Requirements for Account Management in Grids

- Portal and application users need access to resources for data access and management, job submission, etc.
- Standard security mechanism is GSI (Grid Security Infrastructure) typically involves, creation of credentials for a new user, storage of a proxy in MyProxy by user, retrieval of proxy upon user login to portal and configuration of resources to accept credentials. (a complex process)
- Automate and simplify account request and creation process.
- Separate the security system from the portal. Hide all the complexity from the end user.
- Simplify the task of administrators by providing a mechanism to install and configure all the backend security components.
- Synchronization with distributed resources e.g. clusters.

GAMA Features

- Users request accounts through familiar web form.
- Processing account requests is easy, quick, and flexible.
- Single and secure sign-on to portal.
- Administrator manages security server through portal.
- Support multiple distributed portals with one centralized security server, using the Account Import functionality.
- Support non-portal clients: Java apps, Flash, Kepler, etc.
- Technology-agnostic API for talking to security server, allowing changes to server without changing clients.
- Setup automatic rules for account approval or denial.

GAMA 2.0 Features

- The core functionality of the server is made available by a set of application programming interfaces (APIs).
- API’s will be classified as public or private.
- Private API will be deployed as java library and hence will not be available for remote invocation.
- Implementation-agnostic architecture: no explicit reliance on MyProxy, CACL, CAS, etc. Accomplished through a plug-in architecture on GAMA server.
- Server operations customizable and expandable through a workflow like system that can execute arbitrary sequences of tasks for any operation.
- Support multiple sites on one GAMA server. Each site has local admin(s) responsible for managing user accounts for their site in GAMA.
- GAMA users may be given access from only one site or multiple sites.
- More refined administrative console with the capability to add custom plugins.
- Support for both CACL and Naregi CA software.
- Integration with cluster accounts. This feature will support synchronization of user accounts on portal with cluster resources.
- Decrease reliance on GridSphere for administrative functions.

How GAMA Works

- Install command-line security infrastructure on a dedicated, locked-down GAMA server. (wrapped as web services)
- Backend services and components installed and configured easily using the Rocks cluster management toolkit.
- Install GridSphere, GAMA portal services for submitting, managing account requests from users on a portal server.
- Configure GridSphere to automatically retrieve a proxy from the GAMA server when a user logs on to the portal.
- Users can now use the resources securely.

Reference:

GAMA used or evaluated in: BIRN, NBCR, Naregi (AIST), LOOKING, SEEK, CIMA Indiana University, Gemstone, CAMERA, Harvard Crimson grid, HPC Kasettsart University, ELETTRA (Multidisciplinary Synchrotron Light Laboratory, Italy), PRAGMA, Kepler, Optiputer, UK e-Science, etc.