EGEE Management of Rights Workshop, Paris

Experiences in NAREGI Project

June 19, 2006

Data Grid Group Leader, NAREGI Project
Professor, Osaka University

Hideo Matsuda

National Research Grid Initiative (NAREGI) Project:Overview

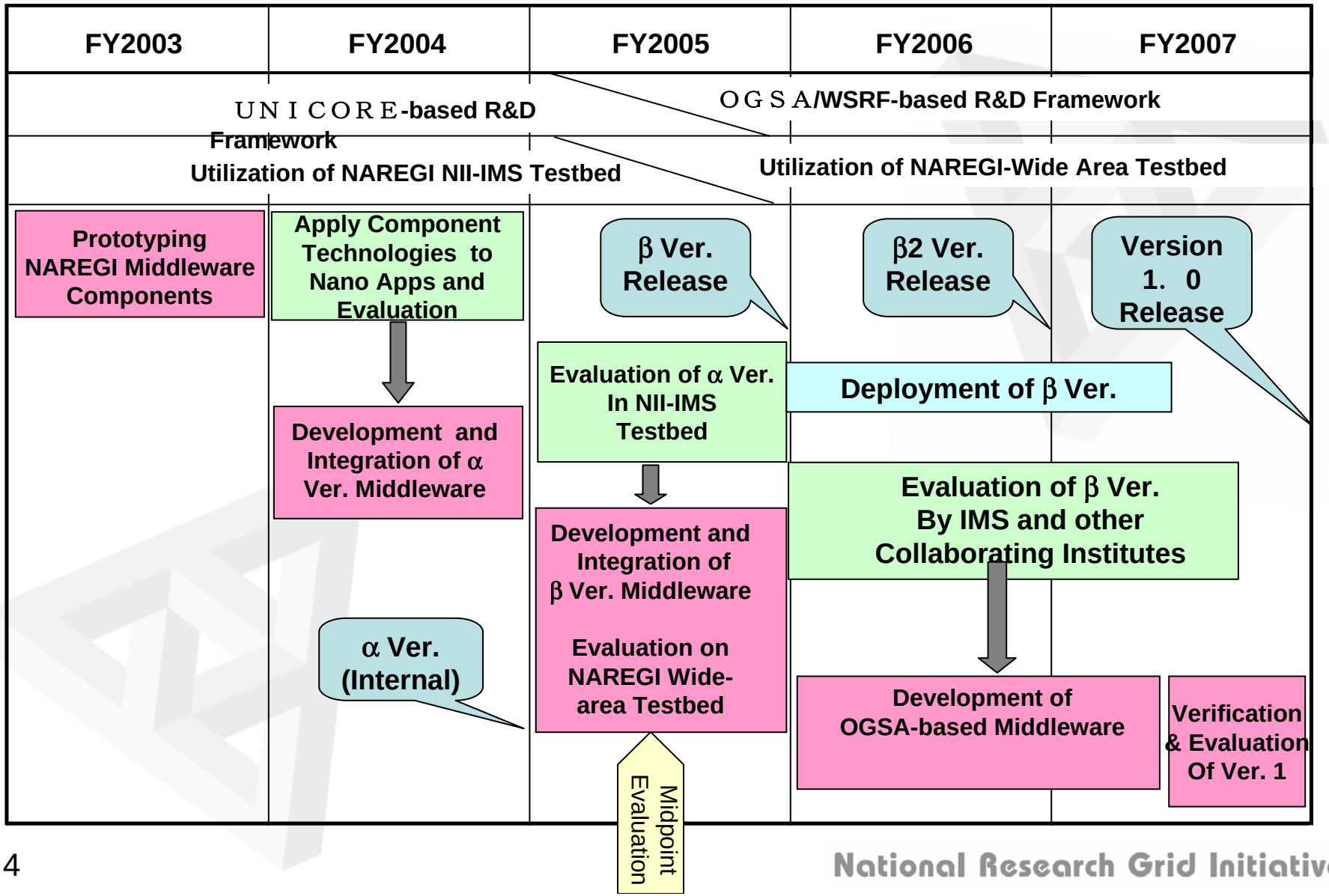
- Started as an R&D project funded by Japan MEXT (FY2003-FY2007)
  2 B Yen(~17M$) budget in FY2003
- One of Japanese Government's Grid Computing Projects
  ITBL, Visualization Grid, GTRC, OsakaU BioGrid etc.
- Collaboration of National Labs., Universities and Industry in the R&D activities (IT and Nano-science Apps.)
- NAREGI Testbed Computer Resources (FY2003)

MEXT:Ministry of Education, Culture, Sports,Science and Technology

National Research Grid Initiative (NAREGI) Project: Goals

1. To develop a Grid Software System (R&D in Grid Middleware and Upper Layer) as the prototype of future Grid Infrastructure in scientific research in Japan.
2. To provide a Testbed to prove that the High-end Grid Computing Environment (100+Tflop/s expected by 2007) can be practically utilized in the Nano-science Applications over the Super SINET.
3. To Participate in International Collaboration (U.S., Europe, Asian Pacific).
4. To Contribute to Standardization Activities, e.g., GGF

Roadmap of NAREGI Grid Middleware



Highlights of NAREGI β release (2005-2006)

1. Resource and Execution Management
   - GT4/WSRF based OGSA-EMS incarnation
     - Job Management, Brokering, Reservation based co-allocation, Monitoring, Accounting
   - Network traffic measurement and control
2. Security
   - Production-quality CA
   - VOMS/MyProxy based identity/security/monitoring/accounting
3. Data Grid
   - WSRF based grid-wide data sharing with Gfarm
4. Grid Ready Programming Libraries
   - Standards compliant GridMPI (MPI-2) and GridRPC
   - Data bridging tools for different applications in a coupled simulation
5. User Tools
   - Web based Portal
   - Workflow tool w/NAREGI-WFML
   - WS based application contents and deployment service
   - Large-Scale Interactive Grid Visualization

The first-ever full WS-based incarnation

NAREGI operating production level CA under APGrid PMA

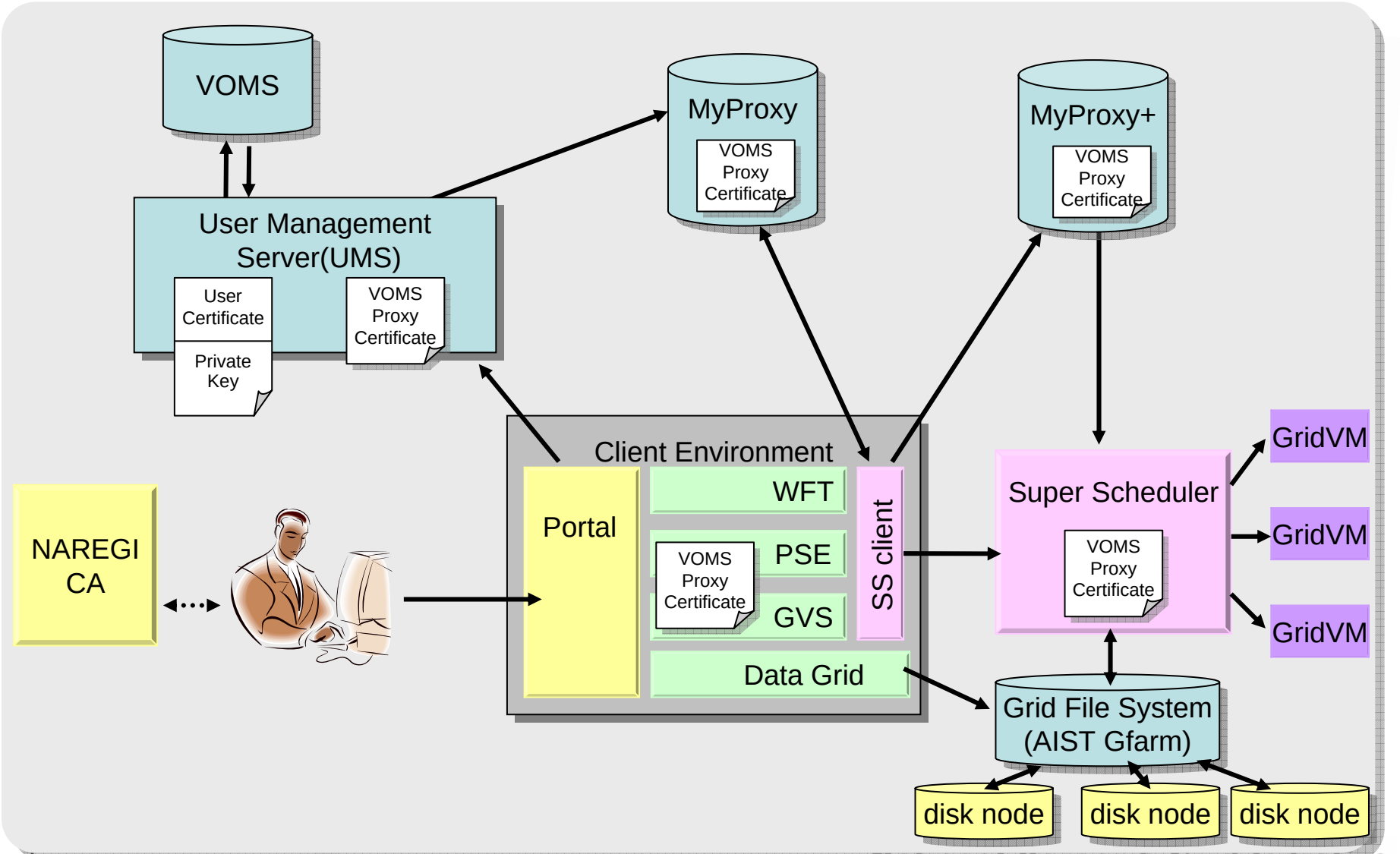
Grid wide seamless data access

High performance WAN communication

Transparent heterogeneous data exchange

A reference implementation of OGSA-ACS

NAREGI Middleware β version

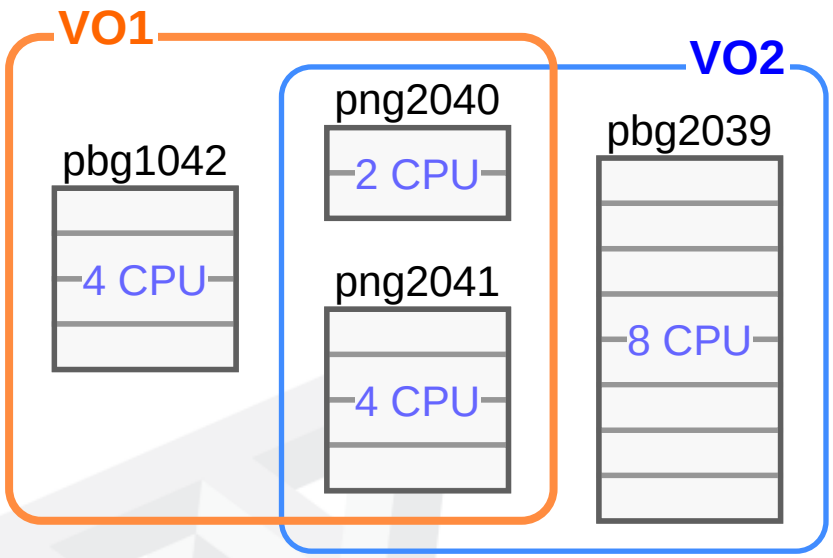


VO and User Management Service

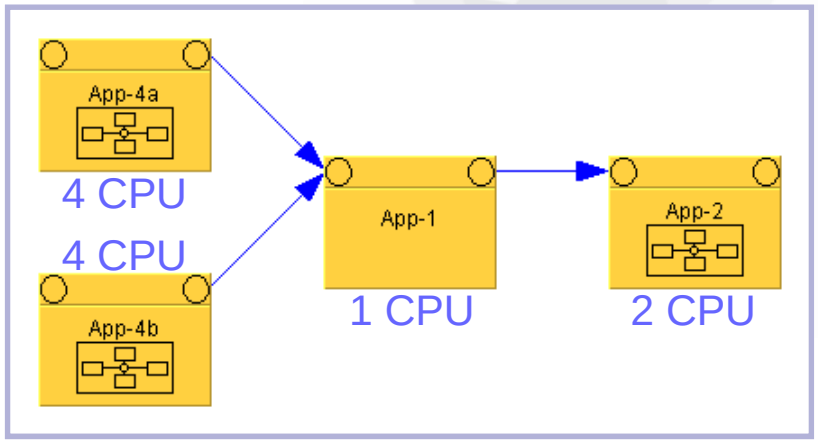
- Adoption of VOMS for VO management
  - Using proxy certificate with VO attributes for the interoperability with EGEE
  - GridVM is used instead of LCAS/LCMAPS
- Integration of MyProxy and VOMS servers into NAREGI
  - with UMS (User Management Server) to realize one-stop service at the NAREGI Grid Portal
  - using gLite implemented at UMS to connect VOMS server
- MyProxy+ for SuperScheduler
  - Special-purpose certificate repository to realize safety delegation between the NAREGI Grid Portal and the Super Scheduler
  - Super Scheduler receives jobs with user's signature just like UNICORE, and submits them with GSI interface.

Computational Resource Allocation based on VO

- Resource configulation



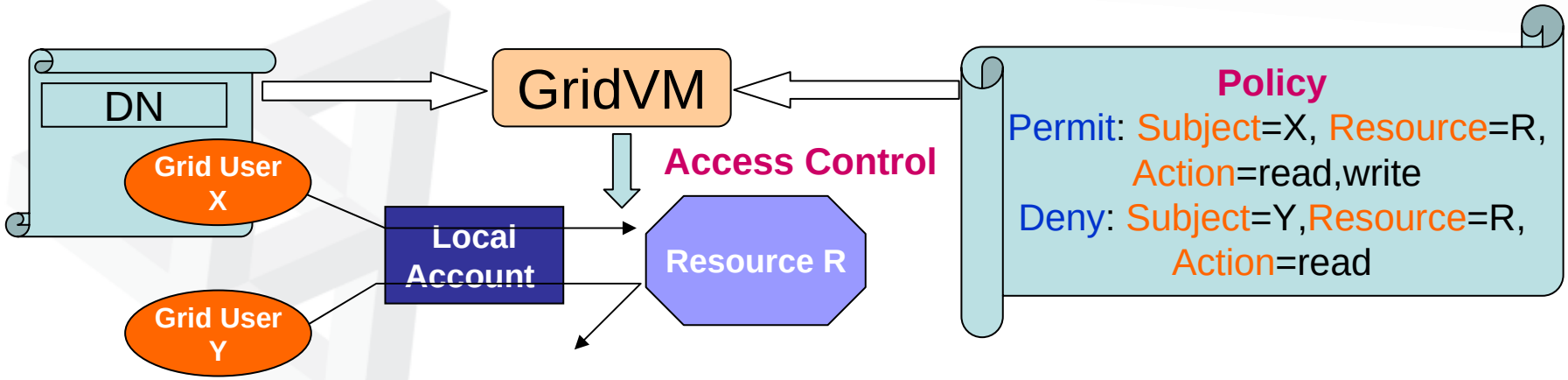
- Workflow



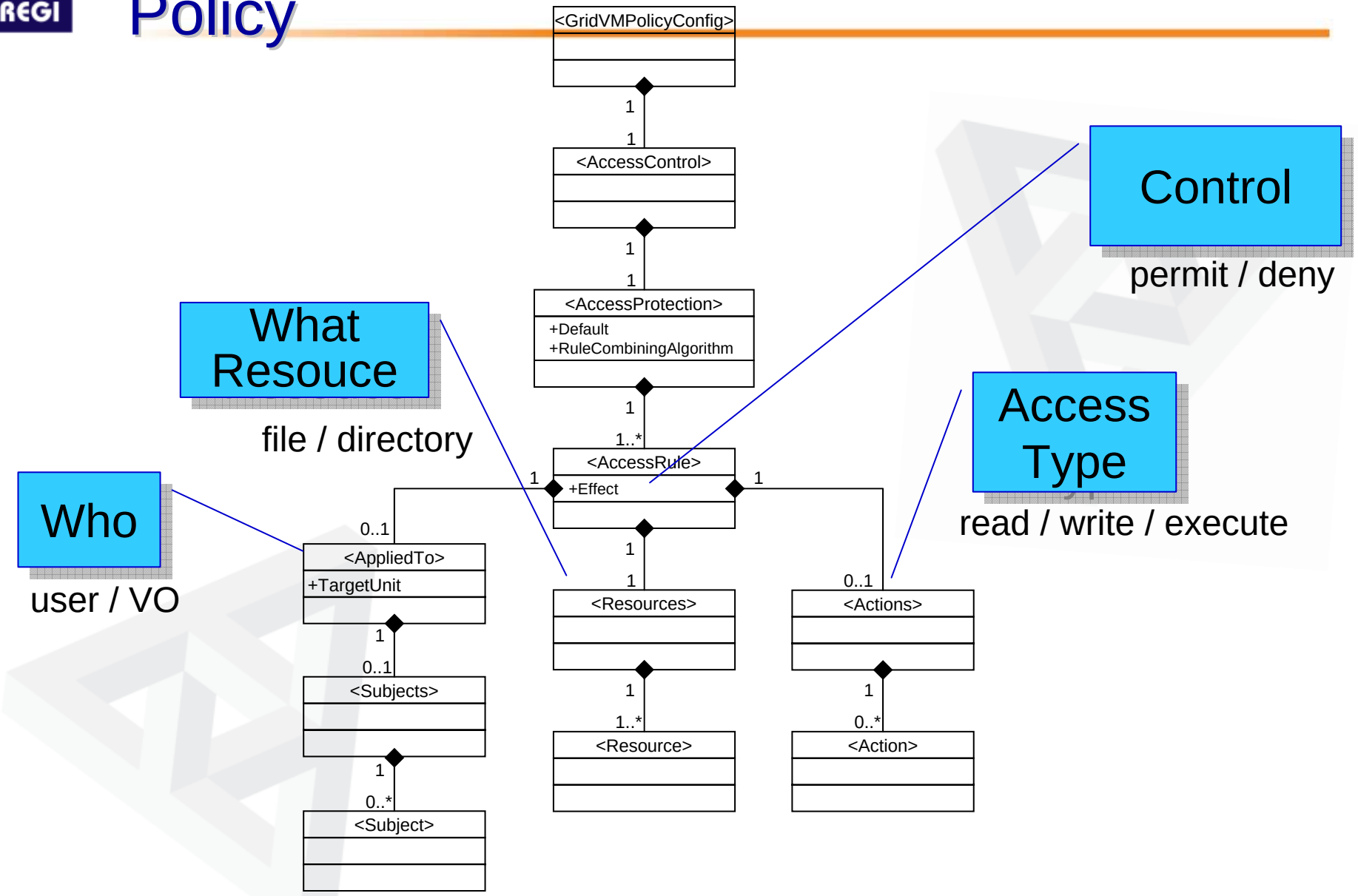
Different resource mapping for different VOs

Local-File Access Control (GridVM)

- Provide VO-based access control functionality that does not use gridmap files.
- Control file-access based on the policy specified by a tuple of **Subject**, **Resource**, and **Action**.
- Subject is a grid user ID or VO name.



Structure of Local-File Access Control Policy



Policy Example (1)

```
<gvmcf:AccessProtection gvmac:Default="Permit"
      gvmac:RuleCombiningAlgorithm="Permit-overrides">

   <!-- Access Rule 1: for all user -->
   <gvmcf:AccessRule gvmac:Effect="Deny">
     <gvmcf:AppliedTo> <gvmac:Subjects> …
     <gvmac:Resources>
       <gvmac:Resource>/etc/passwd</gvmac:Resource>
     </gvmac:Resources>
     <gvmac:Actions> …

   <!-- Access Rule 2: for a specific user -->
   <gvmcf:AccessRule gvmac:Effect=“Permit">
        <gvmcf:AppliedTo gvmcf:TargetUnit=“user">
        <gvmcf:Subjects> <gvmcf:Subject>User1</gvmcf:subject>
</gvmcf:Subjects>
     </gvmcf:AppliedTo >
     <gvmac:Resources>
       <gvmac:Resource>/etc/passwd</gvmac:Resource>
     </gvmac:Resources>
     <gvmac:Actions>
       <gvmac:Action>read</gvmac:Action>
     </gvmac:Actions>
```

Default

Applying rules

Policy Example (2)

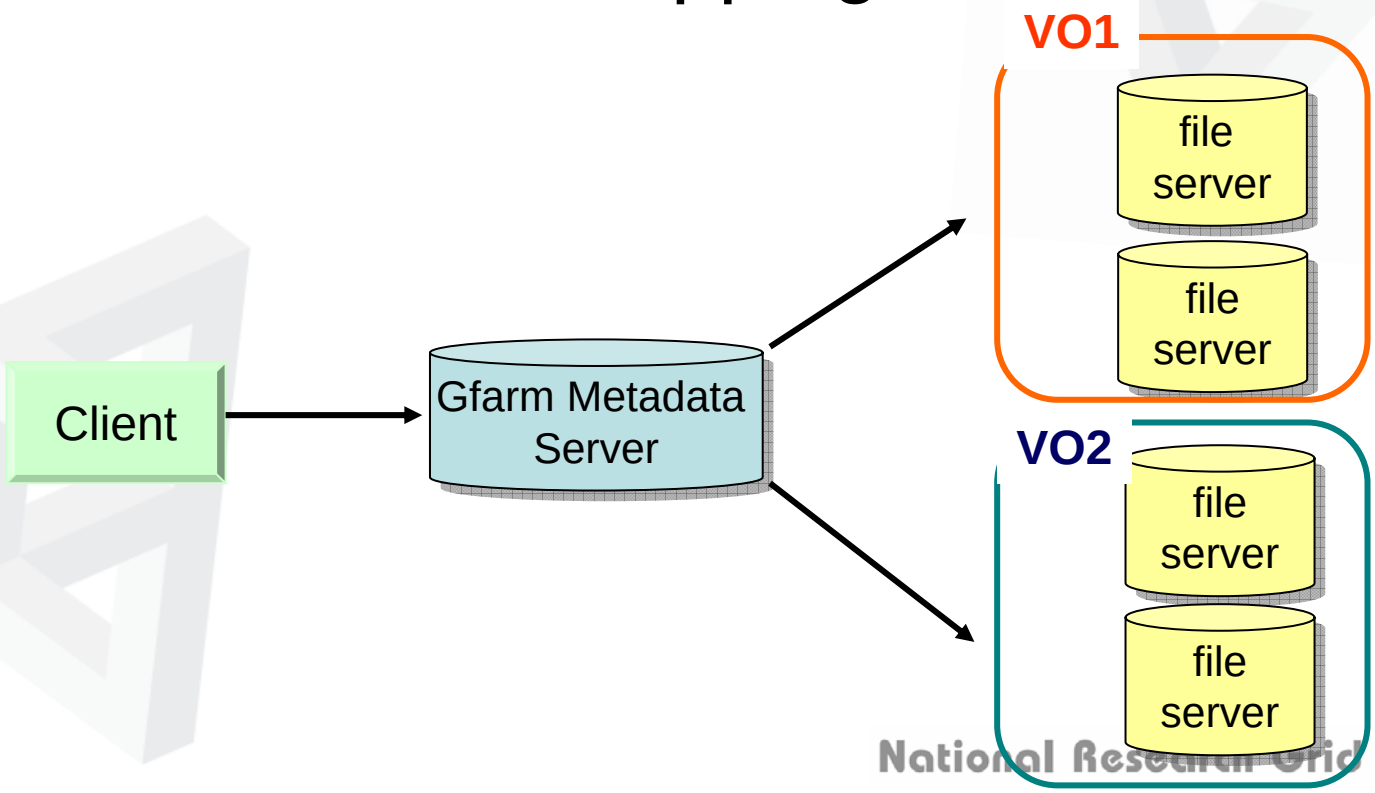
```
<gvmcf:AccessRule gvmac:Effect="Permit">
  <gvmcf:AppliedTo gvmcf:TargetUnit="vo">
    <gvmcf:Subjects>
      <gvmcf:Subject>bio</gvmcf:Subject>
    </gvmcf:Subjects >
  </gvmcf:AppliedTo>

  <gvmac:Resources>
     <gvmac:Resource>/opt/bio/bin</gvmac:Resource>
     <gvmac:Resource>./apps</gvmac:Resource>
  </gvmac:Resources>

   <gvmac:Actions>
     <gvmac:Action>read</gvmac:Action>
     <gvmac:Action>execute</gvmac:Action>
  </gvmac:Actions>

</gvmcf:AccessRule>
```

VO name

Resource name

VO-based Resouce Mapping in Global File System (Planned in β2)

- Next release of Gfarm (version 2.0) will have access control functionality.
- We will extend Gfarm metadata server for the data-resource mapping based on VO.



Current Issues and the Future Plan

- Current Issues on VO management
  - VOMS platform
    - gLite is running on GT2 and NAREGI middleware on GT4
  - Authorization control on resource side
    - Need to implement new functions for resource control on GridVM, such as Web services, reservation, etc.
  - Proxy certificate renewal
    - Need to invent a new mechanism
- Future plan
  - Cooperation with GGF security area members to realize interoperability with other grid projects
  - Proposal of a new VO management methodology and trial of reference implementation.