Rules for Use of the LCG-1 Computing Resources

The LHC Computing Grid Project [(1)]

2003-06-23 (version 2)

1. Introduction

The goal of the LHC Computing Grid Project (LCG) is to meet the computing needs of the experiments being constructed at the CERN Large Hadron Collider (LHC) by deploying a worldwide computational grid service, integrating the capacity of scientific regional computing centres spread across Europe, America and Asia into a virtual computing organisation.

Phase 1 of LCG includes the construction and commissioning of the first global LHC Computing service suitable for physics usage. This service, known as LCG-1, consists of the computing resources made available by the Regional Centres and other sites and the installed Grid middleware and other software.

The purpose of this document is to lay down the rules governing the use of these resources, which may be modified as the LCG project evolves. They are without prejudice to the application of the rules of each LCG-1 Regional Centre and each LCG-1 site, and of any national laws which may apply. The LCG-1 resources may only be used for professional purposes.

This document applies to all users of LCG-1.

2. Definitions

LCG-1

The computing service consisting of all the resources dedicated to the LCG project at the participating sites.

LCG-1 Resources

The term "LCG-1 resources" shall generally be used to describe:

- all the computers, workstations and servers that make up LCG-1;
- the telecommunications networks connecting these computers;
- the data storage systems connected to LCG-1;
- all the other active components and networks connected to LCG-1;

[(1)] http://lcg.web.cern.ch/LCG/

- all the support services, programme libraries, applications and other software, documents or services operating on or connected to the above-mentioned computers and networks.

LCG-1 Site

A physical location or institute providing LCG-1 Resources.

LCG-1 Regional Centre

A computing centre providing resources to LCG-1 on behalf of a country or group of countries.

LCG Grid Deployment Board (GDB) [(2)]

The forum within the LCG project where the computing management of the Experiments and the Regional Centres can discuss and take, or prepare, the decisions necessary for planning, deploying and operating LCG-1.

Certification Authority

A Certification Authority (CA) is a body responsible for establishing and, thereafter, guaranteeing a formal link between a person, application, or server and a public key (chain of 1024 bits or more). Its role is to verify the correctness of the information contained in the electronic identification certificate it issues, as well as to guarantee the validity of this document. The setting-up of a Certification Authority entails the definition of a Certificate Policy (CP) and a Certification Practice Statement (CPS), and the establishment of a set of rules defining the criteria for the award of the Certificate, its detailed scope and any procedures relating thereto.

The approval of Certification Authorities for LCG-1 is subject to a procedure defined by the LCG Grid Deployment Board.

Certificate

The certificate is an electronic document, digitally signed by a Certification Authority, that asserts to an association between an identifier and a particular public key. The Certification Authority asserts, to the level defined in its CP and CPS, that this identifier is associated with an identity (a person, application, or machine), by issuing a digitally signed certificate and by not including this certificate in the Certificate Revocation List published by the CA.

At the moment of issuing a certificate, the CA asserts to a level defined in its CP and CPS that

- for a person, a defined relationship existed between the owner and the identifier or identifiers stated in the certificate,

---

[(2)] http://lcg.web.cern.ch/LCG/PEB/gdb/

- for an application, a defined relationship existed between the signed object and the identifier(s) stated in the certificate,
- for servers, a relationship existed between a known person responsible for this system and the identifier of the system as stated in the certificate.

The certificate is based on standardised protocol X509 (ITU-T X 509 international standard V3 - 1996) (RFC2459).

User

A person with access to the LCG-1 resources.

LCG-1 user account

A LCG-1 user account gives access to the LCG-1 resources made available by the participating sites.

Access authorisations are strictly personal and may under no circumstances be transferred to a third party, not even temporarily. Authorisations may be withdrawn at any time and expire upon termination of the professional activity for which they were granted.

Virtual Organization

A Virtual Organization (VO) is a dynamic set of individuals and/or institutions that are defined according to a set of coordinated resource sharing rules. These sharing rules cover access to all types of resources including computers, software and data.

In LCG-1 there is one VO for each of the four LHC experiments. Other VO's will be created and maintained as required by the project. Users may be members of one or more VO(s).

3. Procedure for obtaining a LCG-1 user account

The procedure for obtaining a LCG-1 user account comprises three steps:

1. obtaining a personal certificate from an approved Certification Authority
2. agreement to these usage rules, and
3. registration with one of the LCG-1 virtual organizations.

4. Organisation of security on LCG-1

To implement the LCG-1 security procedures and to respond to security incidents, each LCG-1 Regional Centre and each LCG-1 site must designate a security officer.

5. Rules governing the use of LCG-1 resources

Although the LCG-1 sites undertake to contribute to the maintenance and protection of their computing installations, they cannot provide a guarantee of the latter's smooth operation or

the confidentiality of the information stored there. Consequently, the LCG-1 sites accept no responsibility in the event of information loss or breach of confidentiality.

All the accounts are equipped with appropriate access protection, such as account codes or passwords, and with an individual certificate issued by the relevant Certification Authority.

All users are responsible for their use of the LCG-1 resources and the network to which they have access. They also have responsibility, at their own level, for contributing to the general security of LCG-1.

Users shall:

1. adhere to the security recommendations of the site to which they belong, the recommendations of the sites they access via LCG-1 and those of LCG-1 itself,
2. report to their local security officer any attempt to violate their user account or workstation and, generally, any anomaly that comes to their attention,
3. report immediately to the issuing Certification Authority any compromise of the private key of their certificates,
4. report any security faults immediately to the local security officer,
5. not try to exploit any security faults in the LCG-1 resources, or to use such faults to the detriment of other computer facilities,
6. select safe passwords, endeavour to keep them and the private keys secret and under no circumstances communicate them to third parties,
7. use the LCG-1 resources without intentionally causing damage to LCG-1, or disturbing its operation unless these activities are part of an authorized stress test LCG-1; use of the LCG-1 resources must be rational and relevant in order to prevent its saturation or misuse for personal ends,
8. use their user account for the sole purpose for which it was granted,
9. not use or attempt to use accounts other than their own or to disguise their real identity,
10. not try to gain unauthorised access to accounts, stored data or data transiting on the network, except under the provisions of the paragraph "Third-party access to user accounts", below,
11. not to give or to allow unauthorised users access to the LCG-1 resources via resources at their disposal,
12. keep confidential all information obtained from access to the LCG-1 resources that they may reasonably be expected to understand is confidential or sensitive in nature,
13. respect the property rights associated with the LCG-1 resources, including the copyright on software and property rights relating to confidential data.

Users shall authorise the publication of their personal details in electronic directories and databases, insofar as necessary for or in connection with the operation of LCG-1. These details may be consulted by all the LCG-1 sites. Users may need to be contacted by some LCG-1 sites for additional information not covered by this agreement. Any such additional information will not be distributed further or published.

Users who have been attributed an account with privileged access in connection with their specific professional duties must advise their supervisor as soon as their duties no longer call for privileged access.

6. Third-party access to user accounts

The officers responsible for computer security at the LCG-1 sites, the computer administrators, and all persons expressly authorised by the LCG GDB national representative(s), have access to the information stored in the LCG-1 computing facilities. Such access is subject to the following conditions:

1. The above-mentioned persons are only authorised to communicate information amongst themselves, except where expressly required for the execution of their duties with respect to LCG-1.
2. Access for such persons must always be in the exercise of their professional duties and shall be authorised, strictly on a need to know basis, for the following purposes only:
    1. to solve problems affecting the LCG-1 computing facilities, including optimisation of the latter or the installation of new facilities;
    2. detection of computer security weaknesses or violations;
    3. monitoring of the resources available;
    4. to conduct an enquiry ordered by the computing security officer of a LCG-1 site or the relevant hierarchical supervisor when a breach of the rules is suspected;
    5. the re-attribution of access rights to accounts or the cancellation of accounts upon expiry of a user's contract with one of the LCG project participating institutes, or when the user's activities are no longer compatible with the aims of the project.
    6. to re-establish the normal operation of the organic unit to which a user belongs when operation is seriously disturbed by the user's absence.

7. Responsibilities

The user concerned shall be liable for damage resulting from any breach of these rules.

In that event and as a general rule, the computing security officer(s) of the LCG-1 site(s) concerned and/or the relevant hierarchical supervisor shall inform the user concerned and explain the nature of the problem detected or breach of the rules observed. In the event of further incidents, the user concerned shall be informed in writing by one of the persons mentioned above of the provisions of the present Rules that have been breached.

In the event of repeated breaches following the measures set out above, or at any time when circumstances so require due to the gravity of the breach committed, the security officer of the site in question may withdraw the right of access to the LCG-1 computing resources from the user concerned.

The security officer of the site where the incident occurred shall advise the security officer(s) of any other site(s) concerned. All the security officers of the LCG-1 sites shall work together to remedy the situation.