# Medical Data Management

Enabling Grids for E-sciencE

## encrypted storage for everyone

Medical community as the principal user
- large amount of images are produced
- privacy concerns vs. processing needs
- ease of use (image production and application)

Strong security requirements
- anonymity (patient data is separate)
- fine grained access control (only selected individuals)
- privacy (even storage administrator cannot read)

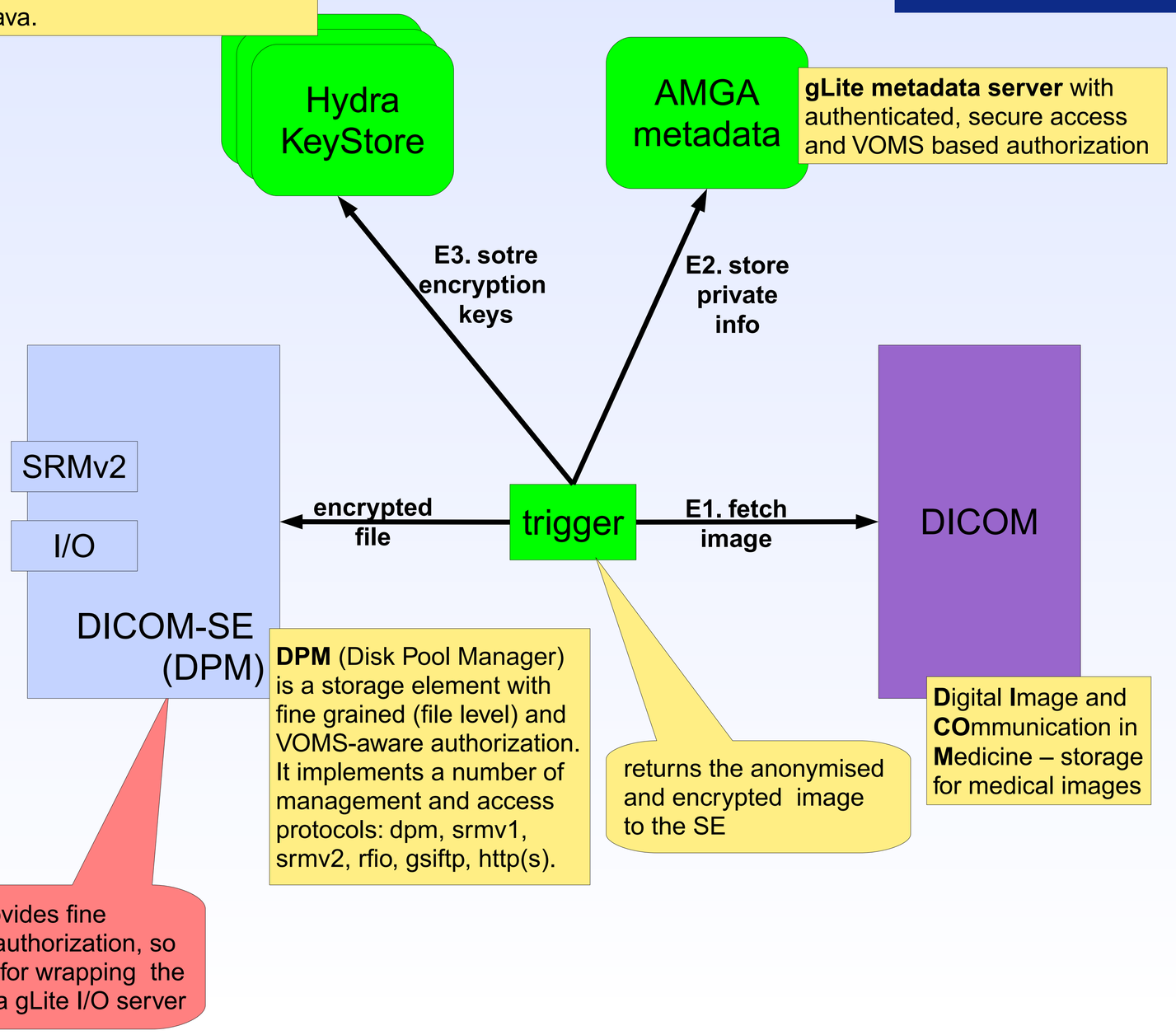
**Hydra KeyStore** – secure key management service with fine grained (key level) and VOMS-aware authorization. It is a web service written in Java.

**Registration of a medical image**
- the private part is stripped and stored in a metadata search engine (AMGA)
- the file is encrypted and become managed by the storage element (DPM)
- the encryption key is split and stored in the key-store (Hydra)

**Encrypted files as grid files**
- encrypted files can be registered in file catalog
- can be transferred and stored in any other storage element (if that provides sufficient authorization; SRMv2)

DPM SE is only required for the DICOM integration

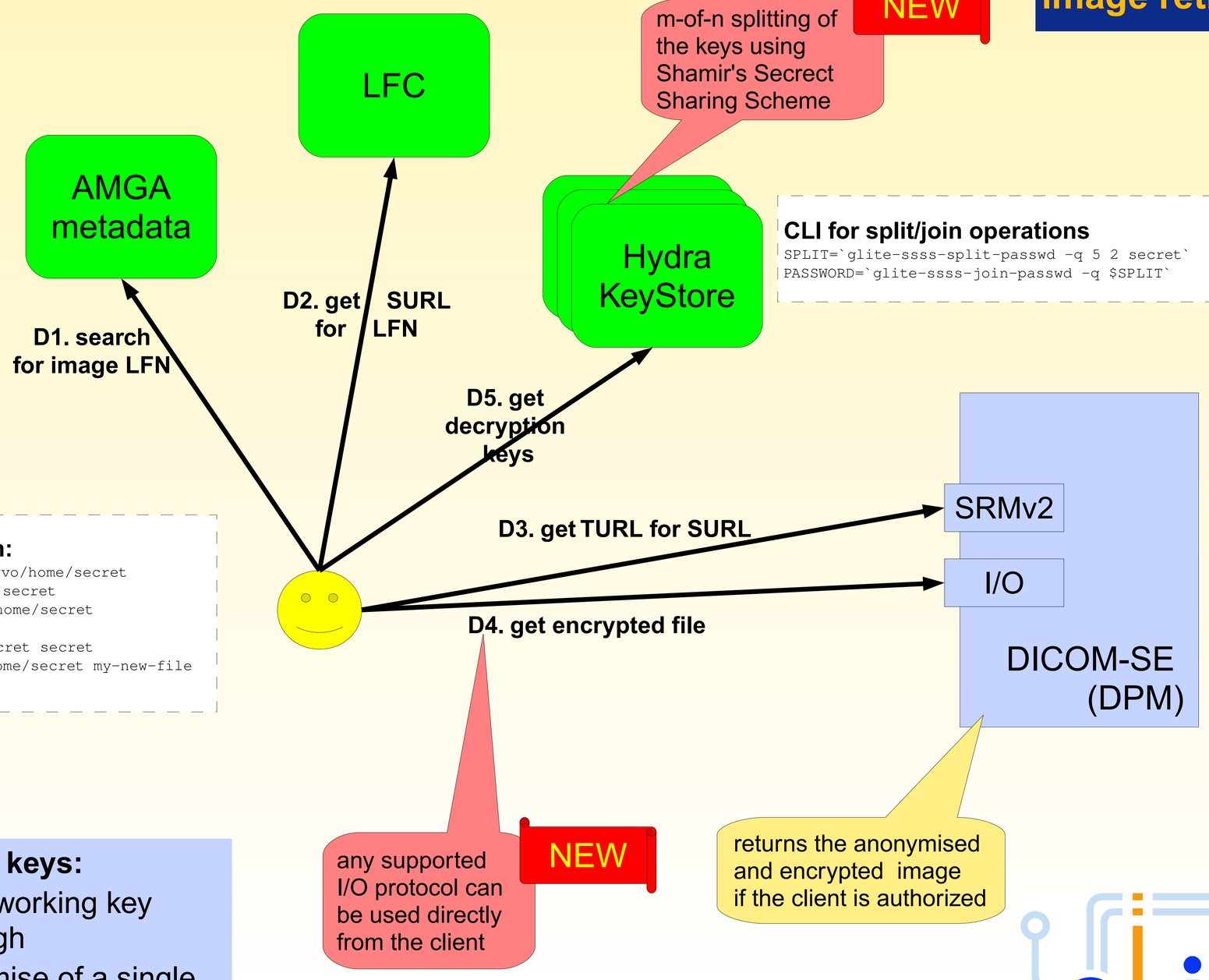
## image registration




## image retrieval

**Retrieval of a medical image**
- any replica of the encrypted file can be retrieved
- the decryption keys are joined and used for in-memory for decryption

The client tools are to be integrated into GFAL and lcg_util.




**m-of-n splitting of keys:**
- reliability: m-of-n working key servers are enough
- security: compromise of a single server does not reveal the keys

Lightweight Middleware for Grid Computing



https://twiki.cern.ch/twiki/bin/view/EGEE/DMEDS
Akos FROHNER, Krzysztof NIENARTOWICZ, Remi MOLLON, Jean-Philippe BAUD, Sophie LEMAITRE, David SMITH, Chang Yeong CHOI