Contribution ID: **51** Type: **Oral Presentation**

A new ”lightweight” Crypto Library for supporting an Advanced Grid Authentication Process with Smart Cards

Tuesday, 12 April 2011 14:00 (30 minutes)

Overview

Many of the existing Grid middleware, and in particular gLite, rely only on the adoption of a Public Key Infrastructure (PKI) of digital certificates for user authentication, and these credentials must be present on each User Interface (UI) which is used by users to access the computational and storage resources. Distributing certificate's private key on multiple locations is considered a security weakness, as the certificate may be subjected to possible fraudulent use by non-authorized people logged to the UI. Furthermore, there is lack of support for other authentication mechanisms such as smart cards even if this hardware with its properties can help in keeping these certificates safe and avoid any fraudulent use. The public part of an X.509 certificate stored on this hardware can usually be accessed by users, applications, portals and/or Science Gateways but the corresponding private key can never be copied off the smart card.

Impact

The work carried out and reported in this contribution is particular relevant for several user communities, applications, Grid portals and/or Science Gateways developers. The library allows to use the credentials stored into smart cards for generating VOMS-compliant proxies thus enhancing the Java technology to deal with private and public keys. The benefits introduced in this work are far-reaching. The new crypto library can be used, for instance, to help developers to design and develop Science Gateways for several scientific communities and provide, especially for non-expert users, a transparent and easy access to e-Infrastructures. Last but not least, the introduction of smart cards for storing digital credentials can massively improve the security of Grid infrastructures since they protect sensitive information from malicious applications. As we mentioned before, the crypto library has been successfully tested on Aladdin e-Token smart cards only. No compatibility tests have been performed on smart cards of other vendors but they can done on request.

Description of the work

In this contribution we describes our work in the design and implementation of a new Grid authentication method based on the use of digital certificates stored on smart cards. The solution we propose extends the native Sun PKCS#11 cryptographic APIs with the Bouncy Castle and the cog-jGlobus APIs library in order to implement a new “lightweight” crypto utility which can be used by users to access the digital certificates stored on a smart card and generate a VOMS proxy. The Bouncy Castle APIs were used to generate version 3 of X.509 certificates reading from the credentials available in the smart card, while the support with the cog-jGlobus was introduced to establish a secure connection with the VOMS server and add the AC attributes to the original Grid proxy. In this first implementation, the library runs with the Aladdin e-Token PRO 32K

directly plugged into a remote 64-bit UI based on Scientific Linux 5 where the Aladdin's e-Token PKI Client software (pkiclient-full-4.55-34) was previously installed. This software enables e-Token USB operations and the implementation of e-Token PKI-based solutions. The library has been successfully tested with both personal user's and robot certificates and used to generate Grid proxies in the new e-Collaboration environment based on Liferay and GENIUS/EnginFrame technologies. It is of course not restricted to any Grid portals and/or Science Gateways. Concerning the credentials stored into the smart card, we used robot certificates issued by the INFN Certification Authority (CA) because they are the type of certificates that best match the use case of these credentials in our environment. Nevertheless, nothing prevents to use personal certificates instead if their planned usage is consistent with the restrictions the CAs put on it.

Conclusions

The Java SE platform provides developers with a large set of security APIs, algorithms, tools and protocols. Among them, we can point out the native Sun PKCS#11 cryptographic tokens which has been used in this work together with the Bouncy Castle and the cog-jGlobus Java APIs to implement a new module for the gLite Grid middleware which allows to sign the proxy certificate using the digital credentials stored in a smart card. The open source solution described in this work can be used by users, applications, Grid portals and/or Science Gateways developers to generate VOMS proxies using Java APIs starting from the credentials stored in e-Token smart cards. The new library provides an asset in raising Grid awareness and encourages broader use by a wider number of potential users.

Primary author: Dr LA ROCCA, Giuseppe (INFN Catania)

Co-authors: Dr FALZONE, Alberto (NICE srl); Prof. BARBERA, Roberto (INFN Catania and Department of Physics and Astronomy of the University of Catania); Dr CIASCHINI, Vincenzo (INFN CNAF)

Presenter: Dr LA ROCCA, Giuseppe (INFN Catania)

Session Classification: Technologies for Distributed Computing

Track Classification: DCI - Implementation