Authorization Issues for LCG

Simple use case

- Production manager needs a sepcial queue and extra storage space
- “almost”: the components can implement the use case, but only with slight modifications
  - who will do the modifications (EDG -> EGEE transition)
  - who co-ordinates the development (LCG Security or Deployment?)
- we should walk through this use case from the idea of having the “production” group in a VO to the actual mapping to a Unix group (if that happens?) at the site/resource

Authz issues

Site authorization issues, which can be standardized

- callout format
- module interface (LCAS modules?)
- wire protocol to the site local authz service
- discovery of the mappings (VO attr -> Unix group)

Alternatives, with slightly different goals

- LCAS/LCMAPS – rules based authz/mapping
- SAZ, LRAS – DB based mapping
- GUMS – DB based mapping

Other components

- GACL
  - will be merged into GridSite – concerns from NorduGrid
  - used in many EDG services as a library (L&B, SE, LCAS)
- edg-java-security – for Java services
- VOMS – couple of new features
  - default semantics for rules (driven by use case)
  - Attribute Certificate format
  - FQAN – common naming scheme across the components
-

Single VO

- Concerns about users actually using the multi VO possibilities
- VOMS client should make it “hard” to request multiple creds
- site/resource authorization modules should be able to restrict usage to a single VO

VO Policy

- VO has to publish its wishes/requirements to the sites
- simlple attr list or LCAS configuration?
- way of merging various VO policies at the sites
- “translating” VO policy for the site authorization tools
-
- Extra questions (e.g. what happens with the files):
    - how to handle group delete?
    - how to handle group rename?