# Rules for Use of the Testbed Computing Resources

Deleted: Guidelines

## European DataGrid [1]

2002-04-09 (version 12)

Deleted: 2001-11-15 (version 10)

## 1. Introduction

The Work Package 6 [2], the Integration Testbed - Production Quality International Infrastructure will demonstrate the effectiveness of the DataGrid in production-quality operation over high-performance networks. The work package will integrate successive releases of the software components from each of the development work packages and deploy these releases on available computing resources. These resources and iterative releases form the DataGrid "Testbeds."

Deleted: (1),

Deleted:

Deleted: "testbeds."

The first prototype, or Testbed, will be launched in the fourth quarter of 2001. This prototype will enable some fifty users to operate the resources made available by the project partners.

The purpose of this document is to lay down the rules governing the use of these resources, in conjunction with the rules of each site concerned. These rules can be modified as the DataGrid project evolves, in conjunction with the rules of the Testbed sites. These rules are without prejudice to the application of the rules of each partners and each site, and of any national laws which may apply. The Testbed resources may only be used for professional purposes.

Deleted: The rules of each partner and each site remain applicable, as does the legislation of each state

Deleted: concerned. The various sites of the various partners shall collaborate to solve security incidents.

This document applies to all users of the Testbed. In the event of an incident or in case of misuse of the Testbed, the rules of the site concerned and the legislation of the state(s) concerned shall be applied.

Deleted: a security incident,

Deleted: State(s)

## 2. Definitions

### Testbed

All the resources dedicated to the development of the DataGrid project at the participating sites.

### Testbed Resources

The term "Testbed resources" shall generally be used to describe:

- all the computers, workstations and servers that make up the Testbed;
- the telecommunications networks connecting these computers;
- the data storage systems connected to the Testbed;

---

[1] IST-2000-25182

[2] Appendix 1 “Description of Works” of the DataGrid project. Doc identifier : datagridannex1v4.doc

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

**Testbed Site**

A physical location grouping Testbed Resources.

**DataGrid Partner**

An institute which is a member of the DataGrid Testbed. Each Partner has a designated representative, who has overall responsibility for Testbed Site(s) belonging to the institute.

**Certification Authority**

Deleted: 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 Certification Policy (CP) and a Certification Practice Statement (CPS), a collection of rules indicating to what the certificate is applicable, by whom, and what are the conditions of the CA's implementation from the legal, administrative and technical viewpoints.

The appointment of Certification Authorities for the Testbed is subject to prior approval by the Security Subgroup of Work Package 6.

Deleted: selected

Deleted: are approved

**Certificate**

The certificate is an electronic document, digitally signed by 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.

Deleted: site),

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,
- 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 Testbed resources.

**DataGrid user account**

A DataGrid user account gives access to the Testbed 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.

Deleted: with due cause

Deleted: , even temporary,

# 3. Procedure for obtaining DataGrid user account

The procedure for obtaining a DataGrid 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 DataGrid virtual organizations.

Deleted: guidelines,

# 4. Organisation of security on the Testbed

To implement the DataGrid security procedures and to respond to security incidents, each DataGrid partner and each Testbed site must designate a security officer.

Deleted: testbed

Deleted: i

# 5. Rules governing the use of Testbed resources

Although the Testbed's constituent 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 Testbed's constituent 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 Testbed resources and the network to which they have access. They also have responsibility, at their own level, for contributing to the general security of the Testbed.

Deleted: Grid

Deleted: Grid.

Users shall:

1. adhere to the security recommendations of the site to which they belong, the recommendations of the sites they access via the Testbed and those of the Testbed itself,

2. report to the 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 Testbed resources, or to use such faults to the detriment of other computer facilities,
6. select safe passwords, endeavour to keep them secret and under no circumstances communicate them to third parties,
7. use the Testbed resources without intentionally causing damage to the Testbed, or disturbing its operation unless these activities are part of an authorized stress test of the Testbed; use of the Testbed 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 Testbed resources via resources at their disposal,
12. keep confidential all information obtained from access to the Testbed resources that they may reasonably be expected to understand is confidential or sensitive in nature,
13. respect the property rights associated with the Testbed 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 the Testbed. These details may be consulted by all the Testbed sites.

Deleted: since these are

Deleted: obtaining access to

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 Testbed sites, the computer administrators, and all persons expressly authorised by the Testbed Partner Representative, have access to the information stored in the Testbed computing facilities. Such access is subject to the following conditions:

Deleted: administrators and all

Deleted: persons

Deleted:

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 the Testbed.
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 Testbed 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;

Deleted: the

Formatted: Bullets and Numbering

Deleted: ,

Deleted: only

Deleted: with the user's consent,

4. to conduct an enquiry ordered by the computing security officer of a Testbed 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 DataGrid project partners, 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 Testbed 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 Testbed 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 partner(s) concerned. All the security officers of the DataGrid partners shall work together to remedy the situation.

**Deleted:** to

**Deleted:** In the event of a security incident, the rules of the site concerned and the legislation of the State(s) concerned shall be applied.

**Deleted:** officer of the partner

**Deleted:** project