



Contribution ID: 409

Type: poster

## Mapping GRID to Site Credentials using GUMS

*Wednesday, September 5, 2007 8:00 AM (20 minutes)*

Identity mapping is necessary when a site's resources do not use GRID credentials natively, but instead use a different mechanism to identify users, such as UNIX accounts or Kerberos principals. In these cases, the GRID credential for each incoming job must be associated with an appropriate site credential. Many sites consist of a heterogeneous environment with multiple gatekeepers, which can make control and security difficult. Therefore, a single site-wide usage policy is desirable. GUMS (Grid User Management System) is such a Grid Identity Mapping Service providing a single site-wide usage policy. It was designed to integrate with the site's local information services (such as HR databases or LDAP) and with GRID information services (such as VOMS). When a request comes in to a gatekeeper, the gatekeeper contacts the GUMS server to verify a user has appropriate membership (via VOMS, LDAP, or manual user groups), and if so, retrieves the mapping to the local identity (via shared group accounts, a pool of accounts, or a manually defined account). GUMS supports extended X509 certificates that include group membership and role, which influence the mappings. It provides a web interface for managing and testing the server as well as a command line tool. It is contained in the OSG RBAC infrastructure. GUMS has been improved to include a more comprehensive web interface, and we plan to implement recyclable accounts to ensure scaling. GUMS is well suited to sites needing secure and centrally managed GRID to site credential mapping capabilities.

**Primary authors:** Mr PACKARD, Jay (BNL); Mr HOVER, John (BNL)

**Presenter:** Mr PACKARD, Jay (BNL)

**Session Classification:** Poster 2

**Track Classification:** Grid middleware and tools