caGrid Security Architecture Version 0.5
Life Sciences Grid Workshop @ GGF14
June 27, 2005

Stephen Langella

Ohio State University

langella@bmi.osu.edu

Agenda

- caBIG Overview
- Security Requirements
- Security Architecture Overview
- Security Architecture Core Components
  - Authorization Manager
  - Grid User Management Service
  - caGrid Attribute Management Service
  - Grid Virtual Organization Service (GVOS)
- Status and Future

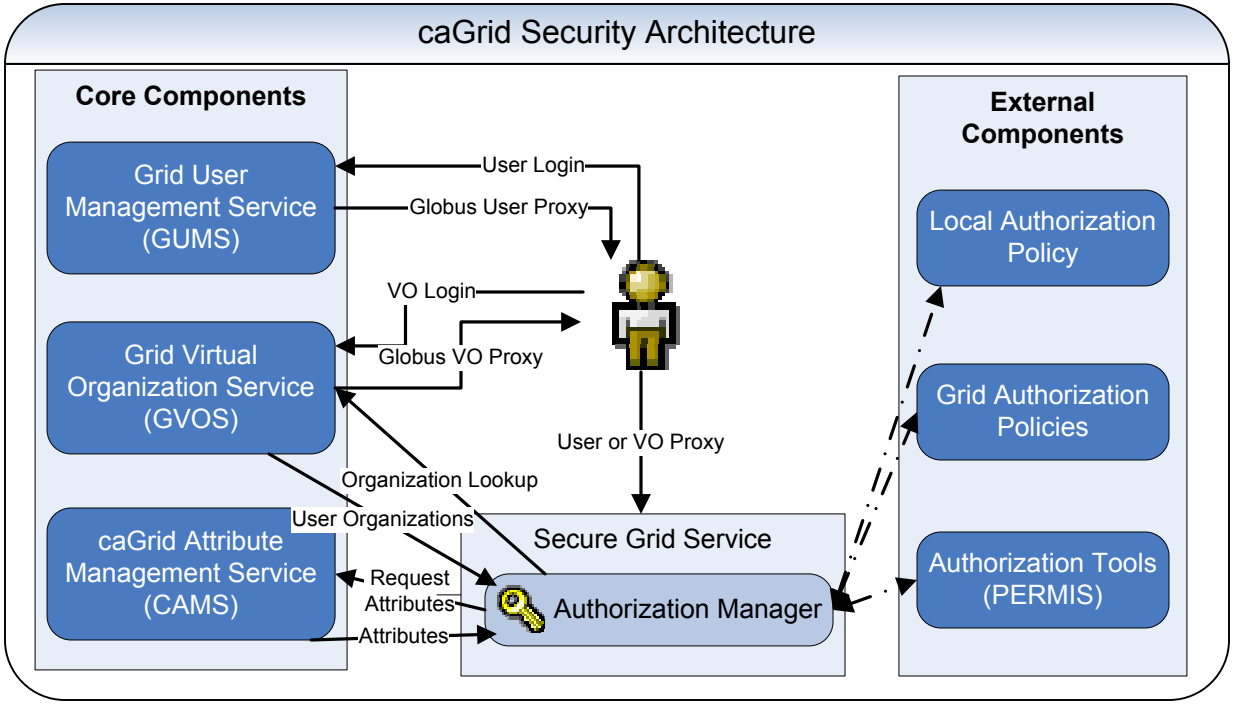
caBIG Overview

- **ca**ncer **B**iomedical **I**nformatics **G**rid (***caBIG™)***
  - Voluntary network or grid connecting individuals and institutions to enable the sharing of data and tools, creating a World Wide Web of cancer research. The goal is to speed the delivery of innovative approaches for the prevention and treatment of cancer. The infrastructure and tools created by caBIG™ also have broad utility outside the cancer community. caBIG™ is being developed under the leadership of the National Cancer Institute's Center for Bioinformatics.
- caGrid
  - Reference Grid implementation of caBIG
- More Information
  - https://cabig.nci.nih.gov

Security Requirements

- ***Secure Communication***
  - *Authentication* - Parties involved can be assured of one another identity
  - *Message Integrity* –Message sent by either party is guaranteed to same message when it is received.
  - *Privacy* – Communication between the two parties can only be interpreted by the two parties
- ***Single Sign On***
  - Users and Grid Services should have one method of authenticating themselves to the grid, all service in the grid should accept this method.
- ***Access Control on caBIG Services***
  - caBIG services should be able to determine, which users or services may access them.
- ***User/Organizational Attribute Management***
  - Services should have a method for determining the attributes of a requesting party. Such attributes may be needed to service the request, for example a username and password is needed to perform a query on a relational database on the party's behalf.
  - Attribute should be standardized such that they may be used across institutional boundaries.
- ***Delegation***
  - caBIG services, should be able to interact with other caBIG services on a user's behalf.
- **User/Organization Management**

Big Picture


caGrid Security Architecture
Core Components
External Components
Grid User Management Service (GUMS)
Grid Virtual Organization Service (GVOS)
caGrid Attribute Management Service (CAMS)
User Login
Globus User Proxy
VO Login
Globus VO Proxy
User or VO Proxy
Organization Lookup
User Organizations
Request Attributes
Attributes
Secure Grid Service
Authorization Manager
Local Authorization Policy
Grid Authorization Policies
Authorization Tools (PERMIS)

Security Architecture Components

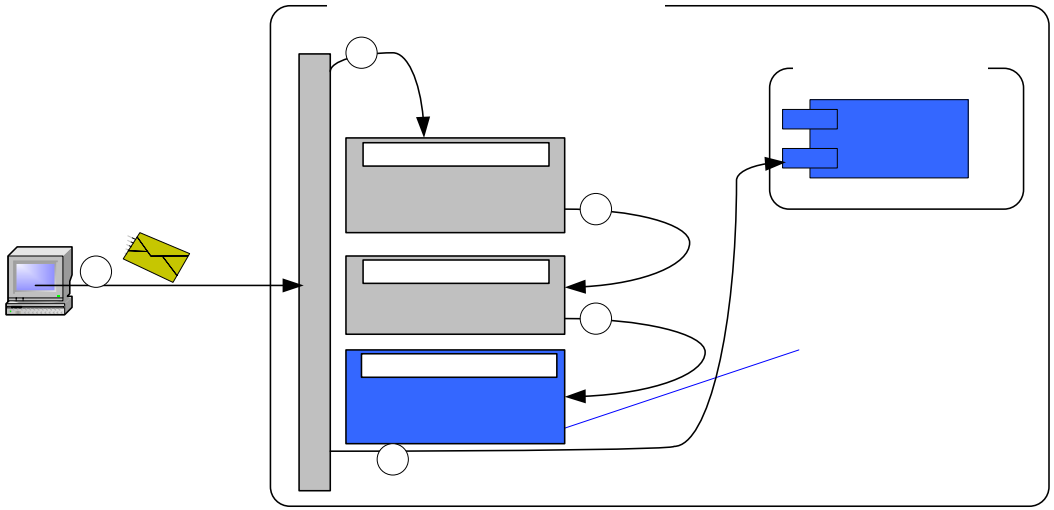
- Core Components
  - GSI
  - Authorization Manager
  - Grid User Management Service (GUMS)
  - caGrid Attribute Management Service (CAMS)
  - Grid Virtual Organization Service (GVOS)
- External Components
  - Local Authentication/Authorization Systems
  - General Authorization Systems (ie PERMIS)
  - Grid Authorization Services

Authorization Manager

- Authorization Manager Overview
  - Extends the Globus Toolkit to provide more dynamic authorization
  - Abstracts away some globus related details.
  - A a general interface in which a caGrid service calls to determine if a user is authorized to perform operation X on resource Y.
  - A caGrid service is configurable to use a specific implementation of the AuthorizationManager interface.
  - Authorization Managers can be used to integrate grid security with external authentication/authorization systems.
    - Local/Legacy systems
    - Other authorization systems.
  - Authorization Managers enable authorization in a diverse ever changing dynamic environment.
    - **ie.** Allow this user access from his work computer during work hours and from his home computer during non work hours.

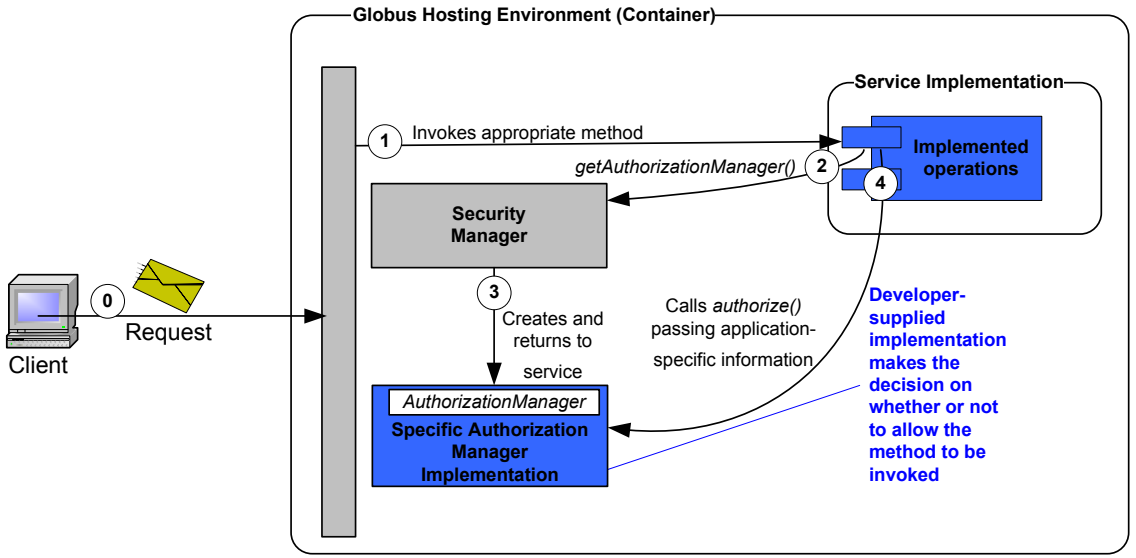
Authorization Manager

- Authorization Manager's Globus3.2.1 Integration
  - Add Additional ServiceAuthorization implementation to SOAP Workflow (CABIGServiceAuthorization)
    - Maps Globus Authorization into calls into the Authorization Manager
    - Instantiates and Authorization Manager and calls into it.
  - Provides operations level authorization
  - Does NOT provide resource level authorization.



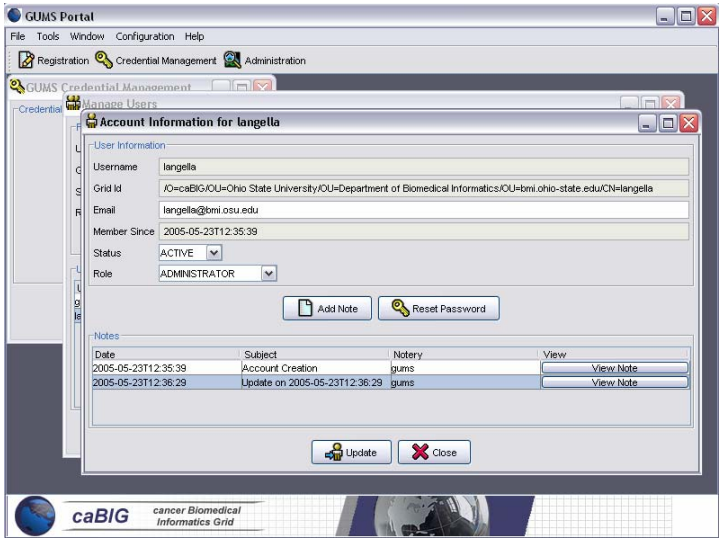
Authorization Manager

- Authorization Manager and Resource Level Authorization
  - Authorization Manager is obtained and called from the grid service implementation
  - Allows application specific decisions to be made on resources etc.



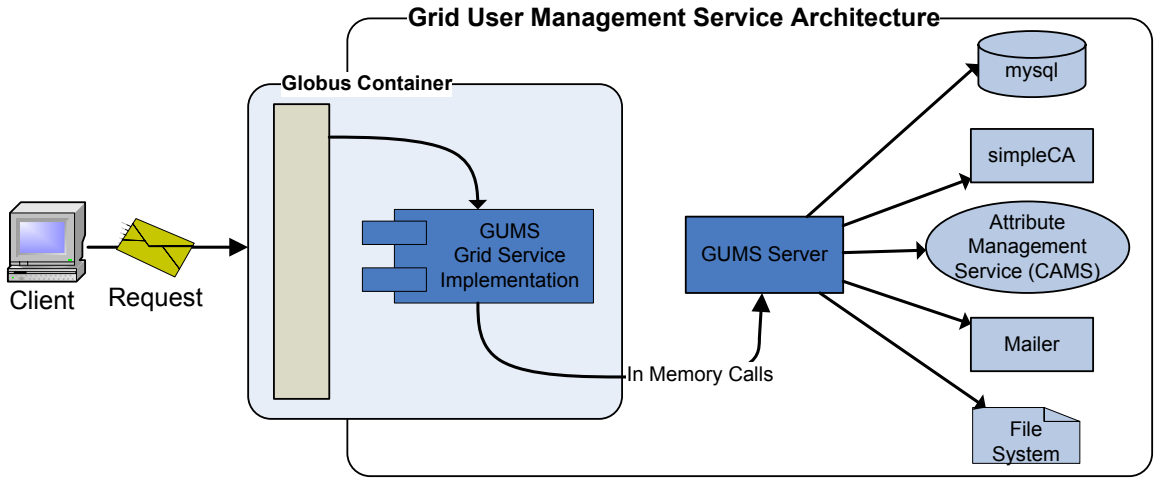
Grid User Management Service

- Grid User Management Service (GUMS)
  - Grid Service that coordinates the process of creating and managing grid users.
    - Manages the simpleCA Certificate Authority
    - Manages Grid certificates for users.
  - Provides a method for users to register for a grid account.
  - Administrators may specify and define attributes that are required to be supplied by the user at the time of registration
  - Administrators can approve or reject a users application.
    - Approval creates an account, which includes the generation of grid credentials.
  - Users authenticate with the system via username and password.
  - Allows users to create/get grid proxies from anywhere.



Grid User Management Service

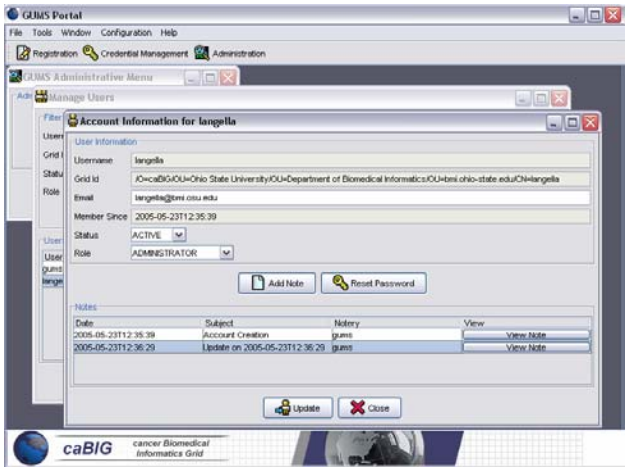
- Architecture Overview
  - Runs as a Globus Grid Service.
  - Grid Service implementation interacts with Server through in memory server API calls.
  - Uses globus simpleCA for Certificate generation and management.
  - Utilizes the Attribute Management Service (CAMS) to store required attributes.
  - MySQL is used for account persistence.
  - Requires an SMTP mail server for mailing user's information regarding their account.



Grid User Management Service

- Globus Client
  - GUMS can be interacted with through the Globus Client API
- GUMS Client API
  - Rich API for interacting with GUMS, consist of three core classes.
    - **GumsRegistrationClient** – Implements Registration interface, provides operation for registering with GUMS.
    - **GumsUserClient** – Implements User Interface, provides method for performing user operations on GUMS (Create,Get,Destroy Proxy).
    - **GumsAdministratorClient** – Implements Administrative Interface, provides methods for administering GUMS.

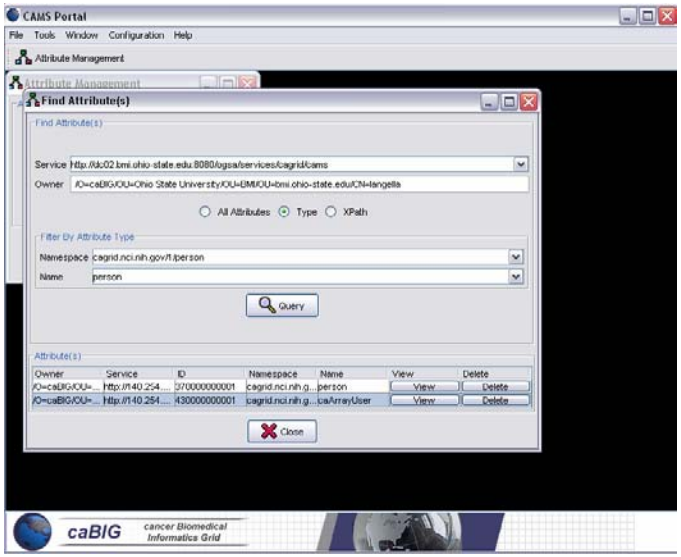
Grid User Management Service



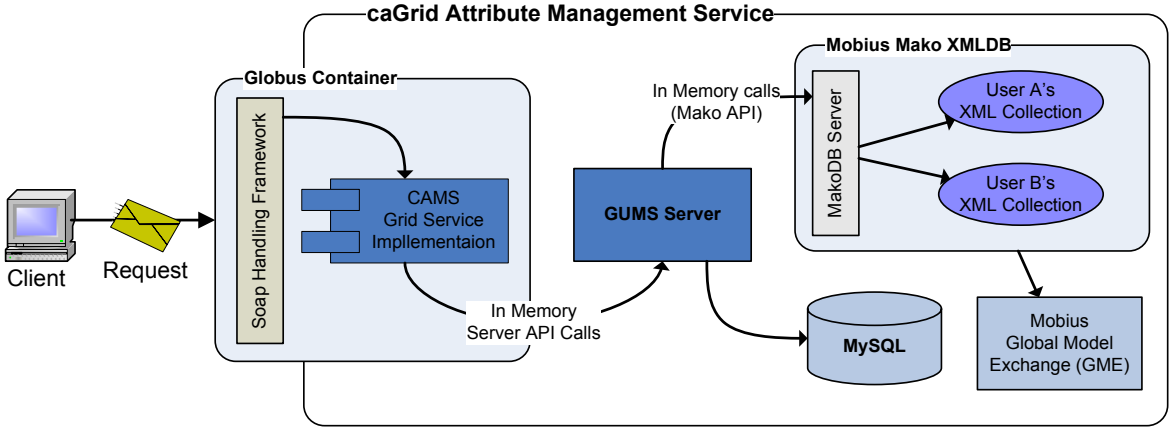
- Command Line Tools (Uses Client API to allow command line functionality)
  - **GridProxyInit** – Creates and obtains a proxy for GUMS and stores it locally for use with other Grid Services.
  - **GetGridProxy** – Gets an already existing grid proxy on GUMS and stores it locally for use with other Grid Services.
  - **GridProxyInfo** – Gets information about a user's existing grid proxy on GUMS.
  - **GridProxyDestroy** – Destroys the user's proxy both on GUMS and locally.
- GUMS Portal GUI
  - Graphical User Interface for interacting with GUMS.
    - Built using the GUMS Client API.

caGrid Attribute Management Service (CAMS)

- caGrid Attribute Management Service (CAMS)
  - Manages attributes for users/virtual organization.
  - Users/Services may request attributes of a given user or VO.
    - Requestor must be authorized to view the requested attributes.
  - Authorization Managers can use CAMS for requesting attributes for making dynamic decisions.
    - ie. If tom can access a given resource from his work computer from 9-5 and from his home computer all other times and the current time is 2pm, I can grab the MAC address of Toms work computer from the attribute service and compare it to the MAC address making the request to determine if Tom is at his work computer.



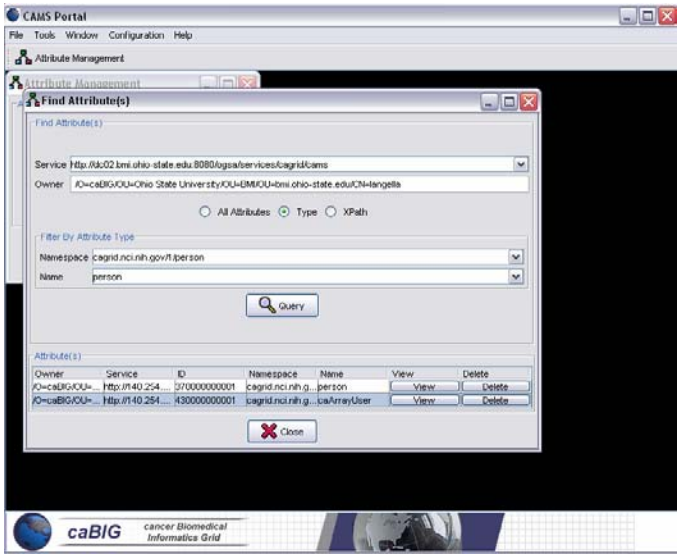
caGrid Attribute Management Service



- Runs as a Globus Grid Service
- Grid Service implementation makes calls into the CAMS server API
- CAMS uses Mobius Mako XML DB for storing attributes.
  - User attributes are organized into XML collections
  - An XML collection is created for each user.
  - Mako uses the Global Model Exchange to resolve XML schemas for validating attributes.
- CAMS uses mysql to manage access control permissions on attributes.

caGrid Attribute Management Service

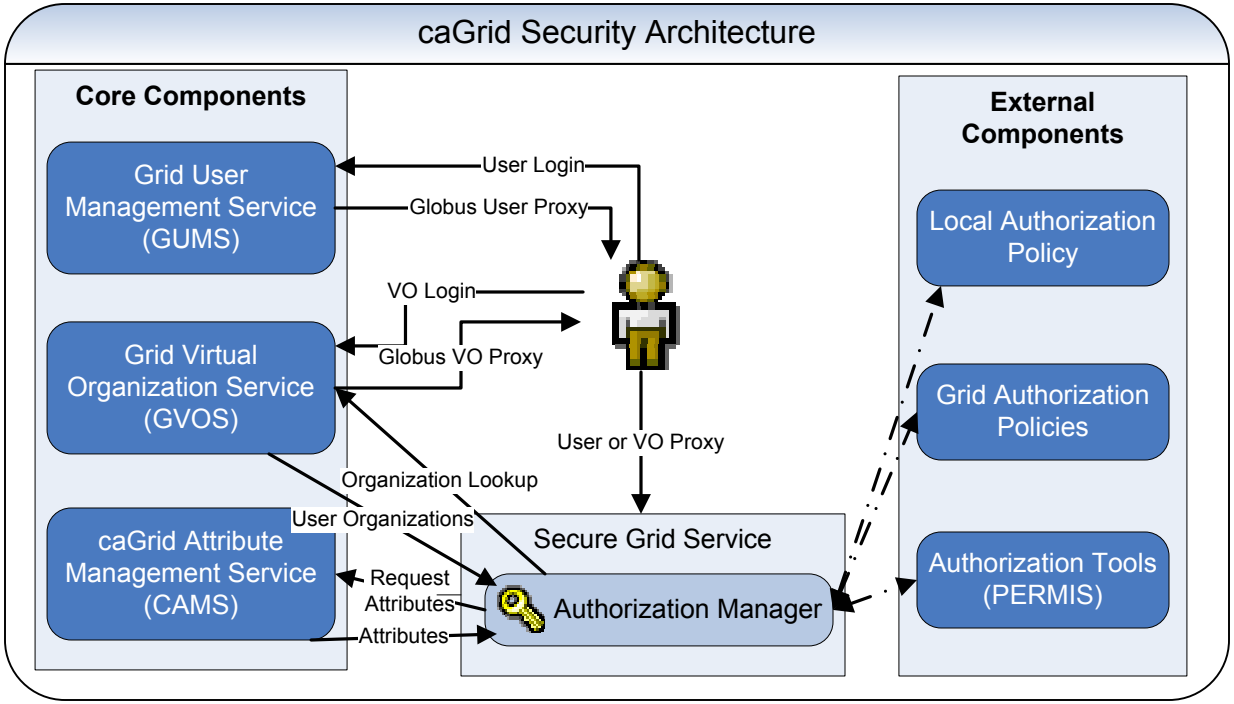
- Globus Client
  - CAMS can be interacted with through the Globus Client API
- CAMS Client API
  - Rich API for interacting with CAMS.
  - **AttributeManagementClient**
    - Complete implementation for invoking all CAMS operations.
- CAMS Portal
  - Graphical User Interface for interacting with CAMS.
  - Uses CAMS Client API to invoke CAMS operations.



Security Architecture Core Components

- Grid Virtual Organization Service (GVOS)
  - Manages a set of virtual organizations.
  - Administrators can create Virtual Organizations
  - Virtual Organization consist of users and other Virtual Organizations
  - Users which are members of a VO can request a proxy for the VO.
  - Users/Services can enquire whether or not a user is a member of a VO.

Big Picture


caGrid Security Architecture
Core Components
External Components
Grid User Management Service (GUMS)
Grid Virtual Organization Service (GVOS)
caGrid Attribute Management Service (CAMS)
User Login
Globus User Proxy
VO Login
Globus VO Proxy
User or VO Proxy
Organization Lookup
User Organizations
Request Attributes
Attributes
Secure Grid Service
Authorization Manager
Local Authorization Policy
Grid Authorization Policies
Authorization Tools (PERMIS)

Status and Future

- Authorization Manager
  - Prototype caGrid0.5 Deliverable
  - Initial Prototype Completed
  - July 2005
    - Test and Refine Prototype
    - Integration with caGrid0.5 Framework
- Grid User Management Service (GUMS)
  - Prototype caGrid0.5 Deliverable
  - Initial Implementation Completed
  - July 2005
    - Test and Refine Implementation
    - Integrate with Prototype Attribute Management Service

Status and Future

- Attribute Management Service
  - Prototype caGrid0.5 Deliverable
  - Initial Implementation Completed
  - July 2005
    - Complete Design of Prototype
    - Implement Prototype
    - Integration with caGrid0.5 Framework
- Grid Virtual Organization Service (GVOS)
  - NOT a caGrid0.5 Deliverable.
  - Summer/Fall 2005
    - Review Existing Technologies
    - Design Prototype
    - Implement Prototype
    - Integration with caGrid Phase II Framework

caGrid Team

- **National Cancer Institute**
  - **Peter Covitz**
  - **Krishnakant Shanbhag**
  - Tara Akhavan
- **SAIC**
  - Manav Kher
  - William Sanchez
  - Ruowei Wu
  - Jijin Yan
- **Ohio State University**
  - **Shannon Hastings**
  - **Tahsin Kurc**
  - **Stephen Langella**
  - **Scott Oster**
  - **Joel Saltz**
- **Booze | Allen | Hamilton**
  - **Manisundaram Arumani**

*** **Blue** denotes members of the security architecture sub team. ***