



Enabling Grids for E-scienceE

JRA1 Workshop Padova, 2004 November 15-17

Security in Data Management

on behalf of the JRA1 DM Cluster:

Paolo Badino, Ricardo Brito da Rocha, Ákos Frohner, Peter Kunszt, József Kovács, Gavin McCance, Krzysztof Nienartowicz, Daniel Rodrigues

www.eu-egee.org



- **Java Services (some code)**
- **C/C++ Clients and Services (some code)**
- **File Transfer: Credential Renewal**
- **Backend Catalogs vs. Delegation**
- **Local to Global Catalog Updates**
- **Integration with Native Environment**



- **Authentication: trustmanager & utils-java** **OK**
- **Authorization: fine grained, internal** **developed**

For developers:

```

cvs co org.glite.security.java-utils          # for SecurityContext
cd org.glite.security.java-utils; ant stage
cvs co org.glite.security.trustmanager        # for authentication
cd org.glite.security.trustmanager; ant stage
cvs co org.glite.security.test-utils          # for certificates
cd org.glite.security.test-utils; ant stage
cd org.glite.data....
ant tomcat.configure
  
```

For installation:

```

rpm -i ...tomcat5.rpm glite-security-trustmanager.rpm
/opt/glite/etc/glite-security-trustmanager/configure.sh
  
```

- DN and attributes are used in fine grained authz code

```
org.glite.security.utils.axis.InitSecurityContext.init();
SecurityInfo si = SecurityInfoContainer.getSecurityInfo();

System.out.println("DN: " + si.getClientName());

List groupList = si.getAuthorizedAttributes();
for (int i=0; i<groupList.size(); i++) {
    System.out.println("  attribute:" + (String)groupList.get(i));
}
```

- **Authentication: CGSI-gSOAP 2.6-1.1.5**
we don't have web service server
- we have the gLite I/O service using plain GSI (auth is GSS, authz is GSI), but it is not a WS for performance reasons (file transfer)
- **Delegation: using GSI in gLite I/O**
one can turn it off to avoid the problem of mismatching Globus versions through the delegation chain
- **Gridsite/mod_ssl: missing an example for gSOAP!**
Unclear: mod_ssl-gsi + delegation + mod_gsoap vs. mod_gsoap + cgsi_gsoap? An example would be nice.
- we will need a C/C++ WS solution soon...
Apache + mod_gSOAP + CGSI_gSOAP?

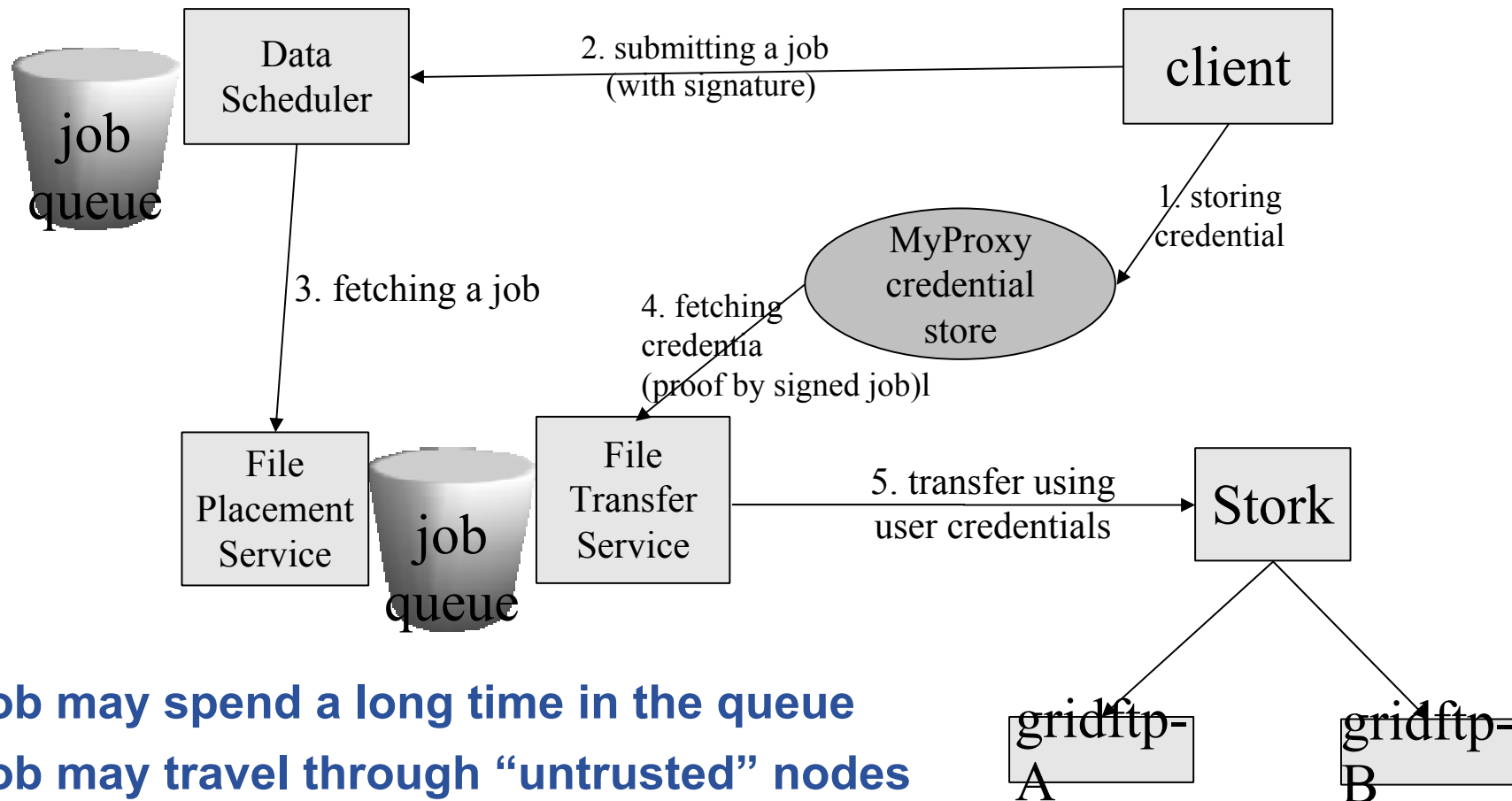
```
#include "cgsi_plugin.h"

int flags = CGSI_OPT_DISABLE_NAME_CHECK;
if(SSL == secure_protocol){
    flags |= CGSI_OPT_SSL_COMPATIBLE;
}

soap_register_plugin_arg (soap, client_cgsi_plugin, &flags);

// do credential re-delegation in an intermediate server
const char * proxy_file = ... // a temporary filename
export_delegated_credential(incoming_soap, proxy_file);
if(use_delegation){
    set_default_proxy_file(soap,(char*)proxy_file);
}
```

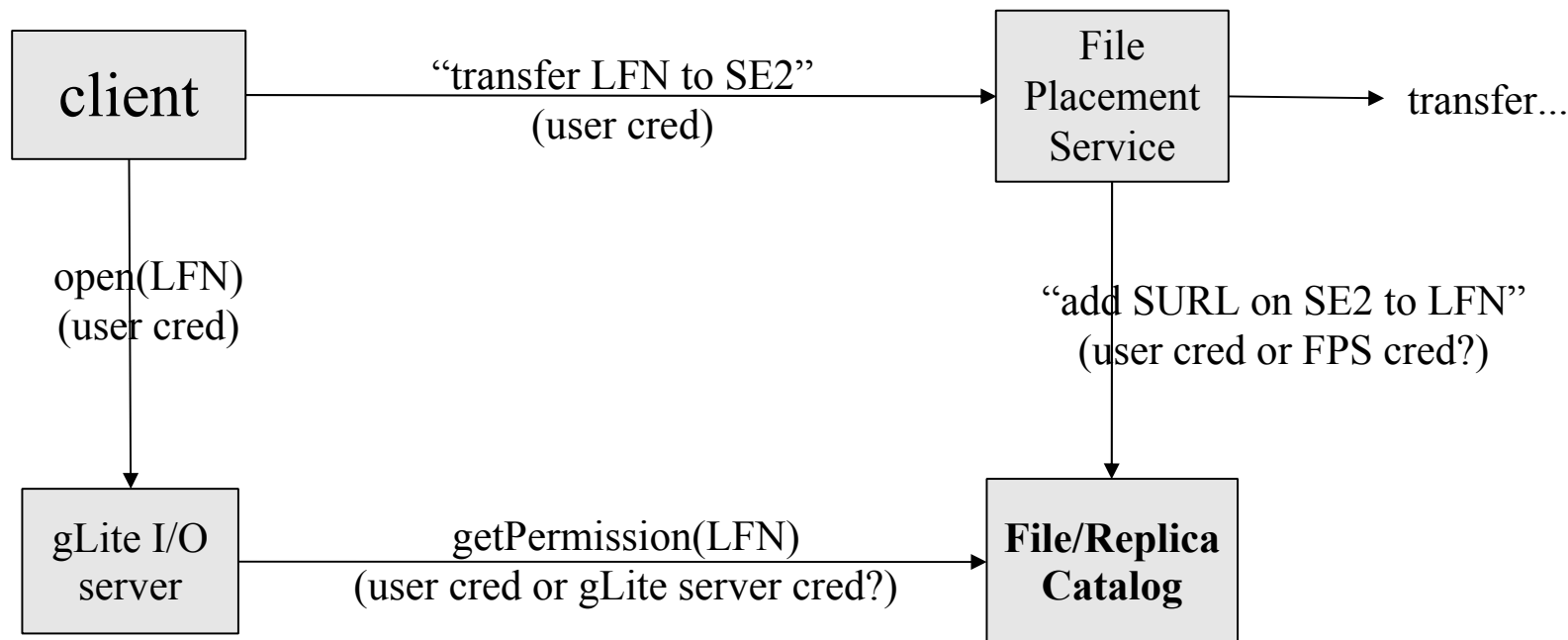
problems similar to job submission:



- job may spend a long time in the queue
- job may travel through “untrusted” nodes

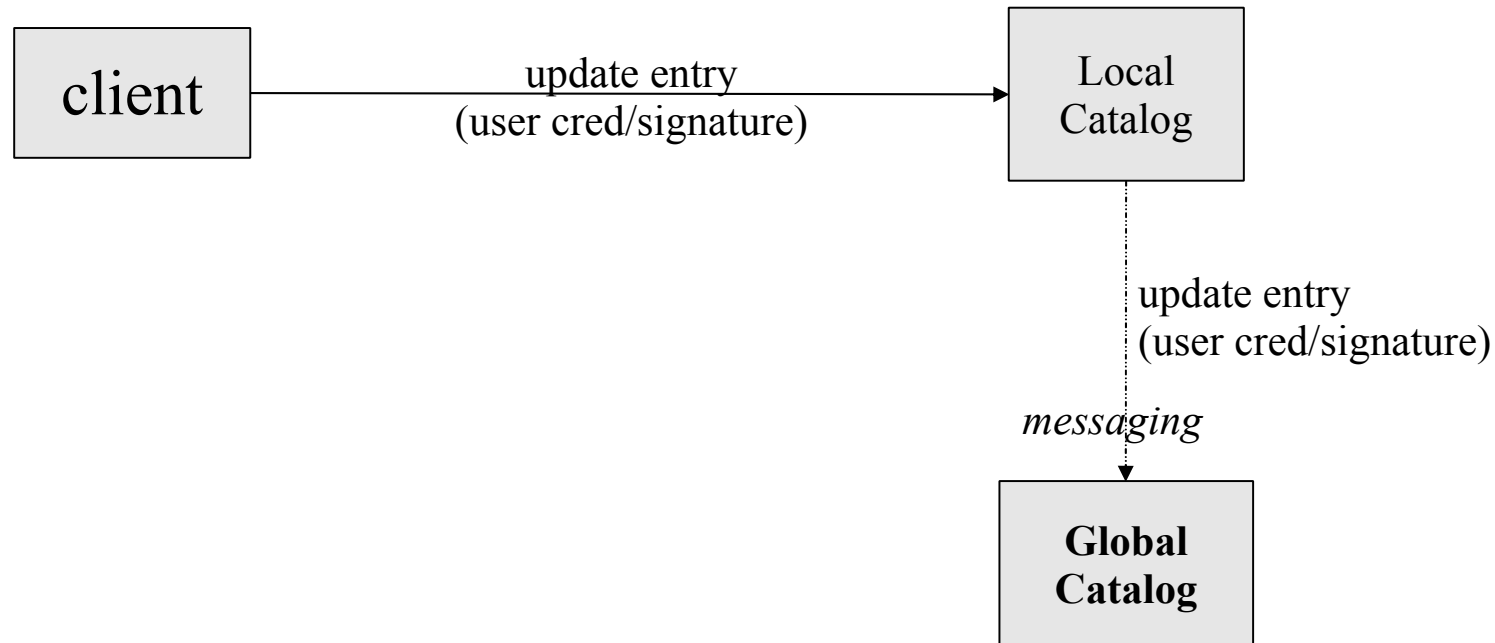
Message Level Security could wash away all problems?!

Services acting on behalf of the user:



- using delegated user credential (GSI works, WS doesn't)
- trusted frontend service forwarding user attributes, for example in SOAP headers (... if services are trusted)

Changes in local catalog are propagated to the global catalog using messaging:

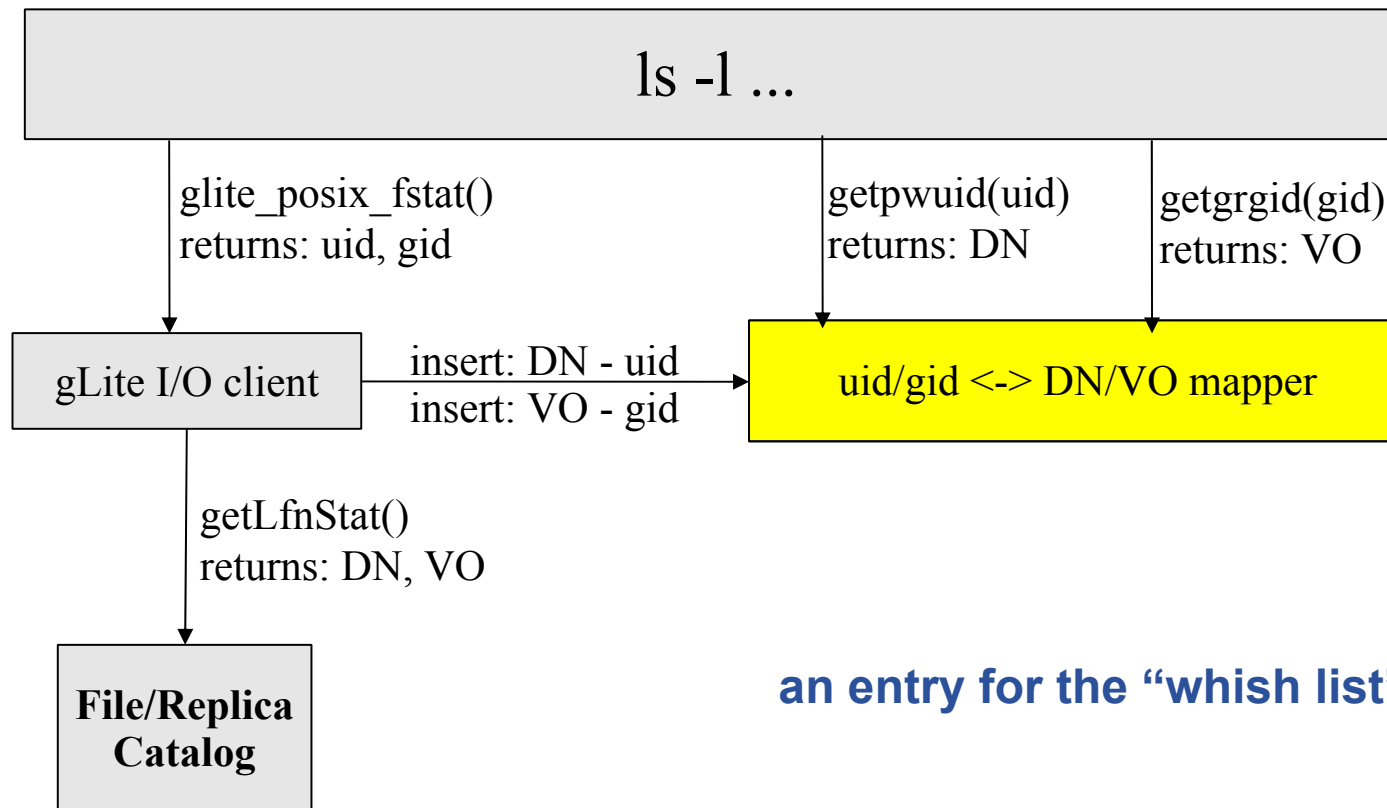


- delegation? – problems with batch updates
- user info attached to change – trusted local catalogs
- message level security – ideal solution?!

Making “ls -l” work as

```
ls -l /grid/egee/home/myfile
```

```
-rw-r--r-- 1 "/C=CH/O=CERN/OU=GRID/CN=Akos Frohner 5317"  
"/egee/Role=Production" 42 2004-11-16 12:00 myfile
```



an entry for the “whish list”

Issues or wish list:

- recommendation for “long jobs” vs. MLS?
- recommendation for a C/C++ web service?
- delegation or trusted frontend services?
- ... small utilities