WP8-9-10 + SG joint meeting

Overview of security requirements for WP10

European DataGrid 7th project conference

Heidelberg, Germany

September 27, 2003

Johan Montagnat, WP10

Biomedical data and metadata security constraints

- Strong security constraints concerning biomedical data
  - Preserve patiens privacy
- Data property constraints:
  - Medical data are owned by the patient
  - Some patented genomic sequences must be protected
- Data privacy must be controlled
  - At the grid level: for all grid users
  - At the site level: for local administrators
  - During network transmission

Users and authorization

- Medical data contain
  - Critical nominative data (usually some metadata)
  - Non-crical images or metadata
- Users
  - Patients owning the data
  - Physicians can access their (and only their) patient data
  - Researchers can only access non-critical data when authorized
  - Accredited administrator per site
- Authorization granularity
  - Medical department (group)
  - Individual level (patient…)

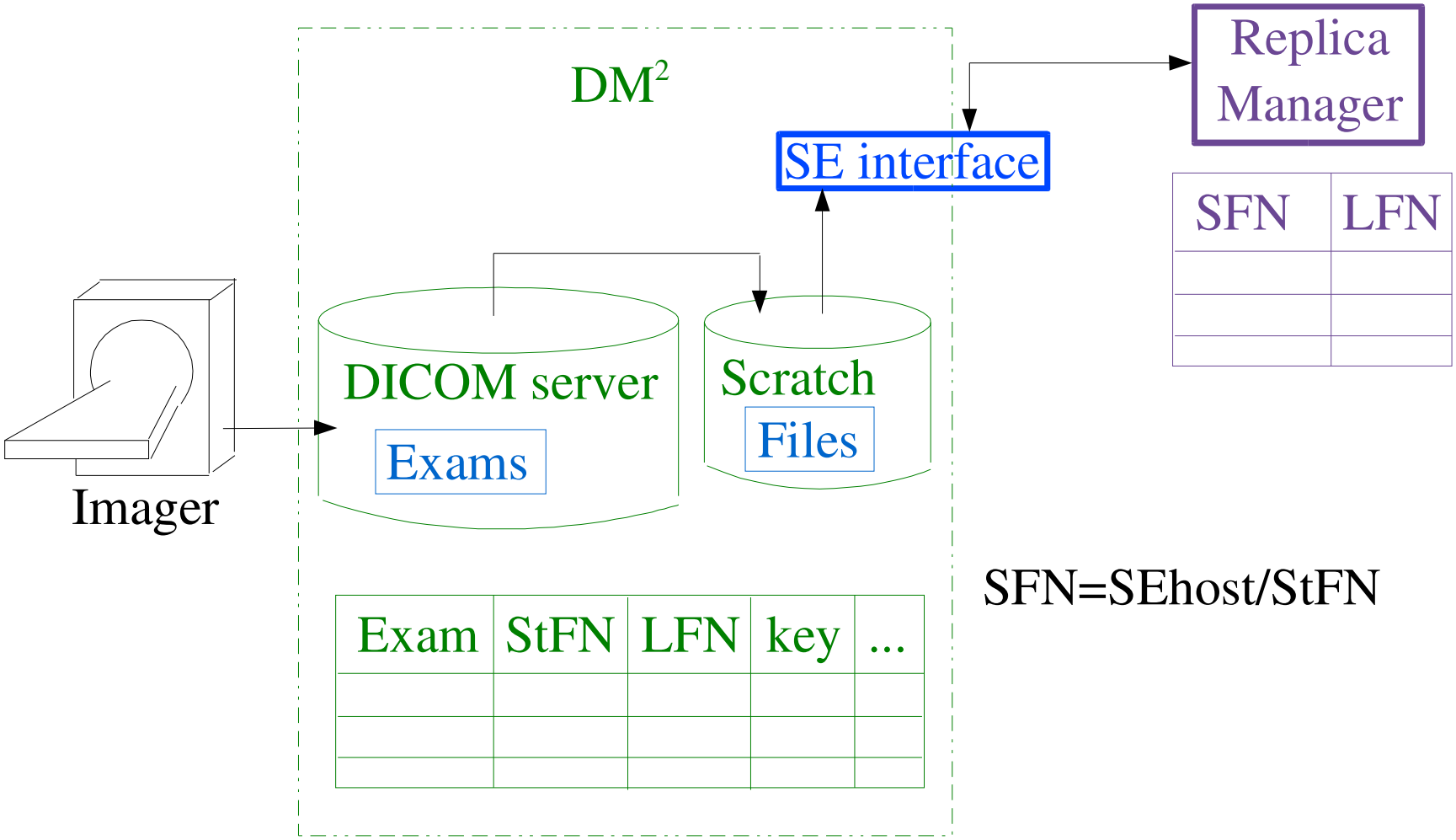
Delegation and acces right control

- A physician (an accredited user) can delegate
  - Full access right to another physician
  - Access to non-critical data to researchers
- A patient can delegate
  - Full access right to a physician
- Some biological data are public (!)
  - And should be accessible by anyone.
- Master medical data are mostly read-only
  - The medical files removal policy is let to the medical site administrator, not the users

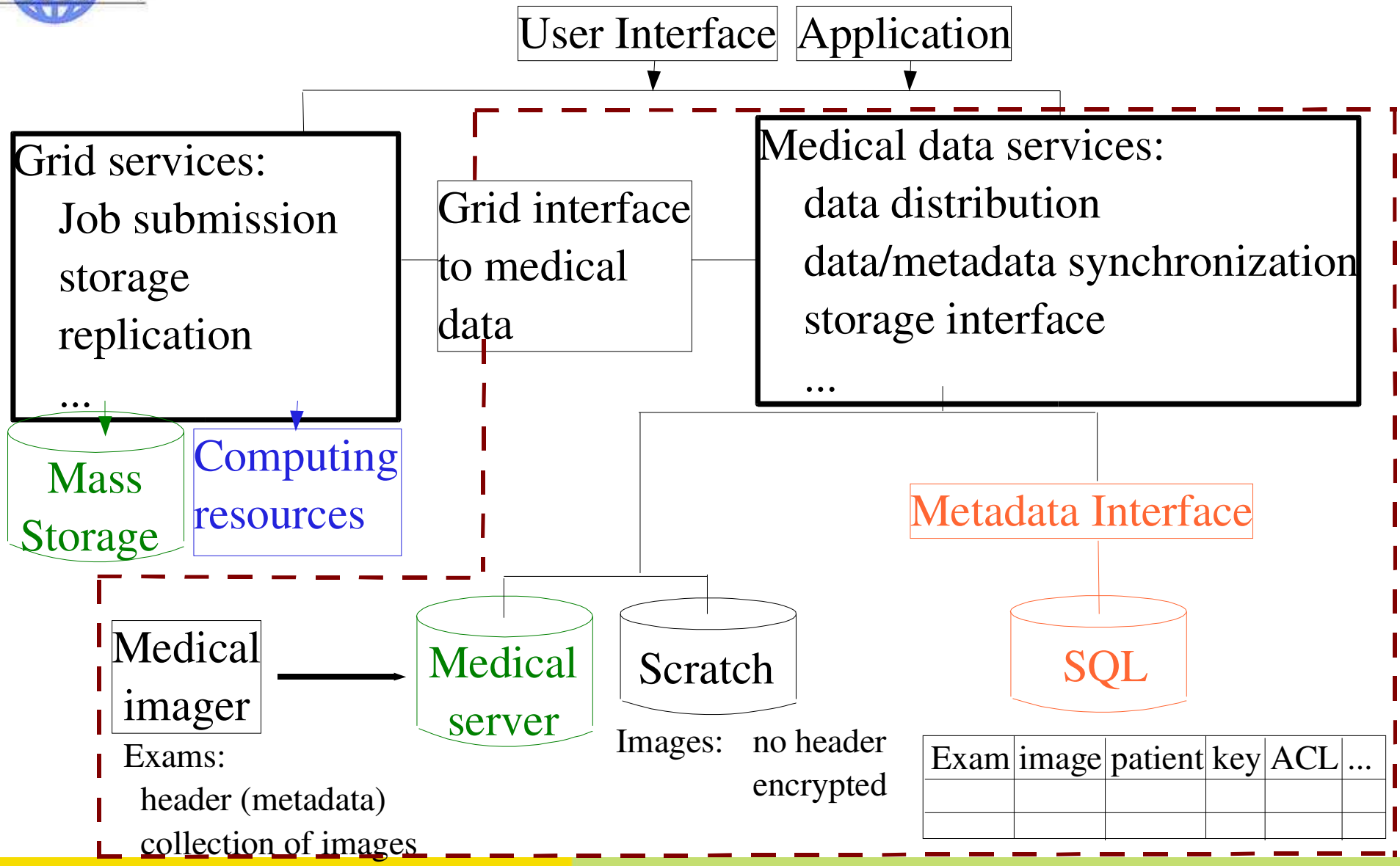
Replicaton and computations

- Master and replicated data
  - Master data on secured medical sites for sensitive data
  - Some data should be filtered before being set elsewhere
- Data replication
  - Should not be possible for critical data
  - A user should be able to conrol possible replication targets for some sensitive data (sub-grid?)
- A user should not be able to determine:
  - What computations are done by another user
  - On which data another user is working

Medical SE


DM2
Replica Manager
SE interface
SFN
LFN
DICOM server
Exams
Scratch
Files
Imager
Exam
StFN
LFN
key
...
SFN=SEhost/StFN

Medical data on the grid



The current status

- VOMS
  - Group level, a user should be able to belong to several VOs
  - Ability to control access rights at the individual level?
- Data access rights on SE
  - ACLs not implemented?
- Encryption
  - No encryption on disk
  - Network encryption in gridftp?
- Replication
  - No user control