

NAREGI makes IT Safe - Grid Security

As a basis of the Cyber Science Infrastructure

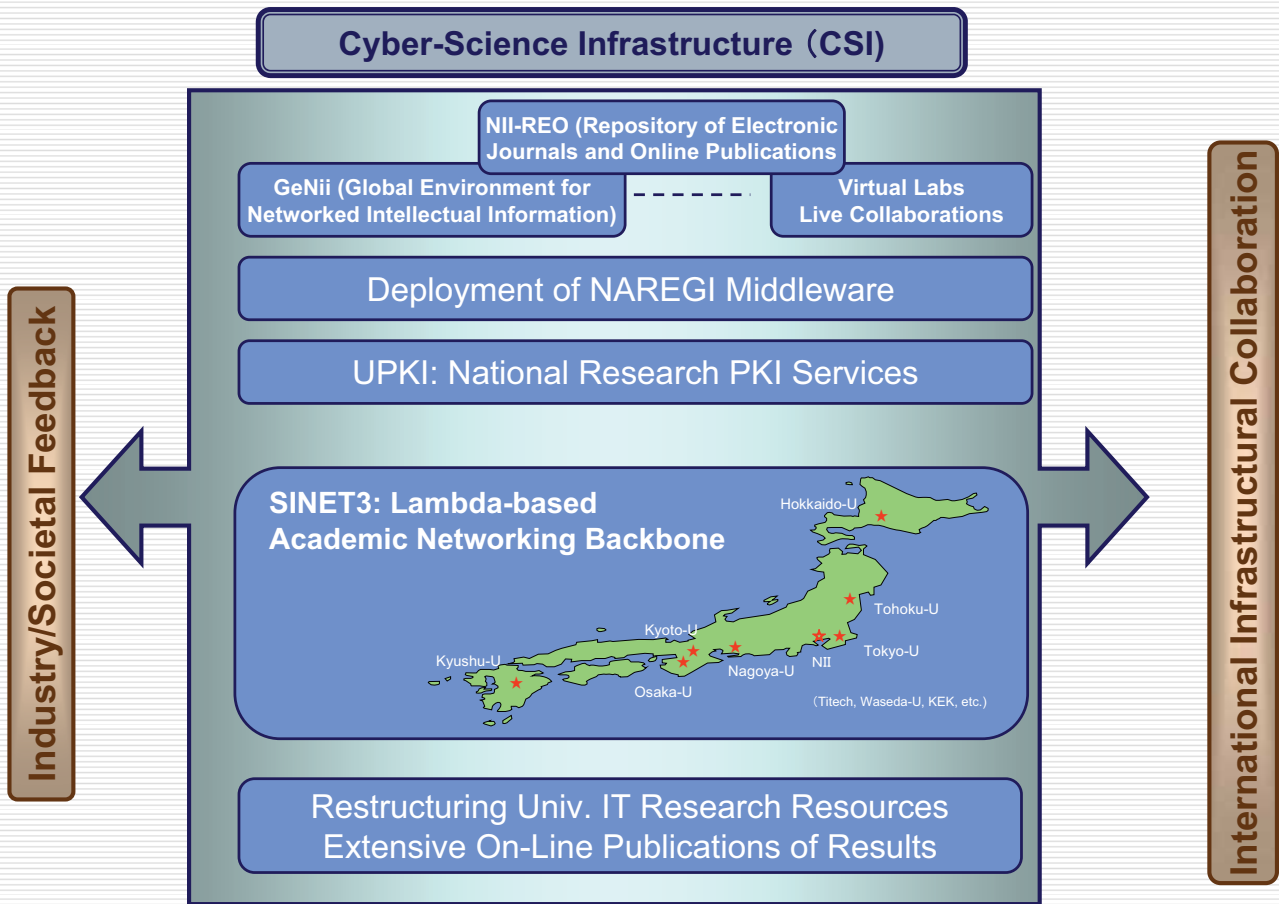
Shinichi Mineo
(National Institute of Informatics)



Outline

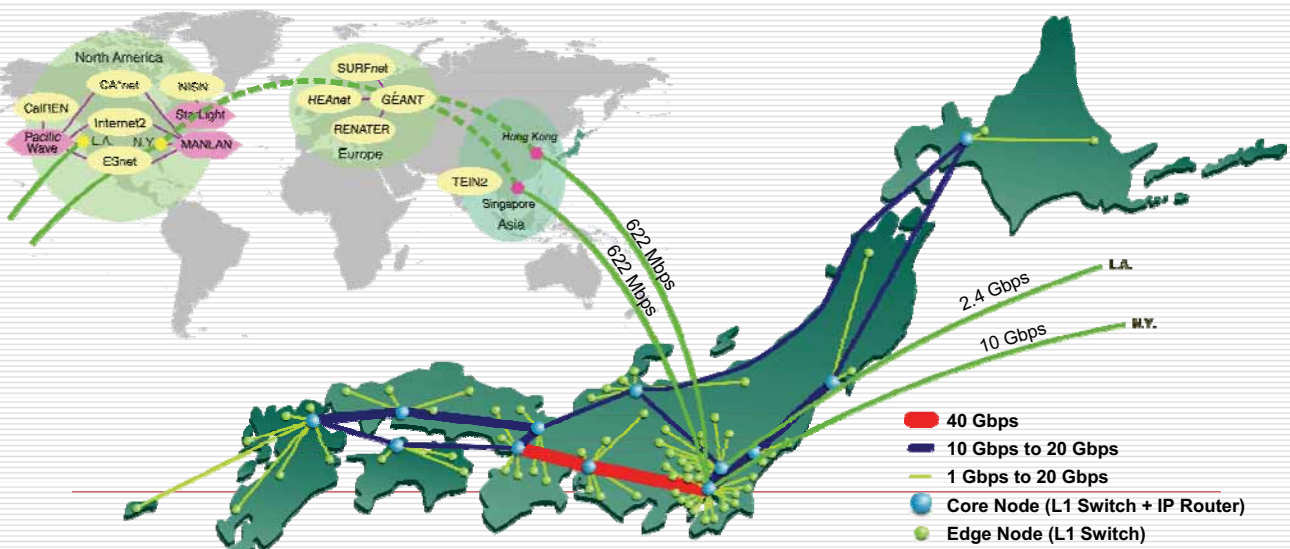
- Introduction of CSI :Cyber Science Infrastructure
 - Concept of UPKI :National Research PKI Infrastructure
 - Security Features developed for NAREGI Middleware
 - Summary & Open Issues
-

Cyber Science Infrastructure for R & D

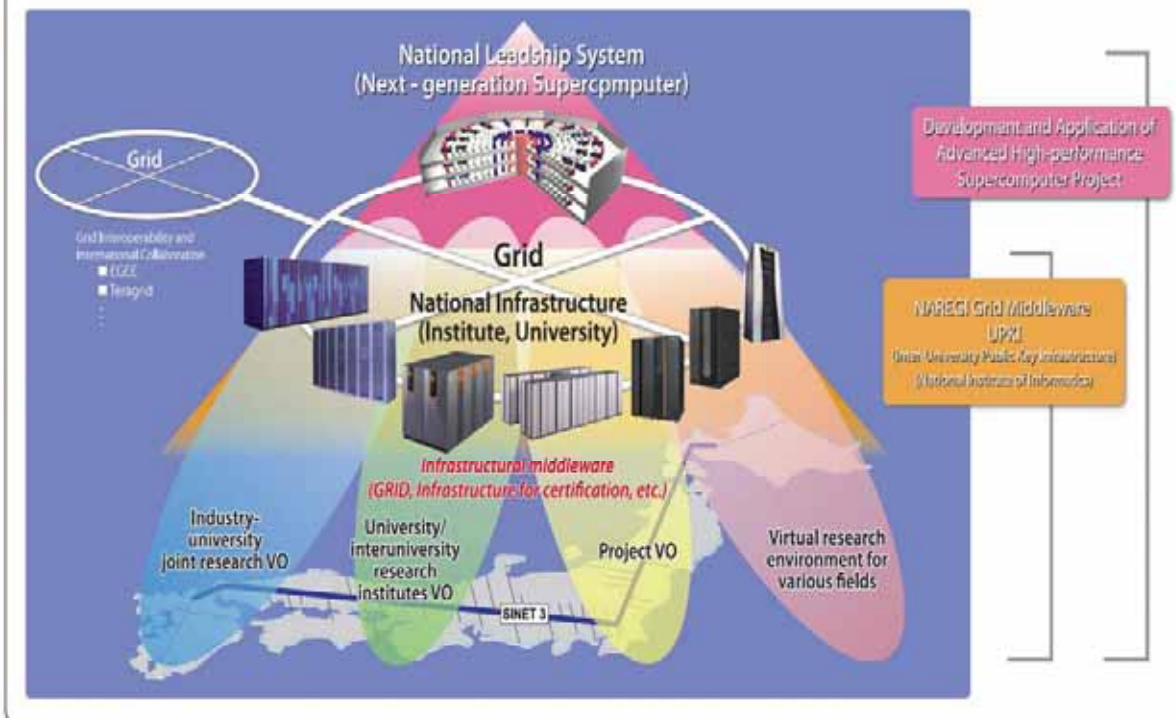


SINET3: Science Information Network 3

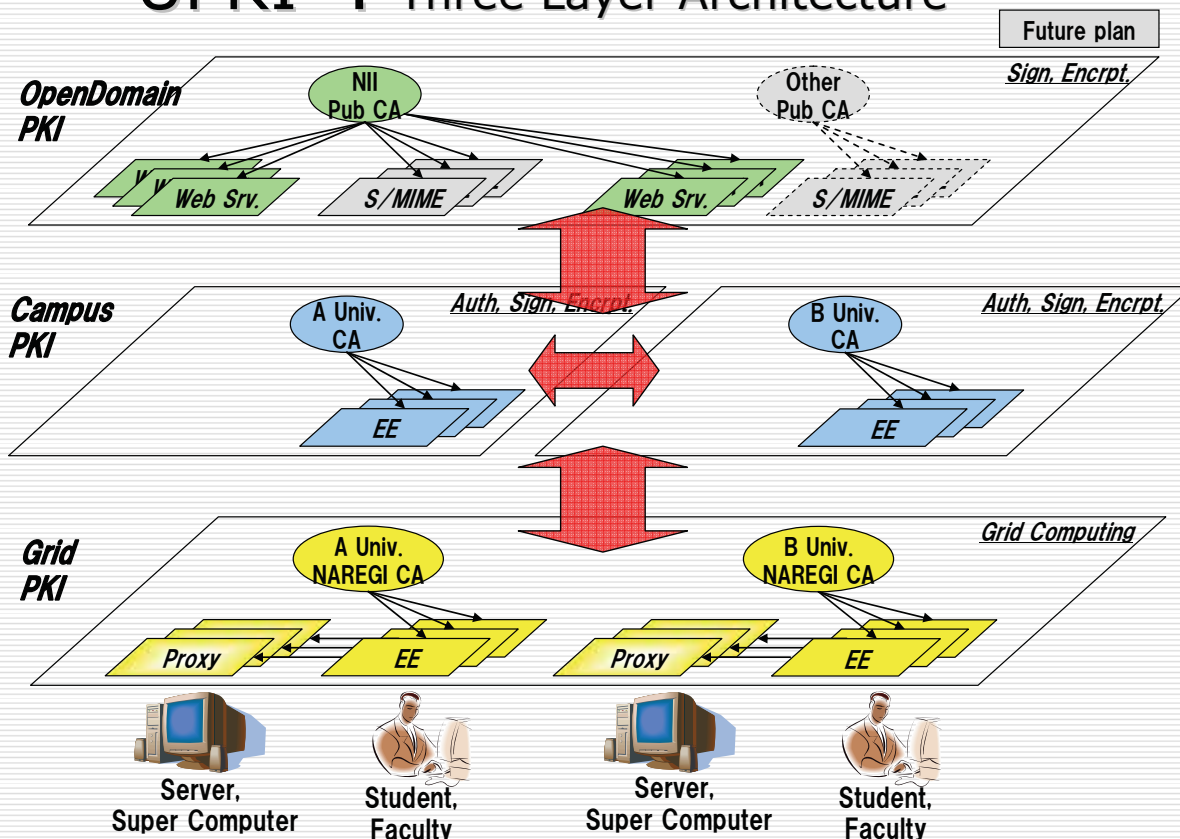
- ★ **Innovative academic infrastructure** for more than 700 universities and research institutions.
 - Provides **wide variety of services** such as multi-layer transfer, VPN, QoS, and bandwidth-on-demand services and **sufficient bandwidth** with Japan's first STM-256 (40 Gbps) deployment.
 - Enables **quick service recovery** by multiple-loop topology against link and node failures.
 - Carries on **its full-scale operations** since June 2007.



Cyber Science Infrastructure Plan Toward Petascale Computing



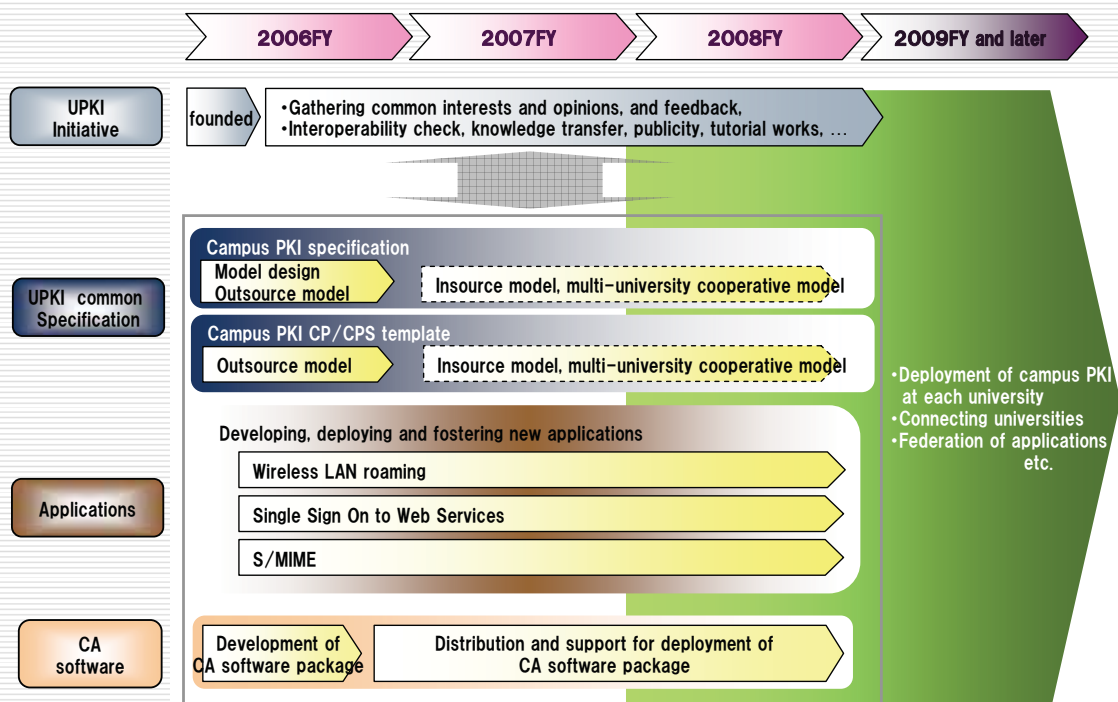
UPKI : Three Layer Architecture



Concept of UPKI

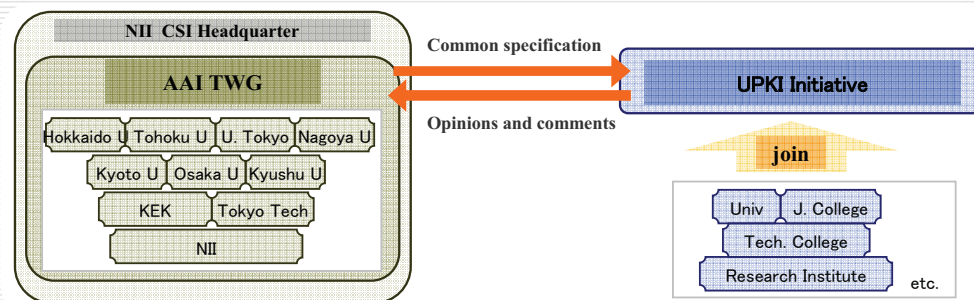
- Open Domain PKI
 - Public Server Certification
 - Digital Signature/Encryption of e-mails by S/MIME
- Campus PKI
 - Identity Management
 - SSO for Web services
 - Wireless LAN roaming and VPN
- Grid PKI
 - Grid Services

UPKI Development Plan



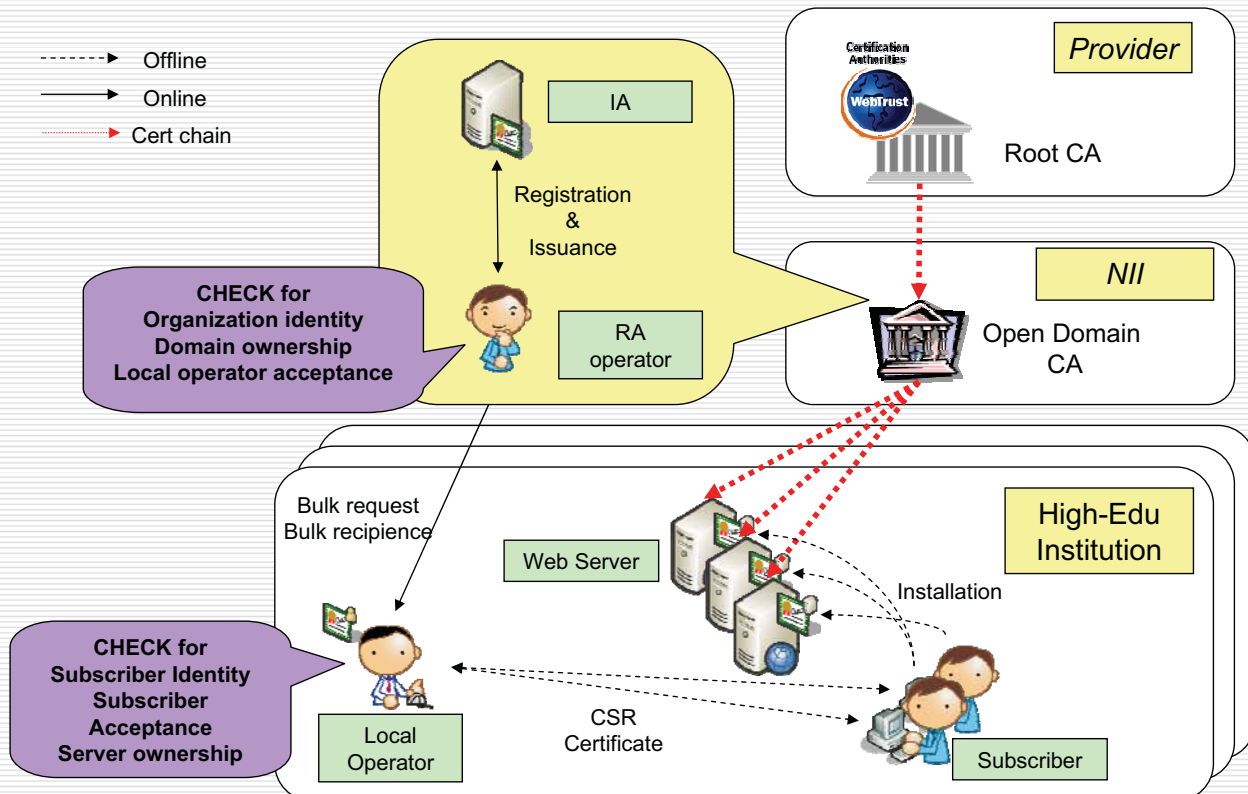
UPKI Initiative

- ❑ Founded in 16 Aug 2006
- ❑ Sponsored by NII AAI TWG
- ❑ Mission
 - Gathering interests and opinions from academic and industry stakeholders.
- ❑ <https://upki-portal.nii.ac.jp/>



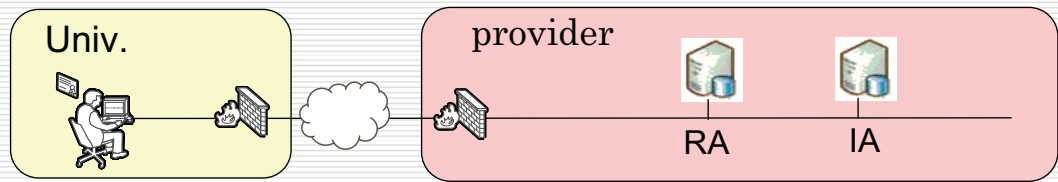
NII Public CA for Open Domain PKI

Now in Test Service

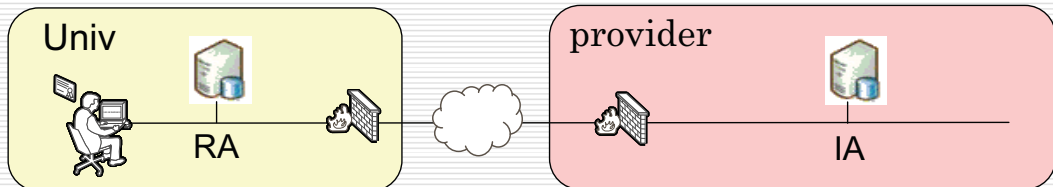


Campus PKI Operation Models

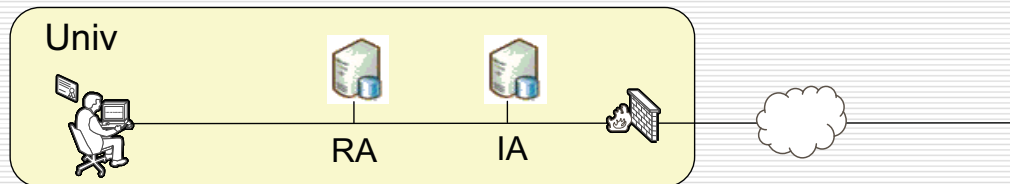
1. Full outsource



2. IA outsource

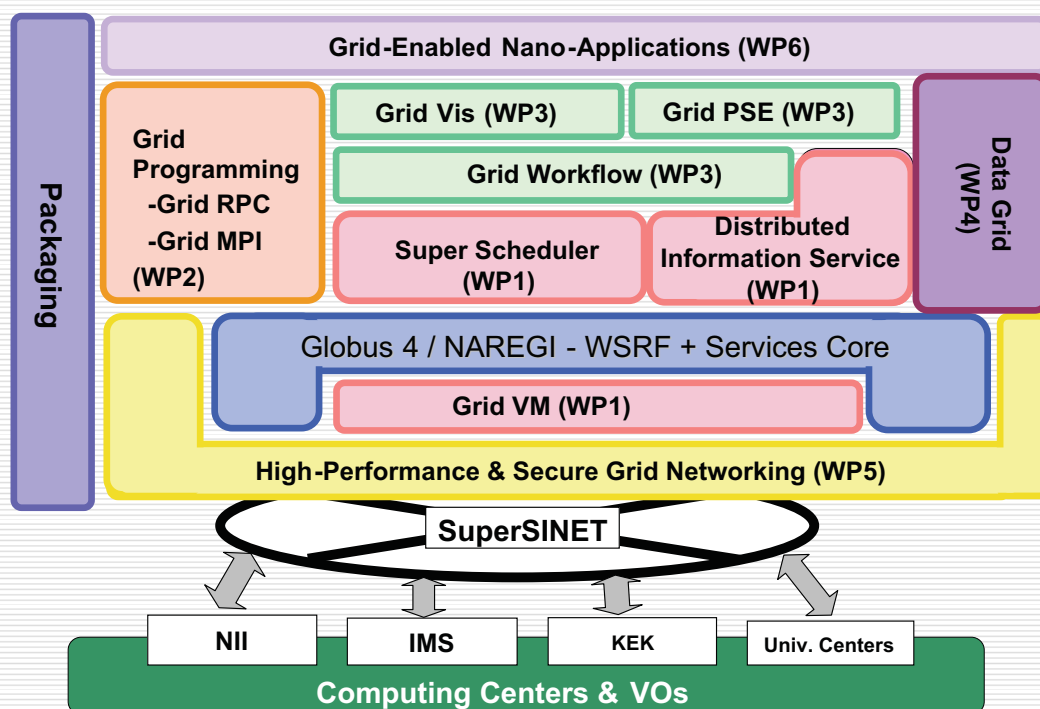


3. In source



NAREGI Software Stack

as of Beta ver. 2006



Requirements in Grid Security

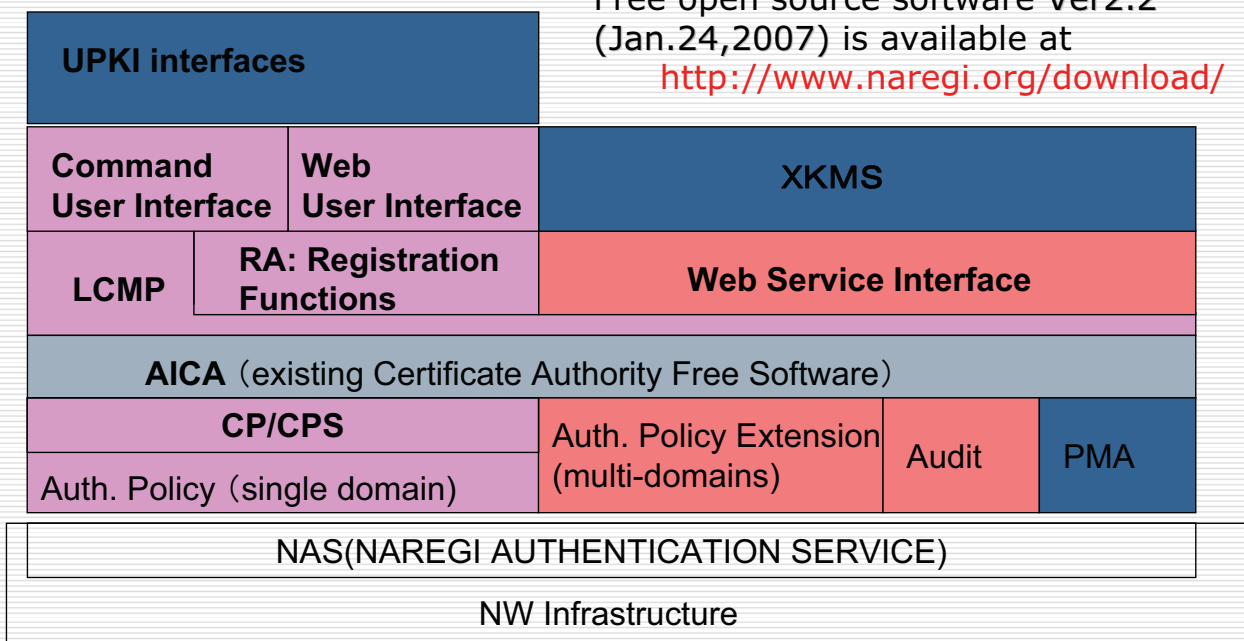
- Authentication
 - PKI based user authentication
 - Compatible with GSI standards
 - Trust federation between CA's*Developed
NAREGI-CA to be
deployed in UPKI*

- Authorization
 - VO management for Inter-organizational collaboration
 - Interoperability with other Grid projects*Developed
VO based AuthZ*

- Accounting
 - ID federation for authn, authz, and charging
 - With privacy protection!*Future issues*

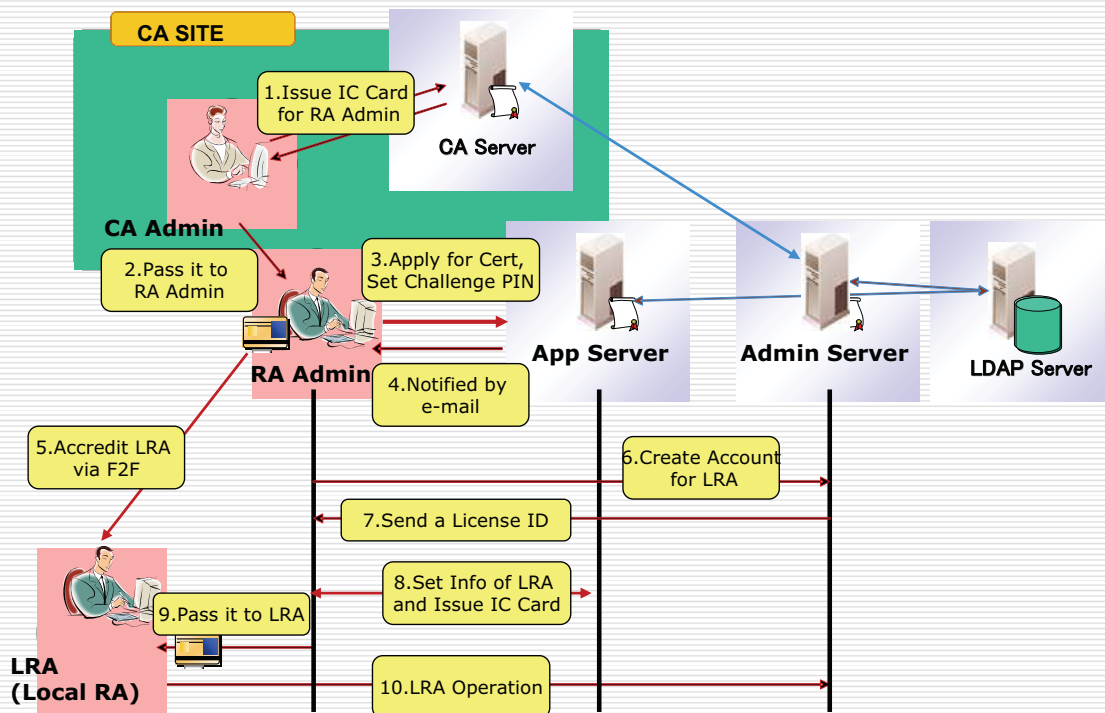
Software Stack of NAREGI-CA

Free open source software Ver2.2 (Jan.24,2007) is available at <http://www.naregi.org/download/>

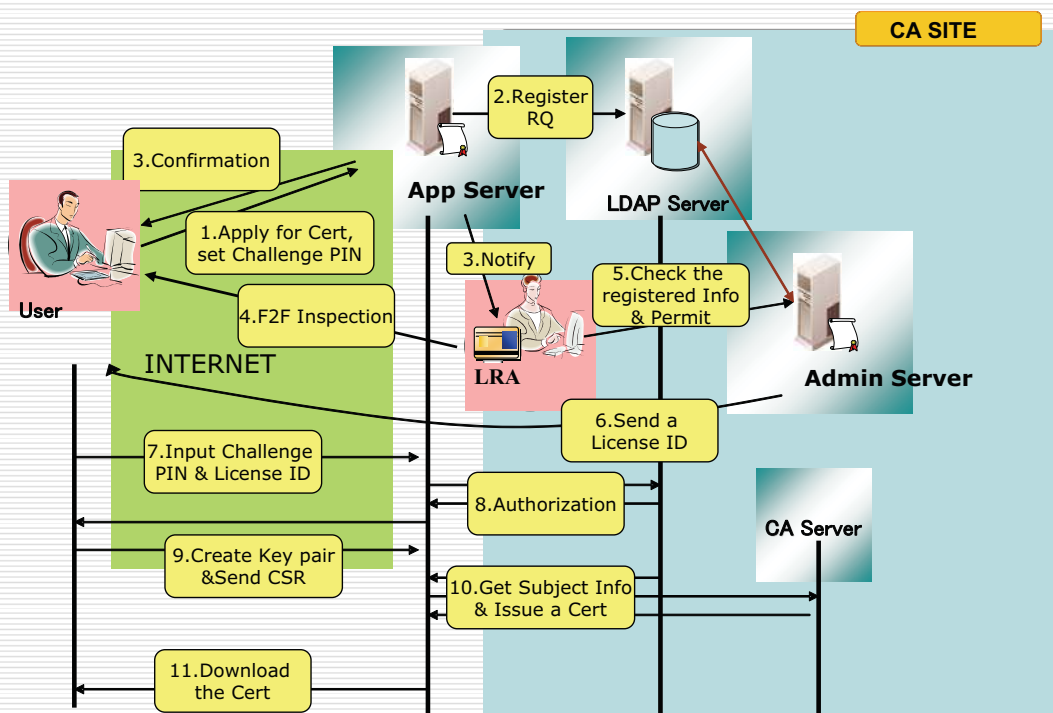


Development in FY 2003(v1.0)
 Development in FY 2004(v1.1)
 Development in FY 2005~

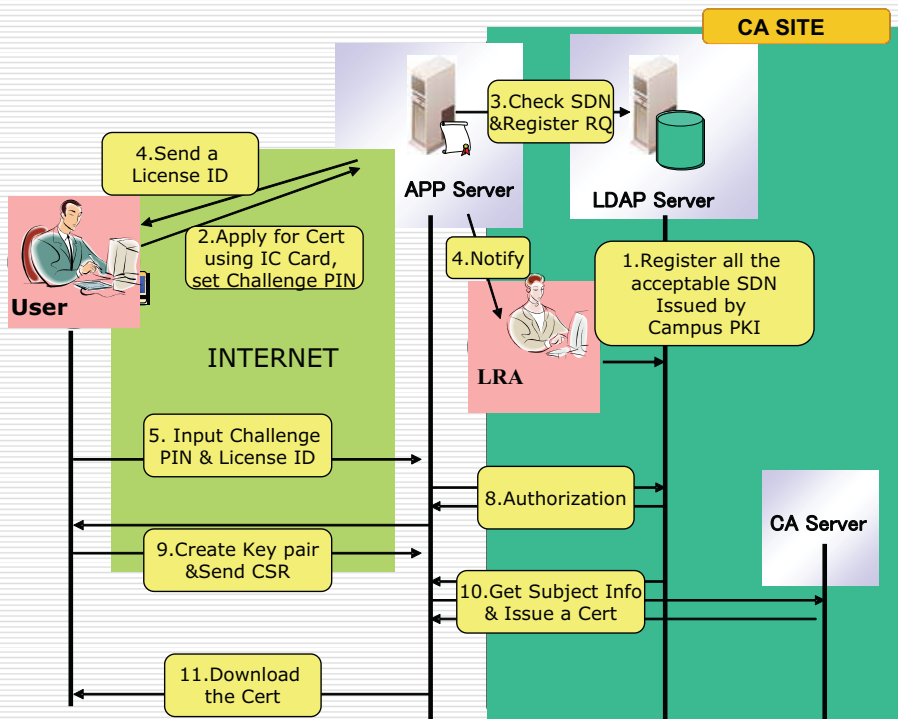
UPKI INTERFACE -1: Distribution of RA using IC Cards



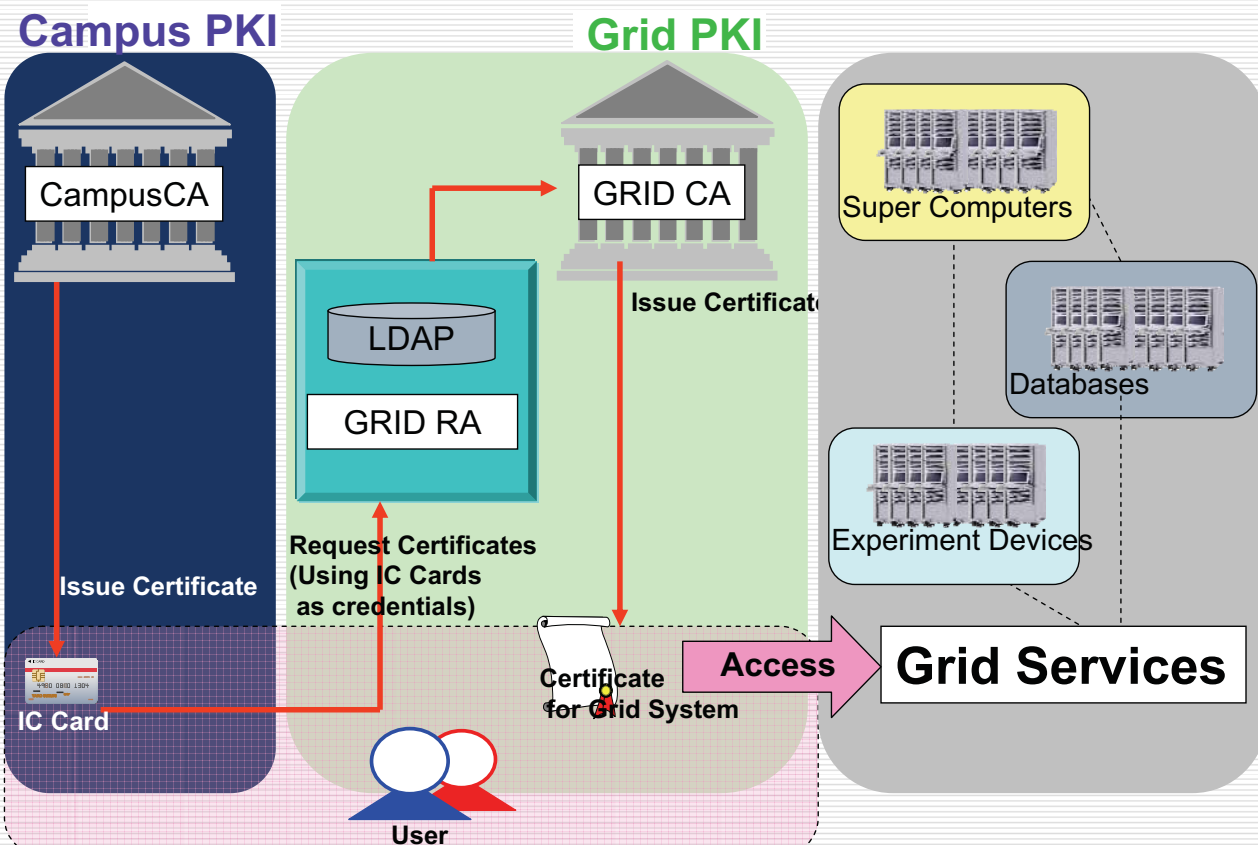
UPKI INTERFACE -2: Self-help Cert Issue using Challenge PIN



UPKI INTERFACE -3: Interoperation with the Campus PKI

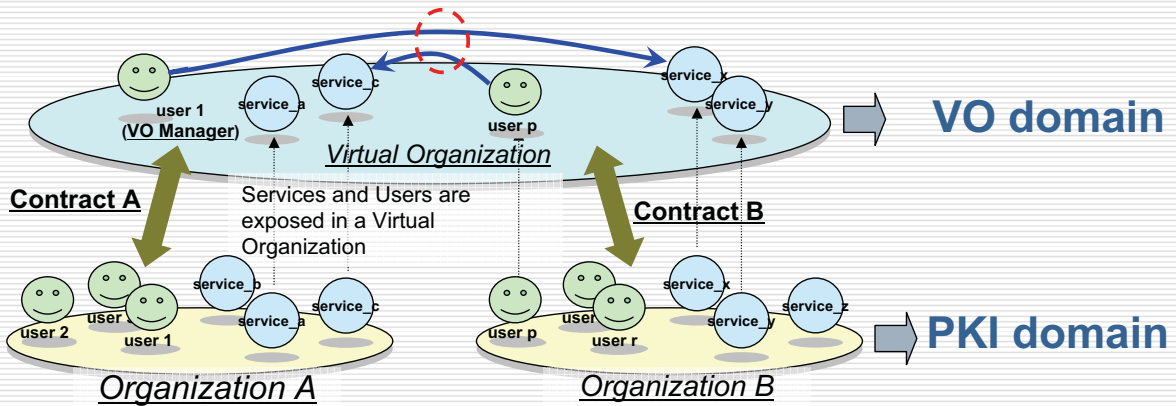


Campus-Grid PKI Federation

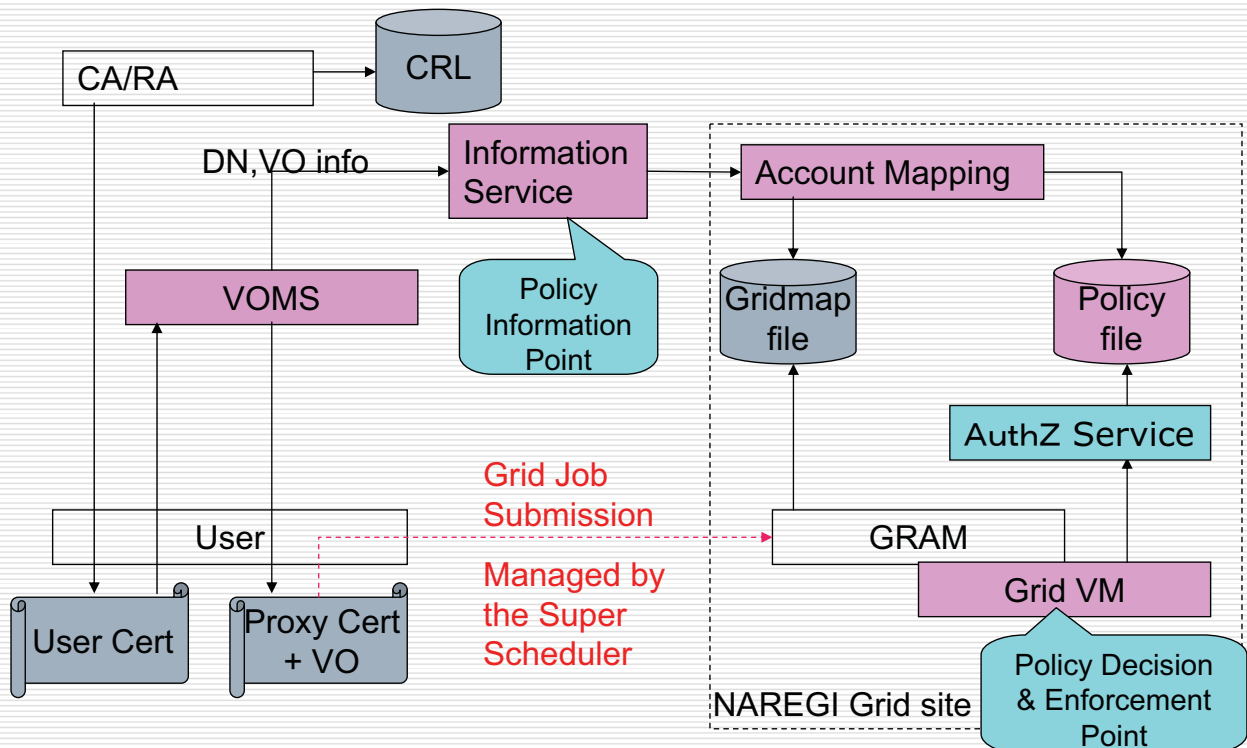


VO based Authorization

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



NAREGI adopts VOMS-type VO Management



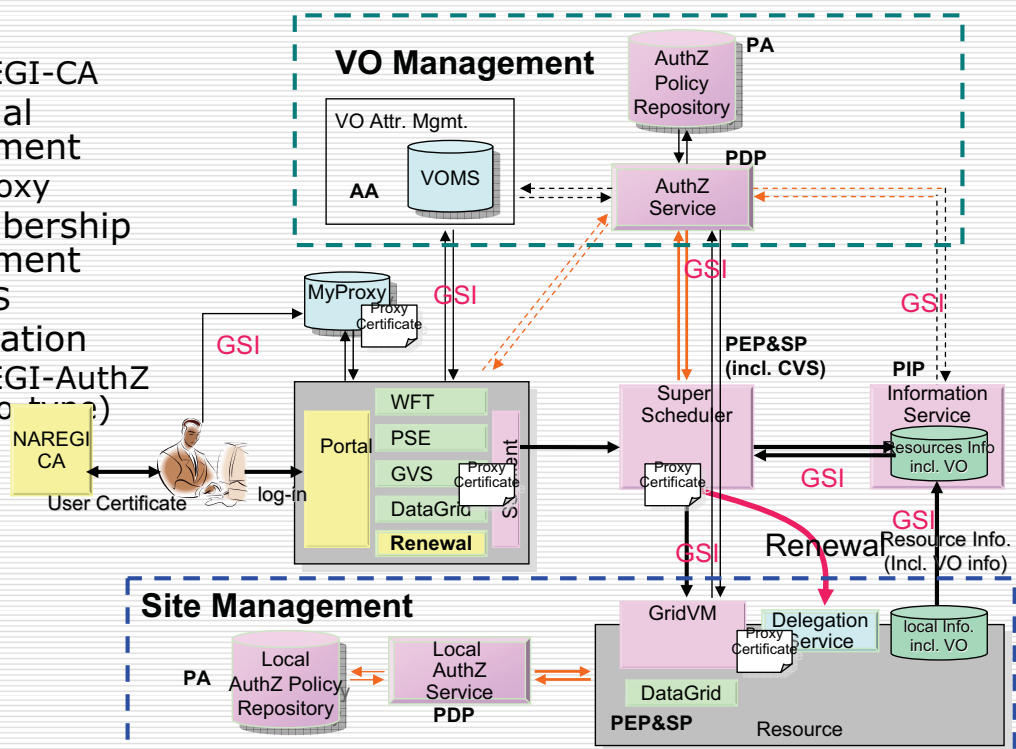
AuthZ Service

Based on SAML 2.0 & XACML 2.0 with GT4.0 AuthZ Framework

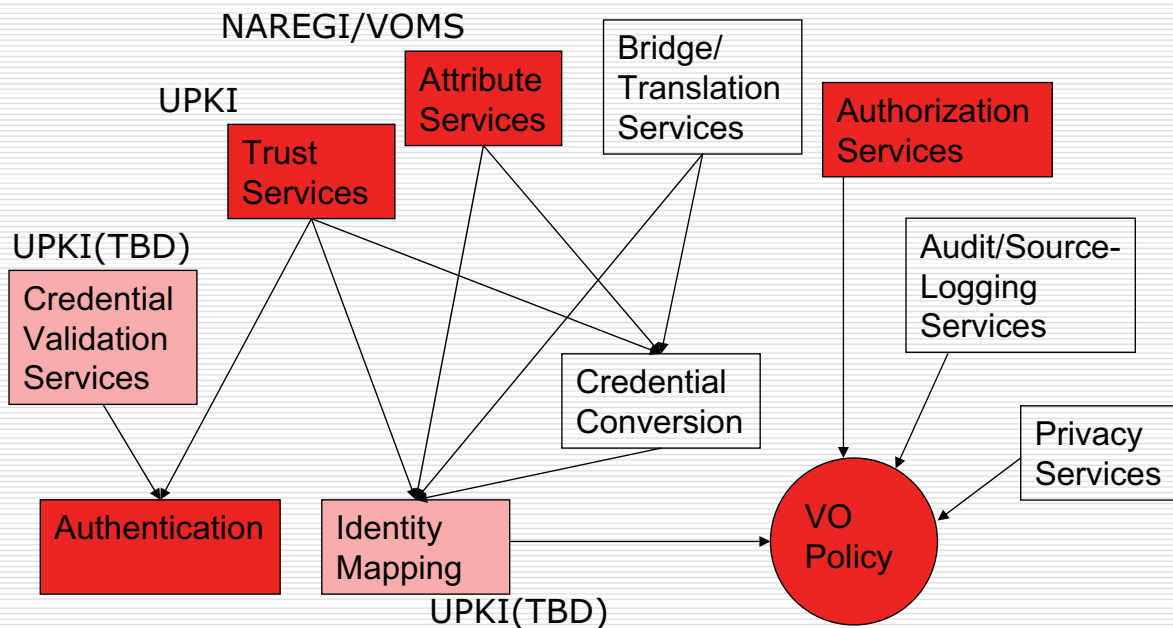
- ❑ NAREGI's XACML profile (A Plan)
 - Subject Attributes:
 - ❑ Maps of VOMS attributes in XACML Subject Attributes
 - ❑ Needs standardized attribute IDs for well-known types of credentials such as VOMS attribute certificate
 - Resource Attributes:
 - ❑ RAFM enables flexible resource attribute retrieval from the request message content to SP
 - ❑ To support for authorization for WS-Resource or finer-grained resource, this kind of mechanism is needed
 - Action Attributes:
 - ❑ Maps GT4.0 AuthZ Framework Property to an XACML Action Attribute
 - ❑ wsa:Action may also work well

Security Architecture - Overview

- ❑ CA
 - NAREGI-CA
- ❑ Credential Management
 - MyProxy
- ❑ VO Membership Management
 - VOMS
- ❑ Authorization
 - NAREGI-AuthZ (Protocol)



So far, we came...



The Open Grid Services Architecture, Version 1.0

Summary & Open Issues

- ❑ CSI is composed of High-speed Backbone NW, UPKI, Grid middleware and various services ,integrating next generation peta-scale computing facilities.
- ❑ UPKI project has started to build national academic authentication and authorization infrastructure, on which Grid technology is widely used.
- ❑ NAREGI at first developed reliable AuthN system to be deployed in UPKI.
- ❑ Now NAERGI is developing VO based AuthZ service based on SAML 2.0 & XACML 2.0 with GT4.0 AuthZ Framework.
- ❑ ID mgt and Accounting are still remaining open issues to be designed jointly with all the stakeholders in CSI community.