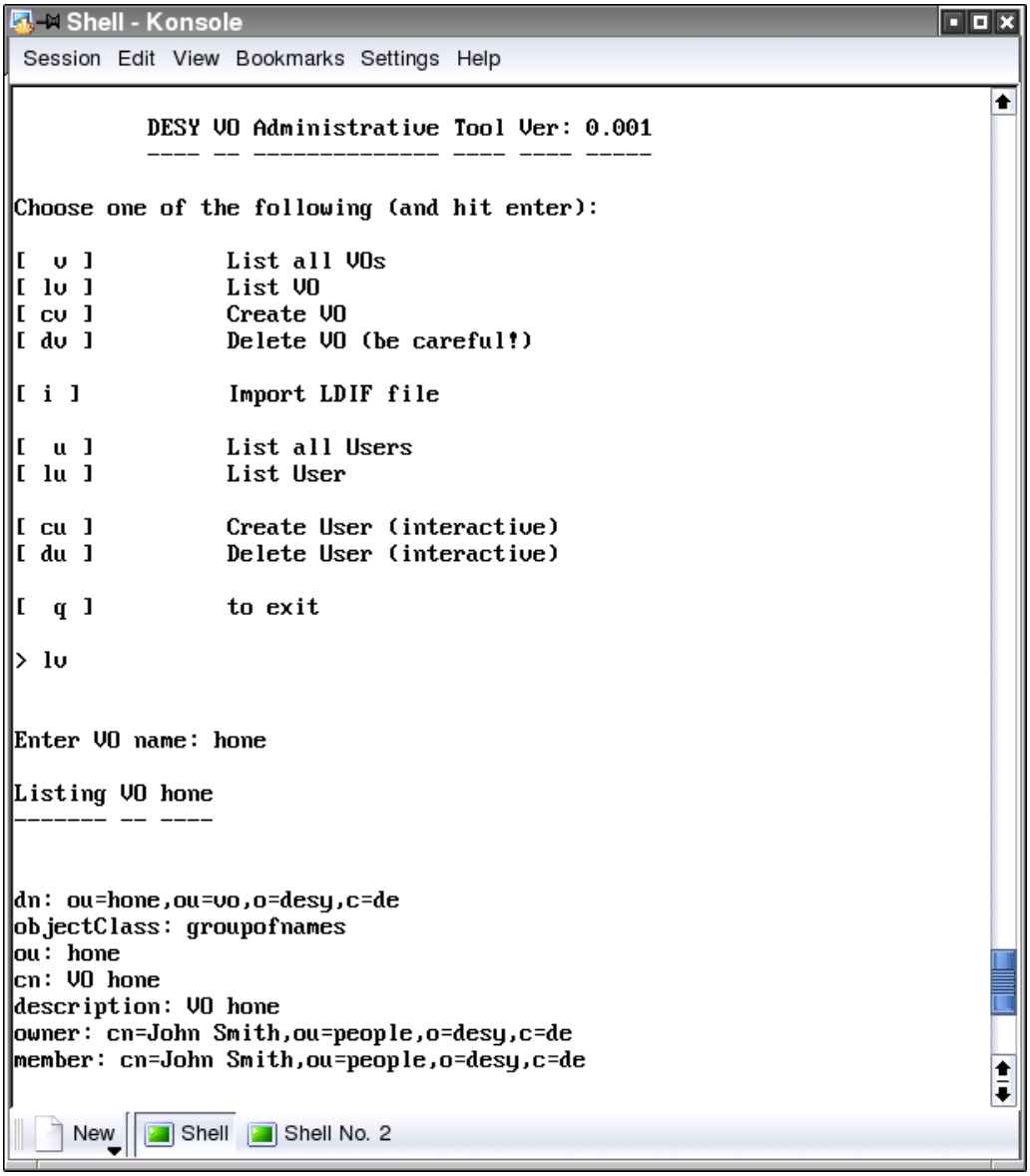

Figure 12: Now using the same script we are listing VO 'hone'. As we see person John Smith is both member and owner. Later the administrator can gain a VO membership to a person.
Using 'du' – Delete user option, it is possible to either delete user from specified VO, or delete user from the database, fully delete.

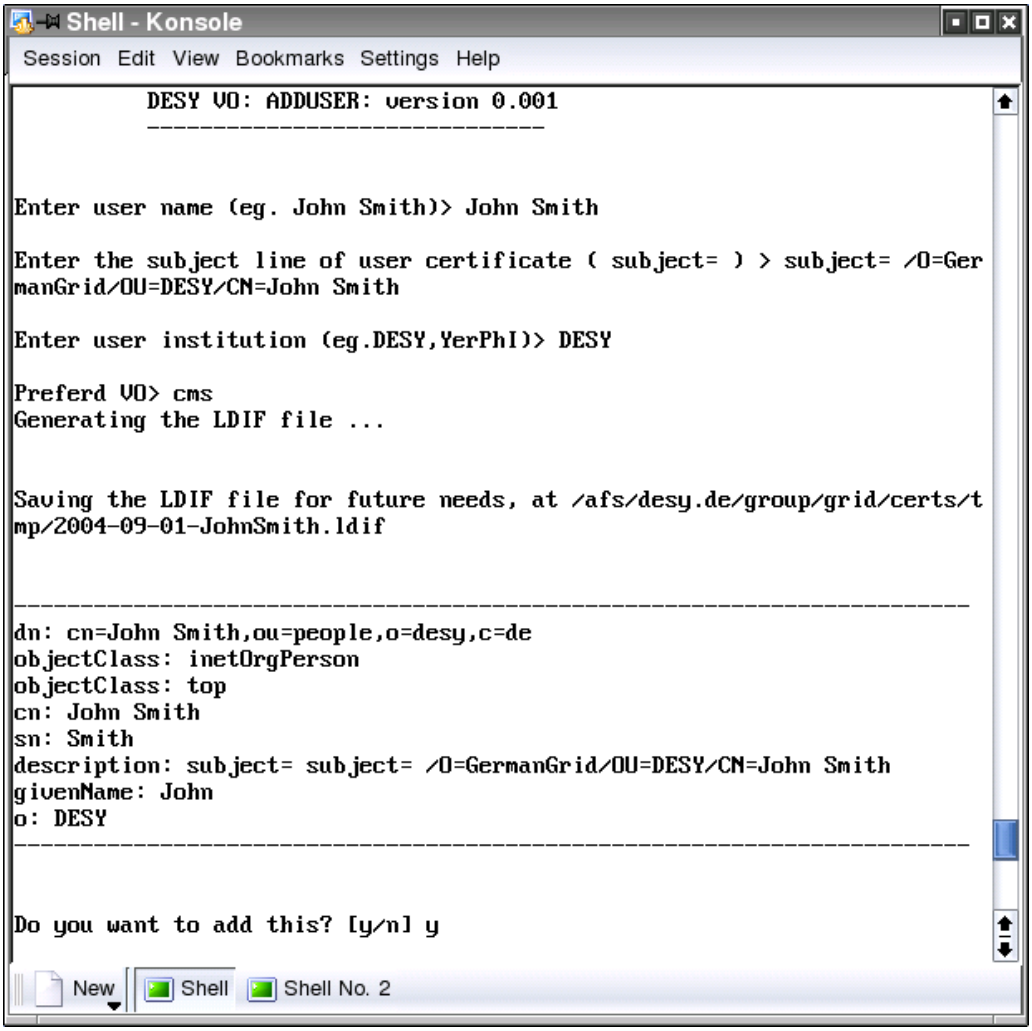

Figure 13: The user creation procedure. Required the user name, the subject line of certificate, preferred VO. It generates an LDIF file, saving the file. Filename consisted of a creation date and the user name. The administrator has not only user's LDIF file, but the creation date.

7 Acknowledgments

I would like to thank DESY for running the summer student program, my supervisor Andreas Gellrich for all his help and instructions during my stay, as well as all IT people for being so supportive.

8 References

[1] *Grid Computing at DESY*
http://grid.desy.de

[2] *LDAP Linux HOWTO*
Luiz Ernesto Pinheiro Malere

[3] *University of Michigan LDAP Documentation Page*
http://www.umich.edu/~dirsvcs/ldap/doc/

[4] *VO Server Information*
J.A. Templon, D. Groep, NIKHEF

[5] Talk
http://grid.desy.de/talks/mkoyan_2004-09-07.pdf