Contribution ID: **115** Type: **Oral**

# Sanctorum: a solution for safe management of digital certificates and passwords in a farm

*Monday 12 April 2010 16:10 (20 minutes)*

Sanctorum is a python tool created to aid sitemanagers to safely manage digital certificates and passwords for hosts in a farm. Motivation for the tool: when releasing a new host certificate, the Italian Certification Authority recommends the site to maintain two backup copies of the private key in a safe place not network reachable. This makes it quite difficult to both respect the CA rule and to efficiently manage the site, especially large ones. The proposed solution makes it possible to manage digital certificates in a comfortable and error free manner while still respecting CA recommendations.

## Detailed analysis

The reliability of common Authentication methods depends on how confidential a piece of sensible information can be kept. Host's Private keys are valid until they are inaccessible to all but the owner. Sanctorum aims to provide a comfortable way to manage host passwords, certificates and private keys while ensuring an adequate security level and preventing risk of human error. The basic idea to achieve this is to keep key/cert pairs in a cyphered database using raid1 disks in a machine with a disabled network. The machine should only be accessed through console or avocent like solutions. When a certificate or other data has to be transferred to/from a host, the network card gets enabled, a firewall rule is added to let the transfer happen, then the network card is deactivated and the fw rule removed. Apart from adding new hosts to the db, there is no frequent need to log on the sanctorum's host: a tool is provided to create new requests for expiring certificates and mail it to an operator; a second one is able to download a newly generated certificate from the CA website and stores it in the db after checking that it matches its key, then it copies the cert/key couple on the target host.

## Conclusions and Future Work

The Sanctorum tool has been designed and developed to allow for the easy management of digital certificates and host passwords in large scale computing grid farms. It complies with the security IGTF approved CA policies and CPS. It is currently adopted by the Italian Tier-1 facility and by several Tier-2 centres of the IGI infrastructure.

## Impact

Maintaining host certificates for a large number of hosts is a time consuming activity. If not strictly planned and performed it might let sporadic errors happen. These in turn may lead into possibly severe unscheduled down of a service. Common practice at site level is to "hide" all private keys into some local filesystem network reachable together with some script used to perform common management tasks. Should an attacker gain access to that hidden place all hosts identities should be considered compromised, all certificates should be revoked and requested again from scratch to the CA. This is why keeping keys not network reachable makes sense. Sanctorum offers a complete set of tools for certificate and password management (check, deploy, get, update etc.) and keeps private keys out of the operator hands. This can only be copied into its host or matched

against its certificate. Any operation is strictly interactive. This avoids the need to build shell loops and gain or save knowledge on many hosts at once. Apart from the setup of new hosts, renewal operations are almost fully automated (the only human intervention is to sign a request mail and bounce it to local RA).

## Keywords

X509, PKI, CA, Certificates

## URL for further information

http://www.italiangrid.org/grid_operations/site/documentation

**Author:** Dr DAL PRA, Stefano (INFN)

**Co-author:** Dr VERLATO, Marco (INFN)

**Presenter:** Dr DAL PRA, Stefano (INFN)

**Session Classification:** Security

**Track Classification:** Software services exploiting and/or extending grid middleware (gLite, ARC, UNICORE etc)