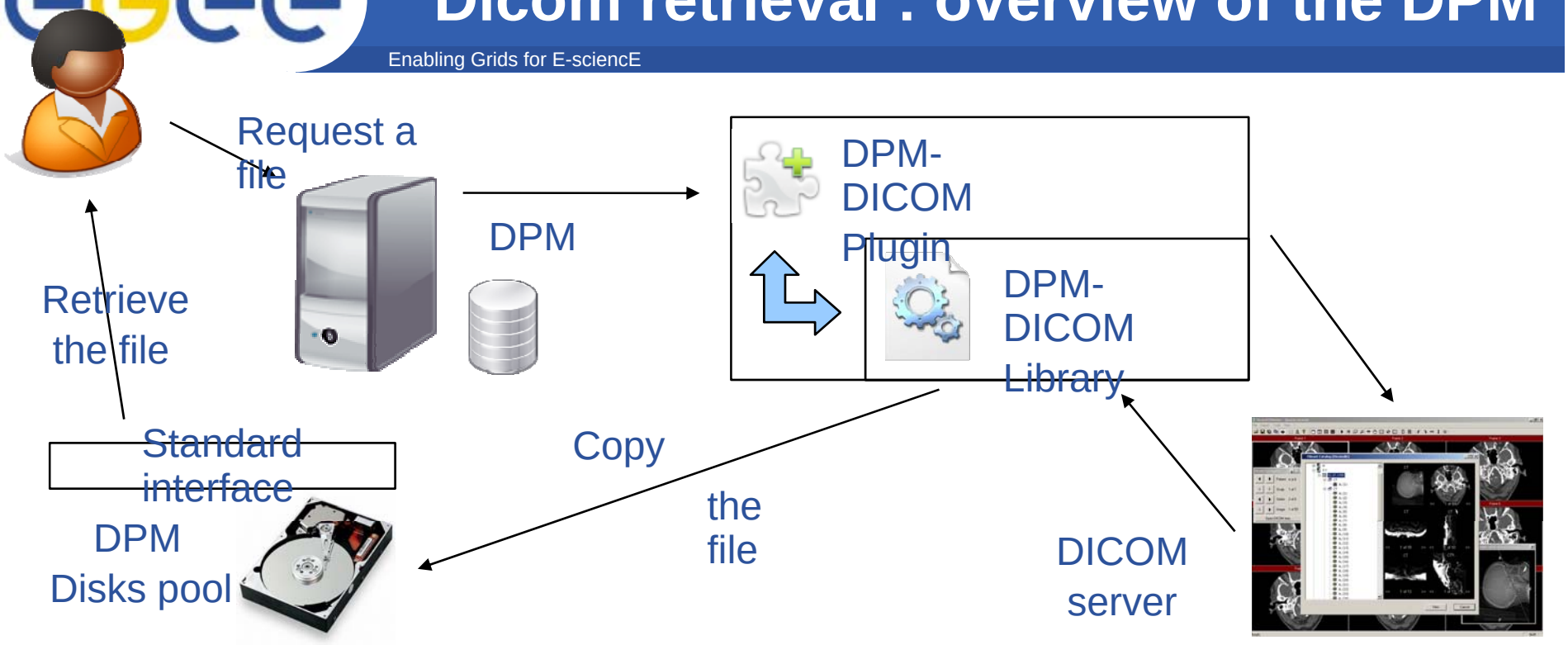
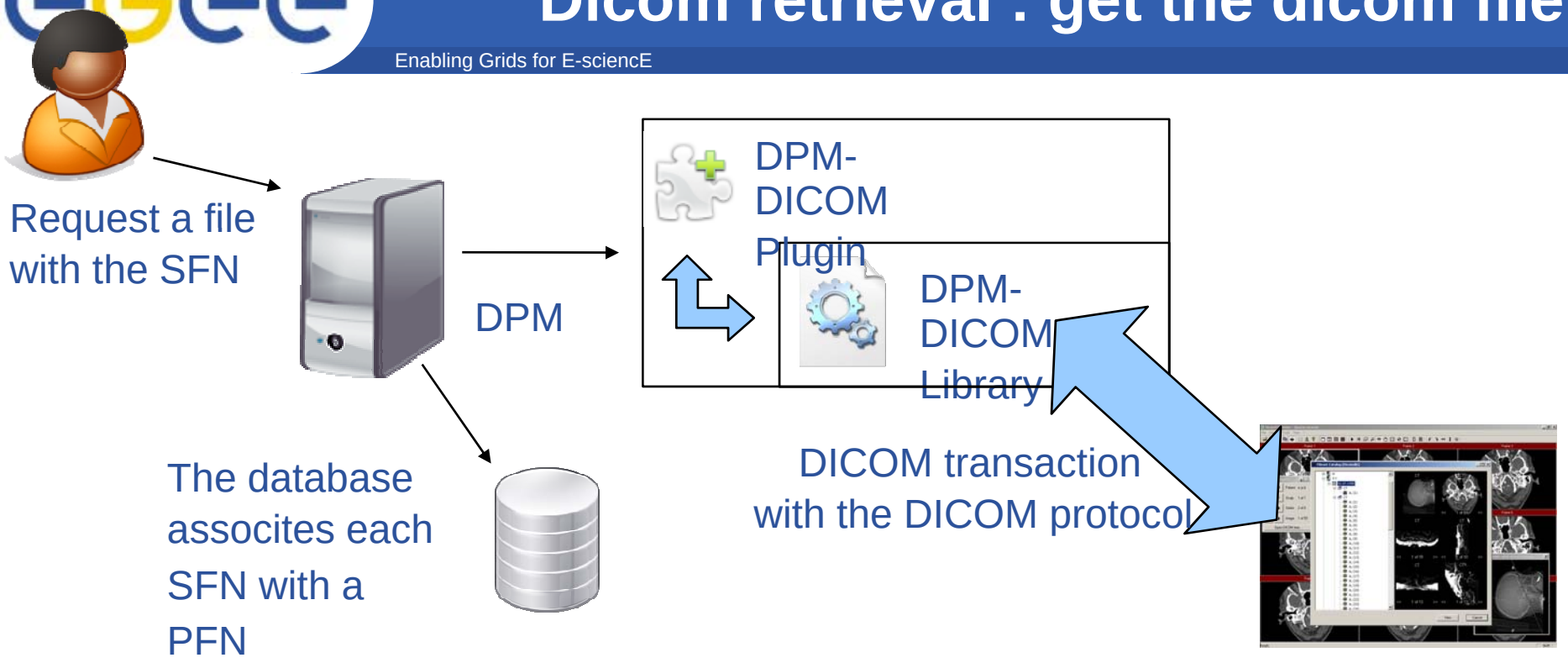
Dicom retrieval : overview of the DPM



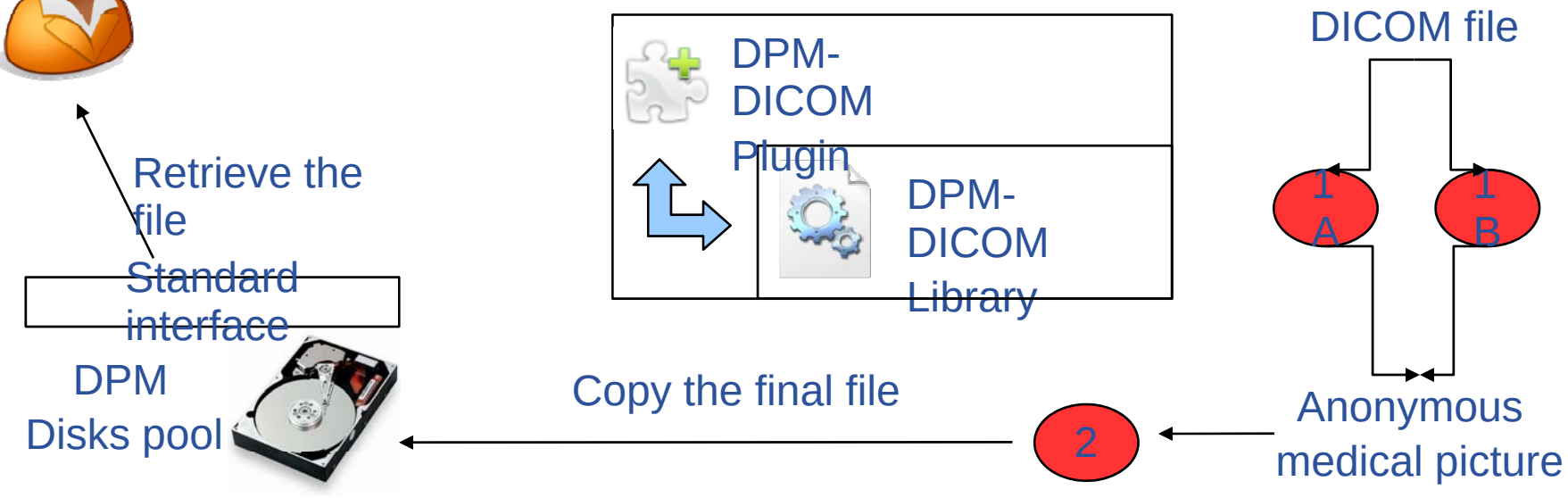
- **One command line to retrieve a file: lcg-cp <file in> <file out>**
- **The interface is a grid standard storage element interface.**
- **The DPM-DICOM library retrieve the file from a DICOM sever and make additional step before storing the file in a disk spool.**

Dicom retrieval : get the dicom file



- **The PFN associates with a DICOM file is handled by the DPM-DICOM plugin.**
- **The plugin make a DICOM transaction with the DICOM server to retrieve the medical picture.**
- **By default, the MDM uses the Conquest server as DICOM server, but any DICOM server can be used**

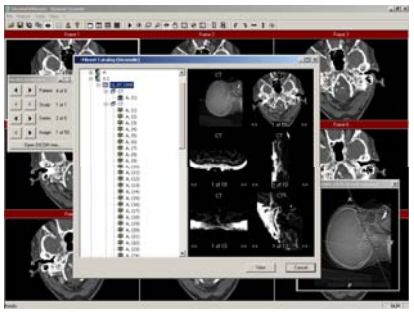
Dicom retrieval : Anonymization and encryption



- **Step 1A: The DPM-DICOM uses the DCMTK library to anonymise the DICOM file**
- **Or Step 1B: The creaLibs convert the DICOM file to an inrimage.**
- **Step 2: The DPM-DICOM call Hydra to encrypt the final file**
- **DPM-DICOM use the RFIO library to copy the file in a spool disk. The spool disk is only a buffer for the file.**

Register a DICOM file

- **The file must be recorded in the DICOM server:**



  - **The file must be registered in all the components:**


AMGA

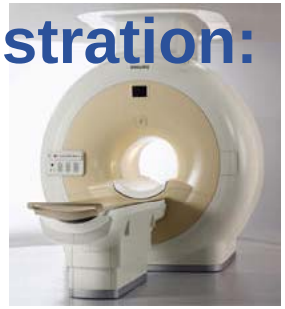

Hydra


DPM

  - **All this step can be done by a command line:**

```
[texier@egee2 ~]$ MDMregister dicom.dcm
```

  - **A DICOM transaction can initiate the registration:**



PUSH
DICOM

Medical Data Manager
(AMGA, LFC, DPM,
Hydra, DICOM server)

Register in Hydra

DICOM image

analyze

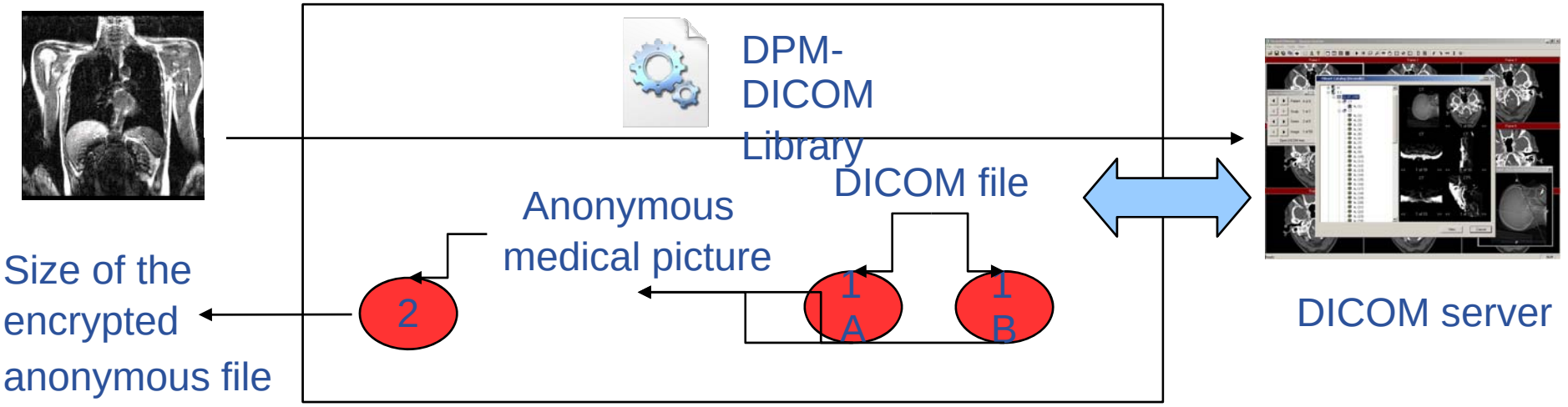
Study ID
Serie ID
Sop ID

Select a cypher and generate a key

Hydra servers

- **The first registration step is a security step**
- **The DICOM picture contains a unique identifier the SOP identifier. The Study/Serie identifier is unique for each study/serie.**
- **The hydra servers generate a key for the selected cypher.**
- **The cyper and the key is associated to the unique DICOM numbers**

Register in the DICOM server



- **In the next step, the DPM-DICOM library records the DICOM picture in the DICOM server.**
- **The DPM-DICOM simulate a user call. It obtain the size of the final file.**
- **The size depends of :**

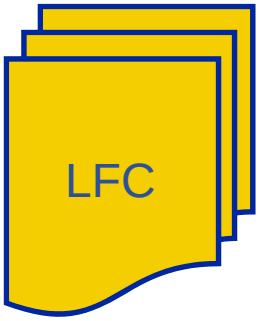
The size of the original file
The DICOM server

The cyper and the key
The fields erased in the anonymous step

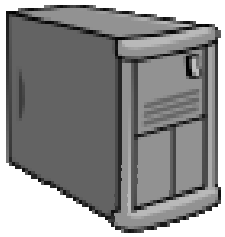
Register references to the file

DPM

- the size of the file
- SFN and PFN
- host of the disk pool
- ...



- LFN and SFN
- size of the file



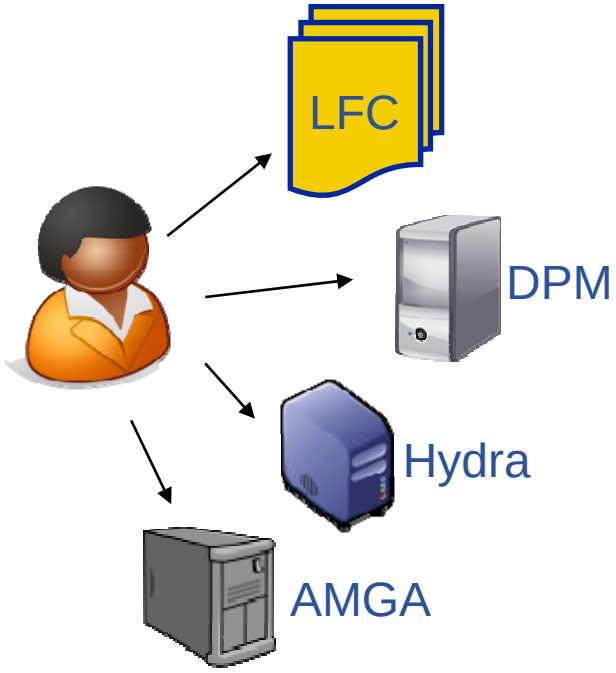
AMGA

- The metadata of the DICOM file

- **A reference to a file is recorded in the DPM, but no copy of the file in the DPM disk pool is needed**
- **Directories with the Study, Sery and SOP identifier are created in the LFC**
- **The data erases during the anonymization step are registered in the AMGA server.**

Strong Security

- **To allow one user to access a medical file and its metadata the owner of the file must set the right in all the component :**



- **Example :**

```
RegisterLfcRight()
{
lfc-setacl -m "m:rwx,u::rwx,g::0,o::0,u:$DnUser:rwx,d:m:rwx"  \
        $BASE
lfc-setacl -m "m:rwx,u::rwx,g::0,o::0,u:$DnUser:rwx,d:m:rwx"  \
        $BASE/$STUDY_INSTANCE_UID
lfc-setacl -m "m:rwx,u::rwx,g::0,o::0,u:$DnUser:rwx,d:m:rwx"  \
        $BASE/$STUDY_INSTANCE_UID/$SERIES_INSTANCE_UID
lfc-setacl -m "m:rwx,u::rwx,g::0,o::0,u:$DnUser:rwx"          \
  $BASE/$STUDY_INSTANCE_UID/$SERIES_INSTANCE_UID/$SOP_INSTANCE_UID
}

SetDpmRight()
{
dpns-setacl -m "m:rwx,u::rwx,g::0,o::0,u:$DnUser:rwx,d:m:rwx" \
        $BASE/$STUDY_INSTANCE_UID
dpns-setacl -m "m:rwx,u::rwx,g::0,o::0,u:$DnUser:rwx,d:m:rwx" \
        $BASE/$STUDY_INSTANCE_UID/$SERIES_INSTANCE_UID
dpns-setacl -m "m:rwx,u::rwx,g::0,o::0,u:$DnUser:rwx"         \
  $BASE/$STUDY_INSTANCE_UID/$SERIES_INSTANCE_UID/$SOP_INSTANCE_UID
}
```

Fine-grained security

- **The user can set the permission a group or a VO**
- **The user can set the ACL for an individual user (based on the DN)**

The permission can be set for :
All the anonymous DICOM picture of a study
All the anonymous DICOM picture of a serie
An individual anonymous DICOM picture
Each element of the metadata of a file

```
Query> getattr /mdm/PATIENT/b67982a3b0e825af054741a58e750ca5cc6278e name
>> Marc-Elian Begin

Query> getattr /mdm/IMAGE/guid:0617a6bf-09ba-428c-b5f4-f674312c5aa0  nx ny  SOPinsUID
>> 256
>> 256
>> 1.2.826.0.1.3680043.2.1143..20060202124502415.63
```

Metadata: AMGA

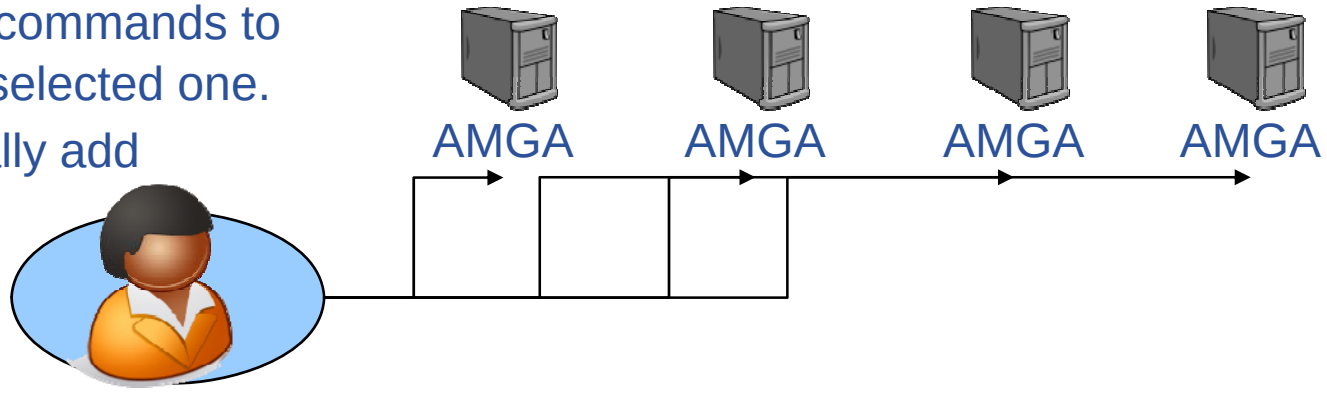
- **AMGA is the ARDA METADA CATALOGUE PROJECT**
  - http://amga.web.cern.ch
- **The purpose is to store the metadata of the patient and of the medical picture**

AMGA is a front-end for PostgreSQL, MySQL, Oracle and SQLite database.
The user VOMS credential can be used for the authentification
The protocol is a streamed ASCII protocol with SSL encryption

Distributed metadata

- **AMGA provides a powerfull but limited distributed schema :**
  - Replication in AMGA follows an asynchronous, master-slave model, and supports partial replication of the directory hierarchy.
  - Slaves can replicate any sub-tree of the metadata hierarchy
- **The MDM needs a full autonomy of the site**
  - The metadata are stored and managed locally
- **The MDM provide a library and a client that provide multi-site communication. This work is based on the AMGA client and used the same syntax.**

- Users can send the commands to all the servers or the selected one.
- Users can dynamically add or remove servers



Distributed Key: Hydra

- **Hydra have been developped at CERN by Akos Frohner**
- **It store key and cypher to encrypt/decrypt file.**
- **Each pair (key,cypher) is associated to a string**
- **The command line is: glite-eds-encrypt <string> <in file> <out file>**
- **It is based on the Shamir's Secret Sharing algorithm**
  - By default the MDM used 3 servers and 2 are need to decypher
  - Each site could install multiple hydra servers
- **Hydra allow a strong security and very reliable service**