BiG Grid
the dutch e-science grid

VO Portal Policy

Document Revision Information	
Document Identifier	BIGGRID-2008-025
Document Version	1.0 (DRAFT)
Last Modified	13-03-2008
Last Edited By	DLG

Table of Contents

Document Revision History

Version	Editor	Comments
1	*DLG*	*Initial draft for our NBIC BioAssist and SCIAGrid portals*

1 Preamble

This Policy applied to all Portals operated by Virtual Organisations that participate in the Grid infrastructure. It extends the joint Security and Availability Policy, and complements the "*Requirements for LCG User Registration and VO Membership Management*". All other Policies, including specifically but not exclusively the LCG Audit Requirements, the Grid Acceptable Use Policy, the VO Acceptable Use Policy and the Virtual Organisation Operations Policy apply.

1.1 Definition of New Terms

Web User – a human individual that accesses Grid resources through a Portal. This individual may or may not be (also) enrolled in a Virtual Organisation

User – a human individual enrolled in a Virtual Organisation

Portal – a web site or web service that provides functionality to Web Users via web-specific applications.

Anonymous Web User – a Web User who does not provide unique credentials to the Portal when invoking functionality

Pseudonymous Web User – a Web User that provides non-authenticated information (e.g. an email address) to the Portal when invoking functionality

Identified Web User – a Web User that provides authenticated identification to the Portal when invoking functionality, but whose credentials and way of authentication are not necessarily compatible or equivalent with Grid authentication.

Strongly Identified Web User – a Web User that provides authenticated identification to the Portal when invoking functionality, where these credentials are valid credentials meeting the authentication and VO enrolment requirements of the Security and Availability Policy and dependent Policies.

Resource Provider – a Grid participant that provides compute, data storage or database resources

Robot – a software agent that perform automatic functions on behalf of a natural person.

Robot Certificate – a certificate issues to a Robot, and whose private key was generated on and is exclusively held on a Secure Hardware Token. The common name in the robot certificates shall identify at least the natural person or group of persons responsible for the Robot.

Secure Hardware Token - those hardware security cryptographic devices or hardware security modules that operate on and hold asymmetric cryptographic key pairs in such a way that the private part of the key pair cannot ever be extracted in unencrypted form, can only be unencrypted inside the device, and the encrypted form, if available, uses 128 bit symmetric key encryption or equivalent or stronger., and where the key pair has been generated inside the cryptographic device. Any tampering, any substitution or extraction of keys, and any unauthorized

modification of the activation data, must leave evidence on the secure hardware token.
Secure hardware tokens and hardware security modules that comply with the requirements of FIPS 140-1 level 2 or higher, or FIPS 140-2 level 2 or higher, and where the key pair has been generated inside the module, are adequate to meet the requirements set forth above. If not FIPS certified, implementation of an equivalent security level and appropriate mechanisms on the token must be demonstrated: the vendor must have built the device with the intention of obtaining FIPS 140-2 certification at level 2 or higher, and must either intend to submit the device for certification, or have it in process of certification.

1.2 Portal classes identified by this Policy

This Policy applies to Portals that belong exclusively in to one of the following classifications:

1. The Web User invokes functionality on the Portal where jobs submitted to the Grid use executable code that is provided by the Portal to the Grid as part of the job submission process. All parameters and input data are defined exclusively by the Portal and cannot be influenced by the user.
2. The Web User invokes functionality on the Portal where jobs submitted to the Grid use executable code that is provided by the Portal to the Grid as part of the job submission process. The Web User may only provide run-time parameter settings from an enumerable and limitative set, and may select data files from a enumerable repository of data files that are pre-vetted for use by the Portal.
3. The Web User invokes functionality on the Portal where jobs submitted to the Grid use executable code that is provided by the Portal to the Grid as part of the job submission process. The Web User may provide run-time parameter settings from an enumerable and limitative set, and may provide non-validated input data to the executable code.
4. The Web User invokes functionality on the Portal where jobs submitted to the Grid use executable code that is provided by the Web User. Whether this code is passed through unmodified by the Portal and is submitted to the Grid as-is, or whether this code is inspected and analysed on the Portal does not change the classification of this Portal.

2 Portal Policy

All Portals, operated by or on behalf of a Virtual Organisation, must comply with the Virtual Organisation Operations Policy, in particular "*You are responsible for ensuring that your software does not pose security threats, that access to your databases is secure and is sufficiently monitored, that your stored data are compliant with legal requirements, and that your VO services [...] are operated according to the applicable policy documents*".

In addition to all other Policies, the following conditions apply to all Portals:

1. The Portal, the VO to which the Portal is associated, the Portal manager are all individually and collectively responsible and accountable for all interactions with the Grid, unless a credential of a Strongly Identified Web User is used to interact with the Grid.

Depending on the Portal class, the following conditions will apply.

2.1 Class-1 "Web Rendering Automaton" Portals

By registering a Robot Certificate associated with a Class-1 Portal in a Virtual Organisation, you agree to the conditions laid down in this section and documents references therein.

1. The Portal may offer services to all Web Users.
2. The Portal must use a Robot Certificate
3. No data may be stored on the Grid as a result of any action by a Web User, except for transient data stored in designated scratch areas on the computational resources provided to the running jobs.
4. The Portal must be capable of limiting the job submission rate, and the maximum average and peak job submission rate by the Portal must be specifically agreed between you and the Grid
5. The Portal must keep enough information to associate any interactions with the Grid with a particular Internet address and tcp port of an end-user.
6. Logged information must be made available to the Grid Management and to any Resource Provider who can justifiably claim to provide or to have provided resources to the Portal.

2.2 Class-2 "Parameter" Portals

By registering a Robot Certificate associated with a Class-2 Portal in a Virtual Organisation, you agree to the conditions laid down in this section and documents references therein.

1. The Portal may offer services to Pseudonymous, Identified and Strongly Identified Web Users.
2. The Portal may use a Robot Certificate or alternatively may use the authentication information provided to obtain a User credential specific to the Web User and use these for interactions with the Grid. Re-usable private data,

including private keys associated with proxy certificates, must not be transferred across a network, not even in encrypted form.

3. The Portal must not store or obtain long-lived reusable authentication information for Strongly Identified Web Users.
4. No data may be stored on the Grid as a result of any action by a Web User, except for transient data stored in designated scratch areas on the computational resources provided to the running jobs.
5. The Portal must be capable of limiting the job submission rate individually for Pseudonymous, Identified and Strongly Identified Web Users.
6. The maximum average and peak job submission rate by the Portal induced by Pseudonymous and Identified Web Users must be specifically agreed between you and the Grid
7. The Portal must keep enough information to associate any interactions with the Grid with a particular user. If the user was Identified or Strongly Identified, all relevant authentication information must be recorded and archived.
8. Logged information must be made available to the Grid Management and to any Resource Provider who can justifiably claim to provide or to have provided resources to the Portal.

2.3 Class-3 "Data Processing" Portals

By registering a Robot Certificate associated with a Class-3 Portal in a Virtual Organisation, or by connecting a Class-3 Portal to the Grid infrastructure, you agree to the conditions laid down in this section and documents references therein.

1. The Portal may offer services to Identified and Strongly Identified Web Users.
2. The Portal may use a Robot Certificate, or alternatively may use the authentication information provided to obtain a User credential specific to the Web User and use these for interactions with the Grid. Re-usable private data, including private keys associated with proxy certificates, must not be transferred across a network, not even in encrypted form.
3. The Portal must not store or obtain long-lived reusable authentication information for Strongly Identified Web Users.
4. When a Robot Certificate is used to store data on the Grid as a result of an action by a Web User, it may only be stored in locations that have been specifically agreed between you and designated Resource Providers, except for transient data stored in designated scratch areas on the computational resources provided to the running jobs. When a User Credential is used, data may be stored in all Grid locations where the User has permission to store such data.
5. The Portal should be capable of limiting the job submission rate.
6. The Portal must keep enough information to associate any interactions with the Grid with a particular Web User.
7. The system used to authenticate Identified Users must be adequately secured. In particular
    a. Re-usable private information used to authenticate end-entities to the Portal must only ever be sent encrypted over the network when

authenticating to any system (including any non-Portal systems) that are allowed to use the authentication database.

b. Web Users must be notified of all registrations, modifications and of removal of their data in the authentication database.
c. The authentication database must contain enough information to contact the Web User for as long as authentication is possible.
d. Entering authenticating information in the database, including resets of such information, must be appropriately authenticated.

8. Logged information must be made available to the Grid Management and to any Resource Provider who can justifiably claim to provide or to have provided resources to the Portal.

2.4 Class-4 "Job Management" Portals

By connecting a Class-4 Portal to the Grid, you agree to the conditions laid down in this section and documents references therein.

1. The Portal may offer services only to Strongly Identified Web Users, or to Identified Web Users where both the Portal system itself and the authentication of Identified Web Users meets the requirements of either the SLCS or MICS IGTF Authentication Profile.
2. The Portal must use User credentials specific to the Web User and use these for all interactions with the Grid. Re-usable private data, including private keys associated with proxy certificates, must not be transferred across a network, not even in encrypted form.
3. The Portal must not store or obtain long-lived reusable authentication information for Strongly Identified Web Users.
4. The Portal should be capable of limiting the job submission rate.
5. The Portal must keep enough information to associate any interactions with the Grid with a particular Web User.
6. Logged information must be made available to the Grid Management and to any Resource Provider who can justifiably claim to provide or to have provided resources to the Portal.