Study on Authorization

Christoph Witzig, SWITCH
(witzig@switch.ch)

JRA1 Oct 25, 2007

www.eu-egee.org

Information Society and Media

Outline

- **Introduction**
  - Goal of this study
  - Priorities of the study
- **Requirements from the experiments and sites**
- **First ideas --> discussion**

  Note: These are ideas and I am now hoping for feedback (in this meeting or by email afterwards)

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 recommendations and a 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**

Disclaimer

In the following I will present some first initial ideas to be discussed

Some of them may end up being recommendations, some may not

Feedback from developers most welcome

Outline

- **Introduction**
  - Goal of this study
  - Priorities of the study
- **Requirements from the experiments and sites**
- **Review of existing authorization mechanisms**
- **First ideas --> discussion**

Requirements from VOs

- **So far spoke with CERN experiments**
  - There are other VOs than LHC experiments
- **Personally I believe many new requirements from VOs will appear once physics data is available**

Requirements from VOs (2)

- **They want a simple system that works and gives them most of the control of the system**
- **< 50 groups, a few roles**
- **Roles:**
  - production: to run production jobs
  - lcgadmin: to install software
  - soft-valid: to run monitor jobs
- **Groups:**
  - Currently very few groups
  - I would expect this will change once we have production data

Requirements from VOs (3)

- **Differerent kind of jobs:**
  - Read data from SE, process and write data to SE
  - Need access privileges for software installation at sites
  - Manipulate data in SE and catalogues which may require special priviledges

Requirements from Sites

- **They want a simple system that gives them all of the control of their site**
- **From their perspective they want minimal installation and maintenance while supporting VOs**
- **They want**
  - simple, clear rules for installation and maintenance
  - configuration files that are simple to set up, change rarely and are intuitive to understand
  - understand and control user mapping
  - have a grasp what the user jobs are doing (security wise)
- **We should be aware that the site administrators community is rather diverse**
  - Knowledge in grid ranges from expert to novice

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

Outline

- **Introduction**
  - Goal of this study
  - Priorities of the study
- **Requirements from the experiments and sites**
- **First ideas --> discussion**