Design and Implementation of GEO Grid Security

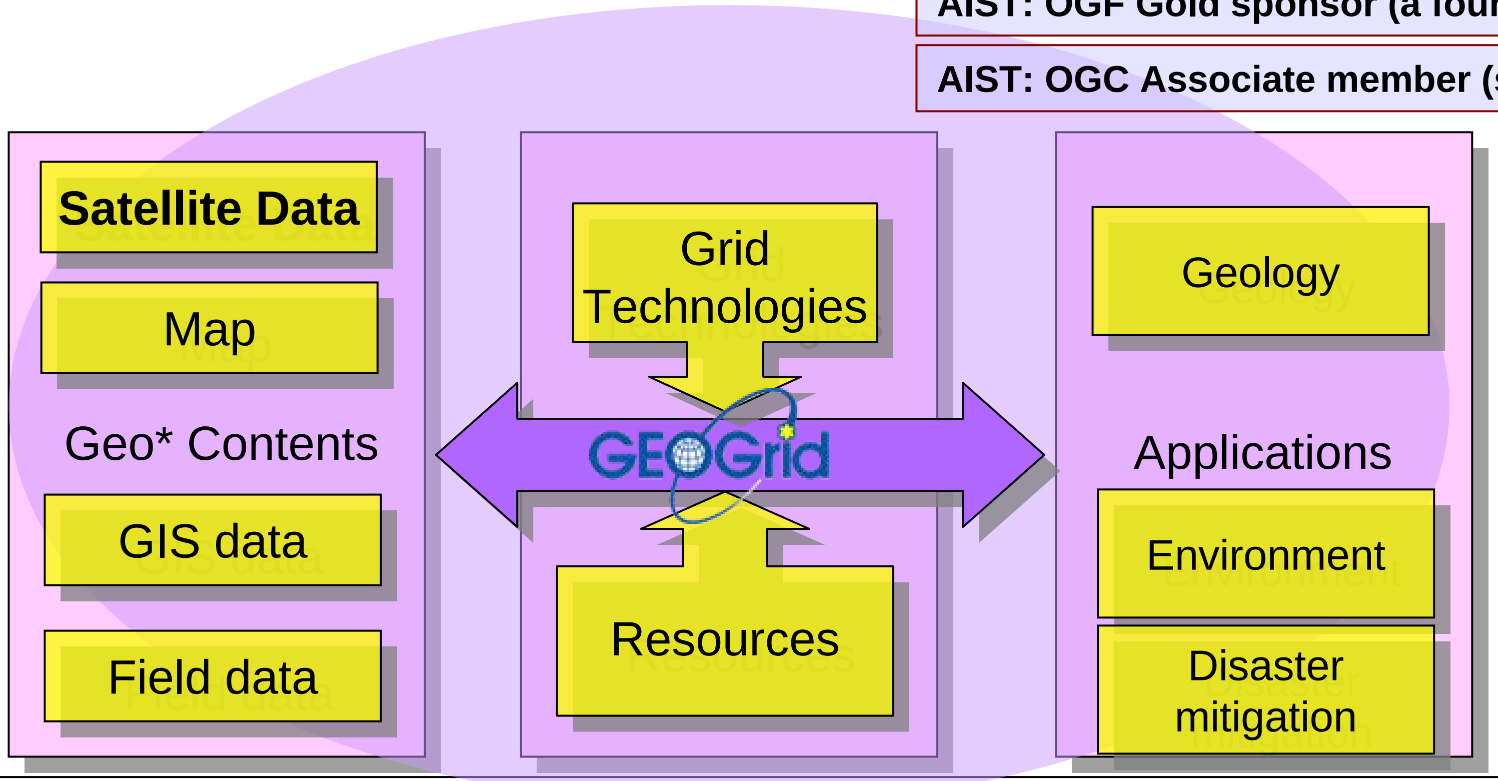
Yoshio Tanaka
National Institute of Advanced Industrial Science and Technology
(AIST) Japan

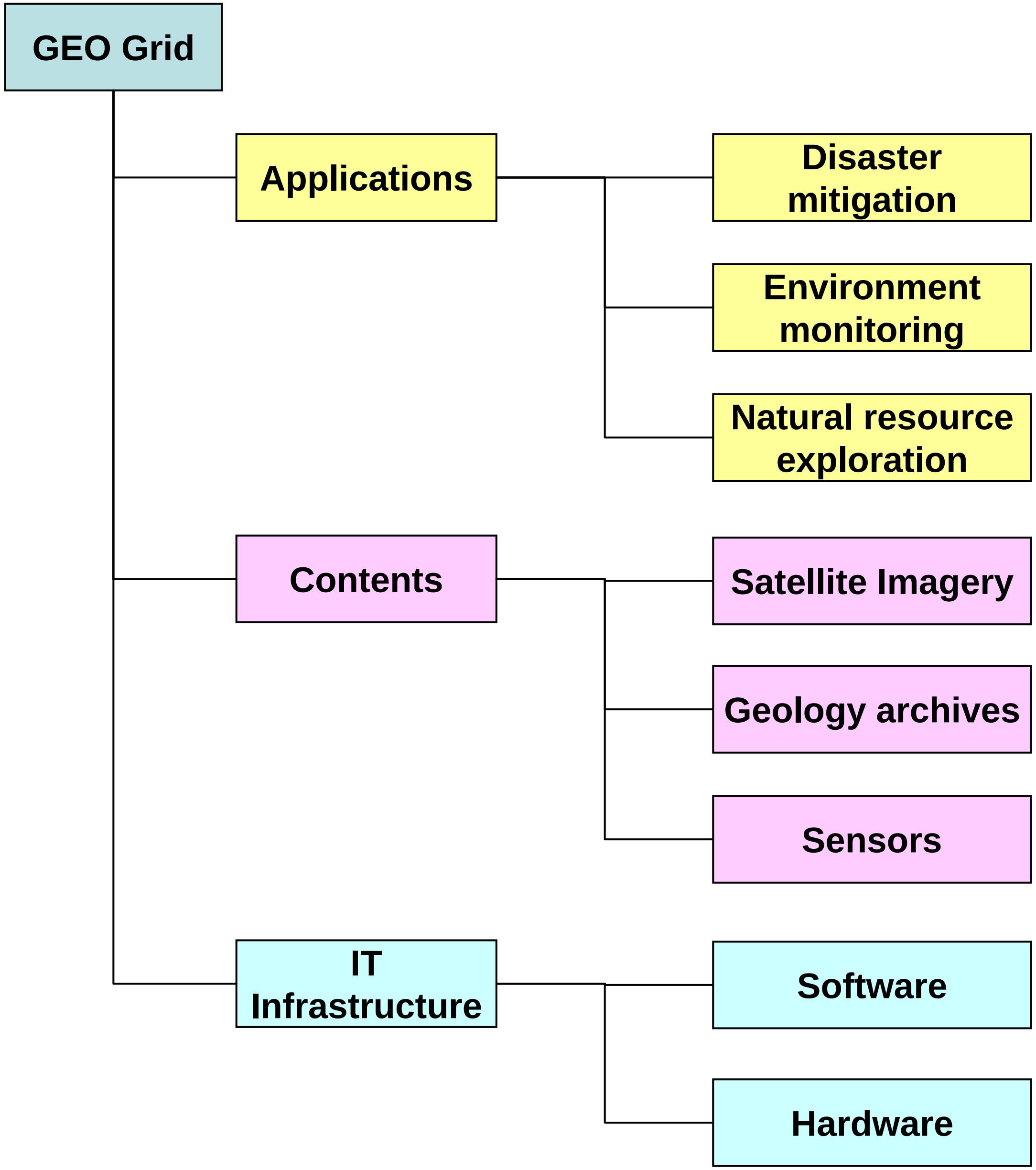
What is the GEO Grid ?

- The GEO (Global Earth Observation) Grid is aiming at providing an _E-Science Infrastructure_ for worldwide Earth Sciences communities to accelerate GEO sciences based on the concept that relevant data and computation are _virtually integrated_ with a certain *access control* and ease-of-use interface those are enabled by a set of Grid and Web service technologies.

AIST: OGF Gold sponsor (a founding member)

AIST: OGC Associate member (since 2007)





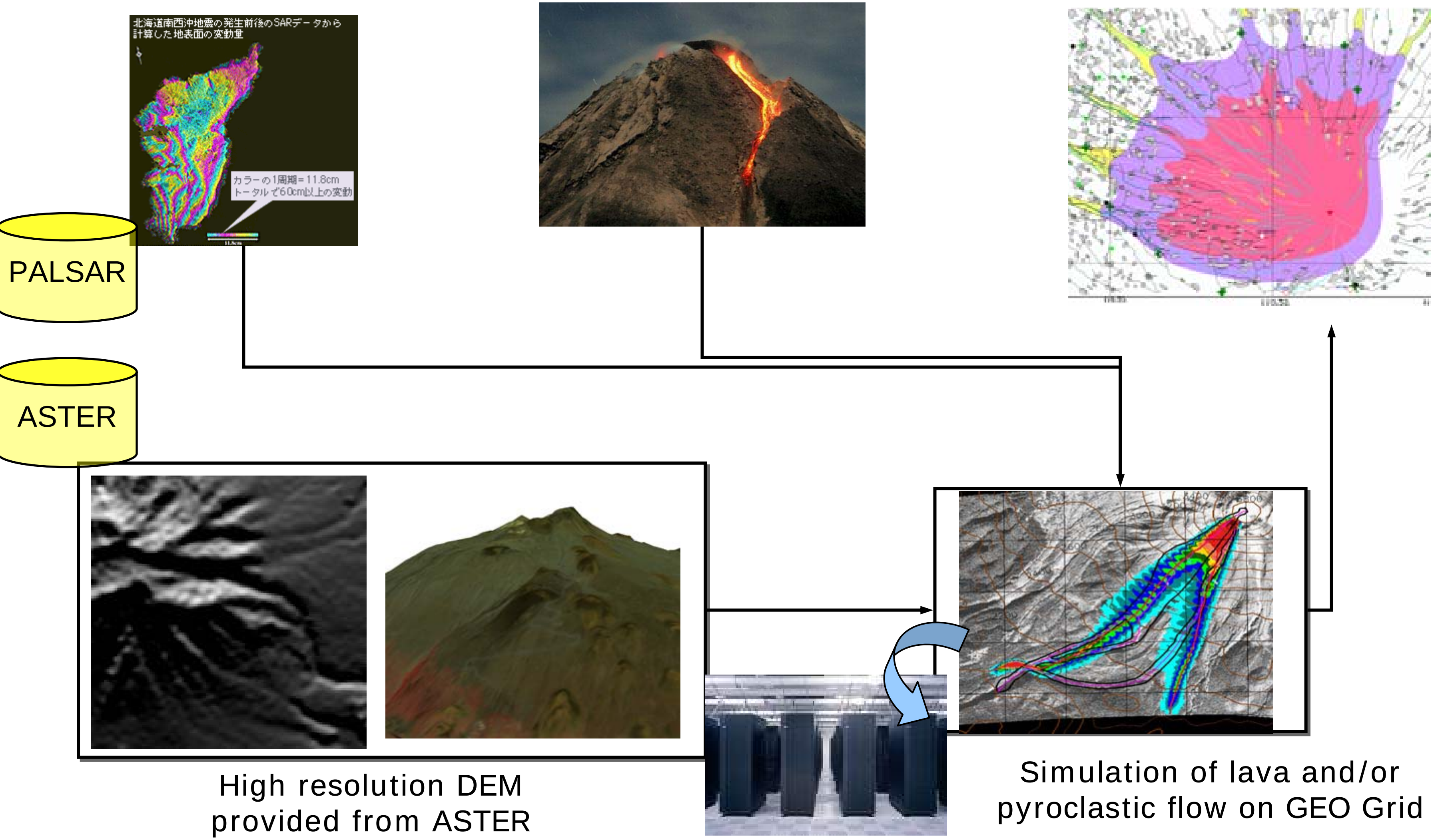
- GEO Grid
  - Applications
    - Disaster mitigation: Land slides, flood
    - Environment monitoring: Global warming, CO_2 flux estimation
    - Natural resource exploration: Oil, Gas
  - Contents
    - Satellite Imagery: Full L0 ASTER on disk; MODIS on disk (East Asia)
    - Geology archives: Japan, SE Asia
    - Sensors: AsiaFlux, Field server
  - IT Infrastructure
    - Software: Security, data access, service registry, resource mgmt., Weg GIS, Workflow, U/I Portal, etc.
    - Hardware: Storage, Servers Cluster computers

A Workflow example “Disaster prevention and mitigation (Volcano)”

Monitoring of crustal deformation by PALSAR

In-situ observations e.g. growth of a lava dome

Hazard Map for Evacuation planning



High resolution DEM provided from ASTER

Simulation of lava and/or pyroclastic flow on GEO Grid

Functional requirements for the IT infrastructure

- Size scalability in near-real-time data handling and distribution
  - Need to manage hundreds tera-bytes to peta-byte of data.
  - Such data will be made available with minimum time delay and at minimum cost.
- Handling wide diversification of data types, associated metadata, products and services.
  - Research communities wish to integrate various data according to their interests.
  - IT infrastructure must support
    - the creation of user groups which represent various types of virtual research/business communities
    - Federation of distributed and heterogeneous data resources which is shared in such communities

Functional requirements for the IT infrastructure (cont'd)

- Respecting data owner's publication policies
  - Some data are not freely accessible.
    - E.g. commercial data.
  - IT infrastructure must provide a security infrastructure which supports flexible publication policies for both data and computing service providers.
- Smooth interaction and loose coupling between data services and computing services
  - A desirable IT architectural style would achieve loose coupling among interacting software agents to allow users both to create services independently, and to produce new application from them.
  - IT infrastructure must support sharing, coordination, and configuration of environments for application programs and resources, depending on the user's requirements.

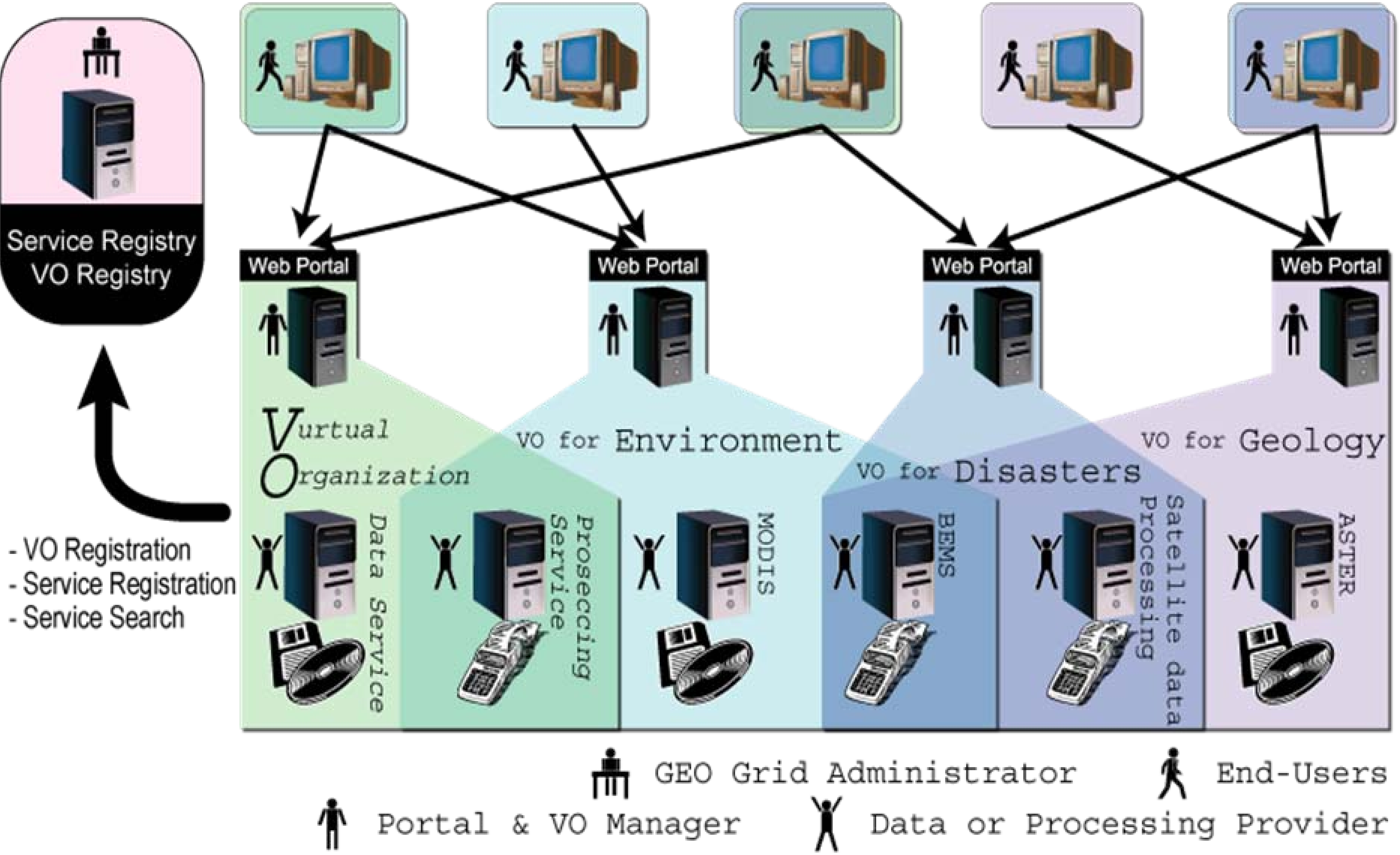
Functional requirements for the IT infrastructure (cont'd)

- Ease of use
  - End users should be able to access data and computing resources without the burden of installing special software and taking care of security issues (e.g. certificate mgmt.).
  - Data and service providers should be able to easily make their resources available as services with desired access control.
  - Administrators and leaders of communities should be able to create virtual communities easily by configuring appropriate access control.
  - We must provide an ease-of-use framework for publishing services and user interfaces.

Design Policy

- Introduces a concept of VO (Virtual Organization)
- Data and computation are provided as “services” via standard protocols and APIs.
- A VO is created dynamically by integrating available services and resources according to the interests and requirements of the VO.
- User-level Authentication and VO-level Authorization
    - User’s right is managed (assigned) by an administrator of his belonging VO.
    - Access control to a service is configured by the service provider according to the publication policy. There are some options of the access control
        - VO-level, Group/Role-based, User-level, etc.
    - Scalable architecture for the number of users.

Overview and usage model of the GEO Grid system

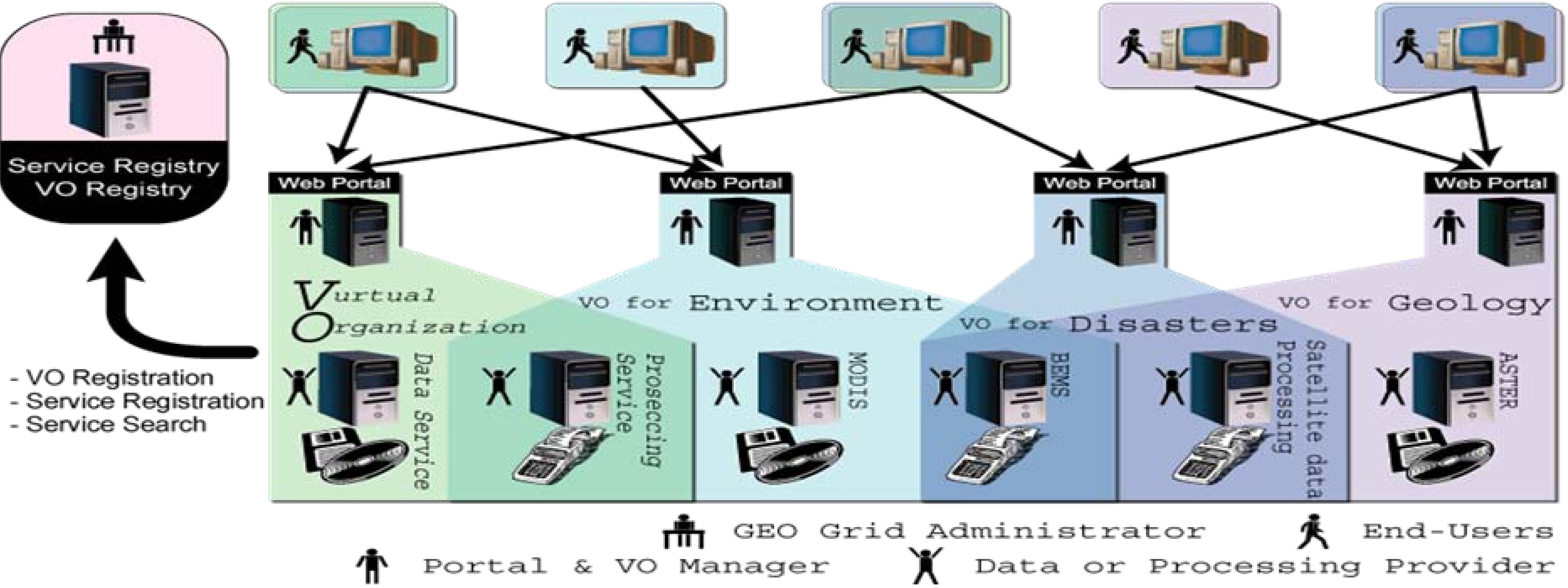


Key Technologies: GSI and VOMS

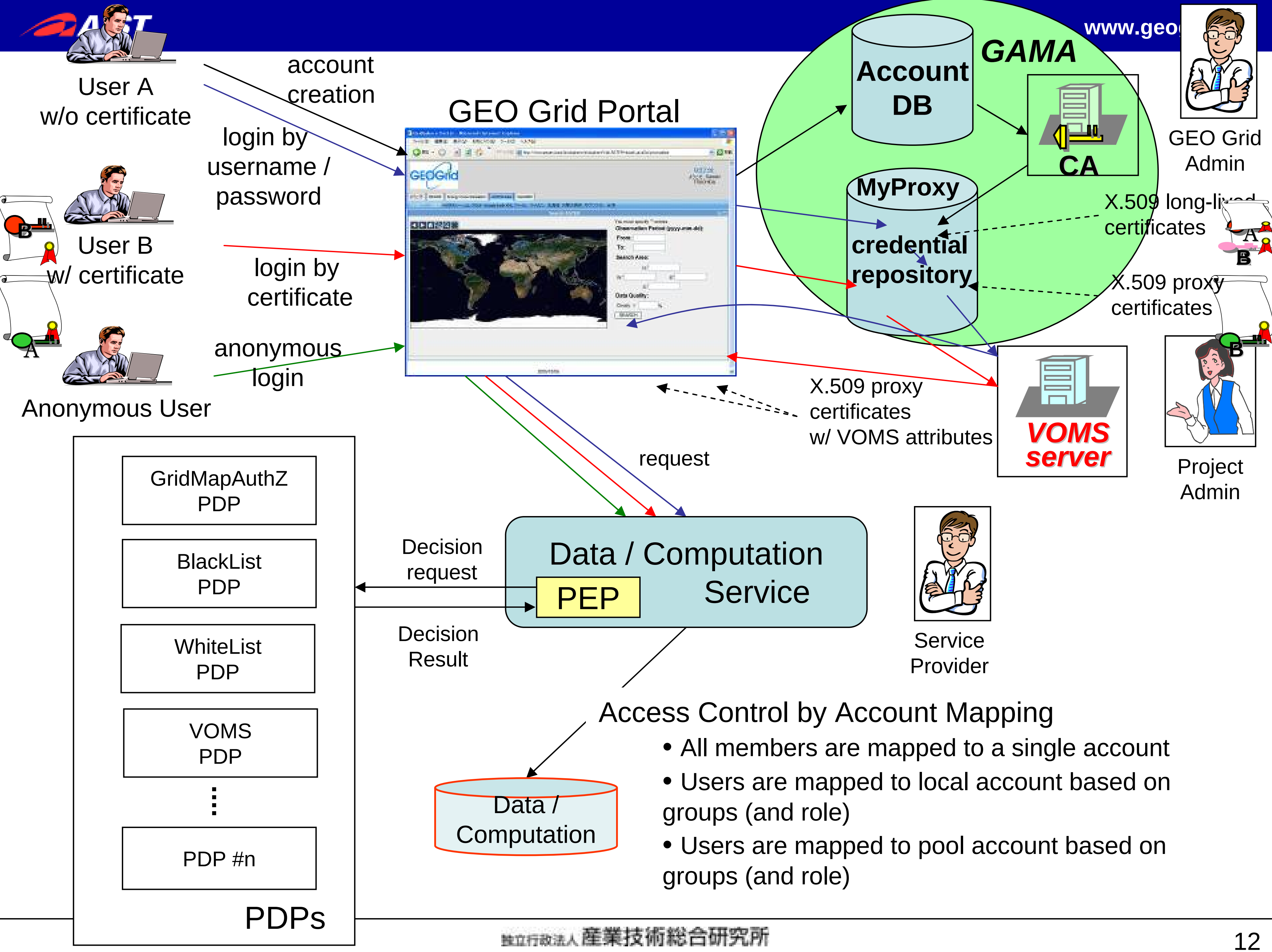
- Grid Security Infrastructure (GSI) is standard security technology used in the current Grid communities.
  - Based on Public Key Infrastructure (PKI) and X.509 Certificates.
- Virtual Organization Membership Services (VOMS) is a software for creating/managing VOs.
  - Developed by European Communities
  - Based on GSI

End users of GEO Grid may not be required to understand GSI, VOMS, etc, but project (VO) admin should understand these technologies correctly.

Overview and usage model of the GEO Grid system



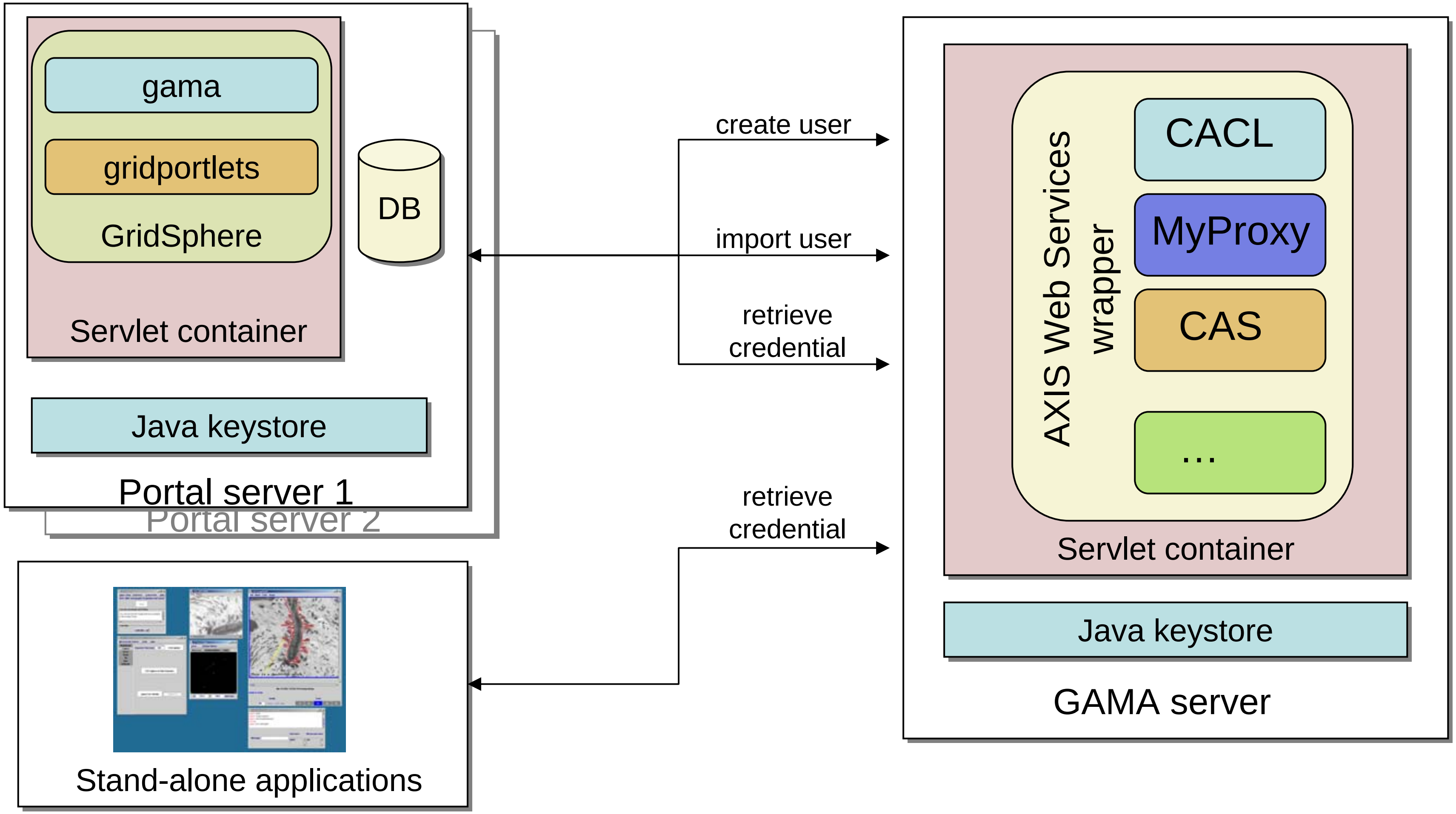
- User-level Authentication and VO-level Authorization
  - User's right is managed (assigned) by an administrator of his belonging VO.
  - Access control to a service is configured by the service provider according to the publication policy. There are some options of the access control
    - VO-level, Group/Role-based, User-level, etc.
  - Scalable architecture for the number of users.



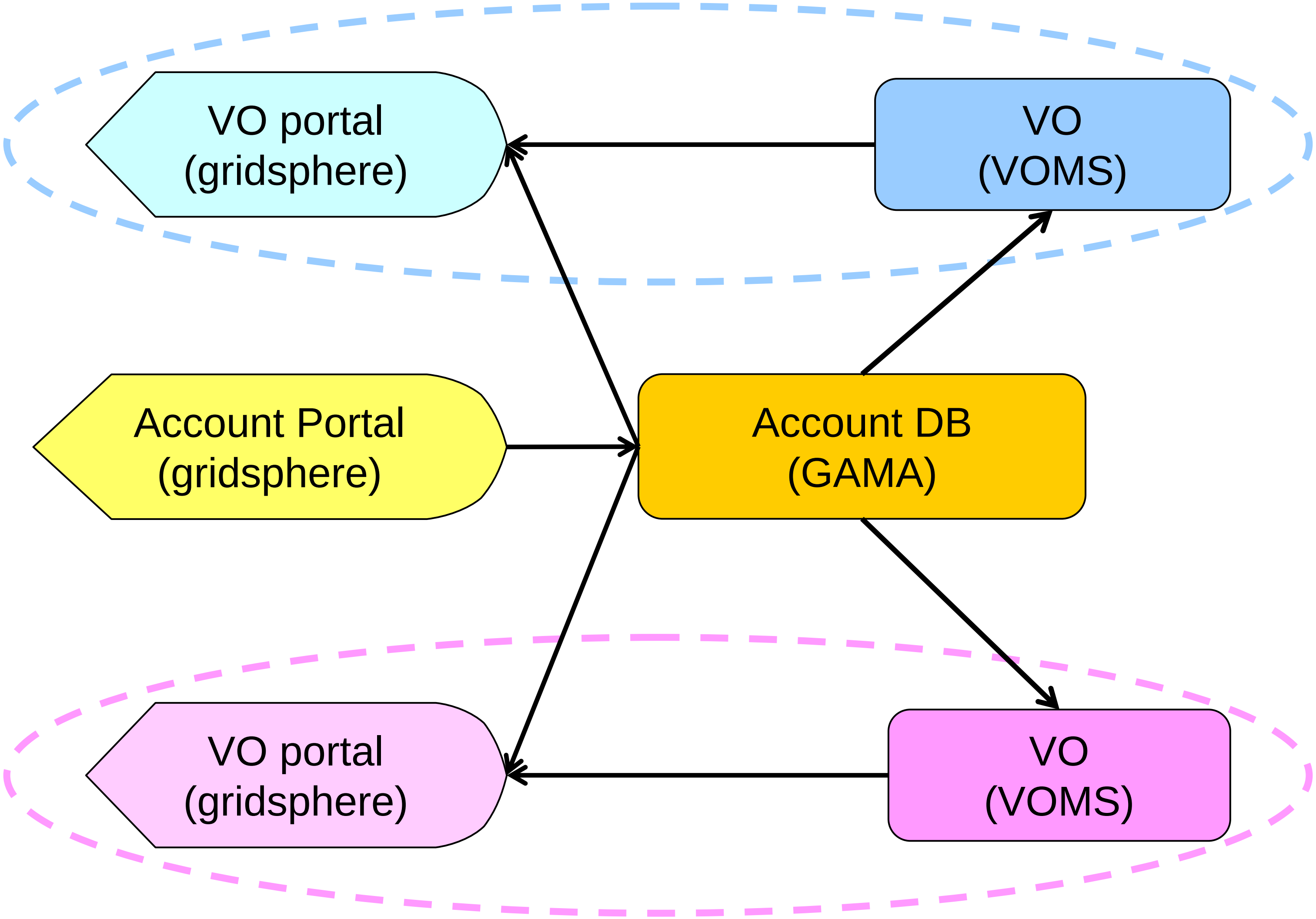
Access Control by Account Mapping

- All members are mapped to a single account
- Users are mapped to local account based on groups (and role)
- Users are mapped to pool account based on groups (and role)

GAMA architecture

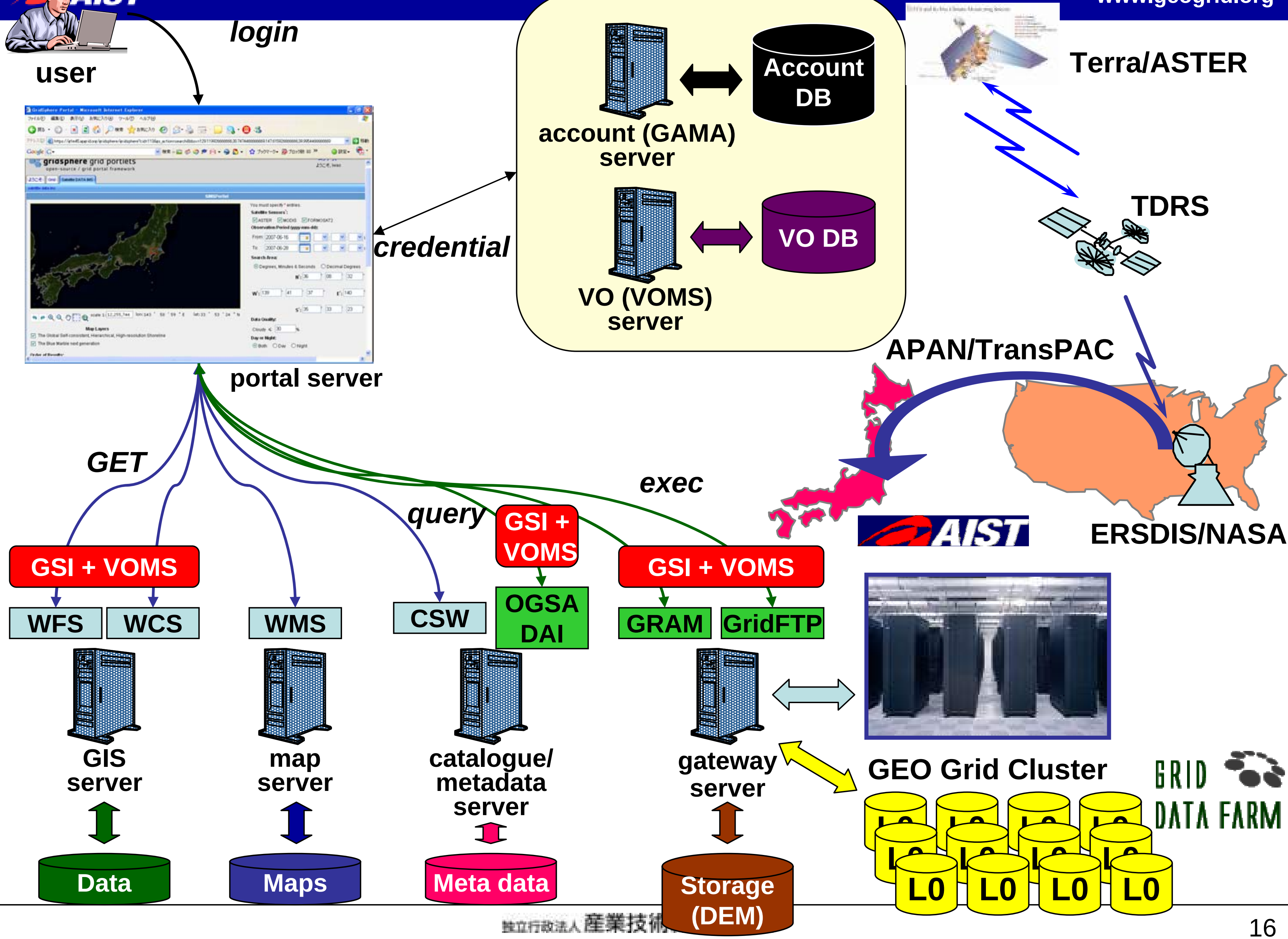


Portal v.s. Accounts v.s. VO

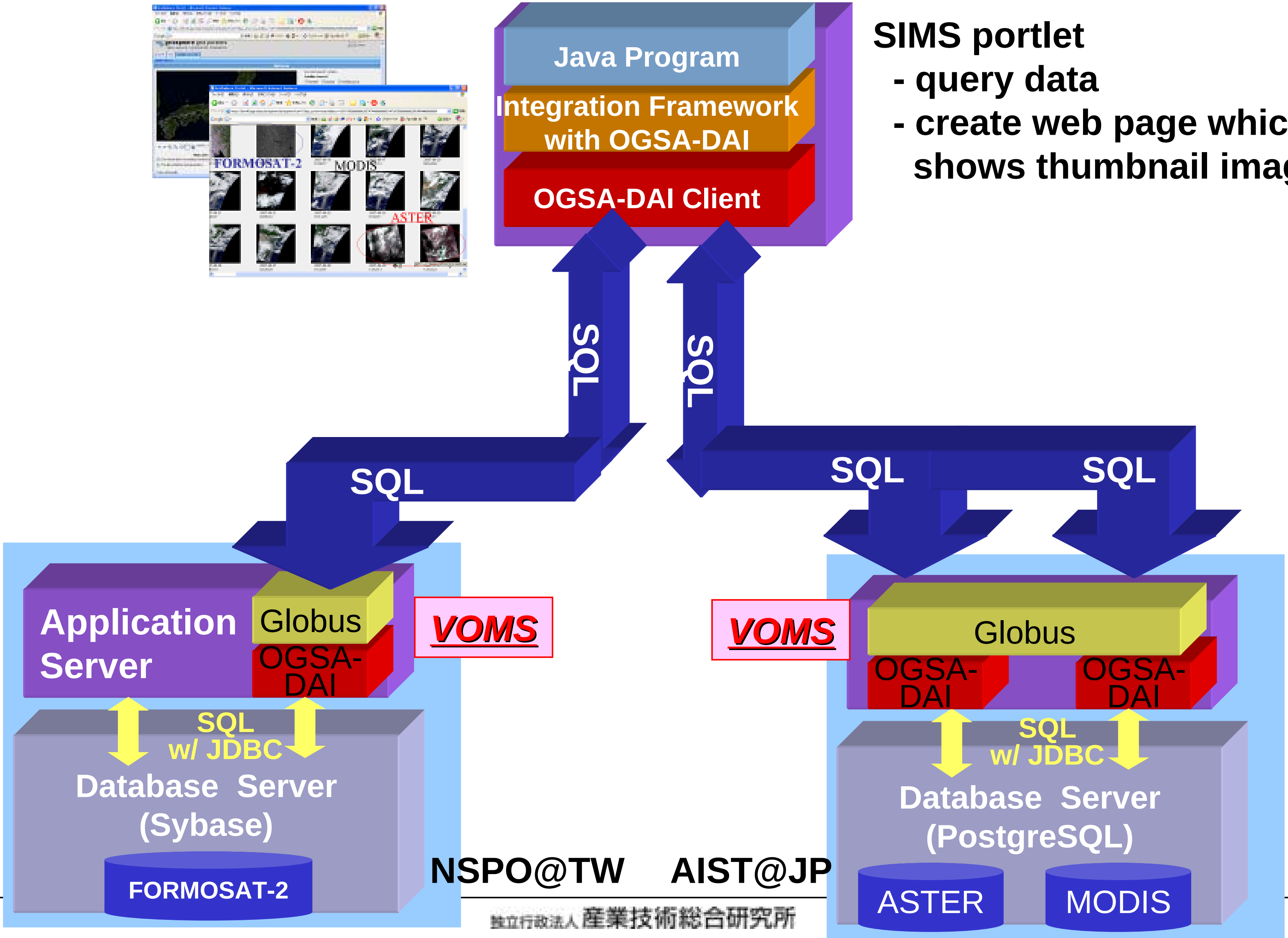


Current status of evaluation, integration, and developments

- Deployed and tested
  - GAMA, VOMS server
  - Pre-WS GRAM w/ VOMS
  - WS GRAM w/ VOMS
  - GridFTP w/ VOMS
  - Apache w/ VOMS
  - OGSA-DAI w/ VOMS
- Authorization using VOMS
  - Different levels of AuthZ
    - VO, Group, Role, User
  - Different method for account mapping
    - Single account, pool account, account for individual user
- Developed two functions for integrating GAMA and VOMS
  - GAMA Portal accesses VOMRS (VO Management Registration Service) to register a new user with the VO when the account is activated.
  - GAMA Portal generate a VOMS proxy from a proxy credential from the MyProxy server.
  - Credential Portlet


user
login
GridSphere Portal - Microsoft Internet Explorer
gridsphere grid portlets
open-source / grid portal framework
You must specify * entries.
Satellite Sensors*:
☑ASTER ☑MODIS ☑FORMOSAT2
Observation Period (yyyy-mm-dd):
From: 2007-06-16
To: 2007-06-28
Search Area:
● Degrees, Minutes & Seconds ○ Decimal Degrees
Data Quality:
Cloudy < 30 %
Day or Night:
● Both ○ Day ○ Night
Map Layers
☑ The Global Self-consistent, Hierarchical, High-resolution Shoreline
☑ The Blue Marble next generation
portal server
credential
account (GAMA) server
Account DB
VO (VOMS) server
VO DB
Terra/ASTER
TDRS
APAN/TransPAC
AIST
ERSDIS/NASA
GET
query
exec
GSI + VOMS
WFS
WCS
GIS server
Data
WMS
map server
Maps
CSW
GSI + VOMS
OGSA DAI
catalogue/ metadata server
Meta data
GSI + VOMS
GRAM
GridFTP
gateway server
Storage (DEM)
GEO Grid Cluster
L0
L0
L0
L0
GRID DATA FARM

Demo Environments - SIMS (ASTER+MODIS+Formsat2)



SIMS portlet

- query data
- create web page which shows thumbnail images