Open Science Grid
Trust as a Foundation
June 6, 2006

Keith Chadwick

Role of Trust in Policy for the OSG

In the process of Fermilab thinking about glide-ins, our thinking has morphed of a more general discussion of:

- "why a Site should trust a VO".
- "why a VO should trust a Site".

These questions are foundational for the larger question of "Trust" across the grid.

At the present, such trust relationships only exist on the basis of, for lack of a better word, "small world" principles.

The veracity and completeness of your statements, your responsiveness, an understanding of the technology you are using, and so forth.

Companies like eBay, for example, make this more scalable, by evaluating the trust with a varieties of policies and technologies.

This is an interesting area for further discussion and exploration.

Trust is not Security!

Here are several examples:

Case I:

-Do I allow user X to use my resources?

-If so, what requirements must be satisfied by such a user?

Case II:

-Do I believe what Provider A says is true and factual?

Case III:

-Do I agree with the answer that is provided by a Provider or Group?

Case IV:

-Do I believe that a Provider or Group goals and/or priorities match mine?

Formal Definition of Trust

Trust of a party A to a party B for a service X is the measurable belief of A in that B behaves dependably for a specified period within a specified context (in relation to service X)

Trust Management

Trust management is the activity of collecting, encoding, analyzing and presenting evidence relating to competence, honesty, security or dependability with the purpose of making assessments and decisions regarding trust relationships.

There are two main approaches for trust management:

- Policy based.
- Reputation based.

Policy Based Trust

Policy based Trust employs different policy languages and engines for specifying and reasoning on rules for trust establishment.

The goal is to determine whether or not an unknown user can be trusted, based on a set of credentials and a set of policies.

Reputation Based Trust (eBay model)

Reputation based Trust uses computation models to estimate the degree of trust that can be invested in a certain party based on the history of its past behavior.

The available information is based on the recommendations and the experiences of others and is typically not signed by CA but (possibly) self-signed by the source of the statement.

This approach supports trust estimates with a wide, continuum range and allows the propagation of trust along the network as well as weighting of values

Trust Lifecycle

Phase I: Service (Provider) Identification

Phase II: Formation and Service (Provider) Invitation

Phase III: Operation and Service (Provider) Interaction

Phase IV: Dissolution

Trust Life Cycle Table

VO Lifecycle Phase	*Trust and Security*	*Service Level Agreement*	*Collaborative Process*
Phase I	Policy Specification. Verify Participant Credentials	Identify SLA Requirements	Define VO Objectives
Phase II	Evaluate Trust using Reputation Repositories	Negotiate SLA(s)	Evaluate Community Trust and Provision Resources
Phase III	Trust Maintenance	Monitor SLA Record SLA Violations	Trust based Service Invocation
Phase IV	Terminate Trust Relationship. Publish data into Reputation Repository	Update SLA	Disengage Resources

Table 1. Trust Lifecycle

Trust - Policy & Reputation

Within OSG:

- Formal Policies serve as the foundation of Trust.
  - User AUP
  - VO AUP
  - Service AUP
  - Site AUP

- Reputation of Users, VOs, Services and Sites will be evaluated on:
  - Their adherence with formal published policies.
  - Their responsiveness to policy issues.
  - The veracity of their statements and methods.
  - The publishing / exchanging of plans and adherence to them.

- Methods for evaluation and maintenance of Trust must be open.

Comments on Trust

Open science grid is an open organization, not only is the science open, but the methods are also open.

VO disclose the tools they use to organize their activities, explain how it works so it can be assessed.

To the extent that we exchange data, we expect that those tools will be accessible to each other.

All organizations in the core grid are subject to evaluation.

Basis of trust is open disclosure of policies, procedures, tools & methods.

Technical discussion of alternate policies, procedures, tools & methods.

Compliance with published and documented interfaces.

Disclosure of metrics

Open Science Grid
Draft VO AUP
June ??, 2006

Keith Chadwick

Who, Where, What, Why, When?

At the Open Science Grid Support Centers Meeting held on May 16&17, 2006 in Indianapolis, IN, Ruth Pordes asked me to work with some of the attendees and put together a draft Virtual Organization Acceptable Usage Policy for the Open Science Grid:

- Doug Olsen
- Horst Severini
- Eric Shook

In addition, the draft was discussed with the following people at the bi-weekly FermiGrid Stakeholders meeting:

- Igor Sfiligoi
- Steve Timm
- Dan Yocum

This draft has been discussed with Ruth Pordes and Don Petravick.

This is still ***very*** draft.

Comments, additions, deletions and alternate methods are welcome - please email them to chadwick@fnal.gov

VO AUP Introduction

All Virtual Organizations that are registered with the Open Science Grid must abide by a common set of basic rules.

This document lists those basic rules.

Note 1: Virtual Organizations and sites may enter into additional agreements pertaining to specific Virtual Organization or site acceptable usage policies - these agreements (if any) are outside the scope of the Open Science Grid Virtual Organization Acceptable Use Policy.

Note 2: The policies corresponding to Open Science Grid User Acceptable Use Policy entries are listed in *italics*.

1 - Membership List

Each Virtual Organization is responsible for maintaining the list of registered members of that Virtual Organization together with such personal contact information as is necessary to contact the individual members of the Virtual Organization.

- VOMS with or without VOMRS will satisfy this

2 - Registration

Each Virtual Organization is responsible for maintaining the Virtual Organization registration information with the Grid Operations Center of the Open Science Grid, including, but not limited to:

- Virtual Organization Membership Service(s)
  - The URL(s) for VOMS and/or VOMRS
- Virtual Organization Administrator(s)
  - The names of the individual(s) who have the VO-Admin role in VOMS.
- Virtual Organization Support Center
  - The individual(s) or email list which corresponds to the VO support center
- Virtual Organization Security Contact(s)
  - The individual(s) or email list which corresponds to the VO security contact(s)
- Virtual Organization Charter
  - The stated goals and policies for the VO.

3 - Accounting

Each Virtual Organization is responsible for the collection, maintenance and retention of:

- Available Virtual Organization accounting information.
- The list of GRID resources which are currently available to the Virtual Organization.
- The historical list of GRID resources where the Virtual Organization has run applications.
- Other?

4 - Applications within Scope of Charter

Each Virtual Organization is responsible for insuring that the registered members of the Virtual Organization only run applications that are within the scope of the Virtual Organization Charter, and only attempt to run applications on sites that have usage policies which are compatible with the Virtual Organization Charter.

(*You shall only use the GRID to perform work, or transmit or store data consistent with the stated goals and policies of the VO of which you are a member and in compliance with these conditions of use*.)

5 - Lawful Use

Each Virtual Organization shall insure that their members shall not use the GRID for any unlawful purpose and not (attempt to) breach or circumvent any GRID administrative or security controls and shall respect copyright and confidentiality agreements and protect GRID credentials (e.g. private keys, passwords), sensitive data and files.

(*You shall not use the GRID for any unlawful purpose and not (attempt to) breach or circumvent any GRID administrative or security controls. You shall respect copyright and confidentiality agreements and protect your GRID credentials (e.g. private keys, passwords), sensitive data and files*.)

6 - Security Incidents

Each Virtual Organization shall immediately report any known or suspected security breach or misuse of the GRID or GRID credentials to the incident reporting locations specified by the Open Science Grid and to the relevant credential issuing authorities.

(*You shall immediately report any known or suspected security breach or misuse of the GRID or GRID credentials to the incident reporting locations specified by the VO and to the relevant credential issuing authorities*.)

7 - Risk

Each Virtual Organization agrees that their use of the GRID is at their risk. There is no guarantee that the GRID will be available at any time or that it will suit any purpose.

(*Use of the GRID is at your own risk. There is no guarantee that the GRID will be available at any time or that it will suit any purpose*.)

8 - Logged Information

Each Virtual Organization agrees that logged information, including information provided for registration purposes, shall be used for administrative, operational, accounting, monitoring and security purposes only. This information may be disclosed to other organizations anywhere in the world for these purposes. Although efforts are made to maintain confidentiality, no guarantees are given.

(*Logged information, including information provided by you for registration purposes, shall be used for administrative, operational, accounting, monitoring and security purposes only. This information may be disclosed to other organizations anywhere in the world for these purposes. Although efforts are made to maintain confidentiality, no guarantees are given.*)

9 - Regulate Access

Each Virtual Organization agrees that the Resource Providers, the VOs and the GRID operators are entitled to regulate and terminate access for administrative, operational and security purposes, and shall immediately comply with the Resource Providers' instructions. In addition each Virtual Organization is responsible for insuring that the users and resource providers under their jurisdiction comply with instructions from the entities described above.

(*The Resource Providers, the VOs and the GRID operators are entitled to regulate and terminate access for administrative, operational and security purposes and you shall immediately comply with their instructions*.)

10 - Liability

Each Virtual Organization agrees that they are liable for the consequences of any violation of the Open Science Grid Acceptable Usage Policy, and the above conditions of use, by their registered members.

(*You are liable for the consequences of any violation by you of these conditions of use*.)

Fin

Any questions?