Study on Authorization

Christoph Witzig, SWITCH
(witzig@switch.ch)

GDB Oct 10, 2007

www.eu-egee.org

Information Society and Media

Outline

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

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
- **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

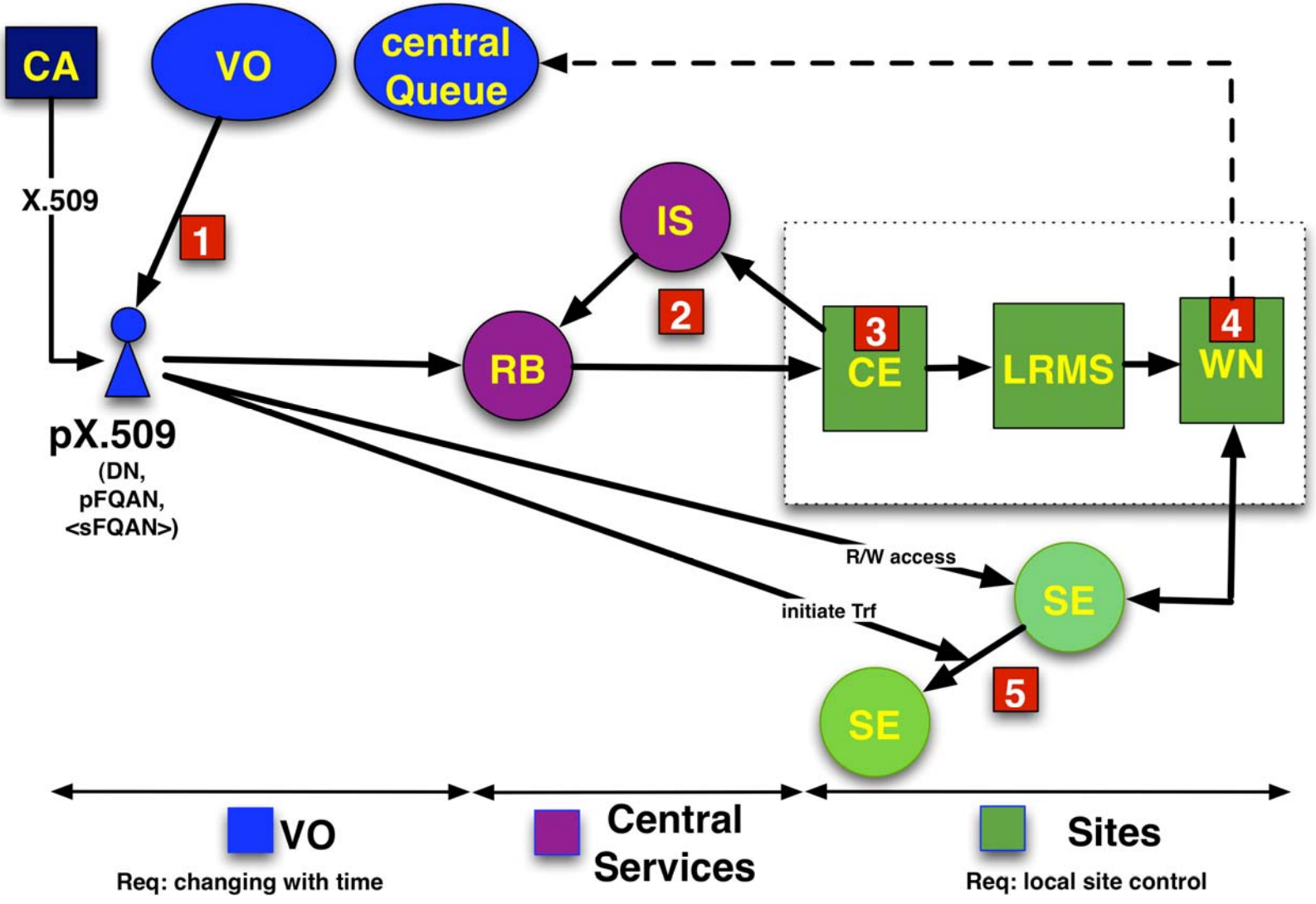
List of priorities in order (as approved by TCG):

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,*
      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. **VO wants to add “attributes” to the user**
   - Is VOMS groups/roles enough?
   - What kind of information does it want to pass along to the user?
   - What kind of information shall be user specify at submission/access time?

2. **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
     - Clearly understand the mapping to uid/gids
     - Simple management
       - *Consider >1 CE per site*
   - VOs want “intelligent” scheduling at the site
     - Mapping of FQANs sometimes statically, sometimes dynamically
   - Change of user at WN (pilot jobs)

3. RB

- Needs info from sites for “push” model
  - IS is mainly for service discovering, has limited capabilities for giving complete overview of situation at CE
  - How should situation at CE be published?
  - Pull model wanted - which problems does that solve/raise?
- Should not send job to CE where it will be rejected (must be “site policy aware”)
- Consistent policy needed between RB and CE

4. DM

- Access rules (security) models differ in DM
- Should the same FQAN be taken for DM operation as for job submission?

General:

- Consistent rules in middleware required
- How should policy changes be propagated?