

**Minimum Requirements for Participation in the Test Bed for
the Texas Internet Grid for Research and Education**

Revision 0.2
February 28, 2006

Purpose

This document establishes the minimum requirements for participation the Texas Internet Grid for Research and Education (TIGRE) test bed. TIGRE intends to operate such a test bed as a continuing part of the development process to achieve its goal of deploying a collaborative grid infrastructure and grid services architecture for the State of Texas. Having such a test bed will help to ensure that the resulting software, grid middleware and client tools, support center tools and other developed resources will be sufficiently interoperable and of sufficient quality to handle user requirements when they are deployed. For consistency, these requirements will be taken to apply continuously to resources and participants as TIGRE approaches operational production status.

Requirement Categories

Project-wide requirement specifications are needed in at least the following areas. As needed, this document will be revised and refined to reflect ongoing development of new requirements or changes to the agreed-upon common definitions in these areas.

Identity Management

TIGRE participants will be required for purposes of access to the test bed resources to be identified only through local accounts (in the case of local system administrators) or by presentation of TIGRE-specified grid credentials. The initial system to be used for such grid authentication is only in the form of X.509 Public Key Infrastructure (PKI) cryptographic certificates issued through a TIGRE-reviewed and approved certificate authority (CA). TIGRE will issue or accept such certificates to individuals or resources only for participation in approved project activities.

In addition to these basic authentication credentials, TIGRE will provide authorization attributes that will enable local authorization decisions to be made within the context of the local administrative systems of each TIGRE resource. Implementation of these authorization decisions will be subject to the policies and procedures in operation at each TIGRE institution. While automated systems to provide this authorization decision may be provided by the project, the final decision regarding access will always be under the local control of the administrators of each TIGRE resource, and subject to their approval.

Software Stack

Participating resource providers in the TIGRE test bed shall agree to install the TIGRE common middleware software stack or to deploy components on their resources that are interoperable work-alike replacements for TIGRE-supplied software. The timing of installation and preliminary testing of any given software release will be up to the local judgment of the administrators of each TIGRE test bed resource. Once a particular software release has been determined to be of operational production quality, all

administrators of TIGRE resources are expected to install that release or to bring their resources to equivalent functional quality as soon as possible.

Contact Information

It is essential for operational purposes that contact information be maintained in a current, accurate form for the administrators and security contacts applicable to each TIGRE resource. At minimum, these must be available through a Web page or other electronically searchable means at each of the TIGRE institutions with respect to their own resources, and links to such listings should be maintained on the common TIGRE site. Contact with users will be through e-mail addresses gathered as part of their registration with TIGRE. Such registration will be required in order to provide individuals access to TIGRE resources, and similar registration including administrative and security contacts will be required to include any given resource into TIGRE. In addition, normal status information messages including down time announcements, maintenance information, etc. will be distributed through optional e-mail lists set up for this purpose.

Acceptable Use Policies and Incident Response Plan

Acceptable use policies for access to resources through TIGRE will be developed by the project as a separate document. These procedures will be in a form that is compatible with current grid usage standards and that is consistent with usage policies at each of the TIGRE institutions.

In addition, an incident response plan giving policies and procedures to be followed within TIGRE in the event of a possible breach of the acceptable use procedures will be developed and provided by the TIGRE project.

Acceptance of each of the above documents by participants and resource providers shall be a requirement for participation in the TIGRE test bed.

Approval

This document will be taken to be operable upon adoption through a vote by the TIGRE Steering Committee.