

WP6: Grid Authorization Service

Workshop in Olomouc

Marcin Adamski, Michał Chmielewski,
Sergiusz Fonrobert, Jarek Nabrzyski
and Tomasz Ostwald

**Poznań Supercomputing
and Networking Center**

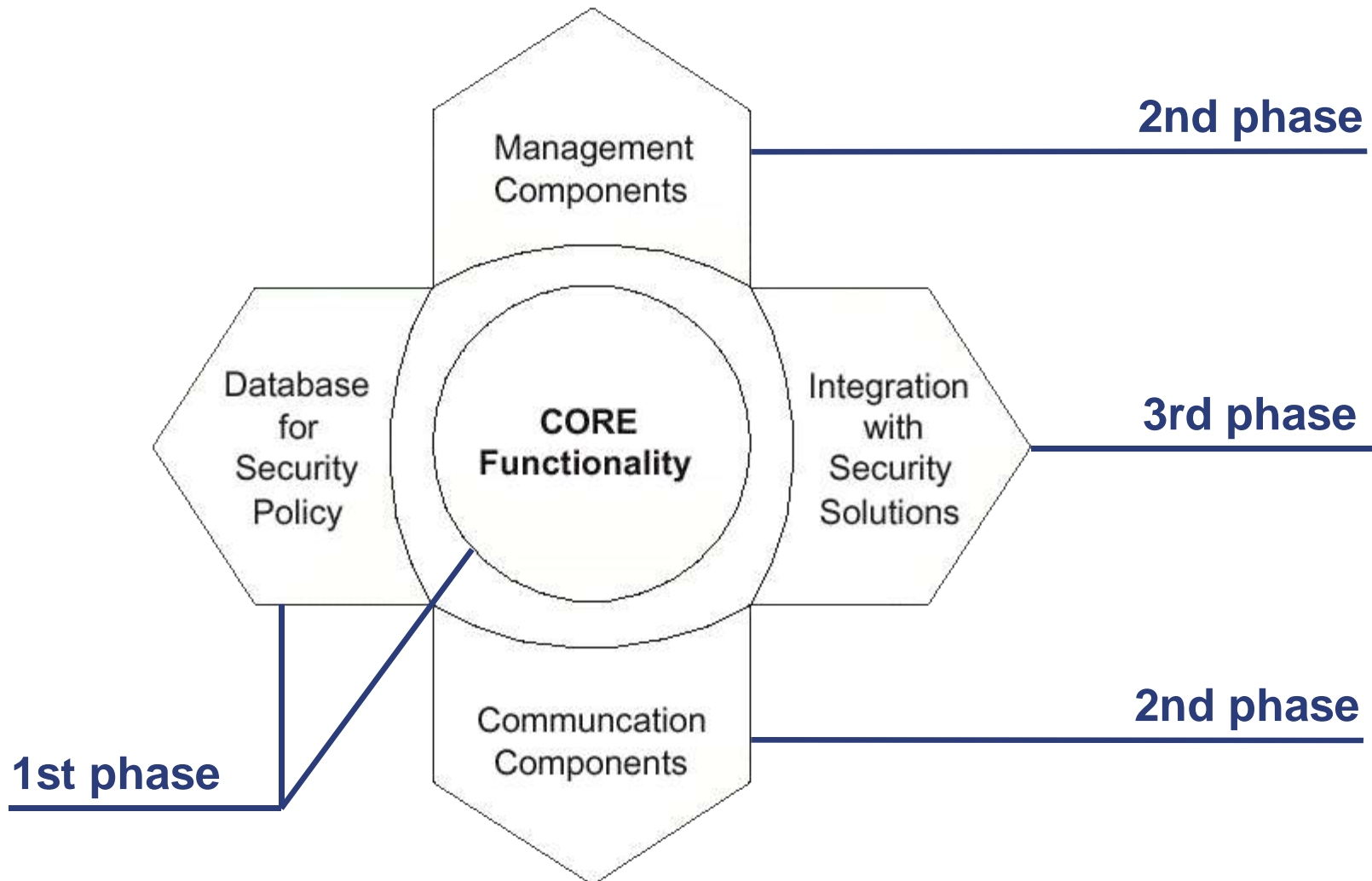
Presentation Overview

- About security in the GridLab Project
- General design of the Grid Authorization Service
Current implementation status
- Plan for the Olomouc meeting

- Security in Grid environments is a significant and still open problem
- The primary goal of Security Workpackage in the GridLab project is to create flexible and universal Grid Authorization Service (GAS)
- The secondary goal is to provide general support to other workpackages in solving detailed technical problems related to the security issues

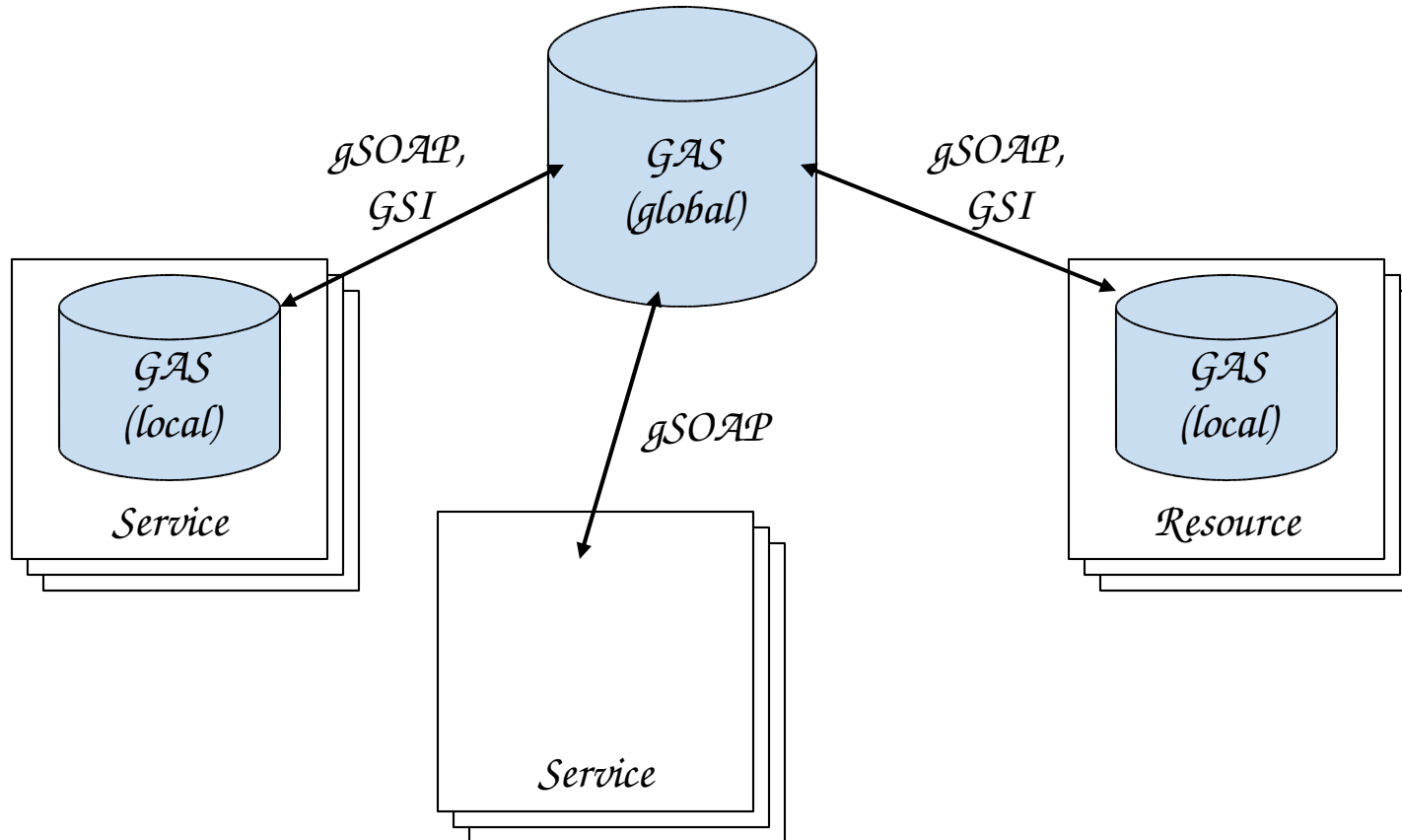
- The main requirement is flexibility of the Grid Authorization Service (GAS)
- The GAS is about to provide universal way of defining security policy for the whole Grid, independent of technologies used at lower levels
- It should be able to implement most security models for Grids and use many different scenarios at the same time
- It should support many different security technologies (ex. GSI and gSOAP, various types of authentication)
- It has to be secure and stable implementation (the GAS is considered as a trusted component of a security model)

The General Design



The GAS architecture

(local, global)





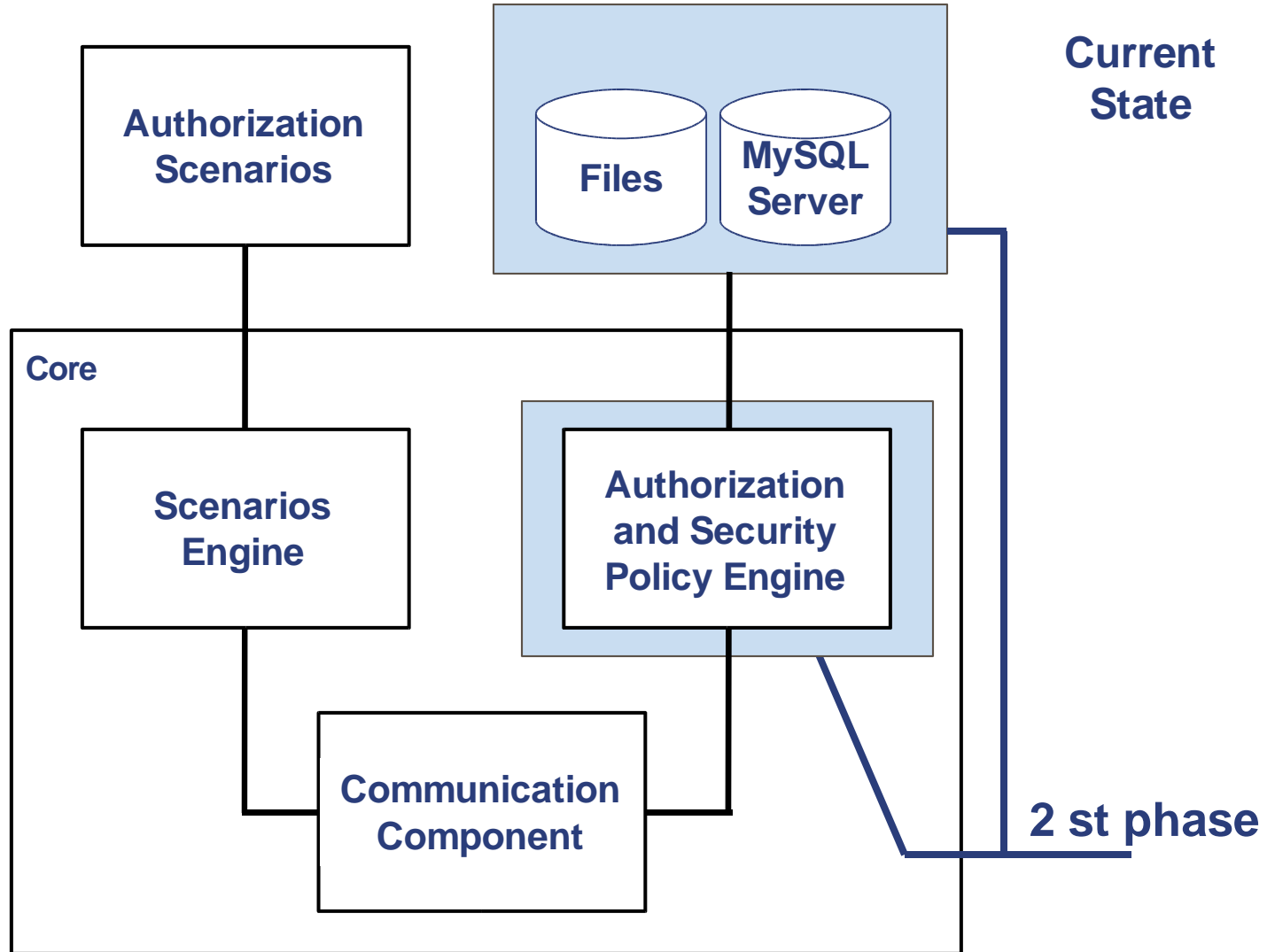
The GAS architecture

(local, global)



- The local GAS contains information which is important locally,
- The Global GAS contains information which is important globally for the whole grid,
- Global and local GAS can communicate with each other,
- Local GAS can contain some main rules which can be used when global GAS is not available.
- The local GAS is very similar to the global GAS ,

Internal modules





The GAS database support

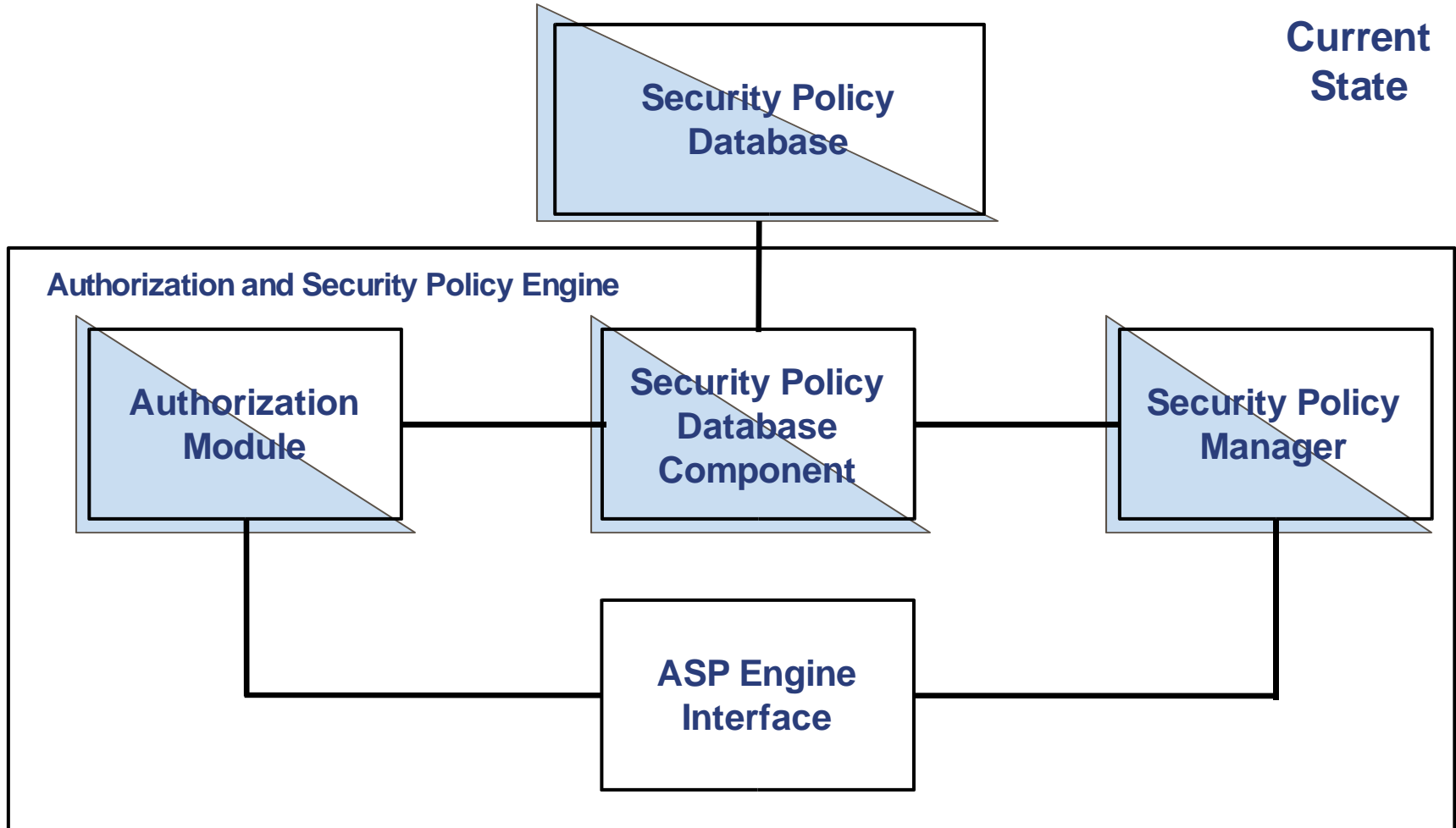


Information Society
Technologies

- unixODBC driver (possible future use of other database servers),
- The MySQL database server,
- Testing data integrity on database level,
- Possibility of storing data in text files (independent from unixODBC driver),

Security Policy Engine

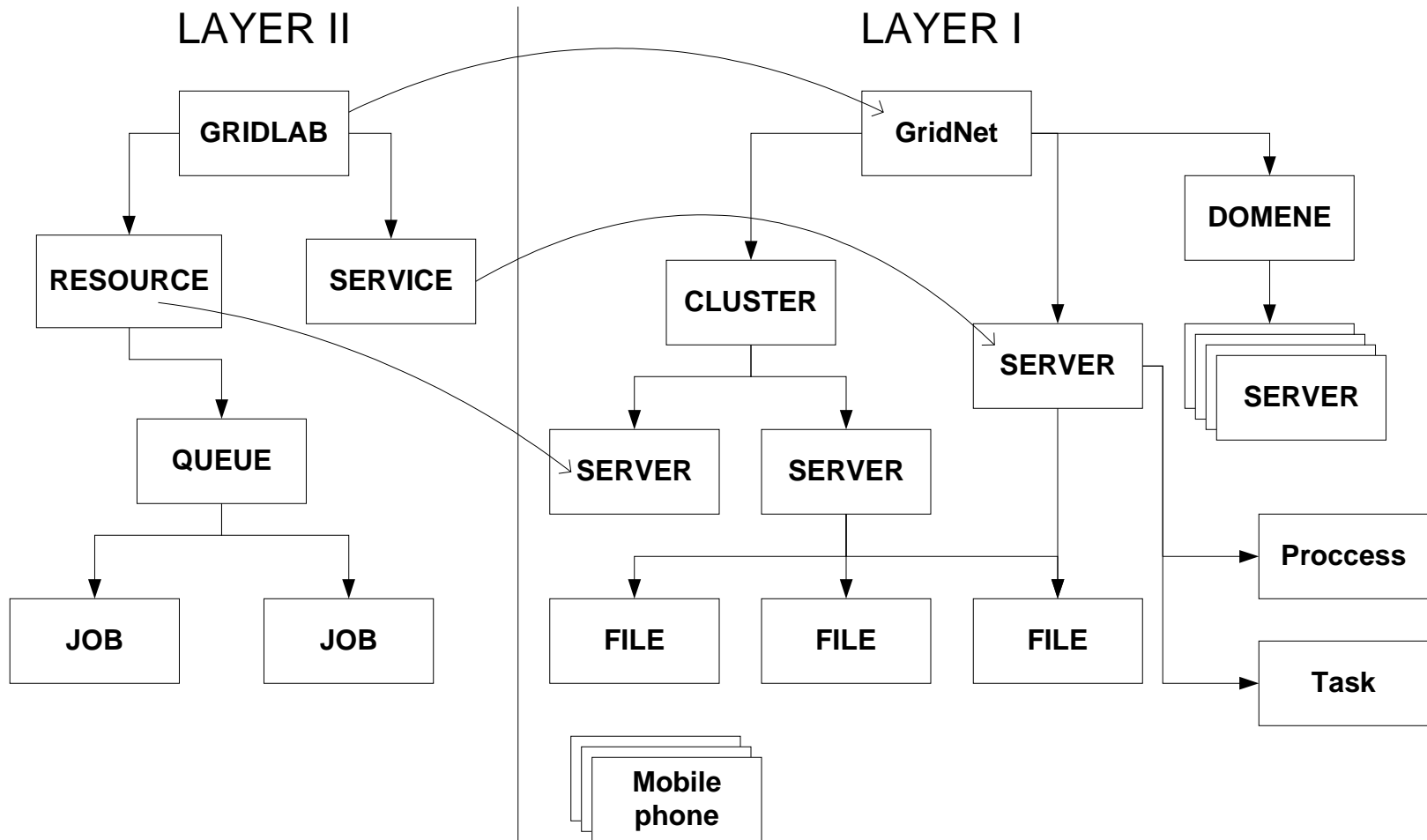
**Current
State**



- Resource centric model
 - Object, Operations, Subjects
 - The RAD (Resource Access Decision)
- Role centric model
 - Role, Object, Operations, Subjects
 - The RBAC (Role Based Access Control)
- Differences with original models (the RAD, the RBAC)
 - Hierarchical objects structure for these two models
 - Static and dynamic Limitations

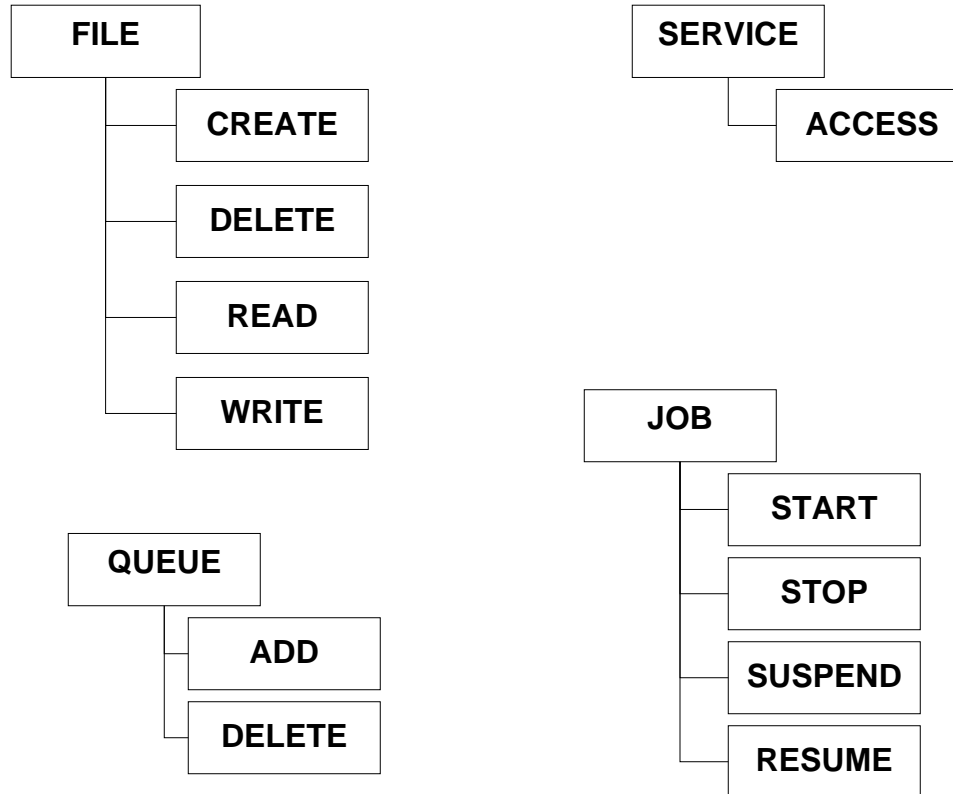
GAS data structures

(samples objects – current state)



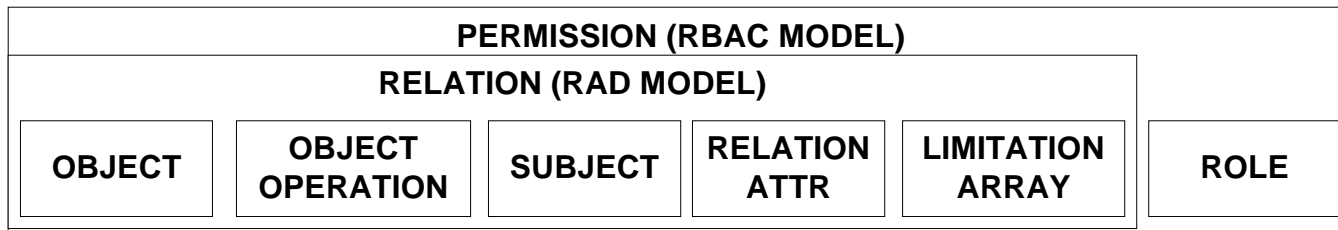
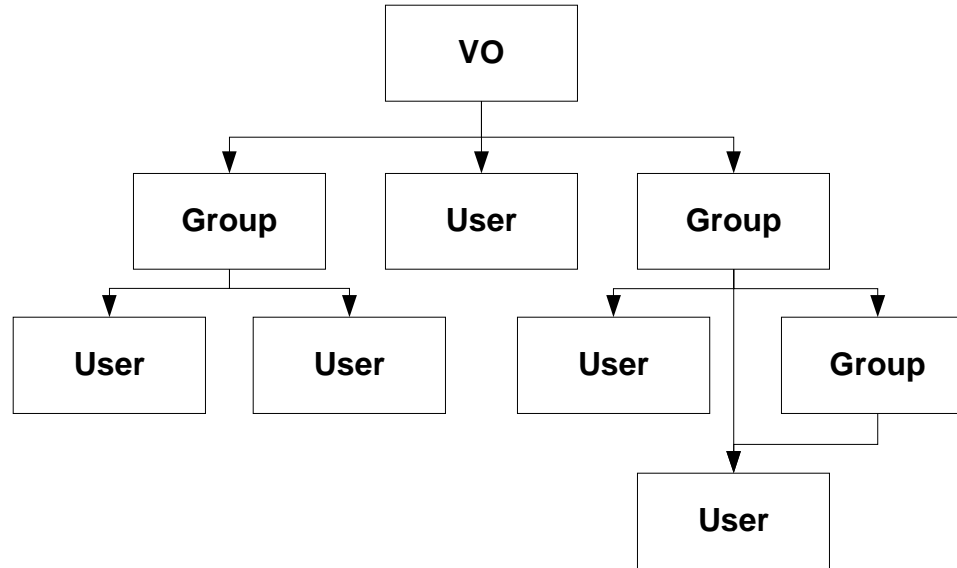
GAS data structures

(some objects operations)



GAS data structures

(subjects, relations, permissions)



- Current state (previous slides)
 - tree structure (hierarchical structure) with layers (for objects)
 - Grid at the top level
 - Services
 - Servers
 - Files
 - Others objects (based upon specific requirements)
- Future
 - All operations on data will be possible (editing, deleting)
 - Testing data integrity on engine level, detecting conflicts
- Currently most of our work is focused on finding data structure for services which will be integrated with the GAS

- Communication:
 - based on GSI protocol,
 - GSI plugin for gSOAP
- Interface (GSI based protocol)
 - for internal use between GAS components,
 - in future may be used to fulfill specific needs of GridLab services
- Interface functions (WSDL):
 - Old functions - getServiceDescription, getResourcesList, getAuthorizationDecision, sendCommandLine
 - New functions - getRBACAuthorizationDecision, getRADAuthorizationDecision

The GAS implementation

- Implementation in C
- Compatibility with
 - Globus Toolkit 2.0
 - Globus Toolkit 2.2
 - CAS version of GT
- Service interface using WSDL
- Implementation status

The Nearest Future

- The GAS administration web client (maybe using the portals framework?)
- Preparing internal policies and data structure for the GAS users,
- Testing and continuing implementation of the GAS internals (the security policy engine, the database engine),
- Integration with the GridLab services,
- Analysis of code security level and quality of implementation.

● Deliverables

● Past

- D6.1 Requirements Document
- D6.2 Technical Specification for Authorization Service
- D6.3 Implementation and Test Plan for the AS

● Future

- D6.4 Documented first release of the security infrastructure and APIs (24 month)
- D6.5 Documented second release of the security infrastructure and APIs (36 month)

● Releases

● Past

- First and second prototype

● Future

- First release (24 month), second release (36 month)

Plan for Olomouc Meeting

- Gathering information about detailed authorization requirements of services which will be integrated with the GAS (structure of objects which are required for a specific service)
- Meeting and discussion with:
 - Portals (WP4)
 - Monitoring (WP11)
 - Resource Management (WP9)
 - Mobile (WP12)
 - Others