Journal of the Technical University of Gabrovo, Vol. 48'2014 (91-94)

ИЗВЕСТИЯ
на Технически университет
Габрово

WEB-BASED REGISTRY FOR VIRTUAL ORGANIZATION IN GRID

Radoslava Hristova[1], Goran Goranov[2], Nikolay Stamboliyski[3]
[1]*Faculty of Mathematics and Informatics, University of Sofia "St. Kliment Ohridski"*
[2] *Faculty of Electrical Engineering and Electronics, Technical University of Gabrovo*
[3]*Faculty of Mathematics and Informatics, University of Sofia "St. Kliment Ohridski"*

Revised 20 October 2014, Accepted 28 October 2014

Abstract: *The virtual organizations in the European Grid Infrastructure (EGI) are managed by VOMS servers. It is extremely important VOMS certificates to be kept up-to-date on all grid services in the infrastructure. In this article we propose a web-based application which represent registry for the available virtual organizations and VOMS certificates. The application provides functionality for downloading, listing and verifying the certificate validity of the different VOMS server and their virtual organizations in the EGI.*

Keywords: European Grid Infrastructure, VOMS, VOMS registry

1. INTRODUCTION

The grid is "a hardware and software infrastructure that provides dependable, consistent, pervasive, and inexpensive access to high-end computational capabilities" [1]. The scientific grid combines distributed resources shared by different organizations, institutes and universities all over the world. It coordinates resources sharing and solving problems in the terms of virtual organizations (VO).

Virtual organizations are groups of people, which shares data and resources in order to achieve common goals. The resource sharing in the grid is controlled, it is clearly defined what resources are shared, who shared them and what are the terms under which the resources are shared. The resource sharing provides not just data transfer, but direct access to the computers, software, data and sensors that can be used for solving the specific scientific problem.

Basic advantage of the scientific grid is that it provides services that allow scientist to deal with large data collections and "unlimited" computational resources for computation of numerous independent jobs. Scientific grid allows data to be distributed and in this way different groups of scientists to work independently using common data for solving coming problems.

Realization of the scientific grid is the European Grid Infrastructure (EGI) [2]. It unites the resources of European scientific institutes and organizations from 24 countries. Basic part of the infrastructure is clusters of computers, connected by high-speed fiber optic internet, which provide computational resources and disk space for data storage. They are accessed by specialized software called grid middleware. The current grid middleware for the infrastructure is EMI [3].

The group of grid services - computing element (CREAM), storage element (DPM), database information index (BDII), workflow management system (WMS) and monitoring system (APEL), which every institute or organization maintains in the context of the European Grid Infrastructure is called grid site. Currently, there are five production grid sites in Bulgaria - one is located at the University of Sofia "St. Kliment Ohridski" and the other four are located at the Bulgarian Academy of Sciences [4].

The grid allows institutions and organizations to share their resources to grid users. Grid technology has a great contribution to the research. The EGI is widely used for applications into the sphere of High Energy Physics for analysis of data from the Large Hadron Collider (LHC), in bio-medicine for images' diagnostic, in bio-informatics for studies of the human genome, in geophysics for weather forecasting, earthquakes prediction and other natural disasters.

The virtual organizations (VO) are an integral part of any grid infrastructure. They represent groups of people (scientists, researchers) with common interests and needs, working together and using shared resources (data, software, processors, storage), regardless of their geographical location. Membership in specific virtual organization requires the consent with certain security rules and policies.

Grid security in the EGI infrastructure is realized via X.509 certificates and Public Key Infrastructure (PKI) [5]. In order to access the infrastructure every grid user has to hold X.509 certificate and to be a member of a virtual organization. Grid certificates are issued by Certification Authorities (CA), recognized by the infrastructure. They have certain term of validity.

The management of the virtual organizations in the EGI is done by service called Virtual Organization Membership Service (VOMS), which is a part of the grid middleware. The service itself is installed on the server, which also requires X.509 certificate in order to be operational.

The role of the VOMS services is to identify grid users belonging to the specific virtual organization, and to certify their rights. Furthermore, in order to implement secure connection between the basic grid services in EGI and the

[1] *E-mail: radoslava@fmi.uni-sofia.bg*
[2] *E-mail: g_goranov@tugab.bg*
[3] *E-mail: nstamboliyski@uni-sofia.bg*

VOMS services, the certificates of the VOMS services have to be installed on all basic services into the grid infrastructure – CREAM, DPM, WMS, etc. The outdated certificate of the VOMS server can cause identification problems with grid users and can be a reason for the occurrence of errors. Not updated certificate of VOMS server can lead to the unsuccessful job execution into the grid infrastructure.

It is therefore extremely important VOMS certificates to be kept updated on all grid services in the EGI. In this article we present web-based registry, which stores the updated VOMS certificates. The application can be used by any grid user for information or by any grid administrators in order to keep updated their grid site.

2. EGI GRID SECURITY

Grid users of the European Grid Infrastructure are organized into virtual organizations, which define their rights (authorities) into the grid middleware. The security architecture of the EGI is based on the X.509 certificates and Public Key Infrastructure (PKI), which are used for authentication and authorization in the middleware. A PKI [6] consists of the following components:

- Digital certificates (X.509 certificates) - digitally signed data, which certify the authentication of certain object (people or services);
- Certification authority (CA) - a trusted organization that issues digital certificates;
- Registration authority (RA) - organization or service that manages the process of requesting new certificate;
- Validation authority (VA) - a service or a software component that checks certificate validity;
- Certificate revocation list (CRL) - a list of certificates, which have lost their validity before they expire;
- Documentation – a number of documents, which describe the principle of action and basic security policies.

The principle of PKI is shown on Fig. 1 [6].

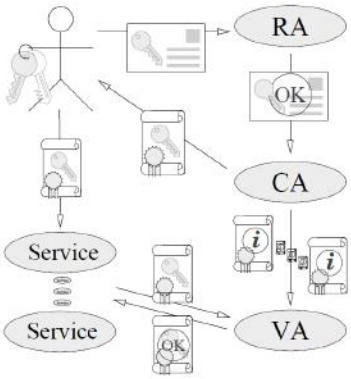

Fig. 1. *Principle of PKI*

The process of certificate request is as follows. First, the grid user generates a key pair (request certificate and private key). The RA verifies the generated request, confirms the user identity and sends the request via signed e-mail to the CA. The Certification authority signed the request and issued user certificate. Usually the certificate validity is 365 days. The Certification authority for Bulgaria is BG.ACAD CA [7] and the Registration authorities are listed in [8]. Once the user has grid certificate he has to apply for a membership into a virtual organization in order to access the EGI.

The management of the virtual organizations and the membership of grid users in them are performed by VOMS service of the grid middleware. This service authorizes grid users in front the available resources in the grid.

The VOMS service is attribute authority that serves as a central repository of virtual organizations. It contains information which is required for the authorization of the users from these VOs.

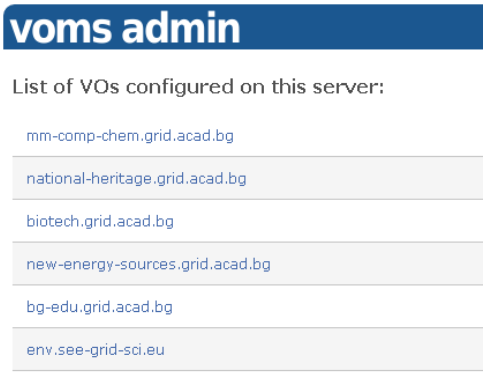

Fig. 2. *VOs on VOMS*

On Fig. 2 is shown VOMS service which serves six virtual organizations. All of them are Bulgarian VOs. VOMS service in EGI provides web interface through which grid user (user with issued grid certificate) can request membership to the specific VO, managed by this VOMS. Through the web interface, grid user also can list all members of the current VO or to see the term of validity of his membership. Usually the membership in the VO has to be renewed on every 365 days.

VOMS service orders users hierarchically by groups according to their roles, rights and other additional attributes. The purpose of the VOMS service is to increase the rights of a user by adding additional attributes to its certificate. In this way grid services can retrieve its rights on the base of these attributes and take authorization decisions based on them.

Once the grid user has certificate and membership to the VO he can use the European Grid Infrastructure.

On Fig. 3 is shown the process of grid user identification in the EGI. First the grid user logged in to the user interface – grid service which provides clients for access to the EGI. The user creates proxy certificate by using his actual grid certificate and his membership into the VO. Usually, the additional attributes which increases user rights are added as X.509 attributes and are embedded into the proxy certificate. These additional attributes indicate the grid services that the user is authorized to perform specific operations into the EGI.

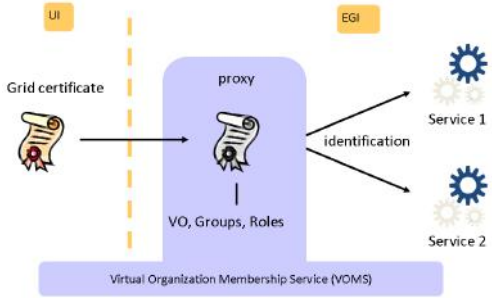

Fig. 3. *User identification in EGI*

The user creates job description and submits it to the EGI. Through its proxy certificate grid user is identified and authorized by the grid services from the infrastructure. We stress again that in order to implement secure connection between the grid services in EGI and the VOMS services, the certificates of the VOMS services have to be installed on all services into the grid infrastructure, otherwise errors like job submission failure can occurs. At the moment, we do not known applications which to provide functionality of centralized registry for virtual organizations and their VOMS server in the EGI.

3. VOMS REGISTRY REALISATION

In order to help grid administrators to keep updated their grid sites with respect to the installed VOMS certificate we designed and developed a web-base registry. The application stores information for the virtual organizations in the EGI and X.509 certificates of the VOMS services that managed them. The main functionality of the registry is the possibility grid user or grid administrator to download the certificate of the specific VOMS service, to list the VO which this VOMS supports and to verify the certificate validity. The registry is intended to be used by grid administrators, but also can be used by any grid user of the infrastructure.

The main requirement to the application is to be accessible from everywhere and the access to it to be secured. That is the reason we developed the application as web-based. The functional and supplementary requirements for the application can be generalized as follows:

- The web-based registry has to store the valid grid certificate of the available VOMS servers from the infrastructure;
- The web-based registry has to support updated information for the VOs that these VOMS server managed.

In order to fulfill these requirements we develop a database which stores this information and web-based interface for access to it. We stress again the fact that the application has to be secured or only users with valid grid certificate to have access to it.

On Fig.4 is presented the architecture of the developed application.

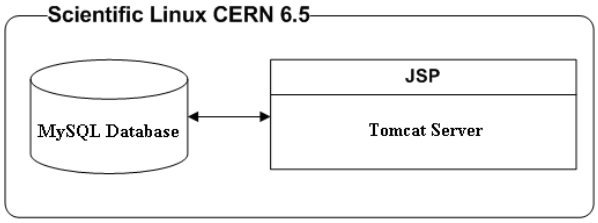

Fig. 4. *Application architecture*

The architecture is three-layered and consists of MySQL relational database, Apache Tomcat 6 application server and JSP pages as client part. For the application implementation we used Java-based development environment - Eclipse IDE for Java EE Developers.

On Fig. 5 is presented the database model of the application. The database is implemented on MySQL server and consists of three basic tables – for users which will access the application, for the available VOMS servers and for the VOs that they managed.

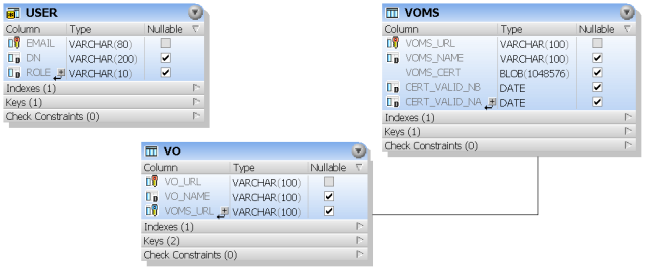

Fig. 5. *Database model*

All of the architecture components are installed on Scientific Linux CERN 6.5 operating system, which is and the base operating system supported by the EGI. The application is deployed on the Apache Tomcat server.

The client interface of the application consists of dynamic HTML pages. Through the web interface the application can be accessed from everywhere. It allows searching information for the available VOMS servers, which are supported in EGI, searching information for the available VOs and list the current members of the specific VO. Also through the web client, every grid user or administrator can download the actual certificates of the VOMS services or to subscribe for notification when a certificate of specific VOMS service expires.

The user access to the application is restricted through SSL identification on HTTPS. The connection between the browser and the web application is secured through certificate exchange. The user has to possess X.509 grid certificate, issued by recognized CA in EGI. With it the user can identify himself by the application. The Tomcat server where the application is deployed also has valid grid certificate. On initial connection to the application mutual SSL authentication occurs - between the user and the application.

The web-based registry for VOs can be accessed on https://portal.grid.uni-sofia.bg:8443/vomscerts/. On Fig. 6 is presented screen with three virtual organizations. Additional information for the members of these VOs, VO URL addresses and the certificates for VOMS servers that managed them can be displayed.

Fig. 6. *Virtual organizations*

On Fig. 7 is presented screen with functionality for VOMS registry administration. From this screen new VOMS servers can be added to the registry by adding them one by one or by pointing a list with URLs where VOMS services are located. The web-based registry supports two roles – administrator of the registry and user. Only the administrator of the web application has access to this screen. The administrator of the application can also remove VOMS server from the registry or update the VOMS certificate of the server.

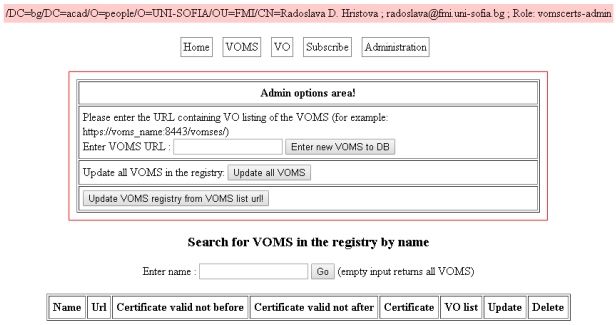

Fig. 7. *VOMS Registry administration*

CONCLUSIONS

The presented web application is useful registry for grid users or administrators. Using its functionality grid administrators can support there grid sites up-to-date with respect to the VOMS certificates, which have to be installed on each base service from the EGI. Currently, the registry is developed to work for the European Grid Infrastructure but it easily can be adapted to work for every grid middleware.

REFERENCES

[1] Foster, I., Kesselman, C. "The Grid: Blueprint for a New Computing Infrastructure. First Edition", Morgan Kaufmann Publishers, 1998
[2] European Grid Infrastructure, http://www.egi.eu/infrastructure/index.html
[3] European Middleware Initiative, http://www.eu-emi.eu
[4] Bulgarian grid sites in EGI, http://gstat2.grid.sinica.edu.tw/gstat/summary/EGI_NGI/NGI_BG/
[5] Public Key Infrastructure, http://en.wikipedia.org/wiki/Public_key_infrastructure
[6] Engelbrecht, G. "A service-oriented Grid environment with on-demand QoS support", 2009.
[7] BG.ACAD CA, http://ca.acad.bg
[8] Bulgarian registration authorities, http://ca.acad.bg/ra_list.html