

Distributed Key Management System for Sensitive Data

¹ Joni HAHKALA, ¹ John WHITE, ² Àkos FROHNER, ¹ Kalle HAPPONEN & ¹ Henri MIKKONEN

¹ Helsinki Institute of Physics, FL

² CERN, CH

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.

From the experience of the pilot 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.