EUROPEAN MIDDLEWARE INITIATIVE

EMI Hydra and Cloud(s)

John White
Joni Hahkala
Henri Mikkonen

Contents

EUROPEAN MIDDLEWARE INITIATIVE

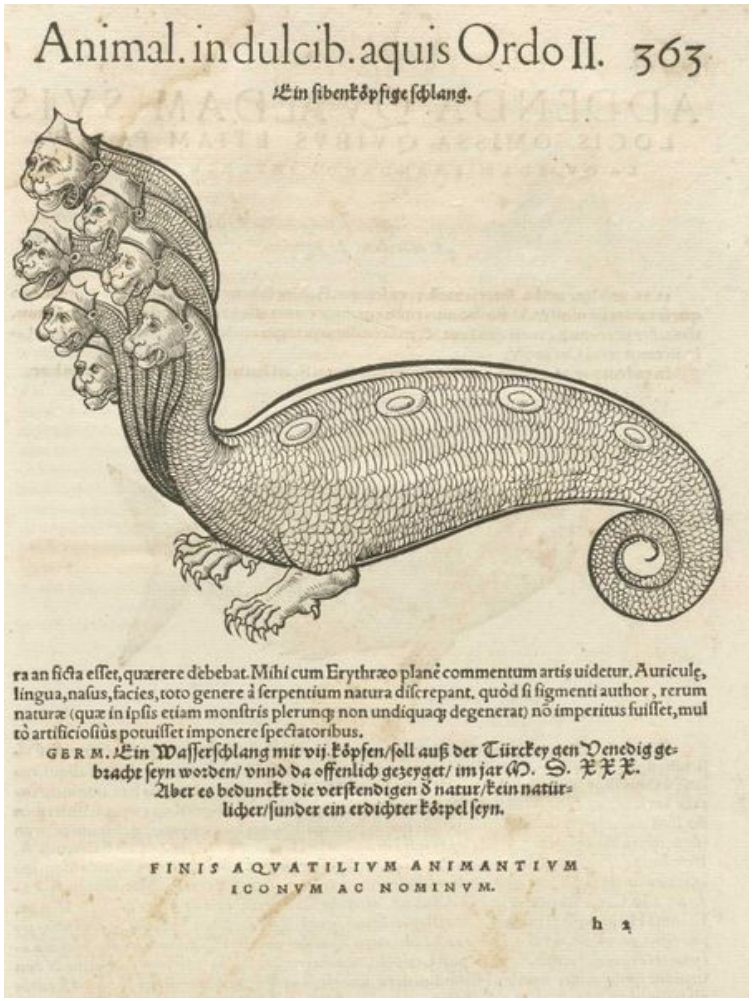
- Hydra background.
- Hydra in EMI.
- Another use-case.

Secure Data Storage

EUROPEAN MIDDLEWARE INITIATIVE

- Some research coummunities demand their data be secured.
  - Metadata and Data files controlled by ACLs.
  - Data files should be encrypted.
- EGEE solution: extension of Data Management tools.
  - Encryption/decryption of data on the fly.
  - Meta-data management.
  - Encryption key management/protection. (**Hydra**)
- Medical data: Managed by DICOM storage.
  - **D**igital **I**maging and **Co**mmunications in **M**edicine (DICOM): standard.
  - DICOM designed for internal hospital usage.
  - Should not be exposed to general Grid environment.
  - DICOM/DPM interface.

What is Hydra?



What is Hydra?

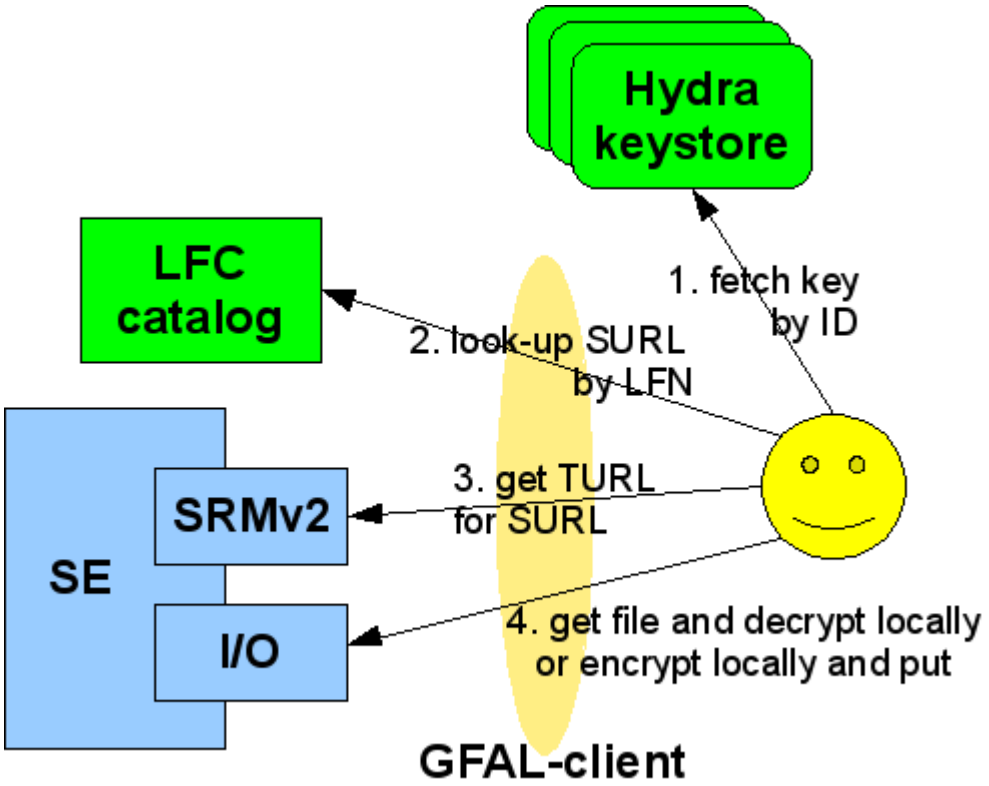
EUROPEAN MIDDLEWARE INITIATIVE

Hydra is part of encrypted file storage.

- Files are encrypted for storage on any GFAL-supported SE.
- The encryption key is the critical information.
- Key split and distributed to multiple locations,
  Hydra keystores.
- The splitting scheme is “non-trivial”...
  Shamir Secret Sharing Scheme.
- Need N out of M key parts to reconstruct key.
  - Secure: $<$ N parts not enough to reconstruct key.
  - Fault Tolerant: unavailability of M-N keystores not a problem.
- **Encrypted Data Storage (EDS).**

Hydra in EDS

General Standalone scheme.

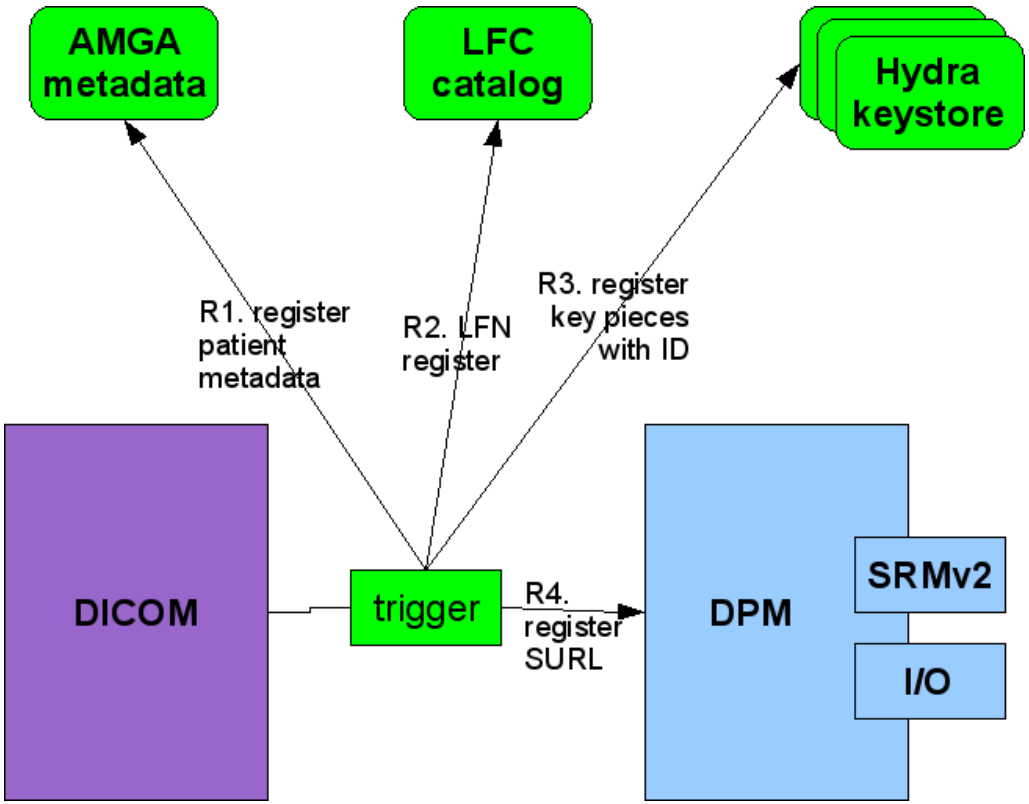


- EMI/gLite solution.
- Key generation in client.
- (De)Encryption locally.
- GFAL-enabled clients.

Medical Data Management

EUROPEAN MIDDLEWARE INITIATIVE

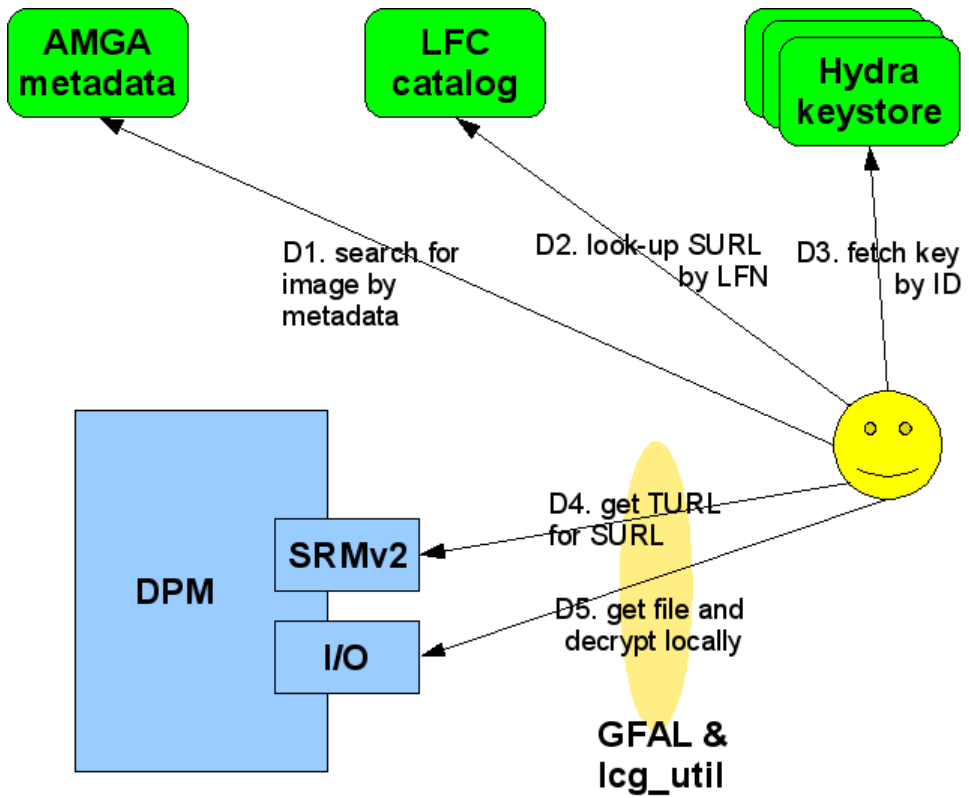
Hydra is combined with DICOM/DPM interface to produce **Medical Data Manager** (MDM).




```
dpm-dicom-trigger <DICOM file name>
```

Medical Data Management

Hydra is combined with DICOM/DPM interface to produce **Medical Data Manager** (MDM).




```
lcg-cp -bD srmv2 <SURL><ID> <encrypted file name>
glite-eds-decrypt <ID> <encrypted file name> <file
```

Hydra in EMI

EUROPEAN MIDDLEWARE INITIATIVE

- Already in use with Biomed community.
- Officially supported in EMI.
  - To be released as update to EMI-2. See:
    `https://savannah.cern.ch/task/?23333`
    `https://savannah.cern.ch/task/?18710`
  - Documentation [1] to be certified by EMI.
  - NAGIOS probe written.
  - GLUE-2 publishing done. Documented.
  - Testing completed [2].
- **Cases other than EMI/Grid Biomed?**

[1] `https://twiki.cern.ch/twiki/bin/view/EMI/EMIHydraDocumentation`
[2] `https://twiki.cern.ch/twiki/bin/view/EGEE/HydraTestPlan`

Hydra and Clouds

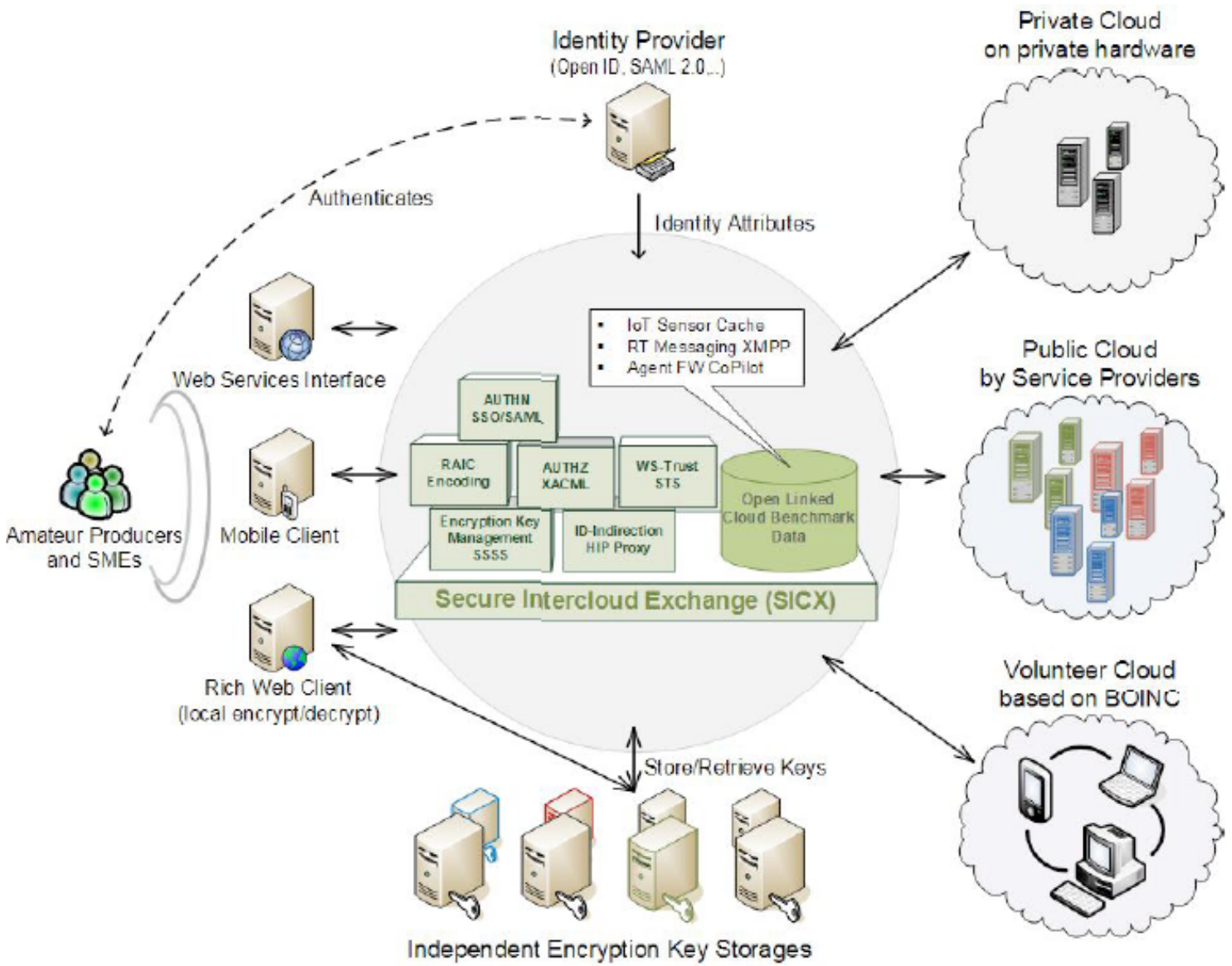
EUROPEAN MIDDLEWARE INITIATIVE

Secure **I**nter**C**loud e**X**change (SICX)

- Multi-cloud storage without vendor and data lock-in.
- Data striped in similar manner as keys.
- Hydra clients re-written in Java.
- Simpler Hydra service created for evaluation.

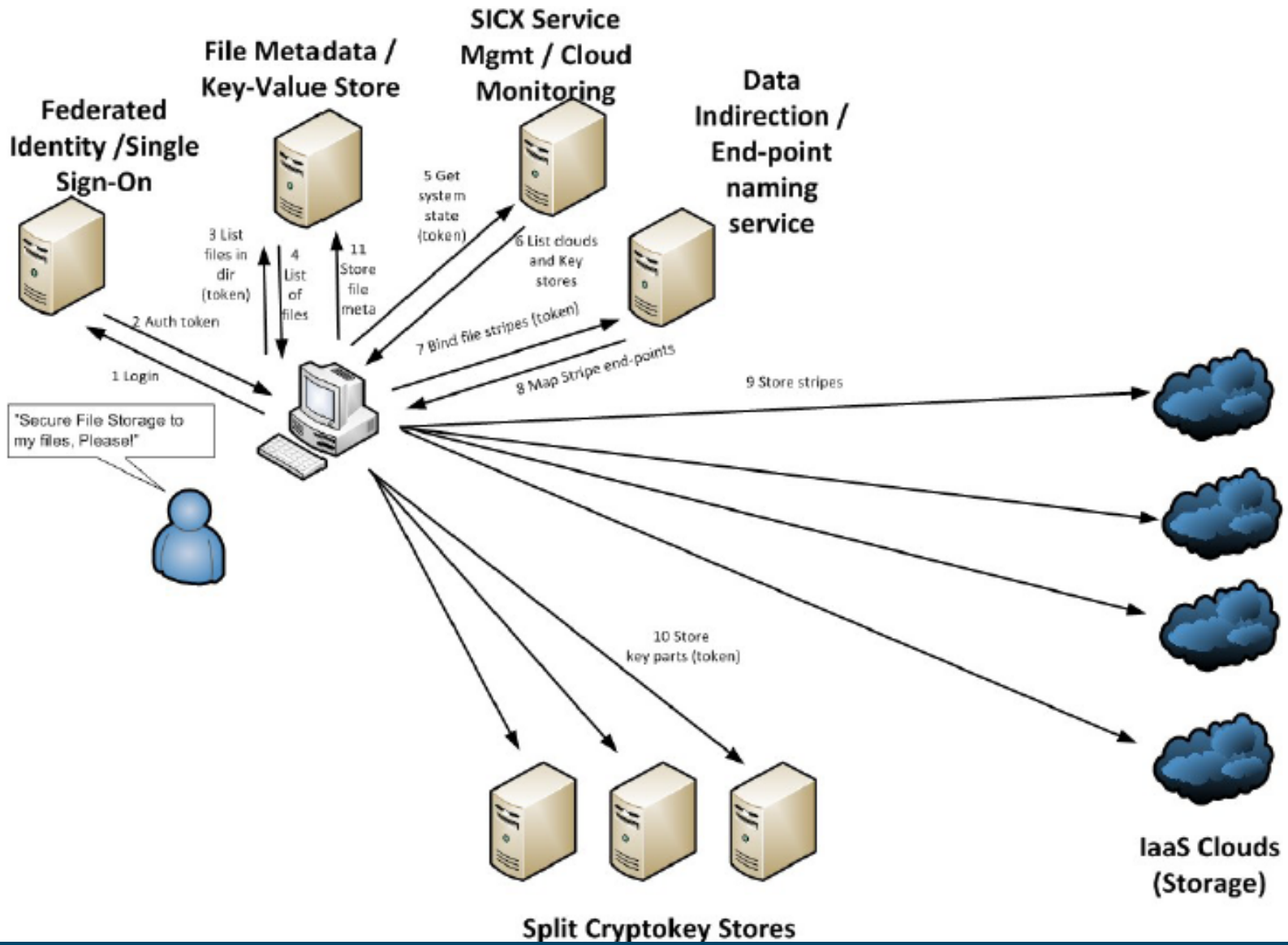
Complete proof of concept system demonstrated to Finnish Technology Funding agency, June 2012

Hydra and Clouds



Hydra and Clouds

EUROPEAN MIDDLEWARE INITIATIVE



Questions?

Thank you!

EMI is partially funded by the European Commission under Grant Agreement RI-261611