Use of a hardware token for Grid authentication by the MICE data distribution framework

Henry Nebrensky
(HEP Group, College of Engineering, Design, and Physical Sciences, Brunel University, UK)
Janusz Martyniak
(High Energy Physics Group, Department of Physics, Imperial College London, UK)

The international Muon Ionization Cooling Experiment (MICE) is designed to demonstrate the principle of muon ionisation cooling for the first time, for application to a future Neutrino Factory or Muon Collider. The experiment is currently running at the ISIS synchrotron at the Rutherford Appleton Laboratory, UK. As presently envisaged, the programme is divided into three Steps: characterisation of the muon beams (complete), characterisation of the Cooling Channel and Absorbers (data-taking restarting in 2016), and Demonstration of Ionisation Cooling (2018).

Data acquisition, in particular, can involve 24/7 operation for an entire ISIS cycle (4-6 weeks) and so for moving data from theDAQ to the Grid a valid, VOMS-enabled, Grid proxy must be made available continuously over that time. Long-lifetime proxies and password-less certificates raise security concerns regarding their exposure, whereas requiring a particular certificate owner to log in and renew the proxy manually at half-day intervals (as the VOMS extensions are limited to 24hrs) for weeks on end is operationally unsustainable. The solution is to use a “robot certificate” (one that does not represent a particular person) stored on a hardware token (from which it is not possible to extract the “private key” part of the certificate, thus proxies can only be used on the very machine that has the hardware token plugged into it).

We chose the Feitian ePass2003 because it was both significantly cheaper and easier to actually purchase; however at the time there was no software support for the hardware. The Feitian ePass2003 is certified by NIST (FIPS 140-2 Level 3).

On Linux, the ePass2003 is supported through OpenSC since version 0.13 but this package is not included in SL6 and the corresponding EPEL repo only included 0.12. Scientific Linux 7.1 does include OpenSC v.0.13.0-9, which ironically is the one minor release for which ePass2003 support was temporarily broken.

Created a “hybrid” SL7.1 system by installing packages from Fedora Core 20:

```bash
eengine_pks11-0.1.8-7.fc20
libp11-0.2.8-5.fc20
openssl-0.13.0-11.fc20
```

This server is isolated from the network and does nothing apart from providing our SL6 UI with a raw Globus proxy.

Now in production use since Sep. 2015, generating separate proxies for both RAW and Reconstructed data.

We are now preparing a CentOS 7 test machine – aim is to both generate the raw proxy and VOMSify on the Grid UI.

Specific thanks to Jan-Just Keijzer and NIKHEF colleagues for help with OpenSSL, proxy generation, and the mkProxy script; and Jens Jensen (UK eScience CA) for help with the robot certificate.

The work described here was made possible by grants from the Department of Energy and National Science Foundation (USA), the Instituto Nazionale di Fisica Nucleare (Italy), the Science and Technology Facilities Council (UK), the European Community under the European Commission Framework Programme 7, the Japan Society for the Promotion of Science and the Swiss National Science Foundation, in the framework of the SCOPES programme, whose support we gratefully acknowledge. We acknowledge the use of Grid computing resources deployed and operated by GridPP in the UK. We are also grateful to the staff of ISIS for the reliable operation of ISIS.

References
NIKHEF: “Using an Aladdin eToken PRO to generate grid proxies” https://wiki.nikhef.nl/grid/Using_an_Aladdin_eToken_PRO_to_generate_grid_proxies