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

Many of the existing Grid middleware, and in particular also 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 are used by the user to access the computational and storage resources of the Grid. 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 (e.g. the system administrator). 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. 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 public part of an X.509 certificate stored on this hardware can usually be accessed by users, applications, Grid portals and/or Science Gateways but the corresponding private key can never be copied off the smart card. This makes such kind of devices ideal for storing sensitive data such as digital certificates. To access and use the credentials stored in the smart card, an user’s PIN is usually requested. This additional feature helps to keep the certificate protected and safe. An additional protection is given to private keys and secret keys which are marked as ”sensitive” or ”un-extractable”. The solution, we propose extends the native Sun PKCS#11 cryptographic APIs with the Bouncy Castle and the cog-jGlobus (ver. 1.8) APIs library in order to implement a “lightweight” crypto utility which may be used by grid users to access the digital certificates stored on a smart card, if any, and generate a VOMS proxy contacting the VOMS server for the given VO using Java APIs. In this first implementation, the library runs with the Aladdin eToken PRO 32K directly plugged into a remote 64-bit UI based on Scientific Linux (SL5) where the Aladdin’s e-Token PKI Client software was previously installed. 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.

Primary authors : Dr. LA ROCCA, Giuseppe (INFN)

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