Contribution ID: **532** Type: **Poster**

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

Thursday, 13 October 2016 16:30 (15 minutes)

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 under construction 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 distribution and archiving, batch reprocessing, and simulation are all carried out using the EGI Grid infrastructure, in particular the facilities provided by GridPP in the UK. To prevent interference - especially accidental data deletion - these activities are separated by different VOMS roles.

Data acquisition, in particular, can involve 24/7 operation for a number of weeks and so for moving the data out of the MICE Local Control Room at the experiment 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 for weeks on end is operationally unsustainable. The MyProxy service still requires maintaining a valid local proxy, to talk to the MyProxy server, and also requires that a long-lifetime proxy be held at a remote site.

The MICE "Data Mover" agent, responsible for transferring the raw data from the experiment DAQ to tape and initial replication on the Grid whence it can be read with other credentials, is now using a robot certificate stored on a hardware token (Feitian ePass2003) from which a cron job generates a "plain" proxy (using the scripts distributed by NIKHEF) to which the VOMS extensions are added in a separate transaction. A valid short-lifetime proxy is thus continuously available to the Data Mover process.

The Feitian ePass2003 was chosen because it was both significantly cheaper and easier to actually purchase than the token commonly referred to in the community at that time; however there was no software support for the hardware. This paper will detail the software packages, process and commands used to deploy the token into production. A similar arrangement (with a different certificate) is to be put in place for MICE' Offline Reconstruction data distribution.

Tertiary Keyword (Optional)

Secondary Keyword (Optional)

Distributed data handling

Primary Keyword (Mandatory)

Security and policies

Primary author: Dr NEBRENSKY, J.J. (Brunel University)

Co-author: MARTYNIAK, Janusz (Imperial College)

Presenter: Dr NEBRENSKY, J.J. (Brunel University)

Session Classification: Posters B / Break

Track Classification: Track 8: Security, Policy and Outreach