Contribution ID: **89** Type: **Poster**

Improved X.509 credentials management

Management of X.509 credentials often seen as one of the obstacles preventing from smooth utilization of the grid infrastructure. These limitations are well understood and attempts have been made in the past to improve the situation. One of the main achievements is certainly the Terena Certification Service, which issues X.509 certificates based on federated identies. However easy to use the TCS is, it still addresses just part of the whole problem of credential management. Users having TCS certificates still need to make sure the files containing the certificate and private key are located on proper places, properly secured, made available during the log-on phase (i.e. creating a proxy certificate), etc.

In this contribution we present a set of tools that make the work with X.509 transparent and thus easier for end users. We will describe a library to obtain credentials from the TCS that does not require to use a browser, which enables to integrate the functionality with e.g. desktop applications. We will also present adaptations of the common VOMS commands that enable support of the PKCS11 interface. Using these changes it is possible to generate a proxy certificate from a smart card or, utilizing a proper configuratiom, directly from the repository of the Firefox browser. With this mechanism a user is not required to handle the files with the credentials but accesses the ones stored in the browser repository where they were stored by the TCS process.

In order to provide a higher level of credentials protection, we have also extended the MyProxy service so that it can be accessed as an remote PKCS11 device. This adaptations provide a virtual smart-card, which accesses the credentials without the private key actually leaving the repository. We provide a client PKCS11 library that can made any PKCS11-enabled application use credentials stored in the MyProxy server. Using this library one can configure e.g. the Firefox browser to authenticate using credentials stored within a MyProxy repository.

Primary author: KOURIL, Daniel (CESNET)

Presenter: KOURIL, Daniel (CESNET)