SECURING REMOTE SERVICES INTEGRATING SECURID STRONG AUTHENTICATION TECHNOLOGY IN EFDA-FEDERATION INFRASTRUCTURE

R. Castro[1], P. Barbato[2], J. Vega[1], C. Taliercio[2]

[1] Asociación EURATOM/CIEMAT para Fusión. Madrid. Spain
[2] Consorzio RFX, Euratom ENEA Association, Corso Stati Uniti 4, 35127 Padova, Italy

Corresponding author: rodrigo.castro@ciemat.es

Remote participation facilities among fusion laboratories require access control solutions with two main objectives: to preserve the usability of the systems and to guaranty the required level of security for accessing to shared services. On one hand, this security solution has to be: single-sing-on, transparent for users, compatible with user mobility, and compatible with used client applications. On the other hand, it has to be compatible with shared services and resources among organisations, providing in each case the required access security level. EFDA-Federation[1] is a security infrastructure that integrates a set of fusion laboratories and enable to share resources and services. This federation is based on an authentication and authorization infrastructure, which has been implemented using PAPI[1]. This technology fulfils the requirements previously described and supports a distributed architecture for improving scalability, users and resources management, and system fault tolerance level. PAPI, and consequently with the federation, has been extended and different types of client applications and services have been successfully integrated: web browsers, JAVA applications, MDSplus[2] applications and services, Tomcat based services, PHP services, etc.

In EFDA community, JET and RFX have security access policies to some of their services that require strong authentication mechanisms. In both cases, strong authentication is based on RSA SecurID tokens. This is a hardware device that is supplied to users by JET or RFX and generates a new password every minute.

The presented job has two main lines of work. The first one is the integration of RSA SecurID into EFDA-Federation. Thanks to it, federated organisations are able to offer SecurID to their users as an alternative strong authentication mechanism, with the corresponding increase of security level, that in some cases is required to access to some restrictive services. The second line of work is the development of a new access control mechanism based on port knocking techniques[3] and its integration into EFDA-Federation. The main features of this mechanism are:

- It is able to filter access to TCP and UDP services.
- It is not required to modify the services to protect.
- Protected services are visible only for authorized users. The ports associated with these services are kept completely closed for the rest of users.

The presented job includes results of the integration based on SecurID technology installed in RFX and the use of the solution as access control mechanism for its MDSplus[2] server.

Finally to remark that the presented solution could be extended to other authentication and authorization technologies, and preserves the characteristics of PAPI and EFDA-Federation: distributed architecture, single-sing-on, transparent for users, and compatible with users mobility.

[1] R. Castro, J. Vega, A. Portas,, et al. ,"PAPI based federation as a test-bed for a common security infrastructure in EFDA sites", Fusion Engineering and Design, Volume 83, Issues 2-3 2008, Pages 486-490

[2] A. Luchetta, G. Manduchi, C. Taliercio, et al. , "MDSplus data acquisition in RFX and its integration in legacy systems", Fusion Engineering and Design, Volumes 66-68, 2003, Pages 959-963

[3] R. deGraaf, J. Aycock, and M. J. Jacobson Jr.,"Improved Port Knocking with Strong Authentication" in Proc. of the 21st Annual Computer Security Applications Conference, Tucson, AZ, Dec. 2005, pp 409-418