Study on Authorization

Christoph Witzig, SWITCH
(christoph.witzig@switch.ch)

JRA1 AH February 22, 2008

www.eu-egee.org

Information Society and Media

Outline

- **Introduction**
  - Goal of this study
  - Priorities of the study
- **Presentation of recommendations**

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: CNAF, HIP, NIKHEF, SWITCH
- **Should specify the 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
- 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
- Period for comments until the end of February

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**

Focus

- **The priorities as well as the JRA1 budget determined the focus of the study, namely**
  - Rather improving and gently extending the current authorization framework than proposing a new, radically different authorization solution
- **Note:**
  - Recommendations reflect my impressions and to a certain degree also my personal preferences

Outline

- **Introduction**
  - Goal of this study
  - Priorities of the study
- **Presentation of recommendations**

Recommendations

- **Recommendations for**
  - Pattern matching rules
  - User Interface
  - CE
  - WMS
  - New Authorization Service
  - Data Management

Pattern Matching Rules (1/3)

- **Recommendation 1:**
- A standard library and a test suite should be developed, which implements the FQAN pattern matching rules. They should become part of the standard gLite distribution. Existing code should be modified to use this library wherever possible. Where this is not possible, the existing implementation should be tested against the test suite.

Pattern Matching Rules (2/3)

- **Recommendation 2:**

  The only supported wildchar should be the asterix character ("*"), and it should only be used

  - In the group string after the trailing slash
  - The "role=" string to denote all possible roles

- **Examples:**
  - /VO1/analysis/* OK
  - /VO1/analysis/*/role=production OK
  - /VO1/analysis/*/role=* OK
  - /VO1/*/higgs NOT OK
  - /VO1/analysis/?iggs NOT OK

Pattern Matching Rules (3/3)

- **Recommendation 3:**
- A command line tool, available on the WMS and CE, should print the authorization decisions for every package in the CE and WMS. The input parameter of this debugging utility can either be the primary FQAN or a proxy certificate.

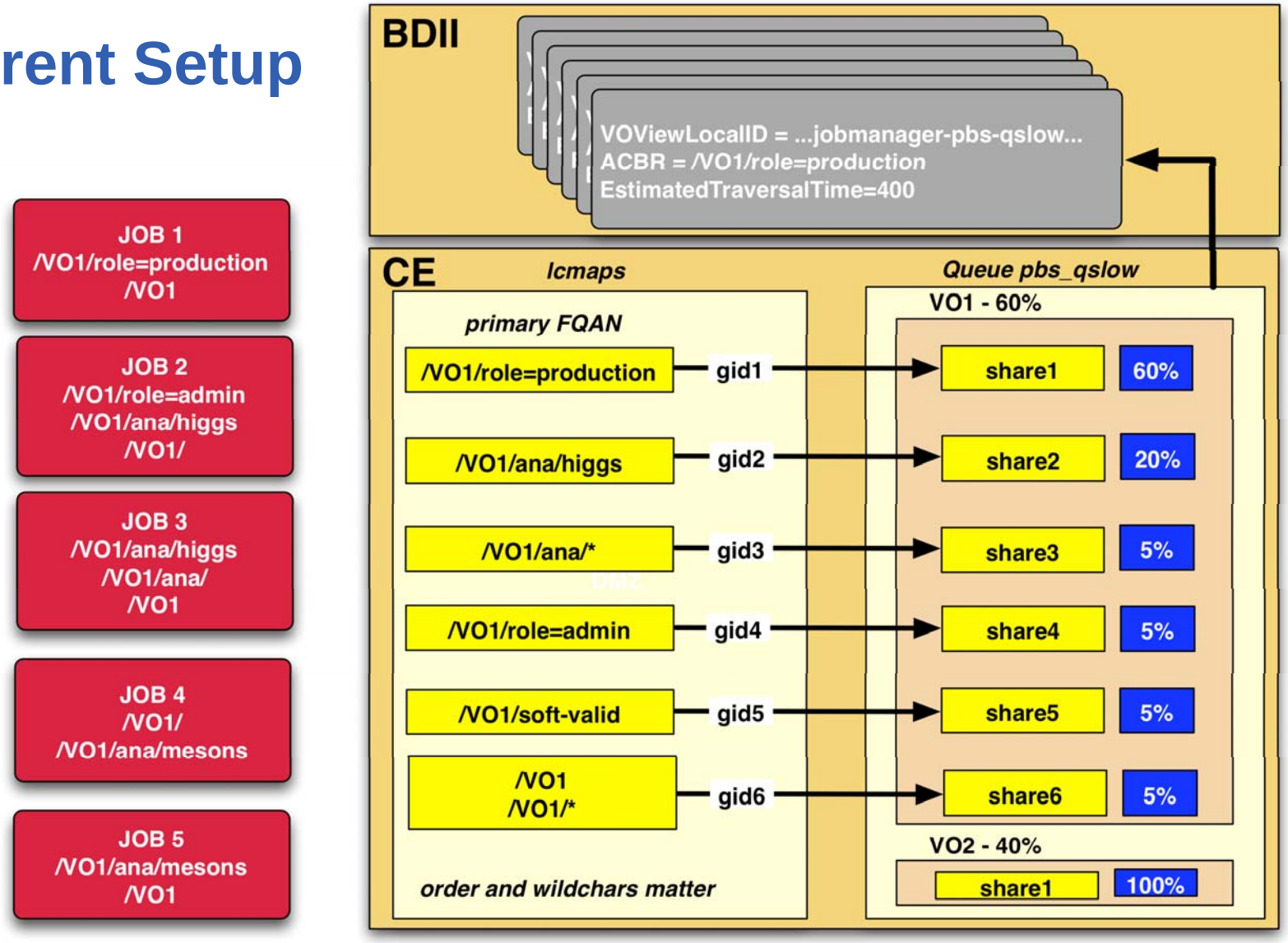
User Interface

- **Recommendation 4:**
- We recommend that the user shall be able to specify the FQAN to be used in the job submission either as a parameter in the JDL file or as a variable in scripts.

- Background:
  - **Currently only one primary FQAN for job handling and data management**
  - **Allows to submit jobs with one primary FQAN while another primary FQAN is taken for the data management**
  - **Implementing a flexible way to set the primary FQAN is hard (DM interfaces)**

CE (1/5)

Current Setup



CE (2/5)

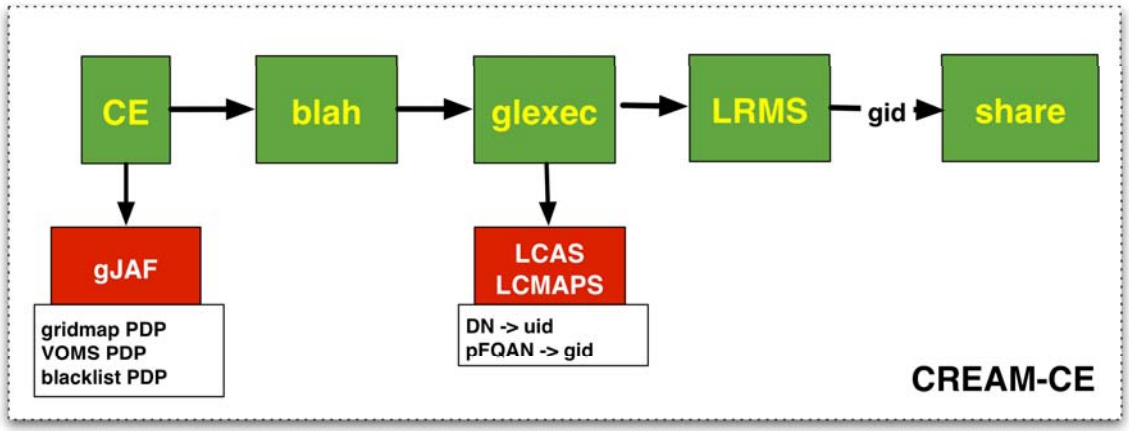
- **Recommendation 5**
- Instead of taking the first match, LCMAPS should return the GID corresponding to the most specific match. The most specific match is the match, which matches the most characters excluding any possible wildchar.

- Note: This replaces the current scheme in which the first match is taken

CE (3/5)

- **Recommendation 6**
- The gJAF framework should be abandoned and replaced with a simple authentication check of the certificate and a simple call-out mechanism to the new site authorization service.

- **Background:**



  - Doesn't make sense to have more than one authZ framework
  - gJAF will no longer be supported within EGEE-III
  - If we need a richer Java authZ framework, then the Globus authZ framework should be considered.

CE (4/5)

- **Recommendation 7:**

- VOViews should publish the entire information for assigning FQANs to shares
  - **The GIP and IS must make sure that all ACBR information, including possible wildchars, is published in the IS. Otherwise the WMS cannot do the matchmaking properly.**

CE (5/5)

- **Recommendation 8**

- The tight coupling between FQANs and shares at the CE should be replaced with a mechanism that allows the VO assign different types of jobs to different shares without site reconfiguration.

- See appendix (slides at the end)

- **Recommendation 9**
- The WMS should only consider one VOView per CE for a given primary FQAN. The selected VOView should be the one, whose ACBR is the most specific match for the primary FQAN.

- **Comment**
  - Verification on impact on matchmaking
  - May mean that not the best solution is taken at all times
    - E.g. another share is empty while the chosen shares (with the most specific match) is full
  - Alternative: WMS submits to VOView (not CE)

New authZ Service (1/2)

- **Recommendation 10**
- We do not recommend the use of the GP-Box in its current form in gLite for the following reasons:
  - **Handling of policy files**
    - **Copying between sites w/ accept/deny**
    - **Policy files includes user mapping**
  - **GUI-based management to edit and co-ordinate policies between sites is considered not suitable for large heterogeneous infrastructure such as EGEE**

New authZ Service (2/2)

- **Recommendation 11:**
- One component of the new authorization service is a policy decision point (PDP) that understands XACML policies. The design of this authorization service should take the existing GP-BOX code base into account and re-use or re-engineer components on an as needed basis.

- Comment:
  - **Design of new authZ service involves CNAF, HIP, NIKHEF and SWITCH**
  - **Work in progress**

Data Management

- **Recommendation 12**
- All storage element implementations should adopt the DPM authorization model.

- Comment:
  - This has already been decided.

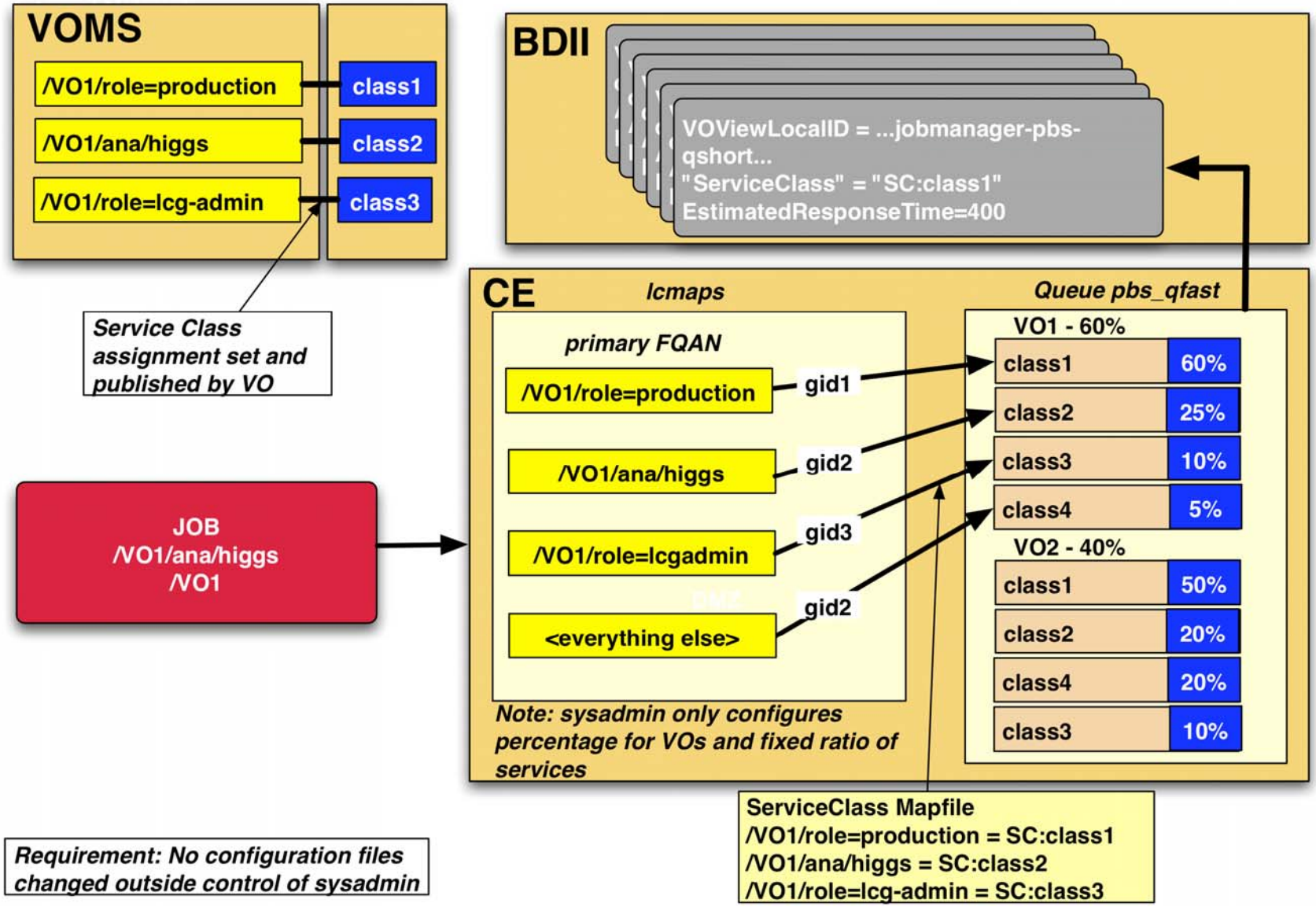
Decoupling FQANs and Shares (1/6)

- **Mapping *FQAN --> GID --> share* links the FQAN to the scheduling**

- **Sites tend to decide share between VOs**
- **VOs tend to decide share between types of jobs (e.g. FQANs)**

- **Sites need to be reconfigured by site admins if VOs wants to change the relative share of the FQANs**

Decoupling FQANs and Shares (2/6)



Decoupling FQANs and Shares (3/6)

- **Note: There are three issues here:**
  - Link: GID <--> share
  - Link: Scheduling <---> FQAN
  - VO has means to influence share usage dynamically (without the need for a local site reconfiguration)

- **These issues can be discussed separately**

Decoupling FQANs and Shares (4/6)

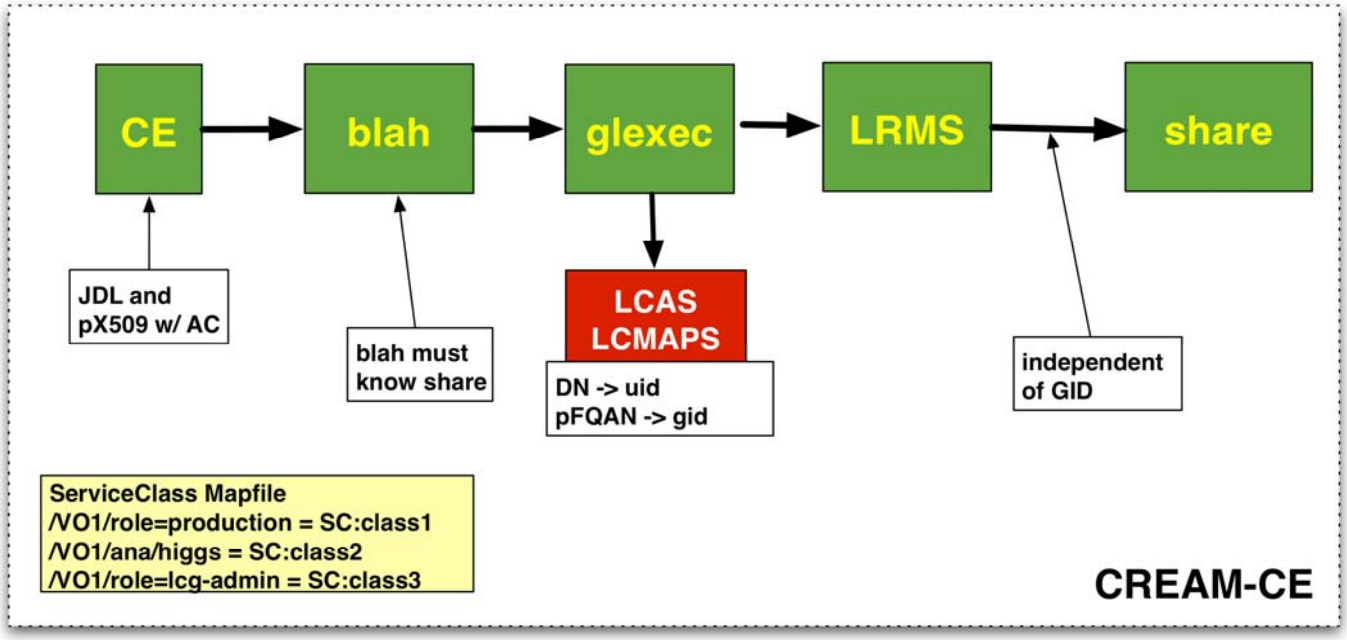
- **Several ways to implement this scheme**
- **Several components have to be adapted**
  - Feedback from middleware developers expected
- **Site retains full control**
  - Site can override the assignment of FQAN service class
- **Note: a site can define additional shares based on FQANs in order to fulfil site-specific requirements**

Decoupling FQANs and Shares (5/6)

- **Consequences:**
  - WMS:
    - MM must either consider FQAN or SC in ACBR:
      - *E.g. Search all VOViews with*
        1. ACBR = SC:class1 OR
        2. ACBR = VOMS:/atlas/analysis/higgs
      - *If both match, take the "most specific one" := FQAN*
      - *Every site has a default share*
  - BDII:
    - ACBR can accommodate SC:class1 as well as VOMS:/atlas/analysis in VOView

Decoupling FQANs and Shares (6/6)

- **Consequences II:**
  - CE: blah must know the share
    - As external input parameter
    - Extracts it from the proxy --> blah needs access to security code
    - External input preferred
      - *Relate to new authZ service*



Summary

- **Documents:**
  1. MJRA1.7 document: authorization in gLite:
     - § milestone Jan 31, 2008
     - § Feedback from JRA1 and others by Jan 25, 2008
  2. Document with recommendations
  3. Design for new authZ service: in progress
  - – **Note**: Document 1 and 2 decoupled from 3

- **TCG has to decide**
  - – How to proceed, set timeline for decision
  - – Accept, reject or defer decision on theses recommendations

Your input is needed now