

# Fabric Infrastructure and Operations



### **CASTOR** and VOMS

Tony Cass
Leader, Fabric Infrastructure & Operations Group
IT Department











- ACLs exist at the nameserver level
  - Based on uid/gid
- SRM v2 interface to set/change ACLs is implemented
  - Can add/delete individual entries, but owner cannot be changed.

CERN - IT Department CH-1211 Genève 23 Switzerland www.cern.ch/it









- GridFTP: support comes with GridFTP2
- rfio/rootd: local protocols; access control based on UID of process running on batch server
  - All access is via SRM, so:
    - File access not allowed: no TURL returned, so no access possible
    - File access allowed: TURL returned based on SE mapping of the DN & role, but ACL must also allow access to uid/gid of process on worker node







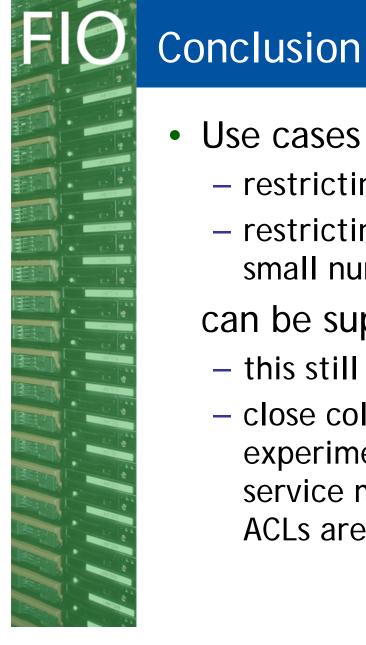




- Are in principle independent
  - But we are one site and we control both...
- CE needs pool of uids for a given VOMS role to be able to distinguish between jobs submitted by different DNs.
  - So SE ACLs have to list all possible mapped uids
    - These ACLs are set by the VO









# Use cases such as

- restricting write access to production users
- restricting read access to a subset of files to a small number of users

## can be supported. However,

- this still needs to be configured
- close collaboration will be needed between experiment production managers and FIO service managers to ensure grid mappings and ACLs are coherent.



