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

JJ Nebrensky[1] and J Martyniak[2]

[1] Brunel University, Uxbridge UB8 3PH, UK
[2] Imperial College London, Physics Dept. London SW7 2BW, UK

E-mail: Henry.Nebrensky@physics.org

Abstract. The international Muon Ionization Cooling Experiment (MICE) is designed to demonstrate the principle of muon ionisation cooling for the first time. 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. The MICE "Data Mover" agent is now using a robot certificate stored on a hardware token (Feitian ePass2003) from which a cron job generates a “plain” proxy to which the VOMS authorisation 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 describes the software packages, process and commands used to deploy the token into production.

1. Introduction

The international Muon Ionization Cooling Experiment (MICE) [1] 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.

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 [2]. The RAW data from the data acquisition system (DAQ) is aggregated into per-run tarballs [3] and uploaded using Grid protocols to the Castor tape robot at the RAL Tier1 centre. It is then replicated to other Grid sites for easy access by users [4]. Meanwhile, we have since updated the offline reconstruction such that the computing is carried out locally at the experiment control room but the reconstructed output must still be published to the Grid by a mechanism similar to that used for the RAW data [5]. To prevent interference - especially accidental data deletion - these activities are separated by using different certificates (i.e. DNs) assigned to different VOMS roles.

Data acquisition, in particular, can involve 24/7 operation for an entire ISIS cycle (4-6 weeks) and so for moving data from the DAQ 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

Interim placeholder PDF for BURA:
Presented at: *22nd International Conference on Computing in High Energy and Nuclear Physics (CHEP2016)*, San Francisco, USA (10th – 14th October 2016); contribution I.D. 532
To be published in: IoP *Journal of Physics: Conference Series (JPCS)*

security concerns regarding their exposure, whereas requiring a particular certificate owner to log in and renew the proxy manually twice a day (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 generated on the very machine that has the hardware token plugged into it).

2. Hardware Token and Hosting Environment

When MICE started this strand of Grid development in 2012, there was already experience in the community with the Aladdin eToken PRO token; but of their two UK agents, one refused to respond to our enquiries while the other set a minimum order size including one charged copy of the Software Development Kit for every token. We therefore chose the Feitian ePass2003 because it was both significantly cheaper (by literally an order of magnitude) 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) [6].

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 did include OpenSC v.0.13.0-9, which ironically is the one minor release for which ePass2003 support was temporarily broken.

We therefore created a "hybrid" SL7.1 system by installing the following packages from Fedora Core 20:

- `engine_pkcs11-0.1.8-7.fc20`
- `libp11-0.2.8-5.fc20`
- `opensc-0.13.0-11.fc20`

This server is isolated from the network and does nothing apart from providing our SL6 UI with a plain Globus (Legacy GT2) proxy (i.e., one without any VOMS extensions).

3. Set-up of the Hardware Token

We initially set up the token with an existing certificate (rather than trying to generate a certificate request straight from the hardware). The first steps simply wipe and then initialise the token:

```
~ > pkcs15-init –E
Using reader with a card: Feitian ePass2003 00 00

~ > pkcs15-init --create-pkcs15 --profile pkcs15+onepin --use-default-transport-key
         --pin **** --puk **** --label "MICE Data Mover Robot 3“
Using reader with a card: Feitian ePass2003 00 00
```

We then write the private key from our existing certificate bundle into the token:

```
~ > pkcs15-init --store-private-key Robot_GridClientTest.p12 --format pkcs12 --auth-id 01
Using reader with a card: Feitian ePass2003 00 00
error:23076071:PKCS12 routines:PKCS12_parse:mac verify failure
Please enter passphrase to unlock secret key: ********
Importing 3 certificates:
0: /C=UK/O=eScience/OU=Imperial/L=Physics/CN=MICERobot:GridClient
1: /C=UK/O=eScienceRoot/OU=Authority/CN=UK e-Science Root
2: /C=UK/O=eScienceCA/OU=Authority/CN=UK e-Science CA 2B
User PIN [User PIN] required. Please enter User PIN [User PIN]: ****
```

[†] If the owner waits the whole 24 hours to renew the proxy, there is a risk that any intermittent problem in the network or VOMS server would cause the renewal to fail, leaving the system with no valid proxy at all

```
~ > pkcs15-tool --list-certificates
Using reader with a card: Feitian ePass2003 00 00
X.509 Certificate [MICERobot]
Object Flags : [0x2], modifiable
Authority : no
Path : 3f0050153100
ID : 84d9fcd5c4e9a7408301c9dc7e9a8bd4040895e4
GUID : {4f53ac2b-fcc1-aa0c-f8da-73edbb026160}
Encoded serial : 02 03 00A3E7
X.509 Certificate [UK e-Science Root]
...
```

If the certificate bundle included the signing chain back to the Certificate Authority then these will also be written to the token. On the machine hosting the token we generate a Globus proxy using the *mkproxy* script published by NIKHEF [7]:

```
~ > ./mkproxy.bash --slot 1 --bits=1024 --id 84d9fcd5c4e9a7408301c9dc7e9a8bd4040895e4 --debug
```

To store more than one certificate within the token we simply write it in using the same command as above (but without re-initialisation). The ID passed to the *mkproxy* script allows us to select which certificate we want to generate a proxy from.

4. Authorisation

The two data-transfer and storage activities that run continuously from the MICE control room – the RAW data uploads and the offline reconstruction uploads – are distinguished both by running as different (robot certificate) DNs, and by using separate VOMS roles. The plain Globus proxies are transferred by a private route from the proxy-generating host to our production Grid UI (running on SL6), where each has the appropriate VOMS credentials applied:

```
~> voms-proxy-init --noregen --valid 24:00 --voms mice:/mice/Role=mvr
Contacting voms.gridpp.ac.uk:15001 [/C=UK/O=eScience/OU=Manchester/L=HEP/CN=voms.gridpp.ac.uk]
"mice"...
Remote VOMS server contacted succesfully
...
```

For production running the Globus proxies are regularly re-created and provided by a cron job to the UI, where the separate task-specific agents each deal with acquiring the VOMS credential for their own particular activity.

5. Renewal

The robot certificates – like normal ones – expire after a year. For the renewal process the Certificate Authority has kindly re-signed the original request (which was already signed by, but *does not embed*, the private key) to create a refreshed certificate (public key). We can collect this from the web portal and add it to the token:

```
~> pkcs15-init --update-certificate RobotNew.pem --id 84d9fcd5c4e9a7408301c9dc7e9a8bd4040895e4
     --auth-id 01
```

This non-standard process allows us to carry out the renewal without having to interact with the private key, which is only on the token plugged into a non-networked server.

6. Operation and Performance

The ePass2003 token has now been in production for the MICE RAW Data Mover since September 2015, and providing both RAW and RECO proxies since June 2016. There is monitoring both for final proxy validity (via Nagios) and for the physical presence of the token itself. The only failure mode is that the token loses its USB connection every 2 or 3 months and becomes invisible to tools such as *lsusb*:

```
Feb  7 23:14:51 host kernel: usb usb1-port1: disabled by hub (EMI?), re-enabling
```

This could stem either from an issue with the kernel letting the device go to sleep incorrectly or, given the physical location within an accelerator complex, it may indeed be triggered by electromagnetic interference.

7. Future Work

MICE has been taking data in the "Step IV" configuration since September 2015 [8], and so as much of the data transfer chain as possible has been frozen (e.g. the data upload UI remains on SL6). Our intent is to move towards a platform based on SL7/CentOS 7 simply to keep up with Grid middleware development; as these have included OpenSC v.0.14 since version 7.2 it should at last be possible for us to both generate the Globus proxy from the token and to request VOMS credentials and carry out the subsequent transactions on the Grid from one machine.

As well as the obvious streamlining of the proxy handling processes, this would also let us move towards using the token to generate the private key in hardware and then apply (or renew) certificates directly in the usual manner.

An extended shutdown will also be an opportunity to replace the present token with one from another batch, shedding light on the USB disconnection issue.

Acknowledgements

We would like to thank Jan-Just Keijser and NIKHEF colleagues for help with OpenSSL, proxy generation, and the *mkproxy* script; and Jens Jensen (UK *e*Science 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

[1] "International Muon Ionization Cooling Experiment" http://mice.iit.edu

[2] Britton D *et al.* 2009 "GridPP: the UK grid for particle physics", *Phil. Trans. R. Soc.* A **367** pp.2447-57; doi:10.1098/rsta.2009.0036

[3] The MICE Collaboration 2016 "MICE Raw Data" doi:10.17633/rd.brunel.3179644.v1

[4] J. Martyniak and the MICE Collaboration 2014 "MICE data handling on the Grid" *J. Phys. Conf. Ser.* **513** 032063

[5] Martyniak J, Nebrensky JJ and Rajaram D 2016 "Data management and database framework for the MICE experiment" CHEP 2016 – The 22nd International Conference on Computing in High Energy and Nuclear Physics, San Francisco, USA.

[6] Feitian Technologies Co. Ltd.: "ePass2003" http://www.ftsafe.com/onlinestore/product?id=3 (retrieved 17:40 3rd October 2016)

[7] Keijser J-J 2008 "Using an Aladdin eToken PRO to generate grid proxies" https://wiki.nikhef.nl/grid/Using_an_Aladdin_eToken_PRO_to_generate_grid_proxies (retrieved 8:43 12th October 2016)

[8] K. Long *et al.* 2014 "The status of the construction of MICE Step IV", *Nuclear Physics B Proceedings Supplement* **00** (2014) pp.1–8

Interim placeholder PDF for BURA:
Presented at: *22nd International Conference on Computing in High Energy and Nuclear Physics (CHEP2016)*, San Francisco, USA (10th – 14th October 2016); contribution I.D. 532
To be published in: IoP *Journal of Physics: Conference Series (JPCS)*