Establishing Grid Trust with Fermilab

What Do User Experiments/Projects Need To Do?

Open Science Enclave Working Group

September 24, 2009
CD-doc-3429-v3

1. Table of Contents

2. Introduction

This document summarizes requirements and steps for an organization wanting to establish a trust relationship with Fermilab, enabling access to Fermilab's grid resources. None of the trust relationships are meant to explicitly give the FermiGrid manager authority over Open Science Enclave (OSE) resources dedicated to another organization.

This document does not cover the case where a Fermilab-originated organization (i.e. a group of Fermilab employees) directly applies to Open Science Grid (OSG), or another grid infrastructure, for membership.

3. Terms and Definitions

- **Abuse of Trust**: Performing an action that is in direct conflict with the actions agreed upon during the establishment of trust. Some examples include: running a job outside of the stated purpose of the organization, terminating another individuals job, running jobs that negatively impact shared resources and being unresponsive to requests to stop.

- **Establishing Trust:** The act of establishing trust communicates an organizations actions within a specified context. Here the context is use of grid-based resources.

- **FermiGrid:** FermiGrid is Fermilab's campus grid. All Fermilab's grid resources are part of FermiGrid.

- **Fermilab Virtual Organization (VO)**: The Fermilab VO is an umbrella VO that includes multiple groups. Groups can have different missions and goals. Fermilab VO management is responsible for managing and over-viewing groups' actions on the grid.

- **Trust:** Trust is the firm belief in the competence of an entity to act dependably, securely and reliably within a specified context.

- **Trust Relationship**: A logical connection that is established between a grid resource provider and an organization so that rights and privileges of the organizations members are recognized on the grid-based resources.

- **Virtual Organization (VO)**: A virtual organization is a group of individuals who share the computing resources of a grid for a common goal.

Roles

The following paragraphs define the roles that need to be filled as part of the process of establishing trust with Fermilab. It is at the discretion of the organization to fill these roles as they see appropriate (i.e. - one person may fill multiple roles).

The individuals acting in the defined roles interface between their organizations and FermiGrid management. They agree to be contacted by the FermiGrid management when there are problems in their designated areas, and they make every effort within their organizations to fix the problem, such as contacting other organization members, fixing software, etc.

Requirements designating which roles need to be filled for type of organization are in Section 5 under each individual 'Initial Requirements' section.

- **Group Manager Role**: A group manager is the person that is appointed to manage the group's grid activities. This person is the group's interface to the Fermilab VO management. This person will ensure that the group complies with the agreed policy and procedures and notifies Fermilab VO managers promptly when compliance is not met.

- **Operations Contact Role**: A group operations contact is a person who has an understanding of operational aspects of the group's work such as production on the grid, adding/deleting members, support, and troubleshooting. This person is responsible for continuous operations of the group. When the group's operations cause an interruption to others, the FermiGrid management will contact this person.

- **Security Contact Role**: A security contact is a person that has an understanding of the security aspect of the organization's work, such as applications, services, and tools. This person is responsible for security of the organization's operations. They ensure that no application, service or tool with known security problems are utilized by the organization, the organization's work does not cause a threat to other groups, or VOs, or to the Fermilab VO. When in doubt, this person informs the FermiGrid management and asks guidance. This person acts as the first respondent for the organization, in case of a security incident involving this organization, and makes his/her contact information available to FermiGrid management. NOTE: The organization may choose to delegate this responsibility to FermiGrid personnel.

- **Spokesperson Role**: A spokesperson or principal investigator is the person that the organization has agreed has the responsibility to speak for

the group in public fora. Under normal circumstances, this person is the experiments' spokesperson.

- **VO Manager Role**: A VO manager is the person that is appointed to manage the VOs grid activities. This person is the interface to FermiGrid management. This person will ensure that the VO complies with the agreed policy and procedures and notifies FermiGrid management promptly when compliance is not met.

4. Types of Organizations

Different types of organizations will establish trust with Fermilab differently depending on their type. Follow the workflow below to determine the type of organization you represent.
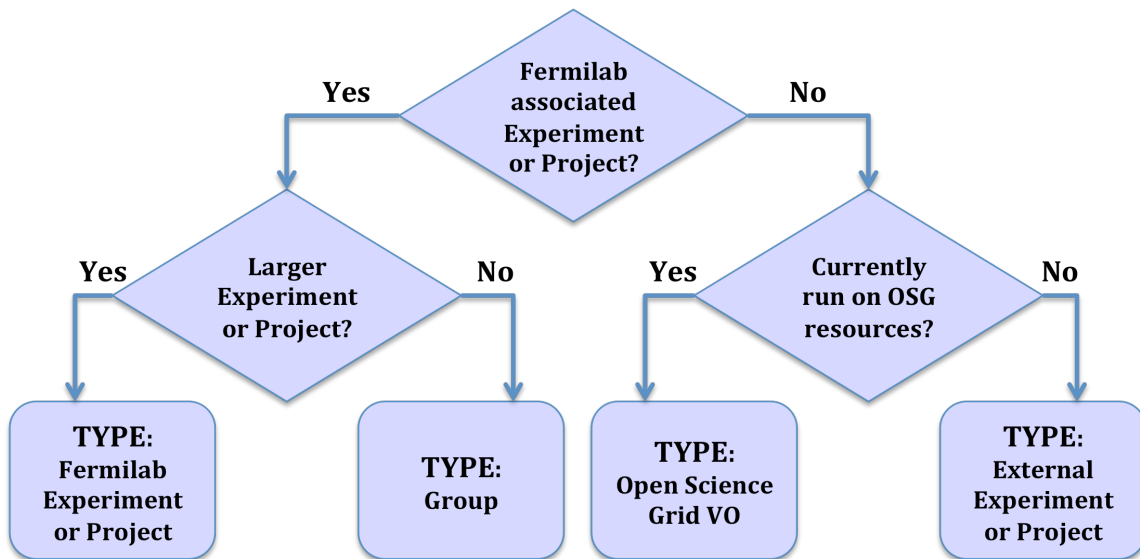
- **External Experiment/Project:** An external experiment/project is an organization of people who wishes to establish a trust relationship with Fermilab in order to be able to access Fermilab's grid resources. The external experiment does not have a formal association with Fermilab but they must be engaged in a collaborative scientific endeavor that aligns with the Fermilab's mission. NOTE: External experiments/projects might not receive the same priority and privileges as Fermilab experiments.

- **Fermilab Experiment/Project**: A Fermilab experiment/project is an organization of people who wish to form their own virtual organization (VO) to access Fermilab's grid resources. The experiment/project members are engaged in a collaborative scientific endeavor that aligns with the Fermilab's

mission. All members of a Fermilab experiment/project have Fermilab issued Kerberos credentials.

- **Group**: A group is an organization of people (e.g. experiment/project) who wishes to join the Fermilab VO to be able to access Fermilab's grid resources. Typically this is a smaller organization with limited resources. The group members are engaged in a collaborative scientific endeavor that aligns with the Fermilab's mission. All members of a group have Fermilab issued Kerberos credentials.

- **Open Science Grid VO**: An OSG VO is an organization of people who have already established a trust relationship with the OSG.

5. What Does the Organization Need To Do?

Requirements for an External Experiment/Project

Initial Requirements

1. The external experiment/project's must provide the FermiGrid manager with a summary of the experiment/project's purpose. The summary should cover how the experiment/project would utilize grid resources and how this is aligned with the experiment/project's mission.

2. The external experiment/project must provide the FermiGrid manager with a list of individuals and their contact information for the following roles: a spokesperson (or principal investigator) if available, VO manager, security contact, operations contact, and a backup person for each contact. A small experiment/project without enough members for each role can delegate these roles to corresponding Fermilab VO contacts if the FermiGrid manager permits.

Ongoing Requirements

1. The external experiment/project must agree not to knowingly cause any disruption to other grid users. The experiment/project will follow the recommendations and instructions of FermiGrid manager and will do its best effort to solve and identify problems.

2. The VO manager will audit the VO members, their trustworthiness, and their adherence to the policies and procedures. Once a year, the VO manager is recommended to check the validity of VO members' contact information and

audit VO membership and prune members who no longer work in the experiment/project.

3. The VO manager will promptly report any abuse of trust to FermiGrid management. The FermiGrid manager may suspend or bar non-complying VO members.

4. The VO manager must promptly inform the FermiGrid management when the VO no longer can comply with any of the requirements. Any changes in mission, contacts name and addresses must also be reported promptly to FermiGrid management.

5. When involved in a security incident, the VO contacts shall help investigate when requested, and co-operate with the Fermilab security team and FermiGrid security contacts.

6. The VO manager shall maintain a list of both onsite and offsite machines and services that are run by the VO for enabling VO members access to the grid, i.e. grid gateways, and make this list available to the FermiGrid management.

Requirements for a Fermilab Experiment/Project

Initial Requirements

1. The Fermilab experiment/project must provide the FermiGrid manager with a summary of the experiment/project's purpose and how that relates to Fermilab's mission. The summary should cover how the experiment/project would utilize grid resources and how this is aligned with the experiment/project's science mission.

2. The Fermilab experiment/project must provide the FermiGrid manager with a list of individuals and their contact information for the following roles: a spokesperson (or principal investigator) if available, VO manager, security contact, operations contact, and a backup person for each contact. A small experiment/project without enough members for each role can delegate these roles to corresponding Fermilab VO contacts if the FermiGrid manager permits.

Ongoing Requirements

1. The Fermilab experiment/project must agree not to knowingly cause any disruption to other grid users. The experiment/project will follow the recommendations and instructions of FermiGrid manager and will do its best effort to solve and identify problems.

2. The VO manager will audit the VO members, their trustworthiness, and their adherence to the policies and procedures. Once a year, the VO manager is recommended to check the validity of VO members' contact information and audit VO membership and prune members who no longer work in the experiment/project.

3. The VO manager will promptly report any abuse of trust to Fermilab VO management. The FermiGrid manager may suspend or bar non-complying VO members.

4. The VO manager must promptly inform the FermiGrid management when the VO no longer can comply with any of the requirements. Any changes in mission, contacts name and addresses must also be reported promptly to FermiGrid management.

5. When involved in a security incident, the VO contacts help investigate when requested and co-operate with the Fermilab security team and FermiGrid security contacts.

6. The VO manager shall maintain a list of both onsite and offsite machines and services that are run by the VO for enabling VO members access to the grid, i.e. grid gateways, and make this list available to the FermiGrid management.

Requirements for a Group

Initial Requirements

1. The group must provide the Fermilab VO manager with a summary of the group's purpose and how that relates to Fermilab's mission. The summary should cover how the group would utilize grid resources and how this is aligned with the group's science mission.

2. The group must provide the Fermilab VO manager with a list of individuals and their contact information for the following roles: a group spokesperson (or principal investigator) if available, group manager, group security contact, group operations contact, and a backup person for each contact. A small group without enough members for each role can delegate these roles to corresponding Fermilab VO contacts if Fermilab VO manager permits.

Ongoing Requirements

1. The group must agree not to knowingly cause any disruption to Fermilab VO management and other grid users. The group will follow the recommendations and instructions of Fermilab VO manager and will do its best effort to solve and identify problems.

2. The group manager will audit the group members, their trustworthiness, and their adherence to the policies and procedures. Once a year, the group manager is recommended to check the validity of group members' contact information and audit group membership and prune members who no longer work in the group and notify the Fermilab VO management.

3. The group manager will promptly report any abuse of trust to Fermilab VO management. The Fermilab VO manager may suspend or bar non-complying group members.

4. The group manager must promptly inform the Fermilab VO when the group no longer can comply with any of the requirements. Any changes in mission, group contacts name and address must also be reported promptly to Fermilab VO management.

5. When involved in a security incident, the group contacts shall help investigate when requested and co-operate with Fermilab security team, Fermilab VO security contacts, or outside partners of Fermilab VO if applicable.

6. The group manager shall maintain a list of both onsite and offsite machines and services that are run by the group for enabling group members access to the grid, i.e. grid gateways, and make this list available to the Fermilab VO management.

7. The Fermilab VO may be in trust relationships with outside parties (non-Fermilab entities), such as OSG. Such relationships may result in the Fermilab VO having to comply with a set of external polices. By being a member of the Fermilab VO, a group may also be able to participate in such relationships indirectly. However, the group's participation is not mandatory and may subject the group to additional requirements. During the registration process of the group to the Fermilab VO, the group manager must understand all the trust relationships Fermilab VO partakes in with outside parties and decide whether to participate in such relationships indirectly or not. The Fermilab VO Manager will explain such outside agreements during the registration application.

Requirements for an Open Science Grid VO

Fermilab has reviewed the OSG VO registration policy (http://osg-docdb.opensciencegrid.org/cgi-bin/ShowDocument?docid=737) and process and believes it is sufficiently rigorous to allow Fermilab to trust those VO's that have successfully completed this process. Fermilab retains the right to disallow a particular VO if necessary.

6. Registration Workflow
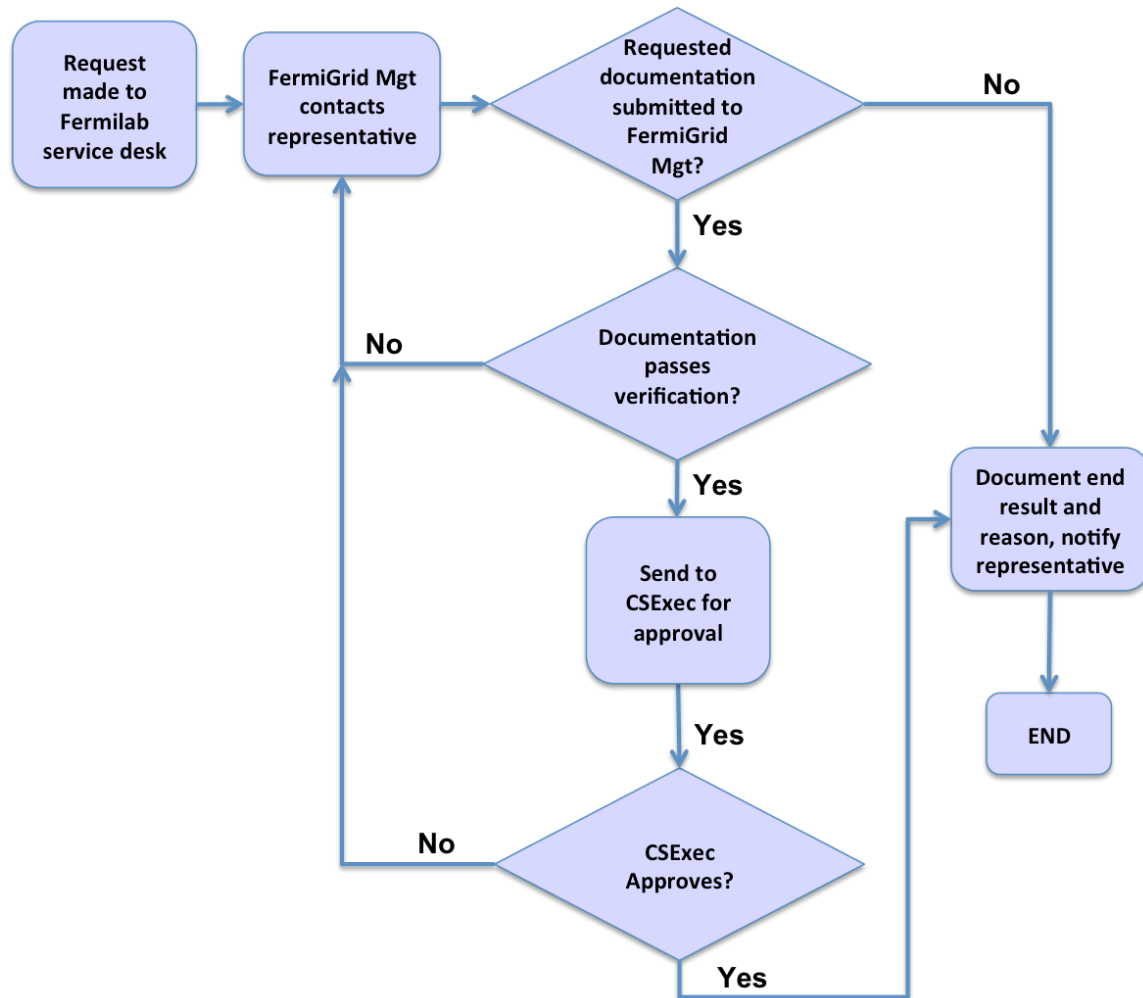
1. An organizational representative makes a membership request to the FermiGrid management by opening a service desk ticket at Fermilab (servicedesk.fnal.gov). The FermiGrid management will initiate communication with the representative.

2. The representative prepares a document detailing the organization's proposed answers to the requirements listed in above sections, and submits

them to the FermiGrid Management. If the appropriate documentation is not submitted, then the FermiGrid Management terminates the process and resolves the service desk ticket.

3. The FermiGrid management verifies the application information. If the application does not pass verification it is returned for revision to the representative. Upon successful verification, the FermiGrid Manager meets with organization members and explains the operational requirements associated with usage of FermiGrid resources, including any applicable trust relationship with third parties.

4. The FermiGrid Manager sends the application to the CSExec.

5. The CSExec reviews the application and reaches a decision whether to authorize the establishment of trust with the organization. The CSExec makes a clear statement under which conditions the approval is given. For example, for groups, an organization that cannot comply with the Fermilab VO agreements with third parties (e.g. Fermilab VO-OSG agreements) can still establish a trust relationship with Fermilab. In such cases, the Fermilab VO management must ensure that the organization will not be allowed to run on such third party resources.

6. The FermiGrid Management communicates the decision to the representative. If trust has not been established, the representative may revise the application further and resubmit. Upon successful establishment of trust, the FermiGrid manager resolves the associated service desk ticket.