Design and development of ApGrid Testbed

Yoshio Tanaka, Satoshi Sekiguchi
National Institute of Advanced Industrial Science and Technology
Tsukuba Central 2, Umezono 1-1-1
Tsukuba, Ibaraki 305-8568, Japan
{yoshio.tanaka, s.sekiguchi}@aist.go.jp

Abstract

ApGrid is a partnership for Grid computing in the Asia Pacific region. One of the most important objectives of ApGrid is building an international Grid testbed called ApGrid Testbed. ApGrid is not a single source funded project and ApGrid Testbed is based on contribution, i.e. participating organizations provides each others computing resources to ApGrid Testbed. This paper describes the technical aspects of overview, running policy, and guidelines on ApGrid Testbed development. ApGrid Testbed is based on standard Grid infrastructure. Security service on ApGrid Testbed is based on GSI and ApGrid Testbed allows multiple root CAs. Information services are provided through hierarchical MDS tree built by GRISes and GIISes. This paper also reports on some tools for managing and operating ApGrid Testbed such as CSR geneartor.

1 Introduction

As Grid computing[1] is regarded as a viable next generation computing infrastructure, it becomes important to develop production Grid for running large scale applications, evaluation of middlewares, and obtaining experiences and knowledge on managing virtual organizations.

ApGrid is a partnership for Grid computing in the Asia Pacific region[2]. ApGird is an open community for collaboration and it is not restricted to just a few developed countries, neither to a specific network nor its related group of researchers. As of the end of October 2002, 40 organizations from 15 countries have been participating in ApGrid. The objectives of ApGrid is to develop a partnership among Asia Pacific communities to

- build an international Grid testbed.
- provide a venue for sharing and exchanging ideas and information.
- provide a venue for helping initiation of new projects.
- collaborate and build on each others work.
- encourage application communities and assist them in using our technologies along with others.
- being an interface to global Grid efforts such as Global Grid Forum[6].

Table 1 shows a brief history of ApGrid.

The first informal meeting was held in Yokohama, July 2000. Dr. Charlie Catlett from Grid Form, Dr. Ben Siegel from CERN, and some Japanese representatives attended the meeting and agreed with launching ApGrid and its overview and policy. HPC Asia in Gold Coast was a good opportunity to gather Asia Pacific Grid researchers and invited them to ApGrid. Actually, the growth of ApGrid and testbed development was accelerated with HPC Asia as a trigger. ApGrid Workshop brings together participants from academia, industry and government to learn about

Table 1: History of ApGrid

Time	Place	Event
Jul. 2000	Yokohama/Japan	Informal meeting for the launch
Oct. 2000	Boston/USA	First presentation at GF5
Sep. 2001	Gold Coast/Australia	Exhibition at HPC Asia
Oct. 2001	Tokyo/Japan	1st ApGrid Workshop
Nov. 2001	Denver/USA	Exhibition at SC2001, ApGrid Panel at SC Global
Jan. 2002	Phuket/Thailand	1st ApGrid Core Meeting
May 2002	Taipei/Taiwan	2nd ApGrid Workshop, 2nd ApGrid Core Meeting

Grid applications and middleware and to discuss future directions for Grid development. ApGrid Core meeting is a closed meeting in which administrative and technical issues for running ApGrid are discussed between ApGrid "core" members.

One of the most important objectives of ApGrid is building an international Grid testbed called ApGrid Testbed. ApGrid Testbed can be used for the evaluation of developed middlewares as well as running large scale real applications. Although there have been various attempts to develop large scale Grid testbed such as Nasa Information Power Grid[3], European Data Grid[4], TeraGrid[5], etc, most of them are either application driven testbeds or organized under the specific alliance or organization, i.e. each testbed has been developed to achieve its common goal. ApGrid Testbed is not an application driven testbed and it is a truly multi national/political/institutional virtual organization. In order to develop ApGrid Testbed as a production Grid, some issues should be considered such as:

- How to motivate Asia Pacific Grid researchers to participate in ApGrid.
- Administrative issues such as membership rule, funding, etc.
- How to develop the testbed.

Since there are differences in policies, interests, etc. between ApGrid participants, these are important issues for the testbed development. Virtual organization is the essence of Grid and experience and knowledge on running ApGrid Testbed could be important and valuable information for building world wide Grid testbed.

These issues have been discussed in ApGrid core meeting (see Table 1). This paper describes the technical aspects of overview, running policy, and guidelines on development of ApGrid Testbed. This paper is focused on the following issues which are considered to be definitely required to run Grid testbeds.

Security Services
ApGrid Testbed build security infrastructure to provide secure and trusted Grid services.

Information Services
ApGrid Testbed provides information services which enable dynamic registration and retrieval of various Grid information.

Guidelines for Resource Contributors
ApGrid Testbed has guidelines on resource contribution.

Guidelines for Participating Users
ApGrid Testbed has guidelines for participating users.

Tools for Managing ApGrid Testbed
ApGrid Testbed has developed some tools for managing ApGrid Testbed.

Sections 2 and 3 describe the security infrastructure and information services on ApGrid Testbed. Guidelines for resource contributors and participating users are described in sections 4 and 5 respec-

tively. Section 6 shows some tools we have developed for managing ApGrid Testbed, and concluding remarks is described in section 7.

2 Security Infrastructure

GSI (Grid Security Infrastructure) would be the best candidate for the security infrastructure on the ApGrid Testbed. GSI is based on public key encryption, X.509 certificates, and the Secure Sockets Layer (SSL) communication protocol. GSI enables secure communication, security services without centrally-managed security system, and single sign-on for users on the Grid.

A central concept in GSI authentication is the certificate. Every user and service (e.g. computers) is identified via a certificate (user certificate, host certificate, etc.). A GSI certificate includes (1) A subject name (2) The public key (3) The identity of a Certificate Authority (CA) that has signed the certificate (4) The digital signature of the CA. Following is a note for the security services and requirements on the ApGrid Testbed (see Figure 1):

- The ApGrid Testbed runs CAs and issues certificates for users and resources.
- The ApGrid Testbed allows multiple root CAs.
- Each country/organization/project could run its own CA and these could be root CAs on the ApGrid Testbed.
- Running ApGrid representative root CA should be considered in the near future. This enables ApGrid participating organizations to run ApGrid sub CA which is signed by ApGrid representative root CA.
- Each organization contributing resources can select one or more root CAs which would be approved as valid root CAs at the organization. This enhances the flexibility of the authentication policy and enables the restriction of the authentication. In Figure 1 for example,
  - Organization A allows the access from user A and user C.
  - Organization B allows the access from user B and user C.
  - Organization C allows the access from user A, user B and user C.
- For participating countries and organizations, it is not a requirement to run their own root CA.
- Every user on the ApGrid Testbed is required to get the user certificate signed by one of the CAs on the ApGrid testbed. In order to get the user certificate, (1) user creates a certificate request (2) send it to the appropriate CA via email (3) the CA authenticates and approves the user (4) if the user is approved, the CA creates the certificate for the user, signs on it, and send it to the user via email.
- Server/host certificate on the ApGrid Testbed is an optional. Since most recent Grid systems require the server/host certificate for mutual authentication between users and hosts, getting the server/host certificate is strongly recommended.
- Running key servers for CAs should be considered for the scalability issue.

3 Information Service

LDAP (Light-weight Directory Access Protocol) based information infrastructure is used for the information services on the ApGrid Testbed. The Testbed information such as available hardware (hostname, architecture, number of processors, physical memory size, etc.) and installed software (name, version, installed directory, etc.) are stored in the form of an LDAP-based information infrastructure (directory tree). Users can retrieve this information by querying the information to the LDAP servers using LDAP protocol.

The ApGrid Testbed provides two kinds of information services:

- **Grid Resource Information Service (GRIS)**
  GRIS provides resource specific information such as hostname, installed software, load,

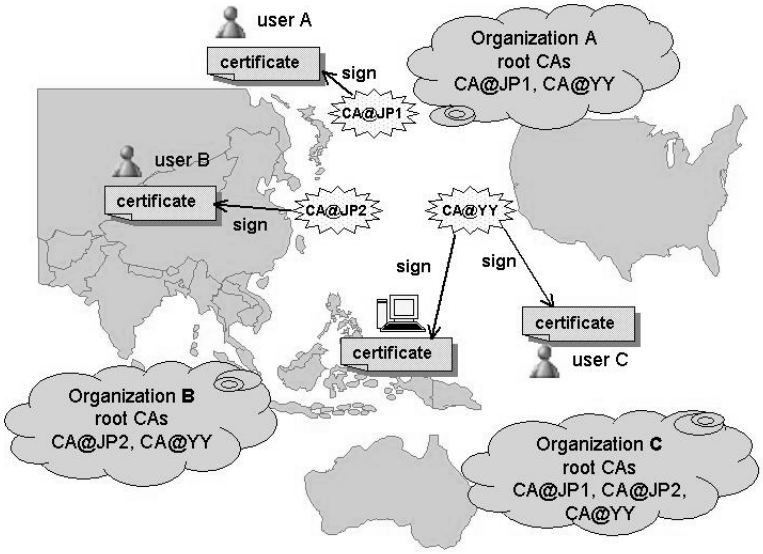

Figure 1: Overview of security infrastructure in ApGrid Testbed

process information, storage information, etc. GRIS gathers this information on demand.

- **Grid Index Information Service (GIIS)** GIIS describes a class of servers. GIIS gathers information from multiple GRIS servers. GIIS is considered as an organizational LDAP server.

GRISes and GIISes could be hierarchical. GRIS runs on the each resource and more than one GIISes run on the ApGrid Testbed which gather information from multiple GRISes (see Figure 2).

Some problems and research issues should be considered such as

- Single Point Failure
- Possibility of running mirror servers
- Overhead incurred by the structure of hierarchical information services
- ApGrid plans to allow ApGrid people to browse the information of the ApGrid Testbed via Web.

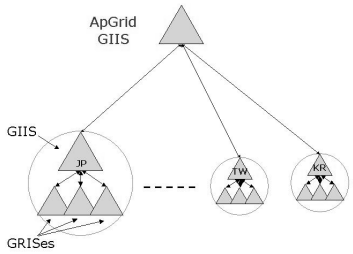

Figure 2: Hierarchical MDS in ApGrid Testbed

- ApGrid plans to allow researchers to search the information with LDAP API for their resource discovery purposes.

4 Guideline for Resource Contributors

4.1 Required Software

Globus Toolkit[7] is used for building software infrastructure in ApGrid Testbed. Globus Toolkit was chosen as a common software since Globus Toolkit has the advantage of several points as below.

- Globus Toolkit provides tools to build GSI based security infrastructure and MDS (GRIS/GIIS) based information service.
- Globus Toolkit is a defacto standard of the low-level Grid middleware and it provides better interoperability with other Grid testbeds

It is strongly recommended to install other Grid middlewares such as MPICH-G2[8] and Ninf-G[9].

4.2 Configure Security Infrastructure

Resource contributors can select one or more trusted CAs by themselves. Resource contributors must put trusted CA's certificate and signing policy file in appropriate directory such as `/etc/grid-security/certificates`. Certificates and signing policy files of all CAs in ApGrid Testbed are put on the ApGrid home page. Resource contributors can download the trusted CA's certificate and signing policy file through secure (https) access. The server certificate of the web server is signed by commercial CA (VeriSign).

4.3 Information to be provided

Root of the hierarchical information tree is mds.apgrid.org, i.e. ApGrid GIIS is running on mds.apgrid.org. Resource contributors must put their resource information into ApGrid GIIS. At the starting point, default information would be registered. Minimum requirements for the information

```
database        giis
suffix          "Mds-Vo-name=AIST, o=Grid"
conf            /opt/gt2/etc/grid-info-site-giis.conf
policyfile      /opt/gt2/etc/grid-info-site-policy.conf
anonymousbind   yes
access to * by * write
```

Figure 3: example of grid-info-slapd.conf

```
# register this server AIST to ApGrid
dn: Mds-Vo-Op-name=register, \
    Mds-Vo-name=ApGrid, o=Grid
regtype: mdsreg2
reghn: mds.apgrid.org
regport: 2135
regperiod: 600
type: ldap
hn: YOUR.HOST.NAME
port: 2135
rootdn: Mds-Vo-name=YOUR_VO_NAME, o=Grid
ttl: 1200
timeout: 20
mode: cachedump
cachettl: 30

# register this server GRIS to this server GIIS
dn: Mds-Vo-Op-name=register, \
    Mds-Vo-name=YOUR_VO_NAME, o=grid
regtype: mdsreg2
reghn: YOUR.HOST.NAME
regport: 2135
regperiod: 600
type: ldap
hn: YOUR.HOST.NAME
port: 2135
rootdn: Mds-Vo-name=local, o=grid
ttl: 1200
timeout: 20
mode: cachedump
cachettl: 30
```

Figure 4: template of grid-info-resource-register.conf

to be provided will be discussed in the near future. Figures 3 and 4 are templates of configuration files of site's GIIS for registering their information to ApGrid GIIS. `grid-info-slapd.conf` should be configured to define site's suffix (Mds-Vo-name). Figure 3 is an example of the configuration file in AIST GIIS. `suffix` should be replaced with the appropriate vo name. `grid-info-resource-register.conf` should be configured to register their information to ApGrid GIIS. In figure 4, `YOUR.HOST.NAME` and `YOUR_VO_NAME` must be replaced with appropriate hostname and site's vo name.

4.4 Announcements

When the resource becomes ready, send an email to the appropriate mailing lists.

4.5 Create login accounts

Each institution participating in the ApGrid Testbed has different procedures for creating login accounts. In order to enhance the security of the ApGrid Testbed, every user should be appropriately authenticated. For creating login accounts, each institution is strongly recommended to request the users to provide their user certificates signed by a trusted CA.

4.6 Maintenance

Donated resources should be monitored appropriately.

5 Guideline for Participating Users

- **Getting User Certificate**
  Users are required to get user certificate signed by trusted CA on the ApGrid Testbed.
- **Getting login accounts**
  In order to get login accounts at each institute, send an email to the appropriate contact(s) at each institute. The contacts are listed at the ApGrid web site.
- **other requests**
  For other requests such as adding user's DN into grid-mapfile, contact to the appropriate contact(s).

6 Tools

We have developed some tools for managing and operating ApGrid Testbed. This section describes the "CSR generator" as an example of such tools. ApGrid participating users are required to get a user certificate. Usually, a unix command provided by CA is used to generate a certificate signing request (CSR). For example, the Globus Toolkit provides `grid-cert-request` command. The CSR will be sent to the CA, and CA will issue and send the signed certificate after the validity check. For application programmers, it is not easy to run such command since it assumes that security related software such as OpenSSL has been installed in advance.

We have designed and implemented the CSR generator. The generator has the following features:

- CSR will be generated at the user's machine. This means private key is kept in the user's machine.
- It is not required to pre-install software used generating a CSR at the user's machine.

We have implemented the CSR generator using CoG kit [10] and Java Web Start[11]. With Java Web Start, applications are launched by clicking on a Web page link. If the application is not present on user's machine, Java Web Start automatically downloads all necessary files. By using the CSR generator, users are required to simply click the links on the web pages. The required software to generate a CSR will be automatically downloaded at the user's machine and the generator will run on the user's machine. Figure 5 illustrates the execution flow of the CSR generator.

When a user clicks a Web page link, the application (CSR generator) and all necessary files such as required Java class libraries are automatically downloaded at the user's machine and CSR generator

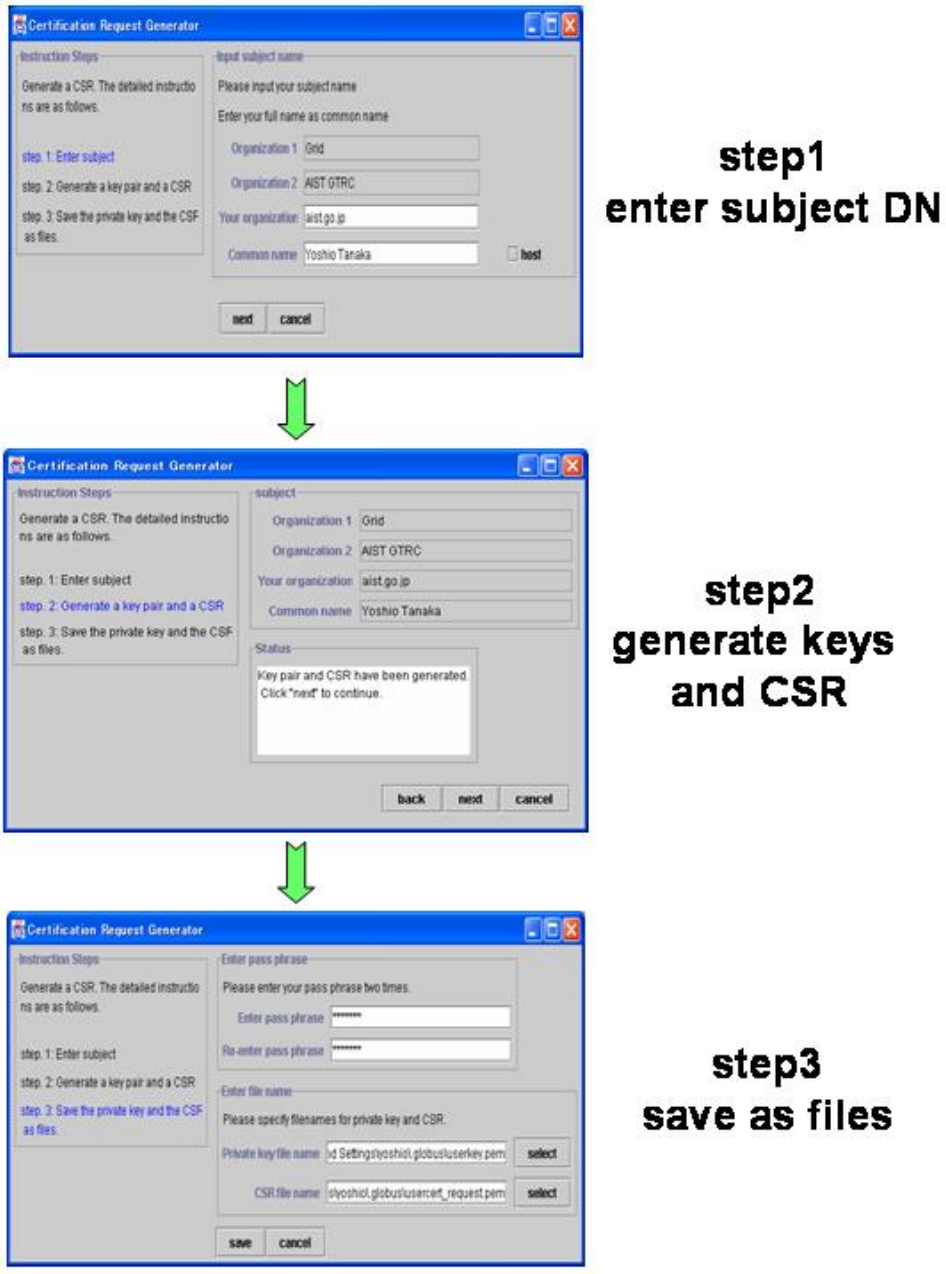

Figure 5: Execution flow of the CSR generator

starts when all necessary files are downloaded. At the first step, the user specifies user's name and email address for generating a CSR for the user certificate (step1 in Figure 5. The user have to specify host's FQDN for generating a CSR for the server certificate. At the second step, a key pare (private key and public key) and a CSR are generated (step2 in Figure 5). At the final step, the generated CSR and private key are saved as a local files (step3 in Figure 5). CSR generator completes its execution and user have to send the generated CSR to an appropriate CA.

The CSR generator enables users to get user's certificates without painful software installation.

7 Concluding Remarks

This paper reports on the technical issues for the development of ApGrid Testbed. ApGrid Testbed is based on standard infrastructure such as GSI and MDS, which provide better interoperability with other Grid testbeds.

Development of ApGrid Testbed has just started and it is still immature status as a production Grid. As of the end of October, the ApGrid Testbed has approximately 200 cpus computational resources, Access Grid facilities including virtual venue servers, databases of bioinformatics, natural science, etc., and human resources. Several groups have experience on running small scale applications and demonstrations on ApGrid Testbed, and they are planning to run larger scale applications on larger scale ApGrid Testbed. As the first milestone, ApGrid Testbed will establish as a large scale (500-1000 cpus, 10-15 organizations) production testbed by the end of F.Y. 2003.

Acknowledgment

The development of ApGrid Testbed is supported by many ApGrid participants. We wish to express our gratitude for all ApGrid participants. We would especially like to thank ApGrid core members and technical contacts for the valuable discussions for the Testbed development at the ApGrid Core meetings.

References

[1] Foster, I. et.al.(eds.): *The GRID: Blueprint for a New Computing Infrastructure*, Morgan Kaufmann (1999).

[2] http://www.apgrid.org/.

[3] http://www.ipg.nasa.gov/.

[4] http://www.eu-datagrid.org/.

[5] http://www.teragrid.org/.

[6] http://www.globalgridforum.org/.

[7] http://www.globus.org/.

[8] http://www-unix.mcs.anl.gov/mpi/mpich/.

[9] http://ninf.apgrid.org/.

[10] http://www.globus.org/cog/.

[11] http://java.sun.com/products/javawebstart/.

[12] http://www.pragma-grid.org/.