



Enabling Grids for E-science

Study on Authorization

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

GDB February 6, 2008

www.eu-egee.org



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

- **Presentation of recommendations**

- **Task by C.Grandi to look into authorization (authZ) in gLite with the goal**
 - review authZ from end-to-end
 - to specify design for “authorization service” work item in EGEE-II/-III
 - EGEE-III proposal: authZ service: Nikhef, UvA, CNAF, 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**

- **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**
- **Request feedback from wider EGEE community in February**

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**

- **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

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

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

- **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.

- **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

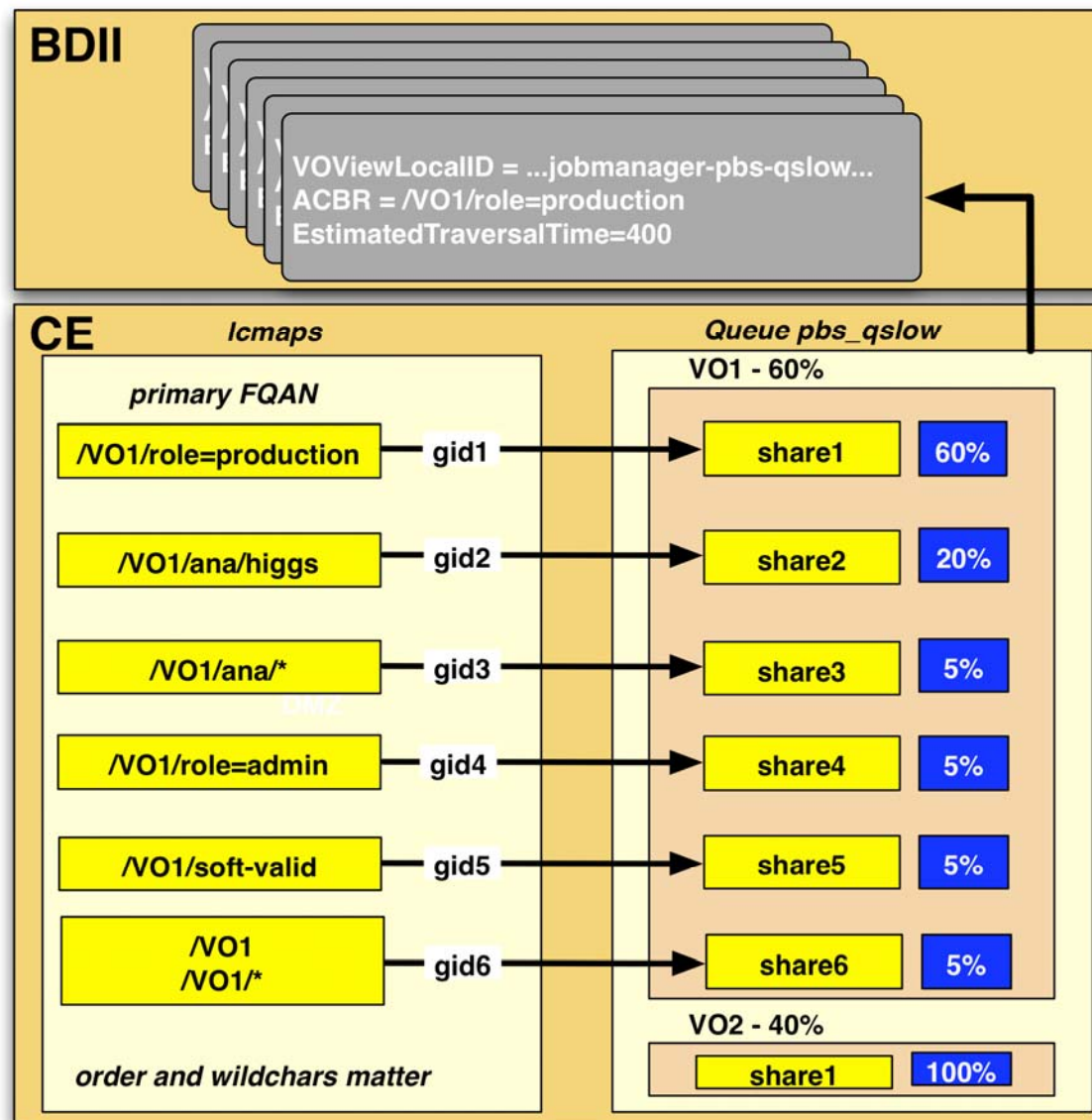
- **Examples:**

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

- **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.

- **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)**

Current Setup

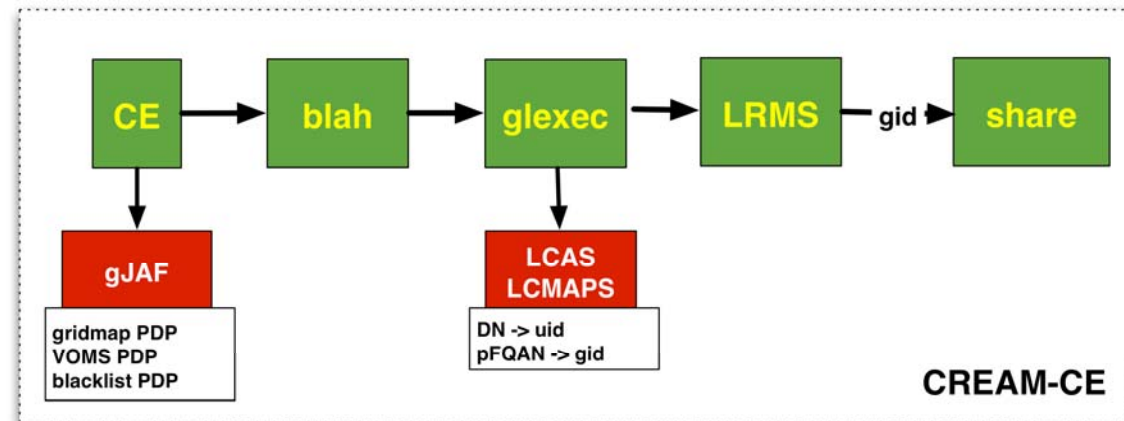


- **Recommendation 5**
- Instead of taking the first match, LCMAPS should return the GID corresponding to the most specific match. The most specific match is the match, which matches the most characters excluding any possible wildchar.
- Note: This replaces the current scheme in which the first match is taken

- **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.

- **Recommendation 7:**
- VOViews should publish all ACBR information necessary for match-making in the WMS
 - **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.**
 - **It does not mean that all the LRMS should be published**

- **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**

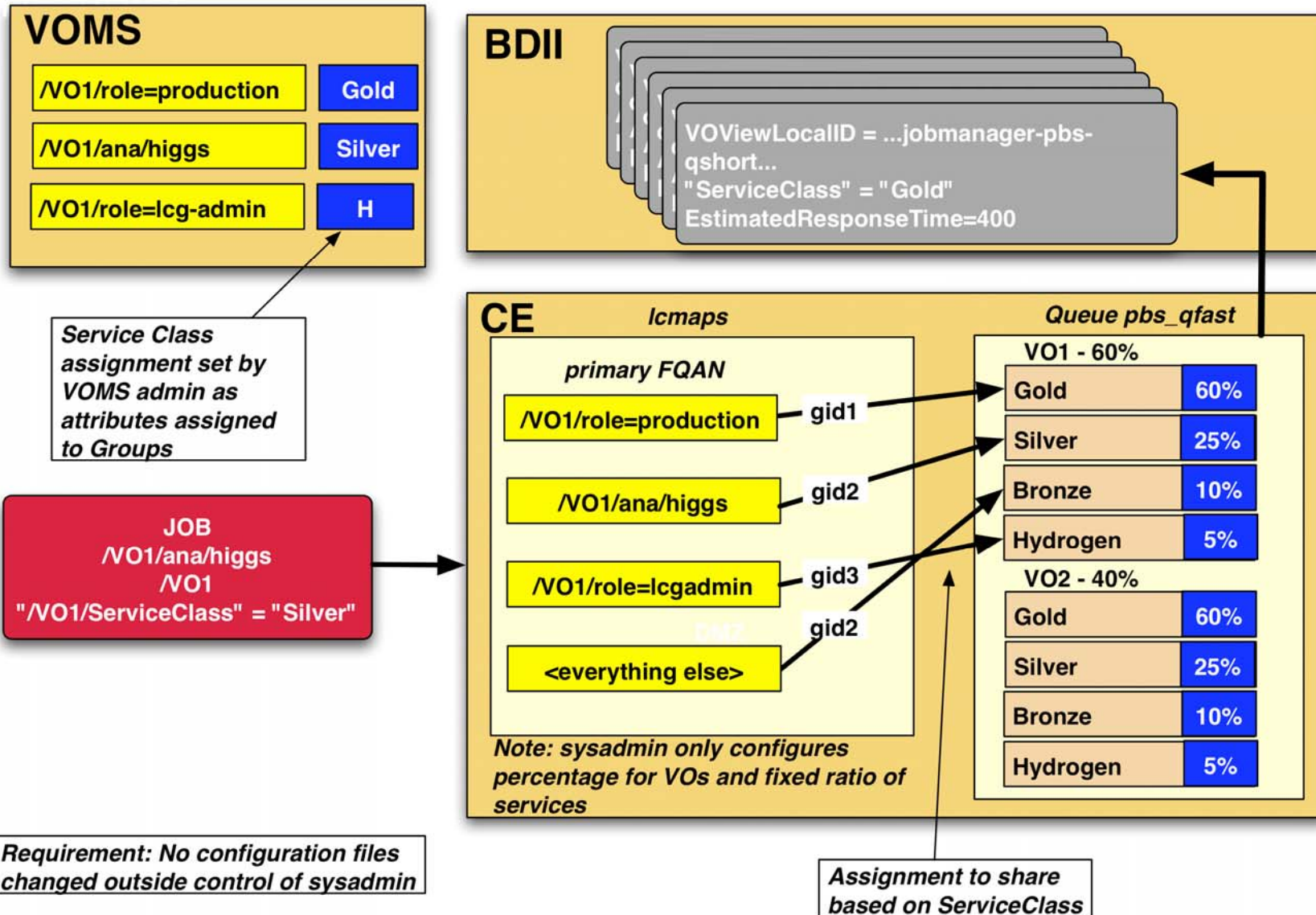
- Verification on impact on matchmaking
- May mean that not the best solution is taken at all times
 - E.g. another share is empty while the chosen shares (with the most specific match) is full
- Alternative: WMS submits to VOView (not CE)

- **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**

- **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**

- **Recommendation 12**
- All storage element implementations should adopt the DPM authorization model.
- Comment:
 - This has already been decided.

- 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
- Note: this is not only an authZ issue



- **There are really three issues coming together in this proposal:**
 1. Decoupling unix GID and scheduling
 2. Decoupling FQANs and scheduling
 3. Dynamic adjustment of assignment FQANs and shares
- **Note:**
 1. 1 can be viewed independently of 2 and 3
 2. Making 2 without 3 doesn't make sense (IMO)

- **Several ways to implement this scheme**
- **Several components have to be adapted**
- **Site retains full control**
 - Site can override the assignment of FQAN service class
- **Next steps:**
 - Feedback from
 - JRA1, sites, SAx needed to decide on this issue
 - Comments welcome until end of February
 - Revisit this issue in TCG in early March

- **Documents** <https://edms.cern.ch/document/887174/1> :
 1. MJRA1.7 document: authorization in gLite:
 - Description of authZ mechanisms in gLite
 - milestone Jan 31, 2008
 2. Document with recommendations
 - recommendations_authZ.doc
 3. Document with proposal decoupling FQANs - shares
 - recommendation_fqans_shares_v1.0.doc
 4. Forthcoming: Design for new authZ service: in progress
- **Feedback needed !**
 - Particularly on proposal decoupling FQANs - shares
 - Deadline end of February
- **TCG will review situation in March**