Comparison of European Grid Projects

Jarek Nabrzyski, Ariel Oleksiak (PSNC)

Project:

GEMSS

Area:

Security Services

Table of Contents

1. Introduction

1.1. Objective and Structure

This document is one of thirteen templates that have common goal to gather information related to main European Grid Projects in order to make their accurate comparison in the framework of GRIDSTART initiative. We believe that the participation of particular projects members in preparation of this document will allow comparing all activities in a credible and exhaustive way.

The proposed structure of the description consists of two parts. The former is concerned with the general overview and architecture together with the contents of layers (the first template). The latter includes the main components of the Grid infrastructure (remaining 12 templates). Since information regarding the project architecture is to be quite general, more detailed description should be provided in the review of the main aspects of the Grid infrastructure. In order to prepare uniform description for each project, we identify the important issues that have to, should or can be included into particular components. Common issues for all components and these specific for this component are briefly described in the next section.

We ask you to proceed according to this schema. However, a feedback is obviously welcome. For some projects the document has been partially completed on the basis of descriptions found at the official web pages. In this case, we ask you to revise already filled in sections, correct and complete them if necessary.

You should take into consideration future plans while you fill in particular sections. Actually they are even more important then the current state of the project components. If you are not going to design some elements in the scope of the project at all, please, note it in the proper section.

1.2. Uniform description

All the descriptions of the Grid infrastructure components are divided into three parts: **General** section includes main requirements and functionality, **Details** section relates to the issues specific for particular component and **External** defines its connections with other components and users.

As it was mentioned above, some of the issues are common for all components or at least repeat for many of them. Such issues, appearing for many or even all areas are shortly characterized below.

In **General** section:

Main requirements determine the objectives and requirements of the workpackage or the software module responsible for the design of functionality related to the particular domain of the Grid infrastructure.

Functionality contains a set of operations provided by the project in the given area.

In **External** section:

Interfaces define services, SDKs, APIs and so forth which can be used in order to access the functionality of the component.

Low level Grid middleware is the middleware providing basic Grid functionality as for example Globus or UNICORE.

Relations with other components determine components that utilize or are utilized by component being described as well as data and information flow between them.

Issues that are specific for this particular domain of the Grid infrastructure are presented in the sequel. Some of them, which we consider to be clear, have been skipped, however, if they turn out to be vague, please, contact the authors of this document (ariel@man.poznan.pl).

The **Details** section describes the security issues essential in the context of the dynamic, distributed and inter-organizational Grid environment.

Assurance describes mechanisms that allow the requester of a service to decide whether a candidate system or service provider meets the requester's requirements for security, trustworthiness, reliability, or other characteristics.

Audit defines which operations performed by a system are recorded and how they are used from the perspective of system security.

2. Security Services

2.1. General

- **Main requirements**
  - Authentication – proof of identity, a PKI will be employed and IETF X.509 standards fully adhered to
  - Confidentiality - protection of patient scan data and commercial model data
  - Firewalls - Grid operation must be compatible with existing site firewalls and policies
  - Formal procedures - each site should have a written security procedure it agrees to adhere to
  - Logging - Auditable logs should be kept of important transactions, in addition to low level security logging
  - Restrictions on data use - Patient data should only be used for the agreed purpose and should only be stored for a period of time to accomplish that purpose
  - Script access - no shell access will be allowed for security reasons
- **Functionality**
  - Public key infrastucture
  - IETF X.509 standards applied
  - Security event logging and an intrusion detection system
  - Written security procedures that each Grid site agrees to adhere to
  - Where possible commercial off the shelf technology will be used, particularly products which actively release security patches

2.2. Details

- **Authentication**

  Single sign-on

  A single sign-on will log users onto the client Grid software. Certificate based authentication is used by the service provider to authenticate client service calls.

  Delegation

Due to our security requirements we do not intend to support Globus style certificate proxies. Instead we intend to be, unlike Globus, X.509 compliant. We are devising delegation mechanisms based on WS-security that will be consistent with this.

Openness

Each site will be permitted to decide which CA's to trust – i.e. there will not be a single overarching GEMSS CA.

- **Authorization**

  Access control methods

  Web services (OGSA) will be used to wrap services to restrict access to a limited set of application function calls. We will not allow remote shell access by the client to a Grid server.

  Restricted delegation

  A data-staging model will be investigated to allow a remote Grid server to farm out jobs to other Grid servers under the control and authorization of the client.

- **Assurance**

  Intrusion detection software will be investigated.

- **Audit**

  Digital contracts will be exchanged before Grid jobs are run, ensuring accountability on both sides prior to financial billing for jobs.

- **Encryption algorithms**

  We intend to implement a PKI.

- **Communication protection requirements**

  Support of reliable communication protocols

  Others

  Anonymization, where possible, of all patient data communicated.

- **Mobile users support**

  Job monitoring may be possible via a simple web browser.

2.3. External

- **Interfaces**
- **Low level grid security middleware**
- **Relations with other components**
- **Integration of global security policy with local ones**