

EMI Storage meets EMI security

Component/ Middleware	Staff
gLite (LFC,FTS,DPM,GFAL)	Oliver Keeble, Jean-Philippe Baud
ARC	Jon Kerr Nilsen
UNICORE	Ralph Müller-Pfefferkorn
StoRM	Riccardo Zappi, Michele Dibenedetto
dCache	Patrick Fuhrmann, Tigran Mkrtchyan

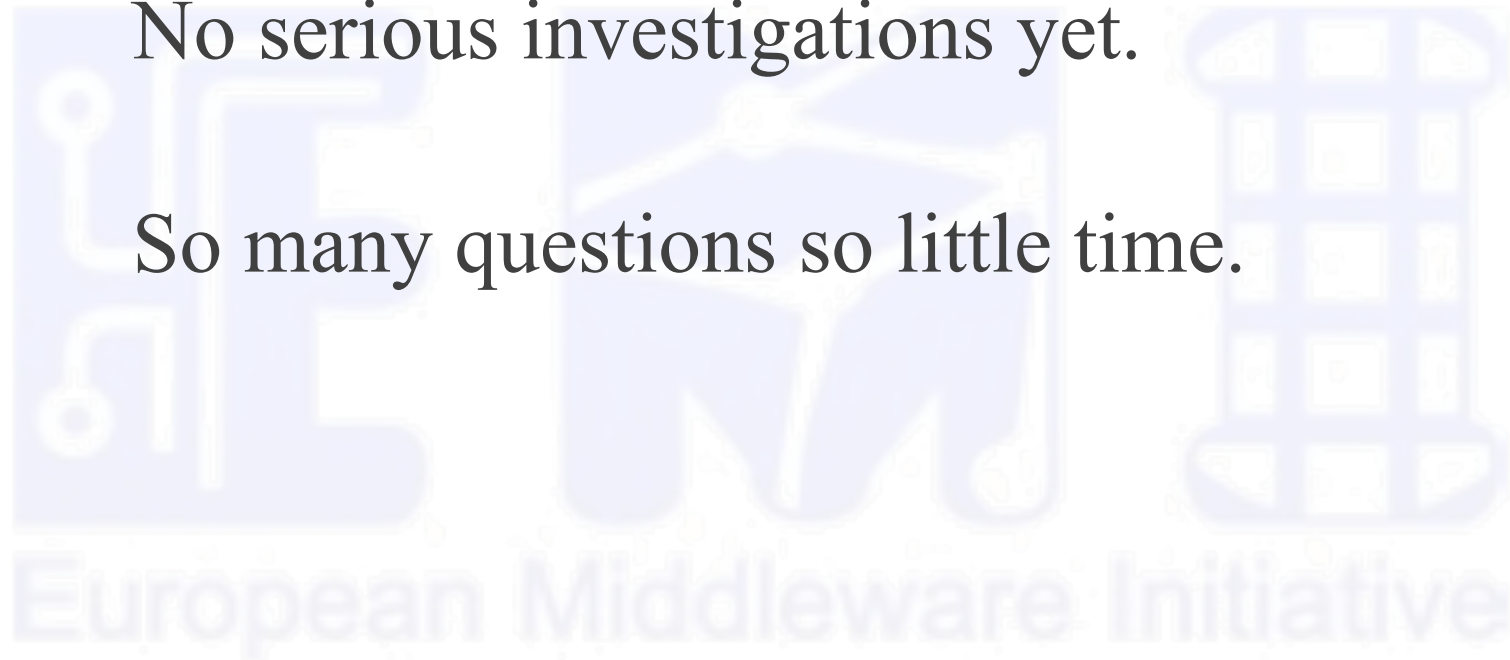
With kind contributions by

Alex Sim (BeStMan, OSG)

Disclaimer

No serious investigations yet.

So many questions so little time.



Topics

Replacement of GSI

Motivation

Possible Showstoppers, Open issues

Migration

Goal

Identity Management

Single Sign-on

Call-outs to Authentication/Authorization services

Replacement of GSI

Motivation

Will be a big/expensive effort -> Good Justification

First discussion on this (in storage) started 2 years ago in the context of the SRM (DESY SRM workshop)

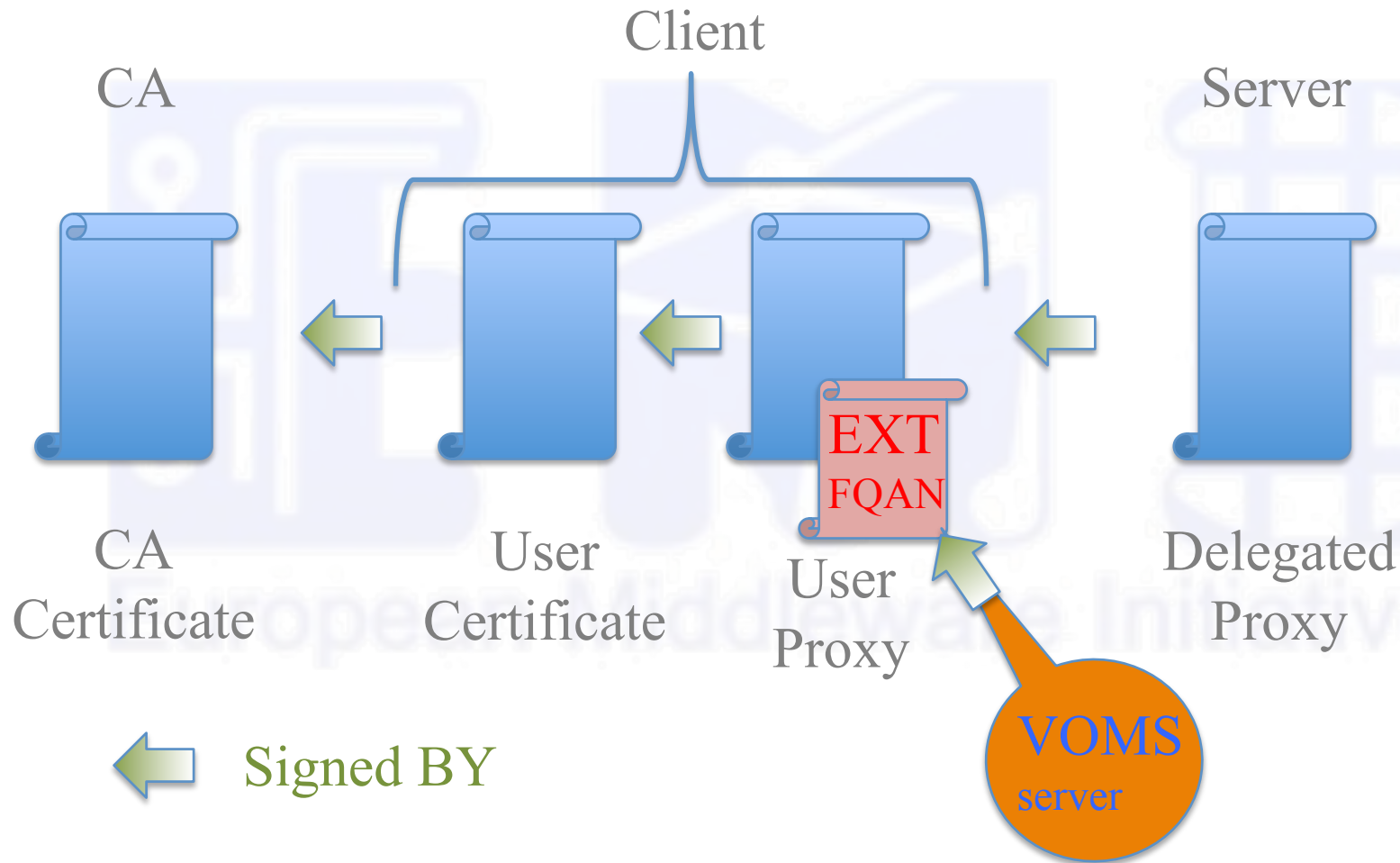
(How) would we profit from a GSI replacement ?

- 'Well maintained' security libraries (e.g. fast security bug fixes)
- Session re-use. Would clients benefit (FTS) ?
- Avoid generating delegated 'proxies' if not needed.
- Relevant services
 - SRM
 - How about gsiFtp ? Should we use FTPS(implicit/explicit) or https?

Would 'fixing GSI' give us similar benefits w/o too much hassle ?

Replacement of GSI

Certificates and Proxies with GSI



Replacement of GSI

Open questions, if we would move to SSL

Proxies (voms-proxy-init)

- Would we use RFC compliant proxies only ?
- Are proxies (certificates not signed by a CA) accepted by SSL libraries?
- Do SSL libraries make 'extensions' available at the server side (FQAN) ?
- Is this true for non CC/C++ frameworks (java, python ?)

Replacement of GSI

Open questions, if we would move to SSL

Delegation Proxies

- Do we need delegation (FTS, SRM-copy, myProxy) ?
- How can we achieve delegation w/o GSI ?
 - Common interface or common service ?
 - GridSiteDelegation(<https://twiki.cern.ch/twiki/bin/view/EGEE/GridSiteDelegation>)
 - Globus MyProxy Delegation (<http://grid.ncsa.illinois.edu/myproxy/delegation>)
 - They don't inter-operate
 - Are there any other options ?

Replacement of GSI

Migration

- Does migration has to be globally coordinated, or can this be smoothly.
 - Europe vers. US : VDT, BeStMan
- Can GSI and non GSI services be run at the same time (different addr.) ?
- What would be the implications for e.g. catalogues ?
- Are there any other implications e.g. order of FQANs in proxy ?

Replacement of GSI

GOAL

- X509 over https would be desirable for
 - WLCG
 - Other Certificate bases communities
- Other/Easier approaches for other communities (see next section)
 - OSG/Alex would be very interested
 - Who do we find out (EGI/NGI customers)

Identity Management

Single Sign-On

- Single Sign-on mechanisms
 - X509
 - Kerberos
 - OpenID
 - Shibboleth
 - US : DOE Entrust, HSPD-12 (Govt)
- UNICORE using SAML-Assertion
- Do we have any experience with non X509
- E.g. : OSG using OpenID for one community
- Do we have any policy/services for mapping between X509 and others.

Identity Management

Identity services

- How important are central identity services for SE's ?
- GUMS and SCAS moving away from SAML and XACML
- Migration should be completed this year. (2010)
- SAML/XACML : Only partially supported by EMI SE's
- ARGUS
 - What are the benefits.
 - We need to investigate : speed and other technical issues.