Svom Science Ground Segment KP Cnes

8 octobre 2019

Jean-Paul Le Fèvre
French science centers Project manager CEA Irfu

www.cea.fr

- Tools have been developed with Xiaoliang Guo

- Data rates between clients and servers are accumulated using a Docker stack based on *influxdb* and *grafana*

- Client-server couples are defined in a json configuration file.
- As this point :
  - Servers : Saclay, Vilnius, Athens, Beijing
  - Clients : Villeurbanne, Saclay, Paris

- New couples can be added easily

- CC In2p3 – Naoc : ~2.5 MB/s

DATA RATE CC-NAOC

`http://svom-fsc-0.lal.in2p3.fr:20033`

- Authorization is based on the RBAC principles,
- Specs were proposed in Svom 2011,
- Pay attention to the BA rights.

Name	Description
investigator	Role granted to the Principal Investigators and the Co-Investigators
advocate	Role played by the burst advocates and the ToO responsible persons
administrator	Role allowing to administrate the system
expert	Role allowing to manage calibration files
collaborator	Role granted to members of the Svom collaboration
fellow	Role granted to scientists associated to the collaboration
visitor	Role given to people interested in the Svom mission

- 2 kinds of principals :

  - Software components : client programs, servers, scripts, *centers, ...*

  - Human beings : regular users, burst advocate, ...

- Components communicate in the network using the http protocol

- Components will be authenticated thanks to their X509 certificates

- User authentication :
    - Based on OAuth
    - Not yet tested for FSGS
    - BA could also use X509 certificates
    - Hope to have something ready before the end of 2018

- User authorization
    - Specs available since March 2011
    - But never discussed ☹

- Component authentication :
    - An implementation is available @ Saclay
    - It works and is rougly documented

The STKI :

- Svom Root Certificate Authority (SRCA) is installed in a secure environment protected from the network

- Svom Intermediate CA (SICA) is in a different computer

- A principal creates a private key and a certificate signing request (a csr)
- The csr is sent to the SICA which creates the certificate
- The principal gets back this certificate signed by the Svom authority

The STKI management :

- For now certificates are managed manually
- A couple of scripts has been written
- But it is to much time consuming

- A tool will be installed asap :

- https://www.openxpki.org/