Enhancing the AliEn Web Service Authentication

Jianlin Zhu 1, Pablo Saiz 2, Federico Carminati 2, Latchezar Betev 2, Daicui Zhou 1, Patricia Mendez Lorenzo 2, Alina Gabriela Grigoras 2, Costin Grigoras 2, Fabrizio Furano 2, Steffen Schreiner 2,3, Olga Vladimirovna Datskova 2, Subho Sankar Banerjee 4, Guoping Zhang 1

1 College of Physical Science and Technology, Central China Normal University, 430079, China
2 CERN, CH 1211 Geneva 23, Switzerland
3 CASED, Darmstadt, Germany
4 LNM Institute of Information Technology, India

E-mail: Jianlin.Zhu@cern.ch

Abstract. Web Services are an XML based technology that allow applications to communicate with each other across disparate systems. Web Services are becoming the de facto standard that enable interoperability between heterogeneous processes and systems. AliEn2 is a grid environment based on web services. The AliEn2 services can be divided in three categories: Central services, deployed once per organization; Site services, deployed on each of the participating centers; Job Agents running on the worker nodes automatically. A security model to protect these services is essential for the whole system.

Current implementations of web server, such as Apache, are not suitable to be used within the grid environment. Apache with the mod_ssl and OpenSSL only supports the X.509 certificates. But in the grid environment, the common credential is the proxy certificate for the purpose of providing restricted proxy and delegation. An Authentication framework was taken for AliEn2 web services to add the ability to accept X.509 certificates and proxy certificates from client-side to Apache Web Server. The authentication framework could also allow the generation of access control policies to limit access to the AliEn2 web services.

1. Introduction

AliEn2[1, 2] is a lightweight Open Source Grid Framework developed by the ALICE(A Large Ion Collider Experiment) Collaboration at CERN with the aim of offering to the end user a transparent access to distributed computing and storage resources all over the world. It started within the ALICE Off-line Project and constitutes the production environment for simulation, reconstruction, and analysis of physics data of the ALICE. AliEn2 is deployed on more than 85 sites all over the world which contributes more than 30,000 CPU cores and 10PB of storage with the number of resources increasing every year.

Even if originally developed for ALICE, AliEn2 can be used by any other Virtual Organization (VO). The services in AliEn2 could be divided into three categories: Central Services, Site Services, Job Agents. In Figure 1, Single VO runs only one set of Central services which can operate many site services. Subsequently, one site service can maintain many Job Agents running on the worker nodes. According to the three categories, services of AliEn2 are as follows:

- Central Services, deployed once per organization - Job/Transfer Manager/Broker, etc.
- Site Services, deployed once per site - ClusterMonitor, CE, PackMan, MonALISA, etc.
General service overview of AliEn2 framework has been presented in Figure 1. The Central Services in ALICE Virtual Organization deployed at ALICE Computing Center. The Central Services along with LDAP Server, File Catalogue, Task Queue and Transfer Queue are responsible for keeping the whole information about users, jobs, transfers, sites, distributing the jobs to the suitable sites, and checking the authentication and authorization of users. The Site Services in one site like siteA deployed inside VOBOX which is used to automatically manage the services, is in charge of asking jobs from Central Services, executing the jobs on the worker nodes, registering the jobs results to the Central Services, saving the results on the Storage Element in Figure 1. There are some other components (i.e. XRootD[3], CREAM[4], etc) working together with the Site Services.

A security model to protect these services is essential for the whole system. In this paper an authentication model is introduced into the AliEn2. Standard X.509 public key certificates[5] are used, Public Key Infrastructure(PKI), the SSL/TLS protocol, and X.509 Proxy Certificate[6] for authentication and message protection.

2. General Authentication View
To interact directly with a remote service a certificate can be used to prove identity. Authentication is the process of verifying one’s claim of identity. Combined with the Authorization in AliEn2, the user could use all the resources distributed all over the world.

2.1. Security Goal and Consideration for AliEn2
Considering that AliEn2 is a grid platform, there are specific aspects that must be addressed by the system, as presented below:

- Allow for the creation and operation of virtual organizations.
- Allow for coordination of shared resources.
- Allow for controlled sharing of resources.
- Allow for access from large number of dispersed users and delegation for the users.
- Allow for Inter operability with other Grid Components.
• Allow for the proxy certificate compatibility.

Based on the fact most of the grid projects use the public-key system, all users participating in the LHC experiments have X.509 certificates. The X.509 certificate interacts directly with a remote service, the X.509 certificate is used to prove the user’s identity. But it is insecure to send the private key to the remote service when the client needs the remote service to do something on behalf of itself. For secure and delegation purpose, the proxy certificate is created to allow limited delegation of rights and acts on the owner’s behalf for a remote service.

Proxy Certificate could be signed by either an X.509 End Entity Certificate (EEC) or by non-limited Proxy Certificate (PC). This EEC or PC is referred to as the Proxy Issuer. It has its own public and private key pair distinct from any other EEC or PC. It has an identity derived from the identity of the EEC that signed the PC. When a PC is used for authentication, it may inherit rights of the EEC that signed the PC, subject to the restrictions that are placed on the PC by the EEC. Although its identity is derived from the EEC’s identity, it is also unique. Proxy Certificates allow an entity holding a standard X.509 public key certificate to delegate some or all of its privileges to another entity which may not hold X.509 credentials at the time of delegation.

VOMS (Virtual Organization Membership Service) proxy certificate [7, 8] can be used in the Grid platform to carry extra user information about the roles and privileges of users within a VO. This extra information is presented to services via an extension to the proxy certificate. When the user wants to generate a VOMS proxy certificate, at the time the proxy certificate is created, one or more VOMS servers are contacted, and they return an Attribute Certificate (AC) that is signed by the VO and contains information about group membership and any requested roles within the VO, the ACs are embedded in a standard proxy. The proxy and each AC has its own lifetime. Typically each AC has the same expiration time as the proxy as a whole, but it is possible that they may be different depending on VO policies and on the times specified when the proxy is created.

From the above discussion, proxy certificates were chosen as the means of authenticating the users and services in the Authentication Model of AliEn2, because proxy certificates have more useful information about the users, allowing limited delegation of rights and a rather short lifetime.

2.2. Authentication model for AliEn2

AliEn2 Authentication model can be divided into five level. General overview of these sections is described in Figure 2. The model supports Grid Security Infrastructure (GSI) based on Public Key Infrastructure. The meaning of each level is explained as follows:

• Message Format is Simple Object Access Protocol.
• SSL/TLS protocol ensures the transport level security. It provides for both integrity protection and privacy (via encryption).
• X.509 EECs are for global authentication. They provide each entity with a unique identifier and a method to assert that identifier to another party through the use of an asymmetric key pair bound to the identifier by the certificate.
• X.509 proxy certificates are extension to X.509 certificates. GSI proxy certificates and VOMS proxy certificates as a means of authenticating user and delegating authority from users to remote servers. They could bridge disparate security mechanisms, basic support for delegation, policy distribution, single sign-on.
• The Authorization uses AuthZ mechanisms in AliEn2. AuthZ mechanisms are based on the File Catalogue and Quota.
All AliEn2 entities joining the grid platform need certificates. The user needs X.509 certificate which has one year validity time and a private key requiring pass phrase protection. The host providing public services needs X.509 certificate without pass phases. The service which has to deal with other services and prove its delegated identity to other services need proxy certificate.

The model is based on the public-key system and is a strong authentication with challenge-response mechanism which is a typical centralized mutual authentication protocol. After the security channel has been established, the next step is authorization. In AliEn2, the information about each user (such as Distinguish Name, roles, etc) is registered in the database and LDAP. If needed, the services could use the information from the certificate to check the right of the user. For instance the Authen service uses the DN got from certificate provided by the user to check whether this user has right to execute the commands and use the resources in the platform. Once the client signs into the system, he could use all the resources with the right permission and all the messages he sent is under protection. The user only enters the password once to generate a proxy certificate. Then the user connects to AliEn2 and can submit jobs or file transfers.

3. Core Components for AliEn2 Authentication

3.1. Implementation of AliEn2 Authentication

Implementation for this security model is as follows:

- Use Apache as the container for running AliEn2 services.
- Use mod_perl[9] for supporting the perl language.
- Use mod_ssl[10] for the SOAP message protection and add patches to mod_ssl for accepting and verifying proxy certificates.
- Use mod_gridsite[11] for dealing with the delegation and access policies.

Mod_perl integrates AliEn2 services with Apache and distributes http requests to different handlers of the services. The mod_ssl and mod_gridsite accepts GSI proxy certificates and VOMS proxy certificates. For the GSI proxy certificate, it has four types of proxy certificates: (1) a limited globus proxy; (2) a legacy globus proxy; (3) a pre-RFC3820 compliant proxy; (4) a RFC3820 compliant proxy.

Now all the services could have three ways to be started. One way is started as a SOAP::Lite[12] server. The AliEn2 services run as a soap server. The second and third way depends on the configuration published at LDAP server and configured at config file of Apache.
In the second method, the services run inside of Apache without the security function. The third way is that if the format of the service address starts with https then the service will commence with enabled security protection. In all of the three ways, only the third way is related to the Authentication Model. The whole process of dealing requests from the client under the Authentication Model has been presented in Figure 3. From the Figure 3, when one side wants to "talk" to one of the services, the whole communication could be separated into two phases. In Phase 1, both sides use SSL/TLS protocol to build security channel. In this phase, AliEn2 supports mutual authentication and both sides must have the certificates. There are two methods provided for the proxy certificates verification. When the SSL session is established, then the process goes into the Phase 2. In Phase 2, the http transaction takes place. AliEn2 is a project written in perl language, and the mod_perl is used to deal with the requests from the Apache server and forward the requests to different services.

There are different ways to use GSI proxy certificates and VOMS proxy certificates. In ALICE experiment, AliEn2 User Interface supports both proxy certificates for Authentication and handling user information stored in database and LDAP for Authorization. Because of the grid platform organized with many middle wares, the sites distributed all over the world and the experts from other experiments. In order to maintain and update the softwares of ALICE experiment, AliEn2 supports VOMS proxy certificates for Authentication and Authorization with different roles and purposes.

### 3.2. Methods for verification

For the AliEn2 services running within Apache, there are two ways to verify the proxy certificates. The attributes of the methods are set in the configure file of Apache before the services are started.

The first one is that we add functions for checking proxy certificates to mod_ssl, through mod_ssl could achieve verify the proxy certificates. The Apache configuration file needs to set up several variables like SSLEngine, SSLVerifyDepth, location of CA. The certificates received from the user side through the SSL handshake are organized into a chain of proxy certificates which is made from generated proxy certificates and the user’s certificate, as well as the proxy key. The depth of the proxy certificate chain should be within the depth of SSLVerifyDepth. Each certificate should be verified according to the algorithms described in RFC3280[6], RFC3281[13].
The second method for authentication is based on the first method, the administrators of the AliEn2 could define the access control policy for each AliEn2 service with GACL (Grid Access Control Language) [14] or the emerging XACML (eXtensible Access Control Markup Language) [15] to service the correct people for doing the soap call. GACL and XACML are both XML based languages and the administrators could modify the file by themselves. They could give different rights to different users according to the DN or VOMS FQAN (Fully Qualified Attribute Names).

The second method is related with the authorization. If the AliEn2 services are ran in a security model, the second method could be used to do some authorization tasks before the Authen Service checks the roles, DN, quotas of the user, and it could save the time.

4. Conclusion
At the end of the 2010, the AliEn2 version in which Authentication with the Authorization were integrated was deployed. All the Central Services work under the Authentication Model with the security protection. Specially for Authen service, it uses the information got from the proxy certificate to check whether the user has the right to do different level operation. After the whole grid platform runs for a time, the efforts will focus on the Authorization Framework along with the Authorization mechanisms in AliEn2 to provide more flexible mechanisms for the sites to control the resource access and for the users to delegate rights.

5. Acknowledgments
The work is supported partly by the NSFC (10875051 and Key Grant No. 11020101060), the Program of Introducing Talents of Discipline to Universities of China: B08033, and CCNU09C01002 (Key Project) of China. We would like to thank all members of ALICE cooperation for providing efforts on developing, maintaining, debugging and deploying the whole system.

References
[1] AliEn2. http://alien2.cern.ch
[2] Bagnasco S., Betev L., Buncic P., Carminati F., Cirstoiu C., Grigoras C., Hayrapetyan A., Harutyunyan A., Peters A. J. and Saiz P., AliEn: ALICE environment on the GRID. Journal of Physics: Conference Series, Volume 119, Part 6
[3] Dorigo A, Elmer P, Furano F and Hanushevsky A, XRootD/TXNetfile: a highly scalable architecture for data access in the ROOT environment. Proceedings of the 4th WSEAS International Conference on Telecommunications and Informatics (World Scientific and Engineering Academy and Society (WSEAS)).
[4] C. Aiftimiei, P. Andreetto, S. Bertocco, S. Dalla Fina, A. Dorigo, E. Frizziero, A. Gianelle, M. Marzolla, M. Mazzucato, M. Sgaravatto, S. Traldi, L. Zangrando, Design and Implementation of the gLite CREAM Job Management Service, Future Generation Computer Systems, Volume 26, Issue 4, April 2010, pp. 654-667, doi: 10.1016/j.future.2009.12.006.
[5] CCITT Recommendation, X.509: The Directory - Authentication Framework. 1988.
[6] Housley, R., Polk, W., Ford, W., and Solo, D., Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 3280, IETF, April 2002.
[7] R. Allieri, et al., From gridmap-file to VOMS: Managing authorization in a Grid environment, Future Generation Computer Systems 21 (2005) (4), pp. 549-558.
[8] V. Welch, I. Foster, C. Kesselman, O. Mulhno, L. Peralman, S. Tuecke, J. Gawor, S. Meder, F. Siebenlist, X.509 Proxy Certificates for Dynamic Delegation. Proceedings of the Third Annual PKI Workshop, 2004.
[9] mod_perl, http://perl.apache.org/
[10] mod_ssl, http://www.modssl.org/
[11] Andrew McNab and Yibiao Li, The GridSite Web/Grid security system. 2010 J. Phys.: Conf. Ser. 219 062058
[12] SOAP Lite, http://www.soaplite.com
[13] S. Farrell, R. Housley, An Internet Attribute Certificate Profile for Authorization, RFC 3281, 2002.
[14] GACL, http://www.gridsite.org/doc/1.0.x/gacl.html
[15] XACML specifications 2.0 and 3.0. OASIS Consortium. http://www.oasis-open.org/