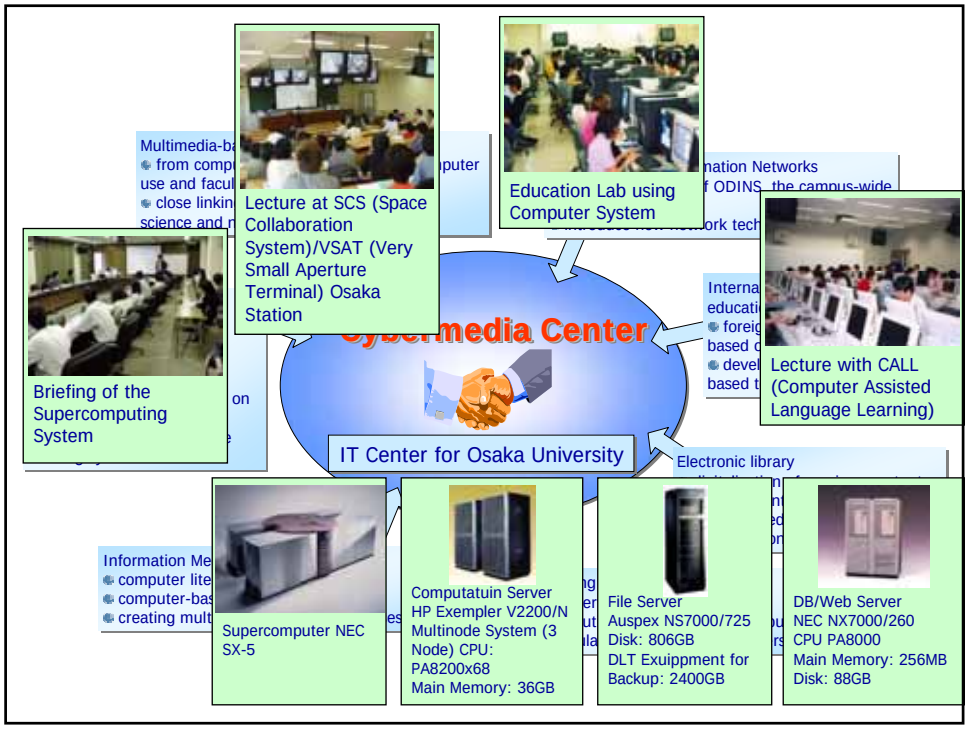
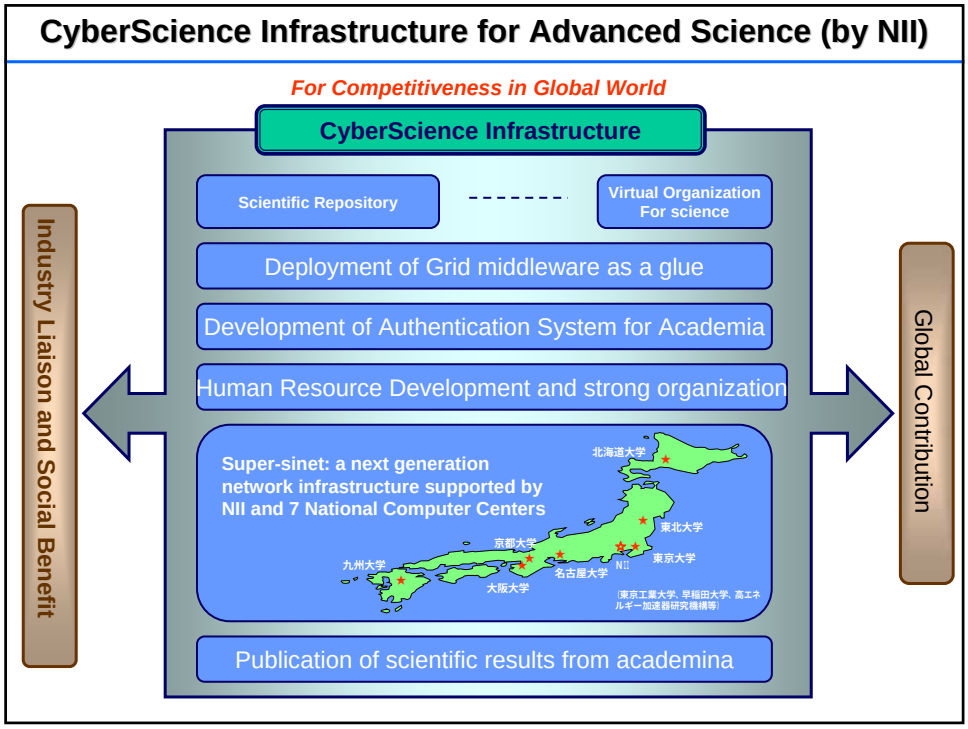
# CA system and CyberScience Infrastructure

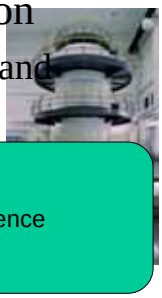
Shinji Shimojo
Cybermedia Center
Osaka University





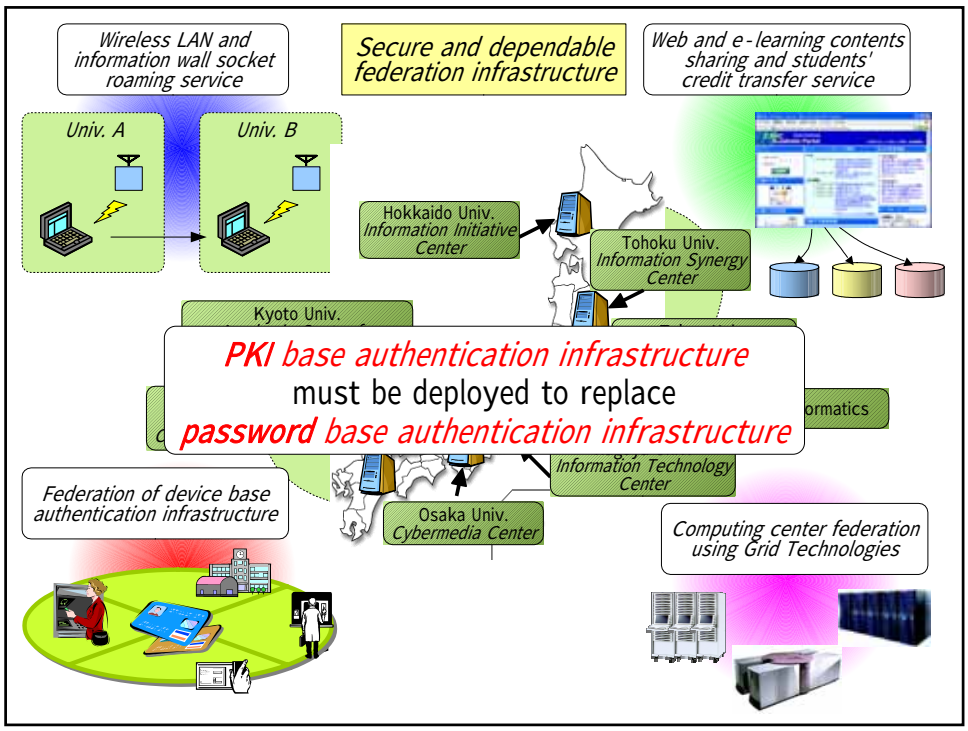

# Why we need CyberScience Infrastructure (CSI) in Cybercampus

- Securely and safely sharing infrastructure
  - Ex. Grid provides heterogeneous large scale computational environment
  - Ex. Large observation device should be shared.
- Securely and safely sharing information
  - Ex. Sharing medical record for research and diagnosis



International and National Collaboration is a key to science

超高圧電子顕微鏡センター




# Requirements for authorization/authentication mechanism

- Information Systems are exist everywhere.
- Password based authorization is no longer safe.
- People are moving around.
- Inter-organizational, institutional and university collaboration is necessary for future science.
- Intra-domain solution is not enough.

# Elements of CSI

- PKI for Global Identity
- PMA for coodinated Trusted Domain
- Identity Mapping
- Single Sign On
- Grid/Web Service Middleware
- Grid(OGSA)/Web Serviced Application

# Related Members

- 7 Computing Centers in Japan
  – Hokkaido Univ. , Tohoku Univ. , Tokyo Univ. , Nagoya Univ. ,Kyoto Univ. , Osaka Univ. , Kyusyu Univ.
- Cooperative activities
  – Authentication Workshop
    Considering Campus-Wide authentication infrastructure
  – Grid Computing Workshop
    Considering computing service federation among Computing Centers
- NAREGI PKI WG
  – Supports activities of 7 Computing Centers from technical aspects

## *National Research Grid Initiative (NAREGI) Project:Overview*

- A new Japanese MEXT National Grid R&D project
  **~$(US)17M** FY'03 (similar until FY'07)

- One of two major Japanese Govt. Grid Projects

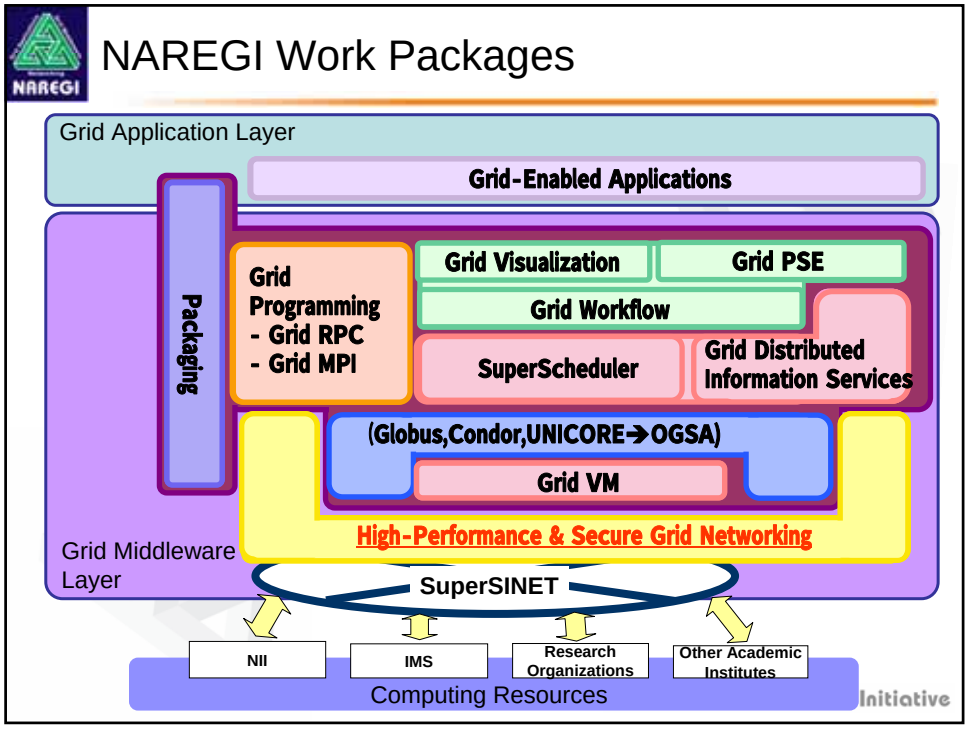
- Collaboration of National Labs. Universities and Major Computing and Nanotechnology Industries

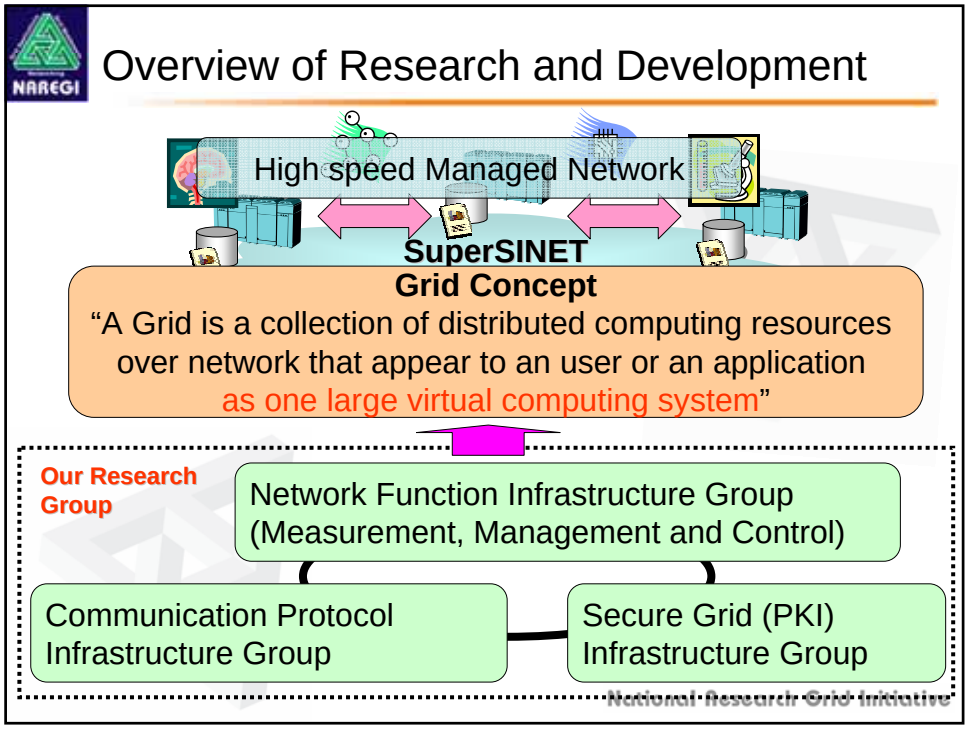
-Acquisition of Computer Resources is done (FY2003)
  -5TFlops, 700GB for development
  -10TFlobs, 5TB for application

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

## *NAREGI Work Packages*

- WP-1: National-Scale Grid Resource Management:
  Matsuoka (Titech), Kohno(ECU), Aida (Titech)
- WP-2: Grid Programming:
  Sekiguchi(AIST), Ishikawa(AIST)
- WP-3: User-Level Grid Tools & PSE:
  Miura (NII), Sato (Tsukuba-u), Kawata (Utsunomiya-u)
- WP-4: Packaging and Configuration Management:
  Miura (NII)
- WP-5: Networking, National-Scale Security & User Management
  Shimojo, Imase (Osaka-u), Oie ( Kyushu Tech.)
- WP-6: Grid-Enabling Nanoscience Applications :
  Aoyagi (Kyushu-u)


NAREGI Work Packages
Grid Application Layer
Grid-Enabled Applications
Packaging
Grid Programming
- Grid RPC
- Grid MPI
Grid Visualization
Grid PSE
Grid Workflow
SuperScheduler
Grid Distributed Information Services
(Globus,Condor,UNICORE→OGSA)
Grid VM
High-Performance & Secure Grid Networking
Grid Middleware Layer
SuperSINET
NII
IMS
Research Organizations
Other Academic Institutes
Computing Resources
Initiative


Overview of Research and Development
High speed Managed Network
SuperSINET
Grid Concept
"A Grid is a collection of distributed computing resources over network that appear to an user or an application as one large virtual computing system"
Our Research Group
Network Function Infrastructure Group (Measurement, Management and Control)
Communication Protocol Infrastructure Group
Secure Grid (PKI) Infrastructure Group
National Research Grid Initiative

## Research Plan of Secure Grid Infrastructure

Develop a security model for Grid based on PKI and realize authentication across organizations and VO management

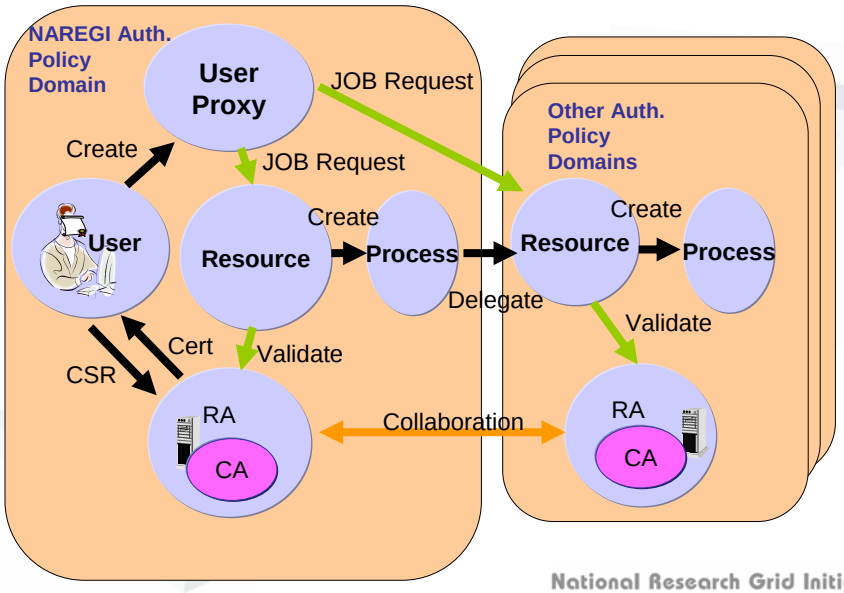
Development and Operation of authentication service for UNICORE and Globus

Development of certification authority (CA) ,registration authority (RA) and authentication policy based on the basic assurance level defined by GGF

Research & Development of authentication mechanism across policy domains to be proposed to GGF

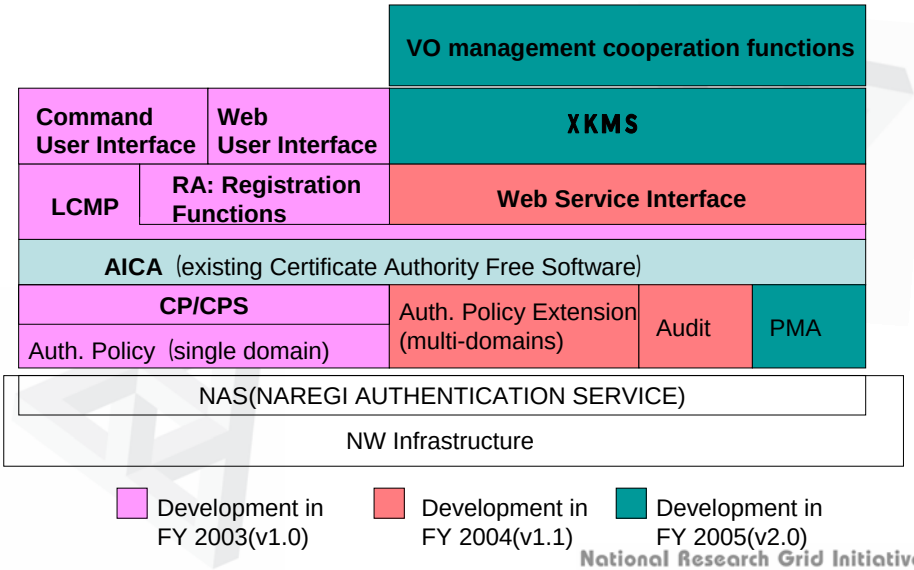
National Research Grid Initiative

## A Security Model of Grid communication platform




National Research Grid Initiative

## Software Stack of NAREGI-CA




National Research Grid Initiative

## NAREGI-CA Features

- Compliance with the basic security level of GGF
  - Independent Registration Authority (RA) Server
  - Practical CP/CPS Template
- License ID management
  - Transfer authentication responsibility to Local RA
- Dual interfaces for certificate request
  - Web & command line enrollment
- Grid operation extensions
  - Batch issue of certificates by command lines
  - Assistance of Grid-mapfile & UUDB creation
- Future extensions
  - Cooperation of CA's by linking policy domains
  - ID federation between sites
  - VO Management

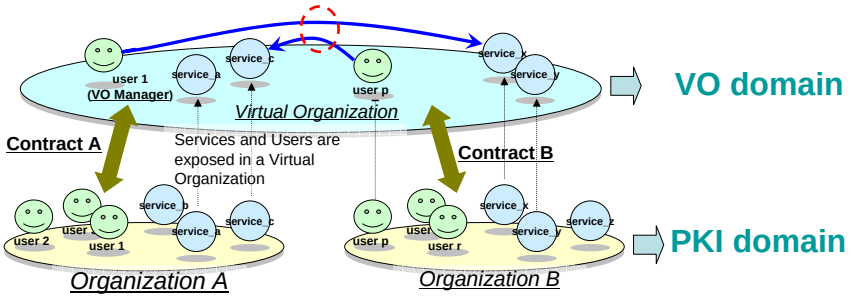
National Research Grid Initiative

# Virtual Organization and Security Domain

峰尾@PKI.NEC

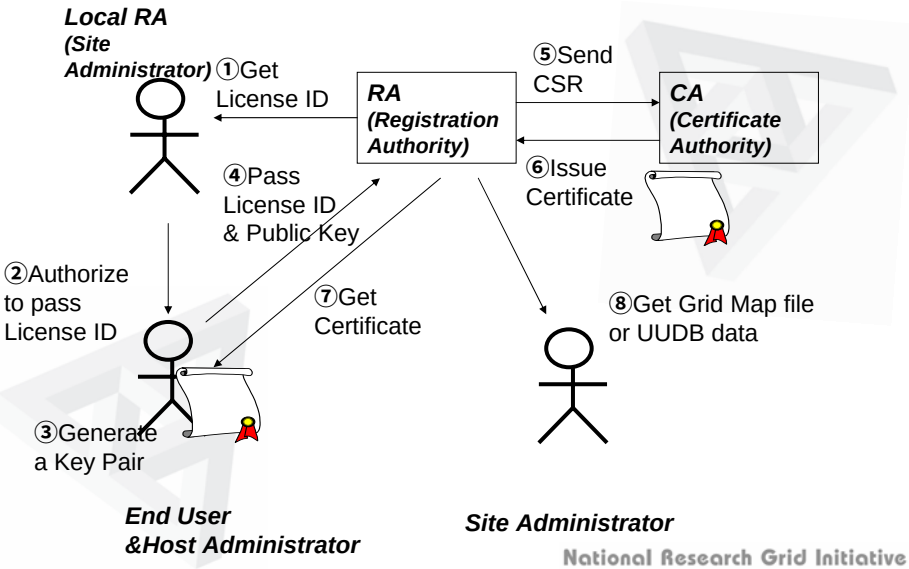
Definition of VO on GGF
- CAS (Community Authorization Service)
- VOMS (Virtual Organization Membership Service)

A virtual organization(VO) is a dynamic collection of resources and users unified by a common goal and potentially spanning multiple administrative domains.

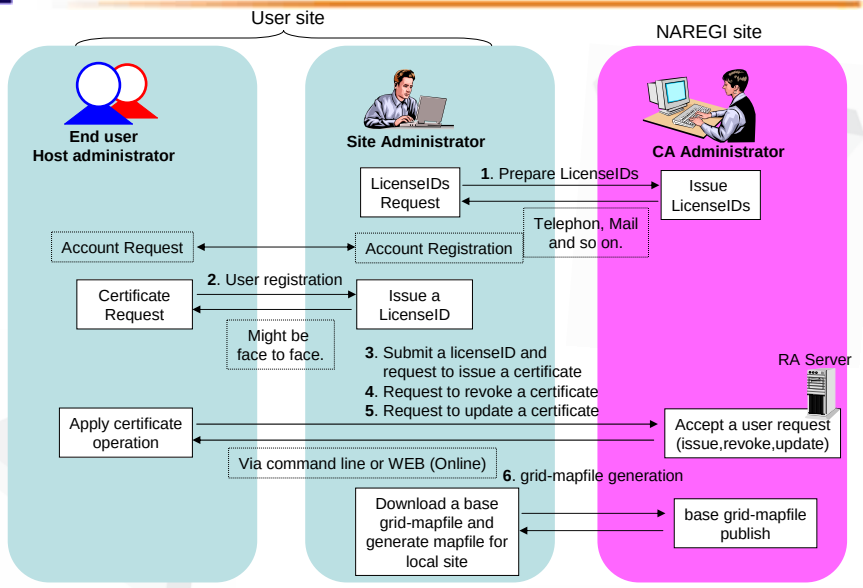





# NAREGI-CA Architecture



# NAREGI-CA Registration Sequence




National Research Grid Initiative

# XKMS Interface in NAREGI-CA v2.0

- Certificate Issue basic Interface
  - Application
    - XKRSS Registration
    - XKRSS Request Authentication
  - Issue Management
    - XKRSS Revocation
- Certificate Information Services Basic Interface
  - Certificate Retrieval
    - XKISS Locate
  - Signature Verification
    - XKISS Validate

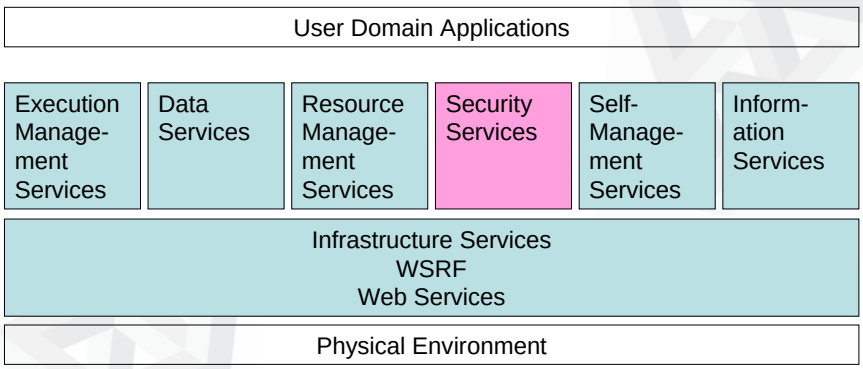
National Research Grid Initiative

## NAREGI-CA Distribution

- Free Software according to the NAREGI intellectual property management rules
- Distribution records of the current version 1.0
  - 61 at GGF, SC2004, etc.
- Research collaboration
  - Audit of CA :AIST, Japan
  - PMA for international cooperation :APGRID
- Future plan
  - Distribution in Rocks Roll by SDSC, USA

National Research Grid Initiative

## Future Plan based on the OGSA Framework

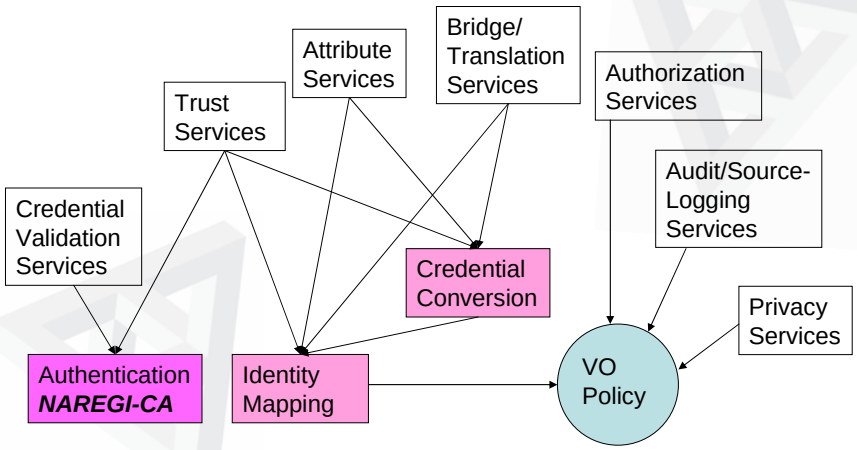



The Open Grid Services Architecture, Version 1.0

National Research Grid Initiative

# Functional Capabilities

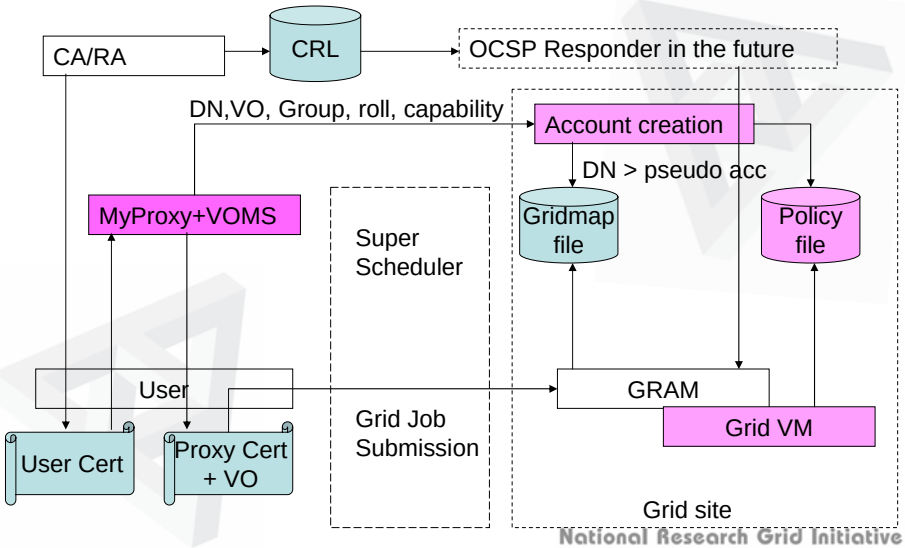
Hypothetical OGSA version 2.0 documents schedule
Security Services :WG draft publication GGF17('06/6)




National Research Grid Initiative
The Open Grid Services Architecture, Version 1.0

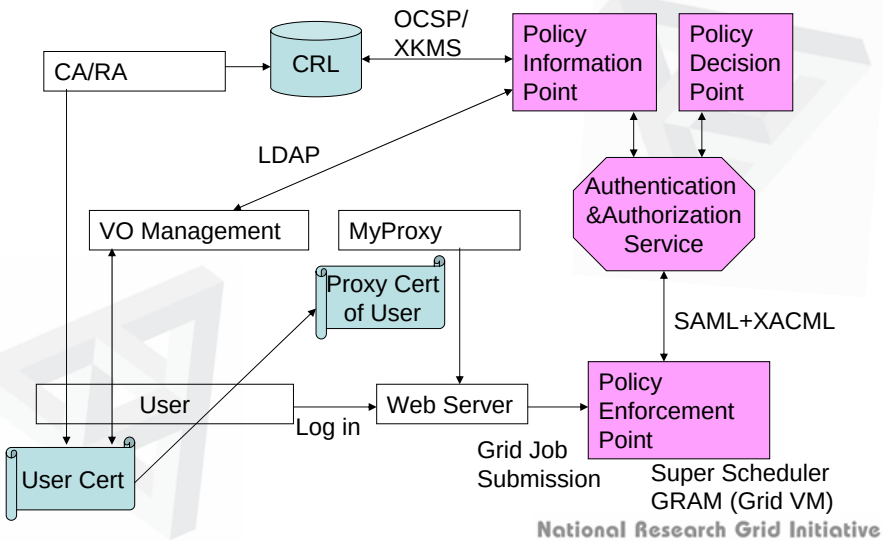
# VOMS-type VO Management

NAREGI Middleware beta version, FY2005




National Research Grid Initiative

# AuthN&AuthZ Services in the future

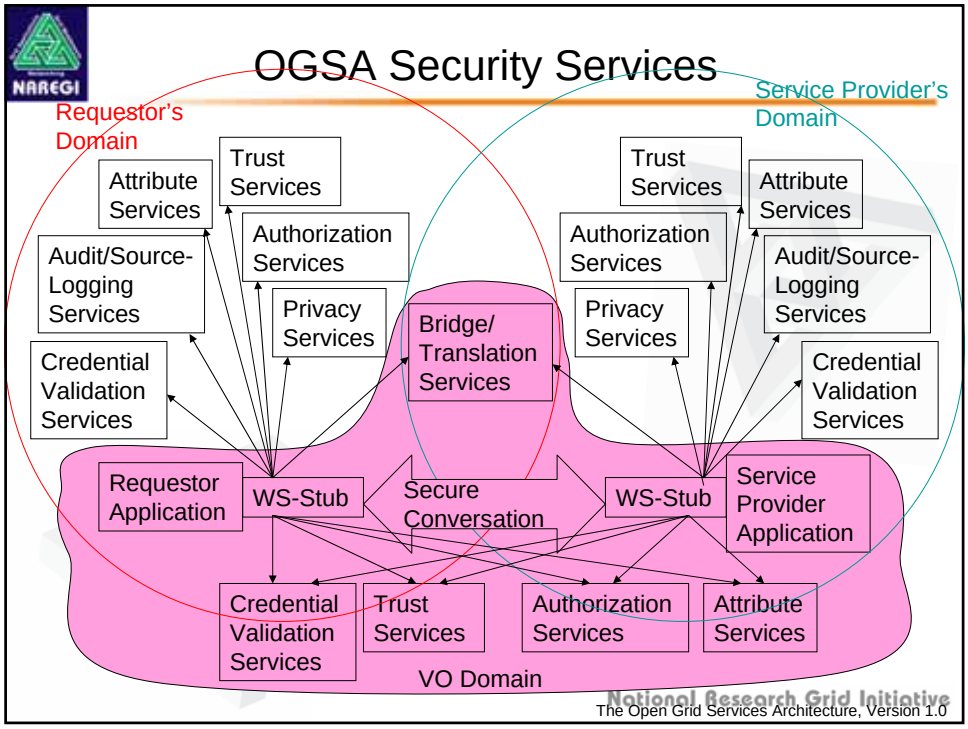



National Research Grid Initiative

# Toward OGSA Security Services

- Core Functional Capabilities
  - Authentication
    - NAREGI-CA
  - Identity Mapping
    - ID Federation
  - Credential Conversion
    - UNICORE-Globus Cooperation
  - VO Management
- OGSA Security Services (T.B.D.)
  - Credential Validation Services
  - Trust Services
  - Attribute Services
  - Bridge/Translation Services
  - Authorization Services
  - Audit/Source-Logging Services
  - Privacy Services

National Research Grid Initiative




## Road to Cyber Science Infrastructure

- 3-4 year plan
- Define Two security domain
  - Equivalent to commercial level domain
  - Grid/PMA (Policy Management Authority) level domain
- Set up national PKI and its operation team
- Build international trust for globus cyberinfrastructure

# Summary

- We need cyberscience infrastructure (CSI) for future collaborative science and education.
- We believe PKI provides secure infrastructure for CSI.
- International collaborative effort is necessary to build global CSI.
- Professional collaboration for science and technology is necessary.