Integrating Certificate Services with Grid Widgets for a Computational Grid Platform

Hui-Shan Chen, Yi-Lun Pan, and Chang-Hsing Wu
National Center for High-performance Computing, Taiwan, R.O.C.
Email: {chwhs, serenapan, hsing}@nchc.org.tw

Abstract—Large-scale parallel computing is increasingly relying on multi-clusters and Grids, and user authorization on computing nodes is an important issue. To contribute the issue, the certificate authority (CA) public key infrastructure (PKI) service has been integrated with Grid Widgets by the Distributed Computing Team in National Center for High-performance Computing (NCHC). NCHC CA PKI service has been operating since 2008, which provides supports for certificate services integrated with Grid Widgets. At a beginning Grid session, a Grid proxy credential should be created to delegate a user identity for Grid interactions. Moreover, the excellent way leads the convenient management of the credential lifetime on the computational Grid platform.

Index Terms—certificate authority (CA), parallel computing, Grid proxy credential

I. INTRODUCTION

The computational Grid platform is constructed from the computing resources at NCHC [6] and Computer and Network Center of National Cheng Kung University (NCKU CNC) [7]. Cross-cluster management can optimize the system throughput and promote the resource utilization. The proposed integration project principally devotes to combine existed Grid services with developed Grid Widgets so it makes users exercise resources readily and knowingly. It also assists NCHC in expanding the scale of the computational Grid platform to provide more computing resources.

The computational Grid platform provides a high quality of research and experiment environment for academia and business community. Furthermore, the lightweight graphical user interface (GUI) framework – Grid WebOS [9] developed by NCHC Grid Research Team integrates multi-site interface platforms seamlessly to enhance the competitiveness of NCHC. On Grid WebOS, a proxy credential needs to be created as a limited delegation of rights for users before submitting jobs. Afterwards, users carry their proxy credentials to acquire services smoothly if authenticated successfully by the accessed resources.

The remainder sections of this paper are organized as follows: Section II gives a briefly review on related studies. The system architecture and the implementation are elaborately described in section III and IV. The achievement demonstration is completely presented in section V. We finally conclude this paper and picture our future plans in section VI.

II. RELATED WORK

Certificate services for Grids have been long researched. Previous works may be considered from different viewpoints or considered without well-laid plans. Differences between these works and our proposed integration project are detail discussed in this section.

Proxy Certificate Trust List (PCTL) is proposed to record the trusted delegation trace for Grid computing in [5]. It provides on-demand inquiry services for real time delegation information of Grid computing underway. However, our architecture adopts automatic mechanism to notice the remainder lifetime of impending overdue certificates for users.

This research has described the architecture for a Grid PKI service to serve a large number of users and improve usability for non-technical users by making the entire certificate and proxy issuance process hidden from users [4]. They adopt their UK e-Science CA for e-Science projects in the UK.

However, NCHC CA is a member of Asia Pacific Grid Policy Management Authority (APGrid PMA [1]) so NCHC CA can be trusted more safely.

The paper [3] proposes a security infrastructure for Grid applications, in which users are authenticated using passwords. It adopts the password-enabled and certificate-free way. However, we adopt Grid Security Infrastructure (GSI) [2]. Users and hosts are identified via certificates which contain information for identification and authentication. The GSI way is more familiar than the password way on Grids.

III. SYSTEM ARCHITECTURE

The system architecture is exhaustively described in this section. For the most parts, we introduce the CA PKI infrastructure and Grid Widgets.

A. CA PKI infrastructure

NCHC CA [8] is located in Taiwan and has been running since 2008. NCHC CA operated by NCHC Certificate Authority Group has a PKI architecture which issues X.509 certificates for end entities including users and hosts. User certificates can be used to authenticate users for sites that have agreed to accept the certificates signed by NCHC CA. Host certificates can be used to identify a fully qualified domain name (FQDN) of a specific host and used for the encryption of TLS/SSL communication.

An x.509 certificate is a digital file used to cryptographically bind an entity's public key with specific related information of its identity. It contains user name or DNS (Domain Name System) name of the host, issuer name, issuer identifier, expiry date, and digital signature, etc. Certificate are signed and issued by CA. Safe communication requires reliable certificates. CA is a trusted third party, and it makes Grid entities use issued certificates and proxy credentials to verify their identity. The flow chart of the certificate service is indicated in Figure 1.
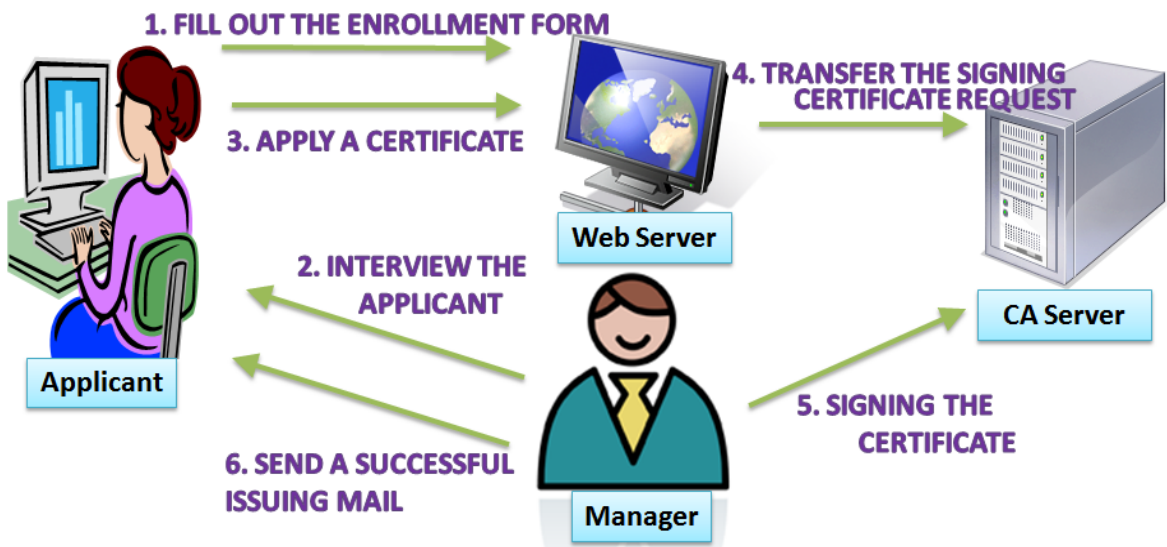

Figure 1. Flow Chart of the Certificate Service

B. Grid Widgets

By integrating Grid technologies and WebOS, we have come up with a new and extremely lightweight approach to acquire Grid services via Grid Widgets in Grid WebOS environment. The designed Grid WebOS has become necessary to provide Grid users with an interface that is both user-friendly and more straightforward. This research focuses on managing computing resources with more interactive graphical environment.

The designed Grid Widgets include fundamental Grid Widgets and customized Grid Widgets. Together, these Grid Widgets provide Grid users with an easy access to integrated and yet distributed computing resources, and also improve the

efficiency of the resources in the heterogeneous and dynamic Grid computing environment. These widgets can be easily customized and configured based on the end user's needs. Several basic fundamental Grid Widgets (Figure 2) such as MyProxy, GridFTP, Job Submission widgets were developed. These widgets address user and proxy management, data movement, file transfer, job submission and execution, Grid resource monitoring, and job status reporting – all within the Grid environment [11].
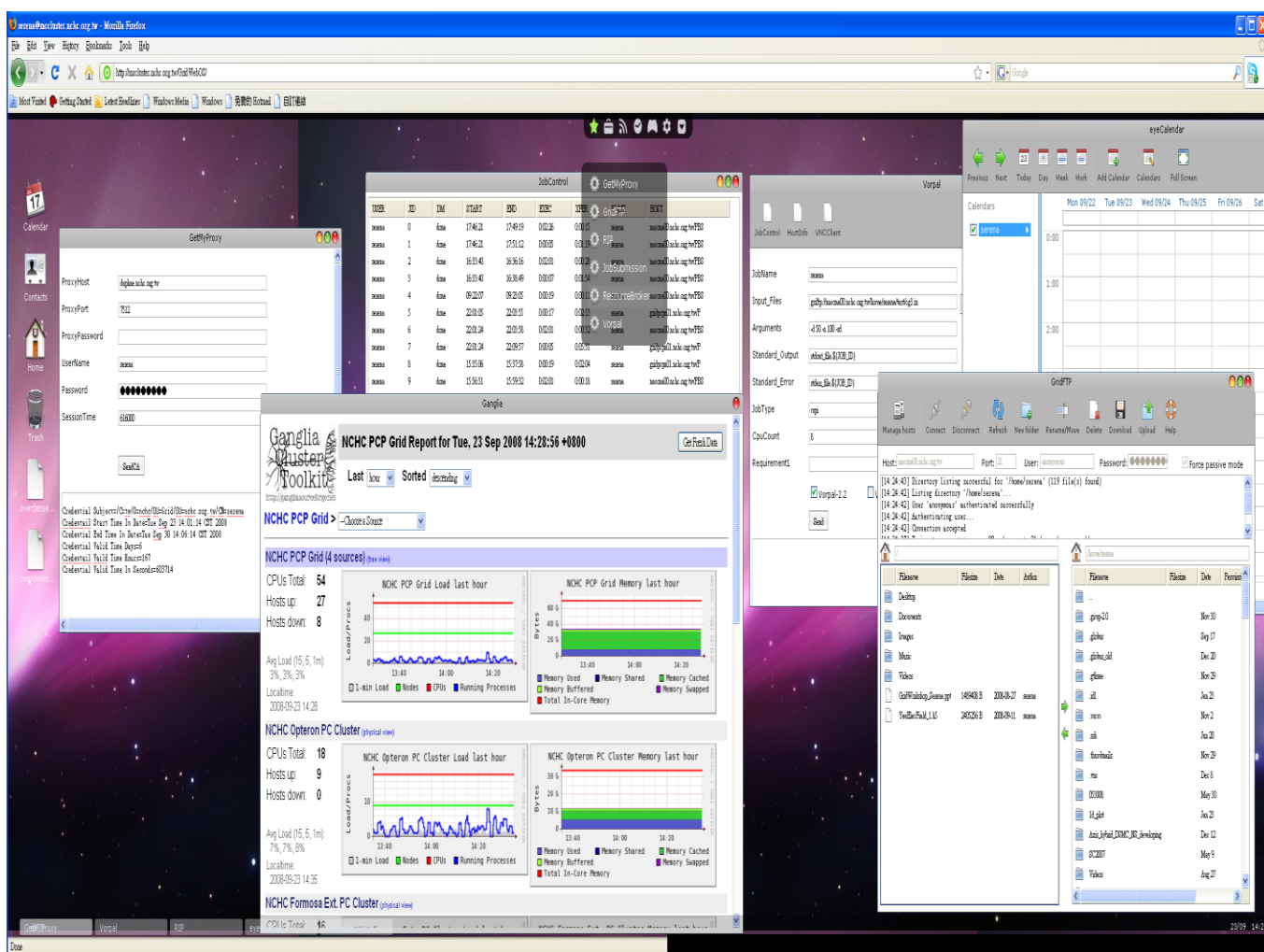

Figure 2. Grid Widgets: Connecting Grid Users to NCHC's Grid Resources

The GetMyProxy Widget, as shown in the Figure 3, is to generate the MyProxy and get the delegation from the remote MyProxy server. A credential with a lifetime of one week (by default) is then delegated to the MyProxy server and stored with the given MyProxy pass phrase. After getting the proxy delegation, Grid users can use Grid Widgets freely. The fundamental Grid Widget is the GridFTP Widget, shown in Figure 4. The GridFTP is a high-performance, secure, and reliable data transfer protocol optimized for high-bandwidth wide-area networks. The GridFTP protocol is based on FTP that is a highly popular Internet file transfer protocol.
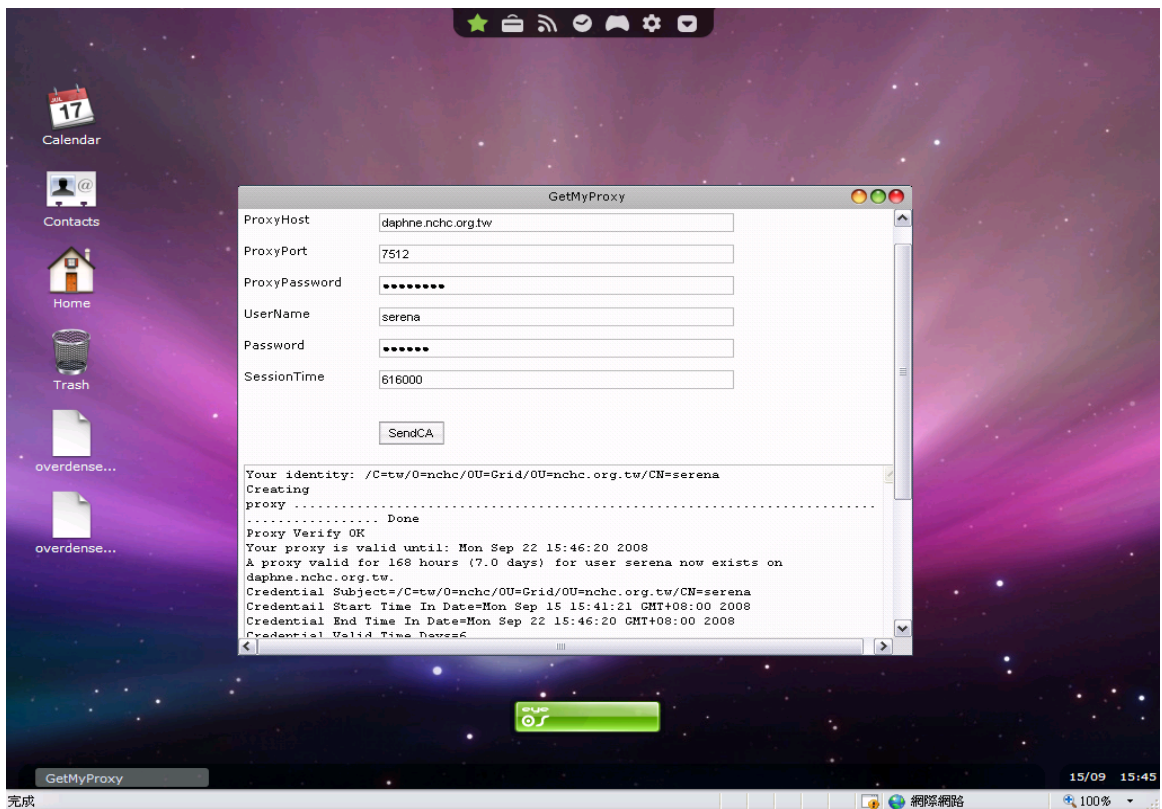
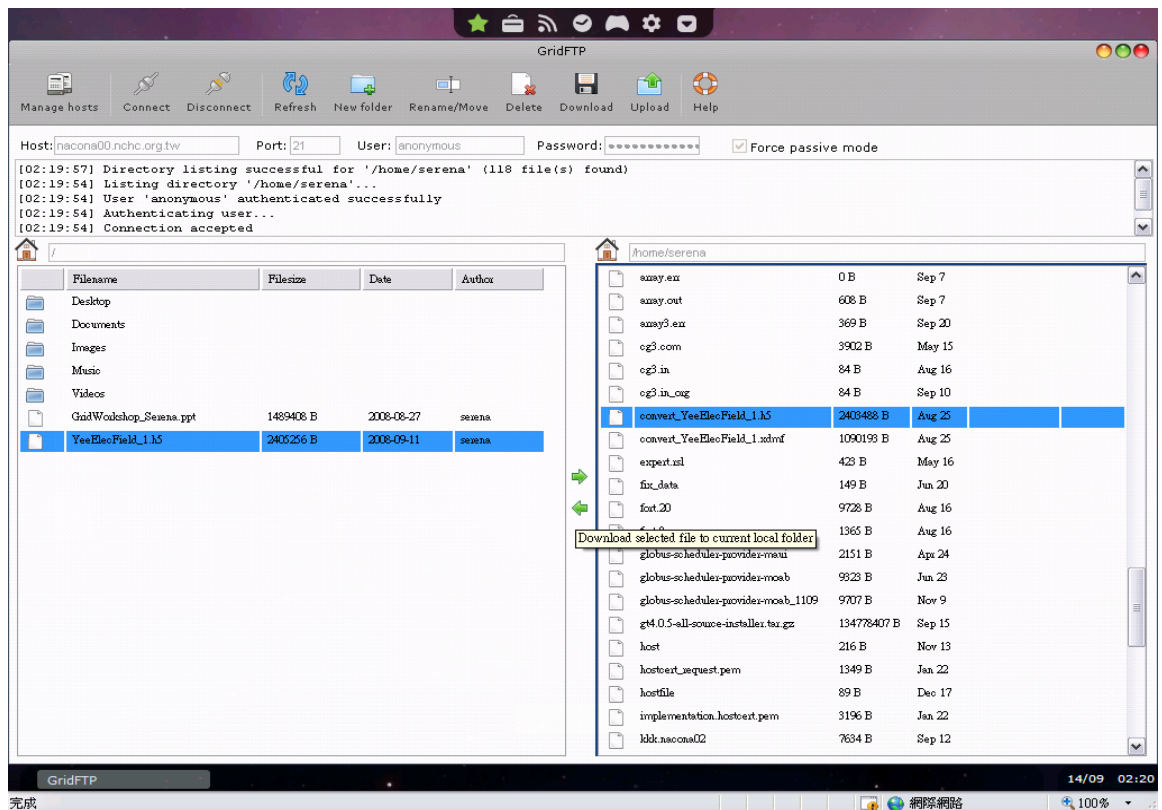Figure 3. GetMyProxy Widget - Proxy Delegation from the Proxy Host

Figure 4. GridFTP Widget – Connecting the Source and Destination for File Movements

The Job Submission Widget provides Grid users with different alternatives of job submissions. Both the interactive and batch mode are provided, as shown in Figure 5. However, to use this widget, users must know exactly, which computing site their programs should be submitted to and where exactly their execution program along with information needed for the jobs are located.
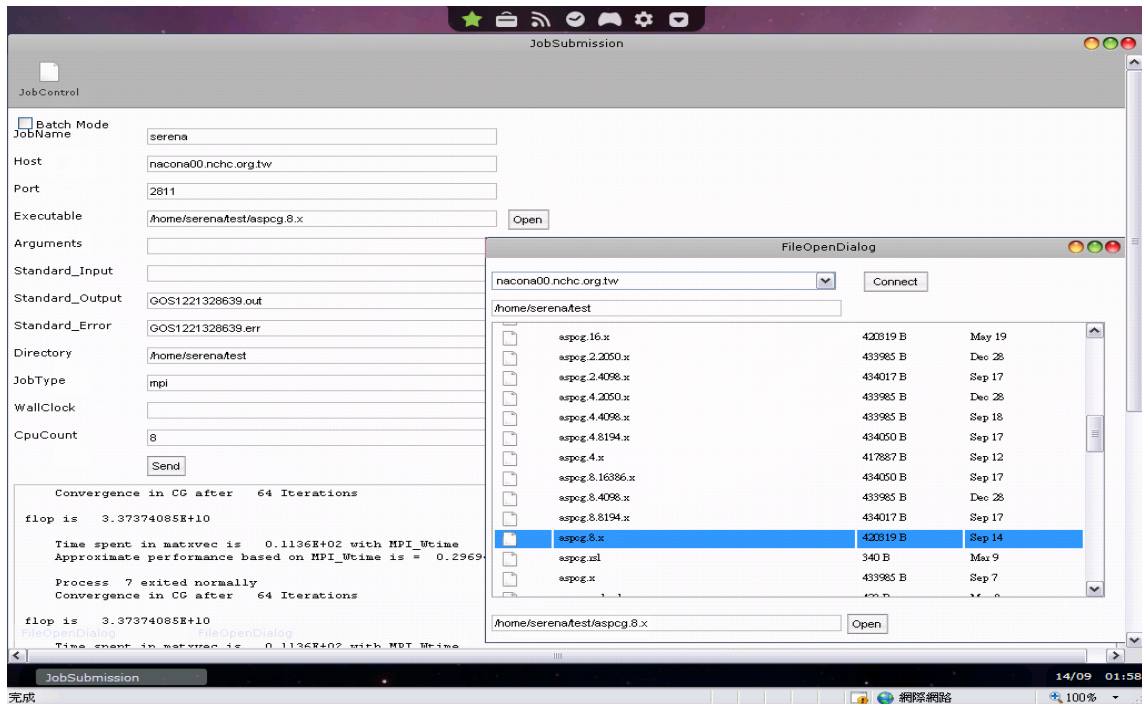

Figure 5. Job Submission Widget – Interactive and Batch Mode

IV. IMPLEMENTATION

In this section we will introduce the implementation part. The environment setup and service integration are shown in following sub-sections.

A. Environment setup

The environment setup is illustrated as follows. There are two main roles: NCHC Account Website and NCHC CA server. NCHC Account Website provides account application services for Grid computing resources. However, NCHC CA server provides certificate services, and it is mostly composed of "myproxy server (Myproxy)", "registration authority server (RA)", and "certificate authority server (CA)".

"Myproxy" is used as a website for applying user certificates and managing user certificates. On the basis of conforming to NCHC Certification Authority Certificate Policy and Certification Practice Statement (CP/CPS) [10] and protecting operating NCHC CA server from harm, Myproxy server contacts with the registration authority server of NCHC CA passively. Therefore, Myproxy server does not have the right to modify the databases related to user certificates.

"RA" is a web server for operating NCHC CA PKI Service and also is a database server for storing the user information. The firewall of RA needs to allow the connection from Myproxy server, and RA would access the certificate data on Myproxy server using ssh-key exchange method. "*CA"* is a certificate authority for signing and issuing certificates. CA host operates certificate services with offline mode. In order to protecting NCHC CA, we do not illustrate it particularly.

B. Service integration

The application process for user accounts and Grid certificate is sketched in the Figure 6. And the detailed operations and interactions among servers within NCHC CA are sketched in the Figure 7.
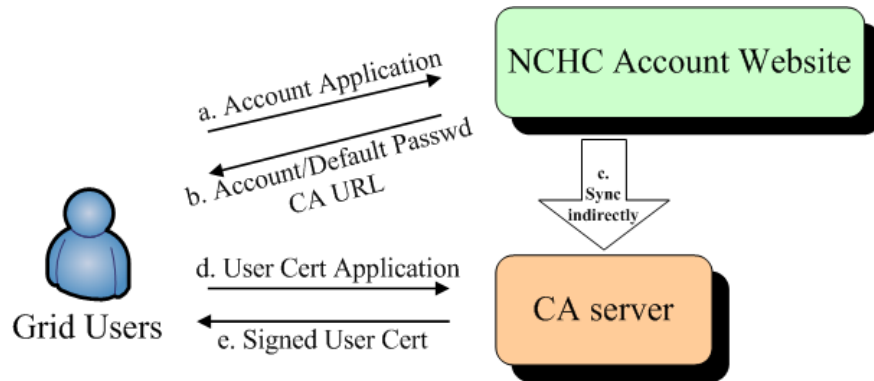
Figure 6. Application Process for User Account and Grid Service Certificates
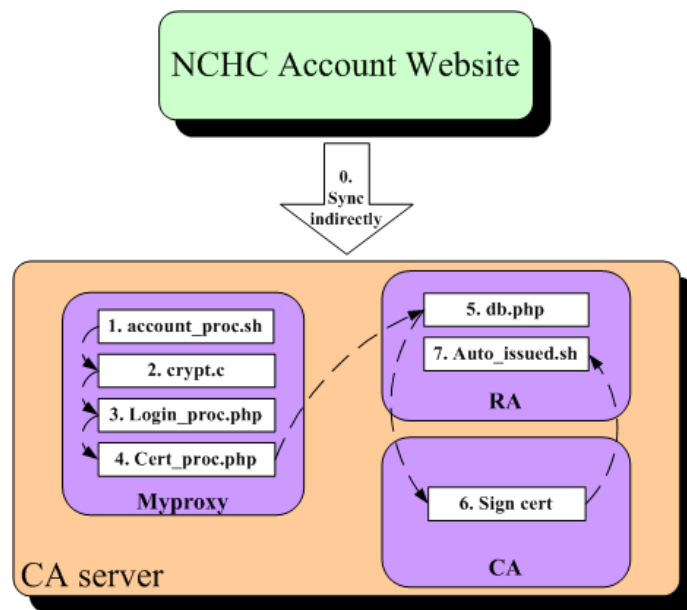

Figure 7. Operations and Interactions among Servers within NCHC CA

Step a and b: After users complete the account application for using Grid computing resources successfully, users will receive a mail containing the account information and a URL for NCHC CA Website.

Step c: "Myproxy" uses account_proc.sh[1] to sync user account/password from NCHC Account Website indirectly and to create user accounts. The account information mainly is provided for users to login to NCHC CA Website.

Step d: "Myproxy" is a NCHC CA Website for the enrollment application. The program- crypt.c[2] can verify the user identity when users login. Login_proc.php[3] processes and judges the application data users input. Then Cert_proc.php[4] handles the certificate signing request and records the user information.

Step e: "RA" uses the cron table (crontab) to execute db.php[5] periodically every day and so retrieves the user information of certificates from "Myproxy". "RA" places the certificate signing requests at an unprocessed directory and writes user information into NCHC CA databases. "RA" would automatically send a notification mail for NCHC CA operators to execute Sign cert[6]. After NCHC CA operators login to "CA" and complete the certificate signing process, Auto_issued.sh[7] on "RA" would publish the signed certificates to the web server of NCHC CA PKI Service. Moreover, the signed certificates would be send back to users and sync to the user directories on "Myproxy".

V. ACHIEVEMENT DEMOSTRATION

Grid WebOS is used as an entrance of Grid

computing resources for Grid users. Every large-scale cluster has a corresponding Grid Gateway Server connecting to Grids. Grid Gateway Server delivers user jobs to the queuing systems of large-scale clusters transparently. Grid WebOS Server acquires the resource information by communicating with all Grid Gateway Servers. The information includes the number of computing nodes, the number of jobs in queues and software versions, etc. With the above information, Grid WebOS Server would start Resource Broker automatically to judge which cluster is fit for job computations. Grid users can monitor the job status from cluster-level schedulers through Grid Widgets on Grid WebOS. After the job completion, execution results are returned back to users. Besides, the operation manner of the integration architecture does not affect the original behavior of local users, and users still can submit their jobs through the front end of local clusters.

The enrollment application of NCHC and NCKU CNC is sketched in the Figure 8.

a. Users login to NCKU Account Website of NCKU CNC and request for the application of using Grid computing resources. After the identity is verified successfully, users will receive a mail containing account/password and a URL of NCHC CA Website.

b. (1) Grid WebOS Server syncs and creates the real system account/password with script files. (2) Grid WebOS Server will create virtual WebOS account/password and NCHC CA Website account/password automatically with the modified login module, and sync with the real system account/password.

c. Users login to CA website using the assigned account/password to complete the certificate application. Through the CA operators handle the signing process and then send the generated CA package (certificate files) to the certificate directory on Grid WebOS.

d. Grid WebOS Server contacts with every GPFS-Wan Gateway Server by GPFS-Wan and finally dispatches jobs to local clusters.
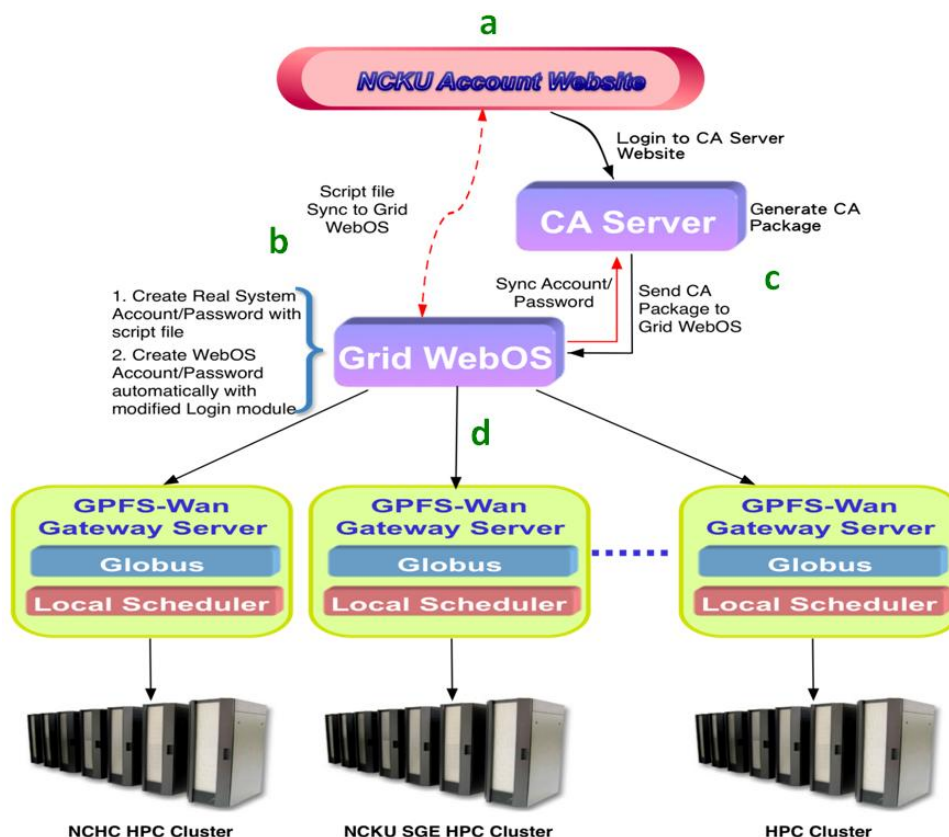

Figure 8. Enrollment Application of NCHC and NCKU CNC

NCHC CA Website for applying certificates is described in Figure 9 and Figure 10. Login and application steps are introduced as follows. Users input account/password on the login page and then enter the request page if authentication successfully. When users comply with the instructions to input the correct information data, system may return messages to help users complete the application. After that, users may receive the signed CA package.
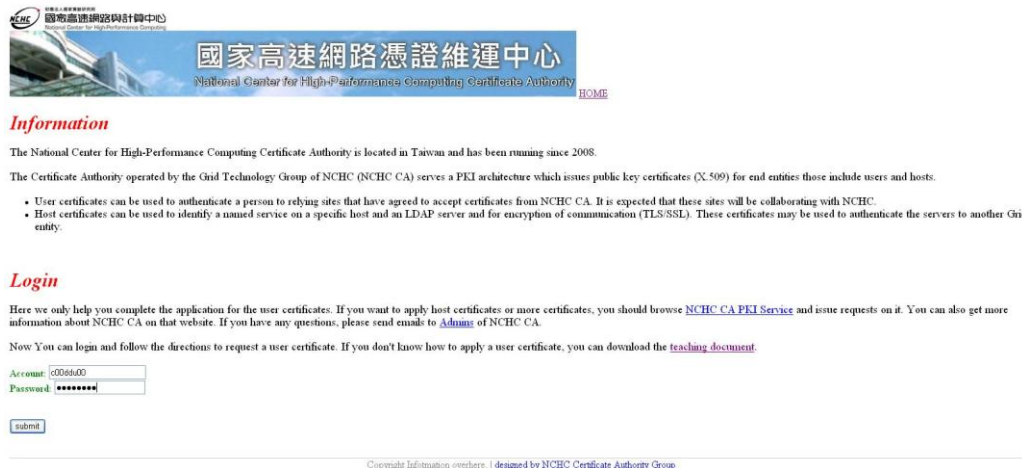

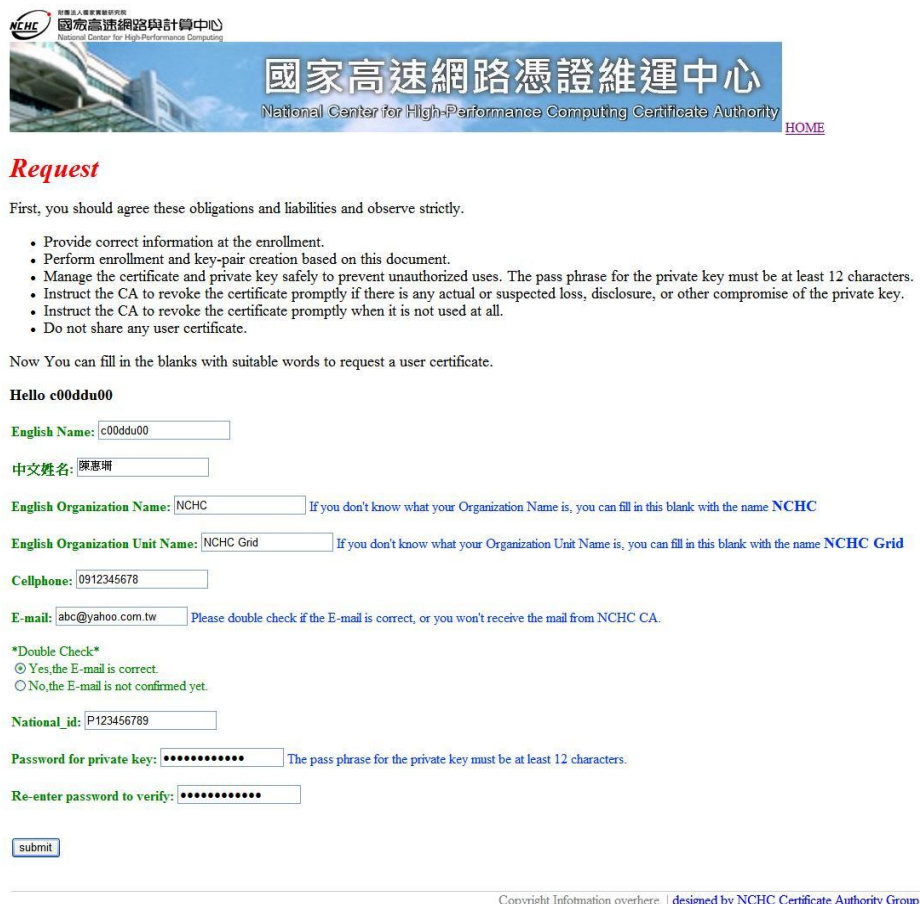Figure 9. NCHC CA Website for applying certificates – Login page

Figure 10. NCHC CA Website for applying certificates – Request page.

VI. CONCLUSION AND FUTURE WORK

We introduce the certificate service into the computational Grid platform. Through the integration of NCHC CA PKI service and Grid WebOS, it is in expectation that users can lightly operate online Grid WebOS and Grid applications. Besides, the service integration can make users access Grid resources with ease, and it also achieve the properties of service-oriented and cross-platform.

Furthermore, integrating certificate services with Grid Widgets mainly provides different-domain researchers a secure certificate way to utilize the across-domain Grid Widgets. Afterwards, the integration can promote the visibility of the association for Grid platforms. In the future, we expect that we have opportunities of collaborating with more international academic community and Grid development organizations, and then establishing a cooperative Grid computing platform for the improvement of resource utilizations worldwide.

REFERENCE

[1] APGrid PMA, "Asia Pacific Grid Policy Management Authority", http://www.apgridpma.org/

[2] Globus Alliance, "Grid Security Infrastructure", http://www.globus.org/security/overview.html

[3] J. Crampton, H.W. Lim, K.G. Paterson, and G. Price, "A Certificate-Free Grid Security Infrastructure Supporting Password-Based User Authentication.", Proceedings of the 6th Annual PKI R&D Workshop 2007, Gaithersburg, Maryland, USA, pages 103-118. NIST Interagency Report 7427, 2007

[4] J. Jensen, D. Spence, and M. Viljoen, "A Scalable PKI for a National Grid Service", 6th Annual PKI R&D Workshop, Gaithersburg MD, USA, 17-19 Apr 2007

[5] L. Xin and M. Ogawa, "Proxy Certificate Trust List for Grid Computing", http://www.jaist.ac.jp/jinzai/Paper/JSSST05.pdf, 2005

[6] NCHC, "National Center for High-performance Computing", http://www.nchc.org.tw/tw/

[7] NCKU CNC, "Computer and Network Center of National Cheng Kung University", http://cc.ncku.edu.tw/bin/home.php

[8] NCHC CA Group, "NCHC CA PKI Service", https://myproxy.nchc.org.tw/, 2008

[9] NCHC Grid research team, "Grid WebOS", https://service.nchc.org.tw/crs/GridComputing/GridComputing.php

[10] NCHC CA Group, "NCHC Certification Authority Certificate Policy and Certification Practice Statement (CP/CPS)", http://ca.goc.nchc.org.tw/nchcca/CPS.html, 2008

[11] P. Yi-Lun, W. Chang-Hsing, and H. Weicheng, "Grid Widgets: The Lightweight Approach to Acquiring Grid Services with Resource Broker in Grid Environment," the International Conference on Grid Computing Applications (GCA), Las Vegas, NV, July 2009.