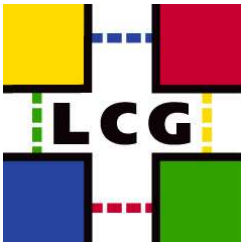

LCG Security Group

User Registration and VO management for LCG-1 in 2003

Date:	**3rd July 2003**
Version:	**1.2**
Status:	**Draft**
Author:	**David Kelsey**

Document Log			
Issue	**Date**	**Author**	**Comment**
1.0	30 June 2003	David Kelsey	Draft in preparation for GDB meeting on 8th July 2003
1.1	2 July 2003	David Kelsey	Mods addressing comments from Ian Neilson
1.2	3 July 2003	David Kelsey	Address more comments from LCG Security group and VO managers. Sent to GDB.

1 Introduction

This paper gives a high-level overview of the procedures for User Registration and Virtual Organization (VO) management for the LCG-1 start of service in July and for the rest of 2003. As presented and discussed at recent GDB meetings, these are largely based on the procedures currently in use in EDG. The descriptions are deliberately very brief. Full technical details may be documented later if needed.

The procedures will be reviewed and, where possible and appropriate, improved by the LCG Security Group for proposal to GDB before the end of 2003. This will take into account the experience gained during the second half of this year. Incremental improvements during the next 6 months will be proposed wherever this is appropriate.

2 User Authentication and Authorization model

This section is a very brief overview of the Authentication and Authorization used in the initial LCG-1 service to set the scene for the procedures described below.

The user is authenticated, i.e. his/her identity proved, by generating a short-lived proxy from the credentials issued by one of the approved LCG-1 certification authorities (CA). The resulting proxy certificate and private key are then used for Grid requests.

Authorization, i.e. permission to access a Grid service, resource or object following successful authentication, is granted via the presence of an entry in the grid mapfile on the host. The certificate distinguished name (DN) will be entered in the mapfile for mapping to a local account, if and **only** if the user's DN is present in **both** the LCG-1 Registration Database **and** the appropriate experiment VO.

The procedures described below are designed to achieve two aims:

a. To give the LCG-1 sites sufficient accurate information about individual users to allow the pre-registration of user accounts and appropriate auditing of all Grid activities at their sites.
b. To ensure that VO managers do appropriate checks on the rights of the user to join the VO, such that LCG-1 sites will grant access to their resources by the VO and its members.

Successful registration with LCG-1 requires acceptance of the LCG-1 User Rules confirmed via the user's private key and certificate.

3 User Registration procedure

The user registers with LCG-1 and **one** VO via the following simple steps:

1. The user registers with an approved CA and learns how to generate Grid proxy credentials. Users are expected to obtain credentials from the CA appropriate to their employing institution. Only CERN staff members are expected to obtain certificates from the CERN CA.
2. The user loads the private key and certificate into his/her local web browser, if not already there. This certificate is used to authenticate with the LCG-1 registration web server.
3. The user completes the LCG-1 User Registration web form giving all of the following required information:
    a. Given name and Family name

   b. Institute name, i.e. the user's employer or home institute. We may provide a pull-down list here.
   c. e-mail address
   d. Telephone number
   e. Certificate DN (automatic – extracted from certificate)
   f. Request to join a single VO (from a pull-down list)
4. The user confirms acceptance of the LCG-1 User Rules and gives permission for the personal information given on the form to be distributed to all LCG-1 site and VO managers by submitting the form.

Notes

I. The registration in 2003 will have an initial expiry date set to 9 months from the date of registration. This is due to the fact that we plan to update the User Rules and the procedures for checking the rights to join a VO by early 2004. Users will have to re-register after expiry of the registration. Subsequent registrations are likely to have longer periods of validity.
II. Users are only allowed to register with LCG-1 if they are eligible to join one of the supported VO's (see later for the list).
III. The User will be warned on the registration web page that checks will be made by the VO manager before they are allowed to join the VO.
IV. Users wishing to join more than one VO can join the second and subsequent VO's, assuming they have the right to do so, via direct requests to the VO manager(s). Today this is likely to require the user to obtain a second certificate with a different DN as current Authorization technology does not enable users to belong to more than one VO with the same certificate.

Following submission of the registration request form a number of actions take place.

a. An e-mail is sent to the User's quoted e-mail address requesting confirmation of their registration. The user confirmation shows that the e-mail address is real.
b. The user's DN and details are recorded in the LCG-1 Registration Database managed by the LCG Registrar.
c. An e-mail is sent to the appropriate VO manager containing the request to join and the details provided by the user.
d. The VO manager checks and confirms the identity and employing institute of the user, their right to join the VO and that the other information looks reasonable. See the later section on VO management for more details of this process.
e. The VO manager adds the user's DN to the VO database, if it is not already there, and confirms registration to the user. The VO manager informs the LCG Registrar of any refused requests.
f. The full details about the user and the name of the VO joined are now mailed (by the VO manager) to all Tier 1/Tier 2 site managers for addition to local registration databases. The CERN LCG team will create and maintain the mailing list(s) of Tier1/Tier2 contacts for use by the VO managers.
g. Those sites needing to pre-register users will do so using this information. Any additional information, hopefully none, required by the site will be obtained by direct contact with the user who may either give the information or not as they wish. The VO manager is not able to check or confirm this extra information.
h. Sites are required to keep all user information private and secure and not distribute this further.

The web servers, LDAP servers and other databases for the above will all be implemented and run by the CERN LCG team. This does not include the experiment VO services (see later).

4 VO management

The following 5 VO's are currently supported by LCG-1, together with the name of the VO manager.

ALICE	Daniele Mura (INFN)
ATLAS	Alessandro De Salvo (INFN)
CMS	Andrea Sciaba (INFN)
LHCb	Joel Closier (CERN)
DTEAM	Ian Neilson (CERN)

The "DTEAM" VO (Deployment Team) is a "catch-all" available to those users not able to join one of the experiment VO's or for more general purposes, such as testing or monitoring.

If and when the LCG-1 wishes to allow access to other VO's these will have to be added as required together with appropriate management procedures.

The duties and responsibilities of the VO manager include:

1. The checks and confirmation of the identity and employing institute of the user and the right to belong to the VO of anyone requesting to register with LCG-1 (see below).
2. The confirmation that the other fields completed on the registration form look reasonable.
3. The addition of new users to the VO database.
4. The maintenance of the user's entry when and if changes are required.
5. The removal of a user from the VO database if requested to do so by the LCG operations team or Operations Centre following their investigation of a security incident or other operational problem. (This may not be necessary as removing the user from the LCG-1 Registration Database will also remove the user from Authorization files and is under the direct control of the operations team?)

The VO manager should check the identity and employing institute by one of the following means:

a. Direct personal knowledge of and direct contact (telephone, personal or video, not e-mail) with the user.
b. Confirmation via entries in an official experiment or CERN database of members of the experiment.
c. Confirmation by the official experiment contact at the employing institute. This should be confirmed via personal contact or telephone/video if the contact person is known, or perhaps signed e-mail (although this would require a database of contact person certificates or other mail signing keys). Or perhaps unsigned e-mail is sufficient for now? See the next section for the creation and maintenance of this list of contact people.

This topic of a distributed VO Registration Authority, i.e. the body doing the checks on the user, is one needing much more work. We need to define and create a robust and scaleable procedure. During 2003 the VO managers can only be expected to offer a best efforts service, particularly if the number of user requests becomes very large. It is also the case today that the VO managers do not offer full cover. There will be times when they are away or busy on other duties and so there could be some delays in User Registration. The improved system for next year will need to have more guarantees on level of response.

The 4 experiment VO servers and databases will continue to be run by NIKHEF. These are the same systems used by EDG. LCG-1 needs to plan for the location of these services in 2004 and beyond. The DTEAM VO (catch-all) will be run by the CERN team.

The tools to extract the information from the VO databases to create the grid mapfiles (mkgridmap) will be distributed as part of the LCG-1 release.

5 List of institutes and contacts

The VO managers need access to an official list of participating institutes and contact people. These VO-specific lists will be used to decide who to contact, when necessary, to check requests to join LCG-1.

The initial version of these VO-specific lists of institutes and contacts could either come from the CERN Experiments Greybook, see http://greybook.cern.ch/ , or from the regularly updated Experiment lists on another CERN database server,
e.g. http://graybook.cern.ch/programmes/experiments/lhc/ATLAS.html
The latter list includes details of institute team leaders.

6 Approval by GDB

The LCG GDB is asked to approve the procedures described here for start-up of the initial LCG-1 service and operation during 2003.