Study on Authorization

Christoph Witzig, SWITCH

EGEE07 - MWSG - Oct 2, 2007

www.eu-egee.org

Information Society and Media

Outline

- Goal of this study
- Priorities of the study
- Definition of the problem and first impressions

Goal of the Study

- **Task by C.Grandi to look into authorization (authZ) in gLite with the goal to specify design for "authorization service" work item in EGEE-II/-III**
  - EGEE-III proposal: authZ service: Nikhef, UvA, CNAF, SWITCH
- **Should specify work in 2008 / early 2009**
  - Comment: should be fully deployed within lifetime of EGEE-III
  - Indicate broader view for the future
- **Deliverable is a proposal with clear recommendations based on input of many people (experiments, SAx, JRA1) to be accepted/rejected by TCG**

Timeline

- **September / early October: requirement gathering**

  PLEASE let me know to whom I should talk to

- **mid-October - late Nov: working out the proposal of the design**

- **Discussion at MWSG meeting in December**

- **Presentation and decision in TCG in January**

Priorities

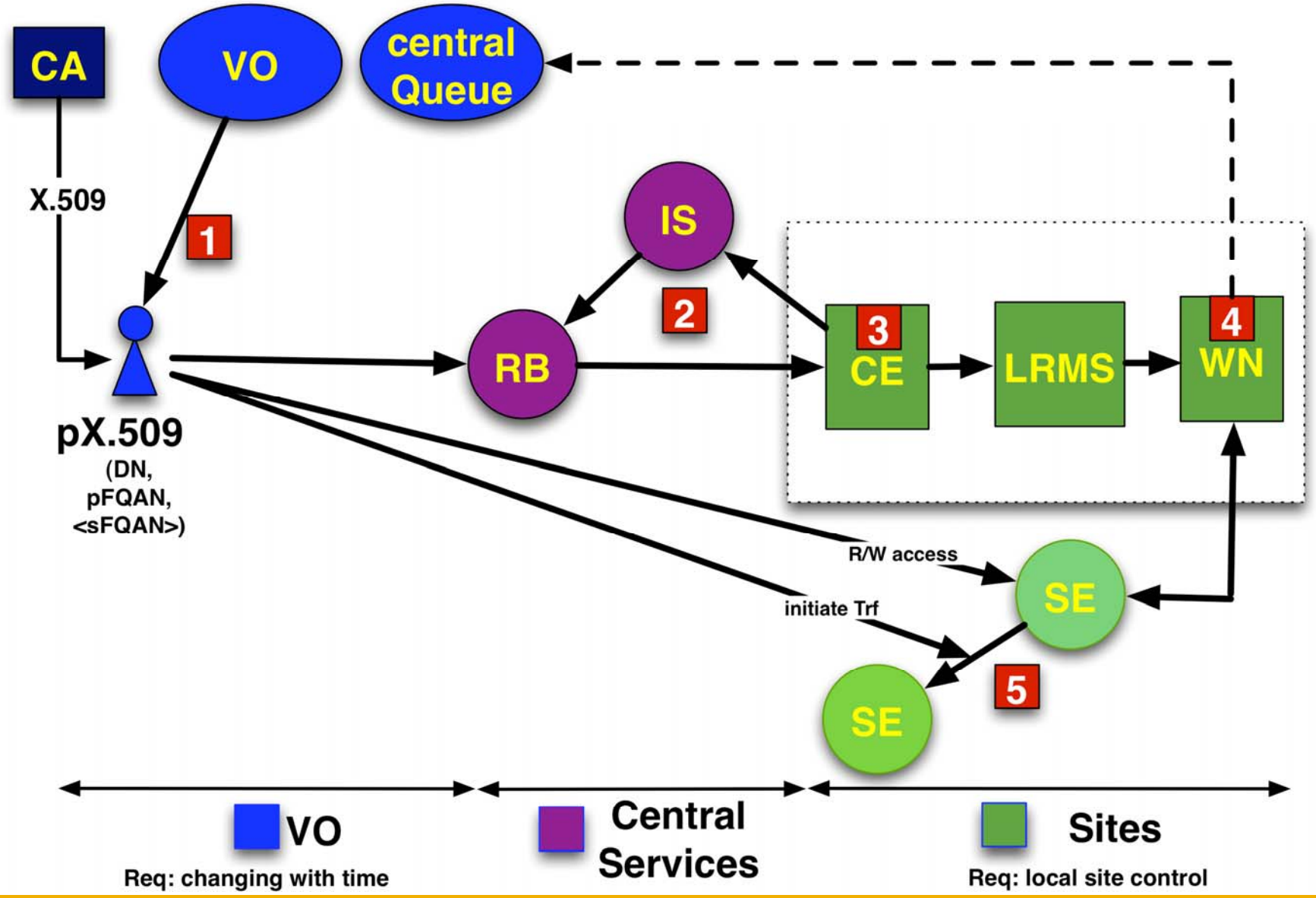
List of priorities in order:

1. **Should fix some of the limitations of the current authZ framework**
2. **Introduce new features to the extend that they are needed by the**
   1. Experiments / VOs
   2. Sites / SAx
   3. JRA1
3. **Interoperability**
4. **Use of standards if possible**

Current authZ Mechanism

- **authZ = permission to access a resource based on a set of attributes**

- **Basic mechanism in gLite:**
  - Proxy certs with VOMS extensions
    - DN, pFQAN, <sFQANs>
      1. *identity of the user (DN, CA)*
      2. *membership in VO (and its subgroups)*
      3. *role (dynamically chosen by the user)*
  - Use of this information by different algorithms at different places in the middleware


CA
VO
central Queue
X.509
1
IS
2
RB
3
CE
LRMS
4
WN
pX.509
(DN, pFQAN, <sFQAN>)
R/W access
initiate Trf
SE
5
SE
VO
Req: changing with time
Central Services
Sites
Req: local site control

1. Virtual Organization

1. **VO needs to add “attributes” to the user**
   - Very simple concept: groups and roles
   - Simple administration tool

2. **Different use cases:**
   - Production / analysis / software manager jobs
   - Pilot jobs

3. **Questions:**
   - Is VOMS groups/roles enough?
     - E.g.: Assign a value to an attribute, e.g. Priority = 3
   - Should a user have multiple roles?
   - Should a user be able to choose which groups in proxy?
   - Why build tie group and role together?

   - What kind of information does the VO want to pass along to the user?
   - What kind of information shall be user specify at submission/access time?

2. Central Services (RB, IS)

1. **Feedback RB - CE (for push model)**
   - No synchronization of access rules between RB and CE
   - “bad” matchmaking
   - “unfavorable” matchmaking
   - No detailed view inside LRMS for a given VO (VOview ?)

2. **But: IS is mainly for service discovering**
   - Has limited capabilities for giving complete view inside CE

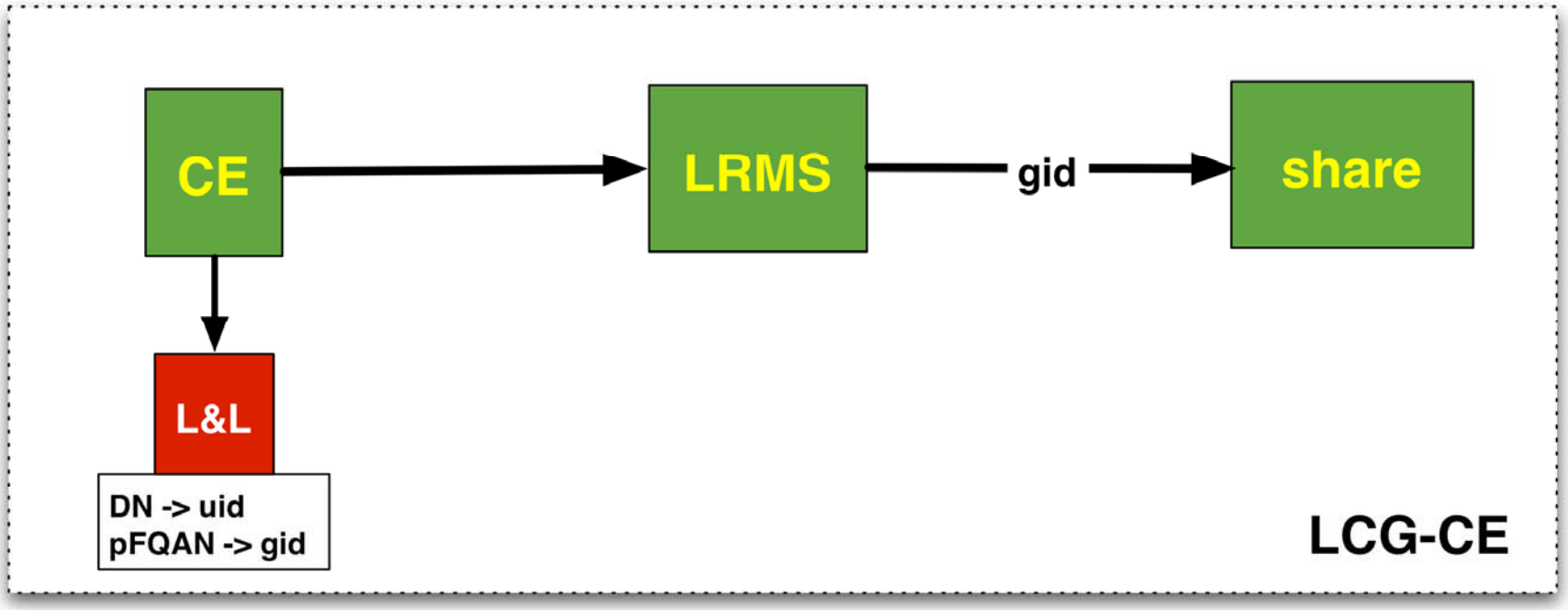
3. **Pull model:**
   - How does CE know which RB to pull from?
   - Does that really solve anything?

4. **Requirements:**
   - Consistent policy needed between RB and CE
   - Should RB pass along information about its decision to CE?

3. Computing Element (CE)

1. **Sites want to authorize the user based on a set of attributes**
   - DN/FQAN --> uid/gid(s) --> share LRMS
   - Connect authZ info with scheduling
     - Shouldn't they be completely separated?
   - Site administrators want to
     - retain complete local control
     - Simple management
       - *Consider >1 CE per site*
     - Clearly understand the mapping to uid/gids
   - VOs want "intelligent" scheduling at the site
     - Mapping of FQANs sometimes statically, sometimes dynamically

Computing Element (LCG-CE)

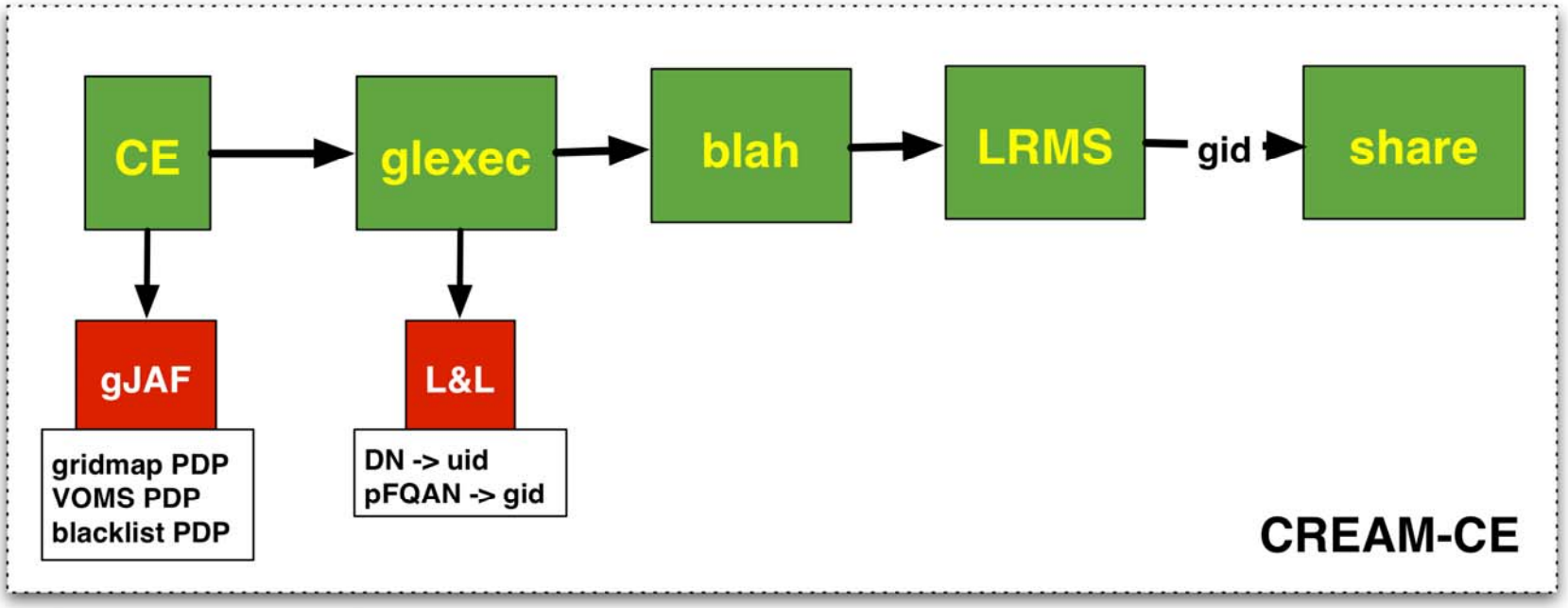


- **Should L&L return uid/gid or uid and <gid's> from which a scheduler can choose?**
- **L&L: first match of pFQAN counts**

- **Comment: see O.Koeroo's talk on further development of L&L**

L&L = LCAS/LCMAPS

Computing Element (CREAM-CE)

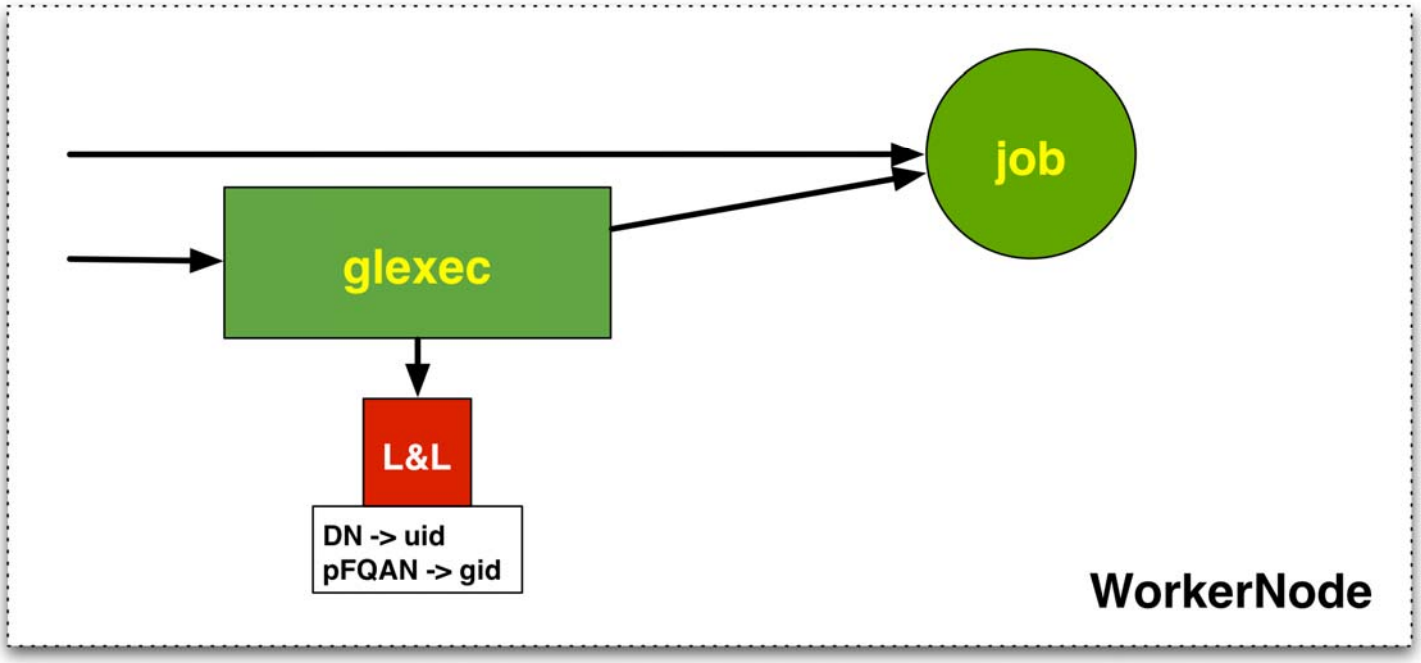


- Same comments as for LCG-CE
- Do we need two authZ frameworks?
- Should glexec receive a token containing the authZ info?

Computing Element (G-PBox)

- **Synchronization RB - CE**
- **Uses XACML**
  - Promise of more complex policies in consistent way
  - “hard to read” -> acceptance by sites?
- **Policy change**
  - From VO -> CE
  - CE -> VO
  - What mechanism is really needed here?
- **If GP-Box should become part of standard gLite distribution within EGEE-III, then we need to decide this soon**

4. Worker Node (WN)



- **Synchronization of mapfiles within a site**
- **Should job write to SE with same/different pFQAN**
  - Different access rights and quotas of SE
  - Example: run as /atlas/production but store as /atlas/switzerland-store
- **Comment: see O.Koeroo and D.Groep's talk**

5. Storage Element (SE)

- **2 Use cases:**
  - User/WN writes/reads file
  - File transfer between two sites
- **DPM, dCache, Castor….**
- **DPM: (consider only voms proxy)**
  - DN -> (virtual) UID
  - pFQAN -> (virtual) GID
    - considers all FQAN for read access
    - No wildchar support
  - ACL support (in addition to uid/gid)
  - Besides “pure” FAQN authZ: include quotas
    - Including hierarchical order?

General Comments

- **FQAN matching:**
  - Inconsistent between services:
    - First match only / all possible matches
  - With/without wildchars
  - Documentation and reference library available now
  - Need to review every service?

- **Use of proxies:**
  - Currently proxies can do everything (exception restricted proxy)
  - Specify in advance what a proxy is allowed to do?
    - DM operations, job submission
    - Pilot jobs

Summary

Next steps:

1. Draft of authZ study by December
2. Finalize in January