
John White, Helsinki Institute of Physics. EGEE JRA1 Deputy Middleware Manager.
Contents

• Overview.
• VOMS.
• Job submission.
• Computing Element.
• Pilot Jobs.
• Authorization Review.
• Interoperability.
gLite middleware essentially defines a Grid infrastructure for a batch-processing system.

gLite “security”:
- A collection of components.
- Protects the middleware infrastructure.

Virtual Organizations, Authentication, Authorization, credential issuance and renewal.

gLite middleware security based on PKI security.

Identity mechanism in gLite:
- Identity of the user (DN) given by Certificate Authority (CA).
- X509 credentials as proxy certificates with added attributes (DN and FQAN)
- Membership in a Virtual Organization (VO) (and its subgroups)
- Role in the VO (dynamically chosen by the user)
Virtual Organization: A collection of people and resources.

- A VO will (probably) be heterogeneous..
  - Members may be in groups and have roles in these groups.
- Credentials managed by the Virtual Organization Management System.
- Consisting of:
  - VOMS server(s)
  - Administrative interface.
  - CLI clients and Java and C APIs.
- From the VO Admin point of view:
  - VOMS-Admin interface to add/delete members/groups/roles.
- From the VO member point of view:
  - Assigned to VO groups and assumes roles within groups.

/fred.example.org/replicator/optimisation/Role=Admin
Every user in a VO is characterized by attributes (group, role, capability).

- The combined values form unique attributes (FQANs).
- Can represent an FQAN as a sequence of group names.
- Each may be qualified with one or several roles and capabilities in that group.

In general, an FQAN has the following form:

/VO[/group[/subgroup(s)]][/Role = role][/Capability = cap]

- eg. the FQAN for the role Administrator in group Nerds of VO campus.example.org is:
  /campus.example.org/Nerds/Role=Administrator

Add the certificate DN and you have a unique ID within the VO.
All phases of a job require a valid credential.
- Submission.
- Reading data.
- Running on Worker Node.
- Sending/storing results.

Job’s lifetime can easily exceed the lifetime of a proxy.
- Overall job lifetime not known in advance.

Impossible to submit a job with long-lived credentials.
- Violates the meaning of short-time proxies.
- Increased risk if the credential is stolen.
- Might be unacceptable for the end resources.

VOMS attributes do not necessarily have same lifetime as proxy.

Proxy needs to be periodically renewed.
- User puts proxy to MyProxy server (VO service).
- Proxy is registered on the WMS with job.
- WMS contacts MyProxy/VOMS as needed (expiry close).
- Proxy renewal library used elsewhere as well (FTS).
LCG-CE (C/C++)

- L&L is LCAS and LCMAPS.
  - LCAS: Local Centre Authorization Service.
  - LCMAPS: Local Credential Mapping Service.
**LCAS: Local Centre Authorization Service:**
- The authorisation decision engine that adds access controls to the “gatekeeper”.
- Pluggable framework of independent authorisation modules.
- Decision based on the requested resources (RSL), identity, authZ credentials in proxy certificate.
- In case of VOMS the VO, group(s) and role(s) will be examined.
- Policy language selects authorisation plug-ins to be invoked.
- Access decision is the logical ”and” of the plug-ins.
  - Allowed and banned-user list inspection based on DN.
  - Wall-time limiting module.
  - VOMS module compares against a site-local access control list.
  - External parties may add own modules.
LCMAPS: Local Credential Mapping Service.
- Maps Grid identity to local uid/gid.
- Similar to LCAS, a pluggable module framework.
- "Acquisition" and "Enforcement" module types.
  - Separation needed to not impede module tasks.
  - Policy description language for configuration.
- Modules.
  - Map to a local Unix account and group. Static from users DN to uid. grid-mapfile.
  - Map to Pool Accounts, i.e. the account lease system. Unix Group also set.
  - VOMS support. VOMS groups, roles mapped onto Unix groups.
  - Map DN to local Kerberos and AFS tokens.
  - Set the real and effective uid/gid for current process.
  - LDAP. Update a fabric-central user directory for uid/gid info.
- External parties may add own modules.
CREAM (Java)

- glexec is front-end to LCAS/LCMAPS.
  - Enables the actual change of uid/gid on the CE.
- gJAF is gLite Java Authorization Framework.
  - AuthZ based on XACML policies.
- glexec performs the uid/gid change.
  - Is a “Grid” version of suexec.
  - Runs as setuid process on CE.
  - Performs switch based on results from LCAS/LCMAPS.
**User grid credential**
(subject name, VOMS, …)

**command to execute**

**current uid allowed to execute gLExec**

gLExec

**Authorization (‘LCAS’)**
- check white/blacklist
- VOMS-based ACLs
- is executable allowed?
- …

**Credential Acquisition**
- voms-poolaccount
- localaccount
- GUMS, …

**‘do it’**
- LDAP account
- posixAccount
- AFS, …

**LCMAPS**

**Execute command with arguments**
- as user \((uid, pgid, sgids \ldots)\)
User jobs are picked up from a central queue. Pilot and user credentials not necessarily the same.
• The credential change must now happen on the WN.
• Security issues with a setuid binary on WN.
• glexec to be shipped with three modes:
  – null.
  – logging only. non-setuid process
  – full uid change. setuid process.
• Sites will be able to choose their setup through configuration.
• Pilot jobs are difficult to prevent.
• glexec provides the traceability for jobs.

We need a centralized LCAS/LCMAPS (SCAS)
Authorization Continued...

- Authorization (AuthZ) system design has been reviewed.
- Extensive operations show areas that can be improved.
  - Consistent AuthZ decisions.
  - Consistent FQAN matching rules.
  - Re-tasking of gLite components (gJAF, G-PBox).
  - Interoperability.
- To provide uniform authorization and policy management in gLite.
  - Compatible with SAML and XACML standards.
  - Built on the experience of previous systems LCAS/LCMAPS, SCAS, G-PBox, gJAF.
  - Not constrained to use any existing implementation, recommended for the sake of economy.
● Three administrative domains (dotted boxes):
  – VO. (VOMS server and central policies).
  – Central Services. (WMS, top-level info systems etc).
  – Site. (CE and WNs. Local policies rule here).
● These domains need the mechanisms to deliver and apply policies.
  – PEP: Policy Enforcement Point. Essentially the policy “client”.
  – PDP: Policy Decision Point. Decision point based on the PAP policies.
  – EES: Environment Execution Service. Determines the job environment. UID/GID or (VM or WS?).
Policy Examples:

- **At the VO level:**
  - VO Membership.
  - Job privileges (e.g., analysis, production, software manager)
  - Privilege to submit pilot jobs.

- **At the Site level:**
  - Accepted VO’s.
  - Access schedules for different VO’s.
  - “Black” lists.
  - Allowed to run different applications.
  - Require VO of pilot job submitter is VO of pilot job executor.
  - No information on priorities of shares in policy files.
  - Policy files contain only authorization information.
Future Situation: FQAN uid/gid and share may be optionally decoupled.

- The uid/gid does not determine the share.
- The submission is still made to a LRMS queue.
- The CE must determine on which share this job should be executed
  - FQAN to share mapping is done entirely by the site administrator
  - The VO assigns FQANs to pre-defined shares (service classes).
1. Job arrives at CE with FQANs.
2. CREAM PEP calls PDP with X.509 proxy as argument.
3. PDP returns AuthZ answer (yes/no), share (and possibly an encrypted token containing the uid/gid(s)).
4. gLExec calls EES to obtain uid/gid(s).
5. EES returns uid/gid(s).
6. XACML request from gLExec on WN to PDP.
7. PDP queries EES.
8. EES returns uid/gid(s) to PDP.
9. XACML response from PDP containing uid/gid(s).
Interoperability

inter-Grid Security systems to exchange AuthZ decisions.

- This is achieved by agreeing on an authorization protocol common to OSG VO services, EGEE, and Globus.
- Revised AuthZ system compatible with SAML and XACML standards.
- Provided OpenSAML2.0 Extension Library to Support SAML2.0 profile of XACML2.0.
  - Protocol used by PEPs (gateways) to interact with PDPs.
  - The PDP informs the PEP on access decision.
  - Also the obligations need to be enforced if access if granted.
    - Obligations are used as a mechanism to restrict privileges at Grid resources.
- SCAS will (does) work with this protocol.
• gLite security middleware in place.
• Authorization services reviewed.
  – New work for EGEE-III identified.
  – Interoperability a key issue.
• Continues to evolve as needed.