Contribution ID: **15** Type: **Oral**

Encrypted Data Storage

Monday, April 12, 2010 3:50 PM (20 minutes)

Biomedical researchers are required to encrypt sensistive patient data before use/storage on Grid Data Management services. The services described enable this operation.

Detailed analysis

Security and Data Management are two cornerstones of the
distributed production computing environment that the EGEE project is providing as a general e-Science infrastructure. An important requirement on the Data Management services
is the provision for securely storing sensitive data.
This privacy requirement has been given by the general Biomedical research community in conjunction with various national and international regulations and is met
through encrypting data and distributing the encryption keys.

The Encrypted Data Storage system is comprised of:

Hydra, the split encryption key storage and retrieval system;
one or more metadata catalogues such as the gLite LFC or AMGA;
a set of clients to communicate with
any GFAL-enabled storage element such as DPM.

The Biomedical research community
typically works with a far lower volume of data than, for instance, the High Energy Physics collaborations. Therefore, the components of the encrypted data storage have been designed and implemented with security rather than data throughput in mind.

Conclusions and Future Work

From the experience of test services, we will describe areas of work that are ongoing or planned as dictated by the user feedback and project technical direction.
In addition, some upgrades and important bug fixes for more general Grid users will be presented.
Future work would inlcude extending this type of service to a Cloud infrastructure.

Impact

This collection of services has allowed parts of the Biomedical community to conduct their research. Further upgrade and generalization of the service for other Grid users will enable others to protect data. As Cloud services become more prevalent, an encryption scheme such as this would add privacy.

Keywords

Data Managment, encryption, keys

URL for further information

https://twiki.cern.ch/twiki/bin/view/EGEE/DMEDS

Primary author: WHITE, John White (Helsinki Institute of Physics HIP)

Co-authors: FROHNER, Akos (CERN); HAHKALA, Joni (Helsinki Institute of Physics HIP); HAPPONEN, Kalle (Helsinki Institute of Physics HIP)

Presenter: WHITE, John White (Helsinki Institute of Physics HIP)

Session Classification: Security

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