Unlocking data: federated identity with LSDMA and dCache

Paul Millar
Academia Sinica, 2015-03-19
What is LSDMA
What is LSDMA
The grid solution: X.509 (user) certificates
X.509 certificates: a huge success!

"It's been a global effort, a global success. It has only been possible because of the extraordinary achievements of the experiments, infrastructure and the grid computing."

Rolf Heuer, the Director General of CERN
X.509 certificates: typical user reaction
Federated Identity

Check who you are & Authorisation decision

Identity Provider (IdP) -> Record information -> Assertion -> Service Provider (SP)
Federated Identity: the vision

The German Scientific Data Cloud
Federated Identity: the vision

The German Scientific Data Cloud
Web portals

• User logs in with Federated Identity authentication.
• Web portal needs access to data but existing infrastructure is X.509 based.

• Two choices:
  • “Generate” X.509 credential,
  • Update infrastructure to support Federated Identity credentials.

• Plan to do both, but focusing on the first one initially.
Credential translation: the plan

User → IdP → WAYF → Credential Translation Service → Online SLCS CA → Globus File Transfer Service

Worker Node → dCache

Data → GlobusFTP

NFS-mount
Command-line support

- Work on hybrid approach
  - Send assertion as a "password"
  - Uses an "ldap façade" service
  - "Password" (assertion) is processed by ldap façade.
  - Requires user to somehow acquire assertion.

- Moonshot is an alternative
  
  See Daniel Kouřil's talk yesterday
AARC

- A **new project** to fix all this!
  - ~€3M budget, 19 funded + 2 unfunded
  - 2 year project, starts 1 May 2015.
  - Broad scope, which includes non-web clients.
- Plan to collaborate with AARC
  (one of the LSDMA institutes is part of the project)
Next steps

- Working on building up a reliable CTS.
- Investigate command-line options
  Continue existing work, liaise with AARC
- Add support in dCache for Federated Identity-based login
  Initial version assumes web-browser and has an Apache front-end.
Thanks for listening.

Any questions?