



LCG Security Group

Requirements for LCG User Registration and VO Membership Management

<i>Date:</i>	1st June 2004
<i>EDMS Reference:</i>	https://edms.cern.ch/file/428034/2/LCG_User_Registration.doc
<i>Internal Version:</i>	2.7
<i>Status:</i>	Final
<i>Author:</i>	Maria Dimou

Document Log			
Issue	Date	Author	Comment
1.0	30 June 2003	David Kelsey	Draft in preparation for GDB meeting on 8 th 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.
2.0	3 February 2004	Maria Dimou, David Kelsey	Change of registration policy following the 15-17 December 2003 workshop at CERN on "Registration, VO mgnt, Authz". Incorporated comments from Ian Neilson. Replacing document https://edms.cern.ch/file/428034/1/LCG_User_Registration.pdf .
2.1	26 February 2004	Maria Dimou	Added comments by David Kelsey and Ian Neilson
2.2	9 March 2004	Maria Dimou	Clarified that a user can register using a <i>personal</i> certificate, to avoid misunderstandings with host certificates.
2.3	25 March 2004	Maria Dimou	Added comments by D.Barberis, F.Carminati, J.Closier, A.Frohner, M.Mazzucato, O.Smirnova and the Security Group members of the 22 March 2004 meeting.
2.4	7 May 2004	Maria Dimou	Added comments by I.Bird, A.Frohner, I.Neilson.
2.5	12 May 2004	Maria Dimou	Added comments by J.Hahkala, D.Heagerty, D.Kelsey, T.Levshina, I.Neilson, D.Skow.
2.6	13 May 2004	Maria Dimou	Added comments by D.Kelsey, T.Levshina, I.Neilson.
2.7	1 June 2004	Maria Dimou	Added comments by M.Delfino, T.Levshina, A.Sciaba.

1 Introduction

This paper defines the requirements for [LCG](#) User Registration and Virtual Organization (VO) management.

These requirements will be reviewed and, where possible and appropriate, improved by the LCG Security Group for approval by the GDB.

2 Definitions

- Data supplied by the user:
 - **Personal user data:**
 - Family Name,
 - Given Name,
 - Institute name, i.e. the user's employing institute,
 - Contact Phone number.
 - **Registration Data:** Authentication (AuthN) related information:
 - Personal user data,
 - Email address,
 - DistinguishedName (DN) extracted from a valid personal digital certificate issued by his/her Certification Authority (CA).
- Other relevant terms:
 - **Virtual Organization (VO):** *"abstract entity grouping Users, Institutions and Resources (if any) in the same administrative domain"*¹. E.g. LCG experimental collaboration.
 - **Site:**² An institute which is providing one or more Services to the Grid.
 - **Site Resources:** The hardware, software, data and supporting infrastructure required to provide the Grid Services operated by that site.
 - **VO Database:** Authorisation (AuthZ) related information, i.e. the user's role(s) in the VO. His/her access rights to a resource and on data stored at it will depend on this information.
 - **VO manager:** The responsible person recording in the VO Database, after appropriate checks, the status of a member of the VO, i.e. performing user entries, assignment of roles, information updates and user removals. The VO management function can be performed by a group of persons delegated by the VO manager.
 - **Institute Representative (IR):** The person at the user's employing institute, who can check the validity of his/her data and confirm the identity of the user and his/her right to become or remain a member of a VO.
 - **Usage Rules:** The rules (sometimes mentioned as Guidelines) governing the use of Grid resources.
 - **Resource Administrator:**³ The person responsible for providing and maintaining a Resource or Service at a given Site. (several individuals may be involved to provide this function, including system programmers, operators, user support staff, networking staff and security personnel.)

¹ I. Foster, C. Kesselman and S. Tuecke, The Anatomy of the Grid, International Journal of High performance Computing Applications, 15, 3 (2001).

² Site, Resources and Resource Administrator definitions taken from https://edms.cern.ch/file/431463/1/Resource_Administrators_Guide.doc

³ The term "Resource Administrator" is used instead of "Site Administrator" because of the clarity of its definition in the Resource Administrators' Guide.

3 User Registration Requirements

An important purpose of the registration process is to record the explicit acceptance by the user of the [LCG Usage Rules](#)⁴ as well as the acceptance, by the user, that part of his/her information including Personal user data may be distributed to the LCG sites.

3.1 Registration

The main objective of the registration process is to collect the user's Registration Data. Duplication of Personal user data and the procedures of validation and authentication should be avoided so that Grid users register only once and their Registration data are checked only in a single place.

Robust documented verification procedures must be used to establish the link between a person, his/her Registration data and the associated AuthZ data.

The procedures must unambiguously assign the individuals who take responsibility for the validity of the Registration data provided, and those with the authority to exercise control over the rights of the user to use Grid resources.

3.2 Removal and renewal

The following conditions should trigger a timely re-evaluation of the user's right to remain a member of a given VO:

- User or user's IR request. A mechanism prompting the VO manager to remove the user on request by the IR or the user should be provided.
- End of the user's membership period in the VO. A way to record the "User Registration Date" and "User Participation-End Date" should be foreseen for auditing and accounting purposes. Provided the user's contract with the institute is of a longer duration, an initial value, not exceeding one year, should be assigned to the "User Participation-End Date" at registration time. A mechanism prompting the user to re-register, before the "User Participation-End Date" is reached, should be provided.
- End of collaboration between the user's institute and the VO.
- End of collaboration between the user and the VO.
- End of collaboration between the user and his/her institute. Documented procedures provided by each VO should explain how to timely reflect changes of user's collaboration with the institute and/or the VO.
- Major change of the Usage Rules. The Usage Rules' version number that was valid at registration time should appear on the user's record. If they are subject to major changes, the user should be prompted to re-confirm his/her acceptance of the Usage Rules.

3.3 Suspension

A security incident⁵ associated with a VO member should result to:

- A "User Suspended" status, removable by the VO manager after verification with the [Grid Operations' Centre](#) (GOC).
- Update of the history of a user's association with past security incidents, recordable and viewable in the VO database.

⁴ https://edms.cern.ch/file/428036/LAST_RELEASED/LCG_Usage_Rules.pdf

⁵ Incident definition and response defined in https://edms.cern.ch/file/428035/1/LCG_Incident_Response.pdf

4 VO manager's responsibilities

The duties and responsibilities of the VO manager include:

1. Management of the Registration Data verification process by using existing reliable sources of information, consulting the relevant IRs or by means of other appropriate auditable procedures.
2. Addition of the new user to the VO Database, after successful completion of step 1 or notification to the user with the reasons of his/her denial.
3. Logging information including the date when the user registered (User Registration Date). Each request received and the checks made to validate the request should be recorded, for auditing purposes. Audit logs should be kept by the VO manager for two years, even if the member has left the VO.
4. Timely maintenance of the user's entry when changes are required.
5. Removal or suspension of a user from the VO database as per conditions listed in section 3.1.
6. Notification to those sites that wish to receive information about a new user who joined the VO.
7. Provision of secure read access to the Registration Data for authorised use only.
8. Ensuring Personal user data is not distributed except for authorised and necessary purposes. The VO Manager must ensure that the VO membership is aware of the circumstances under which their Registration Data will be distributed.
9. Authorise the Resource Administrators to have secure read access to the VO database.

Generic mailing lists with names *project-lcg-vo-[VO-name]-admin@cern.ch* are defined and maintained by the LCG Deployment Team at CERN, containing the names of the VO managers. The [VOs supported](#)⁶ can be found from the [LCG User Registration web site](#)⁷.

5 Site responsibilities & requirements

- Any information additional to that defined as Registration Data, required by the site should be obtained by direct contact with the user who may either give the information or not as they wish. The VO manager is not involved in this bilateral negotiation.
- A mechanism should be provided to the sites allowing them to “subscribe” to the Registration Database and securely access for reading Personal user data, if they wish.
- Sites are required to keep all user information private and secure and not distribute this further.
- Sites must have a local mechanism to authorise/allow/deny user access to their resources at the level of individual user.
- Specifically, the GOC, following investigation of a security incident or other operational problem, may ask the VO manager to remove or suspend the user from the VO.

⁶ https://lcg-registrar.cern.ch/virtual_organization.html

⁷ <https://lcg-registrar.cern.ch/>