NAREGI
Certificate Policy
and
Certification Practice Statement

Ver. 3.0

December 10, 2007

NAREGI Policy Management Authority

Change History

Date	Ver.	OID	Comments
2005.7.15	1.0	1.2.392.00200181.1.1	Initial version
2005.9.27	1.0.1	↑	Erratum correction
2006.4.28	1.0.2	↑	Change: Certificate user must be approved by user administrator.
2006.7.7	2.0	1.2.392.00200181.1.2	Policy ID and OU Name correction
2007.4.2	2.1	↑	Delete: The rule of account registration application. ADD: The rule of personal information use purpose. Change: User certificate validity period.
2007.12.10	3.0	1.2.392.00200181.1.3	Remedial action based on external audit.

1. Introduction

This Certificate Policy and Certification Practice Statement (CP/CPS) describes regulations related to operation of a Certification Authority (CA) operated by Development & Application of Advanced High-performance Supercomputer Project, Science Grid NAREGI Program (NAREGI), referred to as NAREGI CA.

This document is structured according to the Internet Engineering Task Force (IETF) Public-key Infrastructure Working Group (PKIX) Request for Comments document, RFC 2527, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

The NAREGI CA Certification Policy (CP) is also covered in this CP/CPS.

* *NAREGI (National Research Grid Initiative)*

1.1 Overview

This CP/CPS describes the various procedures related to issuing and revoking certificates and other operations and administration tasks performed by the NAREGI CA.

The NAREGI CA issues client certificates for authentication of grid computing users as well as server certificates required to use a grid computing environment. NAREGI CA issued certificates are available only to NAREGI partner research and development facilities and organizations recognized by the Director of the Center for Grid Research and Development , NAREGI (hereafter, "Special Participating Organizations").

1.1.1 Types of Certificates

The NAREGI CA issues the following certificates:

Client Certificate

Server Certificates:

Unicore Server

Globus Server

Web Server

LDAP Server

1.1.2 Related Specifications

None.

1.2 Identifiers

The NAREGI CA uses the following identifiers to identify this CP/CPS document and certificate policies.

Table 1-1 OIDs and Objects

OID	Object
1.2.392.00200181	Research Organization of Information and Systems, National Institute of Informatics, Center for GRID Research and Development
1.2.392.00200181.1.X (Note)	CPS
1.2.392.00200181.3	NAREGI CA certificate policy
1.2.392.00200181.3.1.1	Globus server certificate policy
1.2.392.00200181.3.2.1	Globus client certificate policy
1.2.392.00200181.3.3.1	Unicore server certificate policy
1.2.392.00200181.3.4.1	Unicore client certificate policy
1.2.392.00200181.3.5.1	LDAP server certificate policy
1.2.392.00200181.3.6.1	Globus/Unicore dual shared client certificate policy
1.2.392.00200181.3.7.1	Web server certificate policy

(Note: X is assigned for each major CPS version)

1.3 Community and Applicability

1.3.1 Applicability

This CP/CPS applies to certificates which provide the authentication function required to use grid computing environments.

1.3.2 Organization

(1) NAREGI Policy management authority

Decisions regarding the types of NAREGI CA operational issues indicated below are made by the NAREGI Policy Management Authority (NAREGI PMA). They include:

Decisions regarding and approval of this CP/CPS,

Decisions on countermeasures when the CA private key is compromised,

Decisions on countermeasures in emergencies,

Decisions on other important matters related to CA operations.

(2) Operating organization

The following diagram shows the authority system architecture for the operation of NAREGI CA.

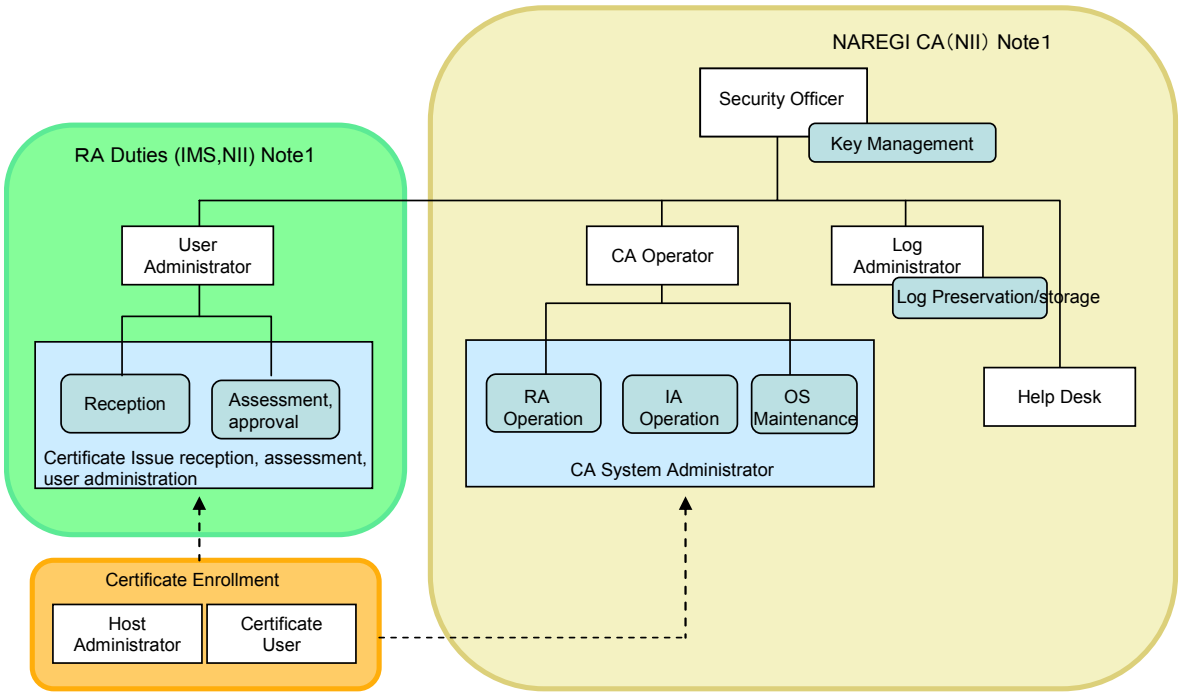

Fig. 1-1 Operating Structure and Roles

Note1. IMS: National Institutes of Natural Science, Institute for Molecular Science
NII: Research Organization of Information and Systems, National Institute of Informatics

Table 1-2 Operating Structure and Roles

Structure Elements	Major Roles
Security officer	・Does overall management of all CA tasks ・Manages CA private keys
CA Operator	・Activates/deactivates CA private keys ・Manages RA server, CA server ・Generates and distributes license IDs ・Maintains the CA systems
Log Administrator	・Manages audit logs and archive media
Help Desk	・Handles inquiries regarding certificate use
User administrator	・Accepts user enrollment, registration ・Assesses user information and approve the user
Certificate user	・Uses a certificate issued by NAREGI CA
Host administrator	・Manages servers which uses certificates

RA: Registration Authority, CA: Certificate Authority, IA: Issuing Authority

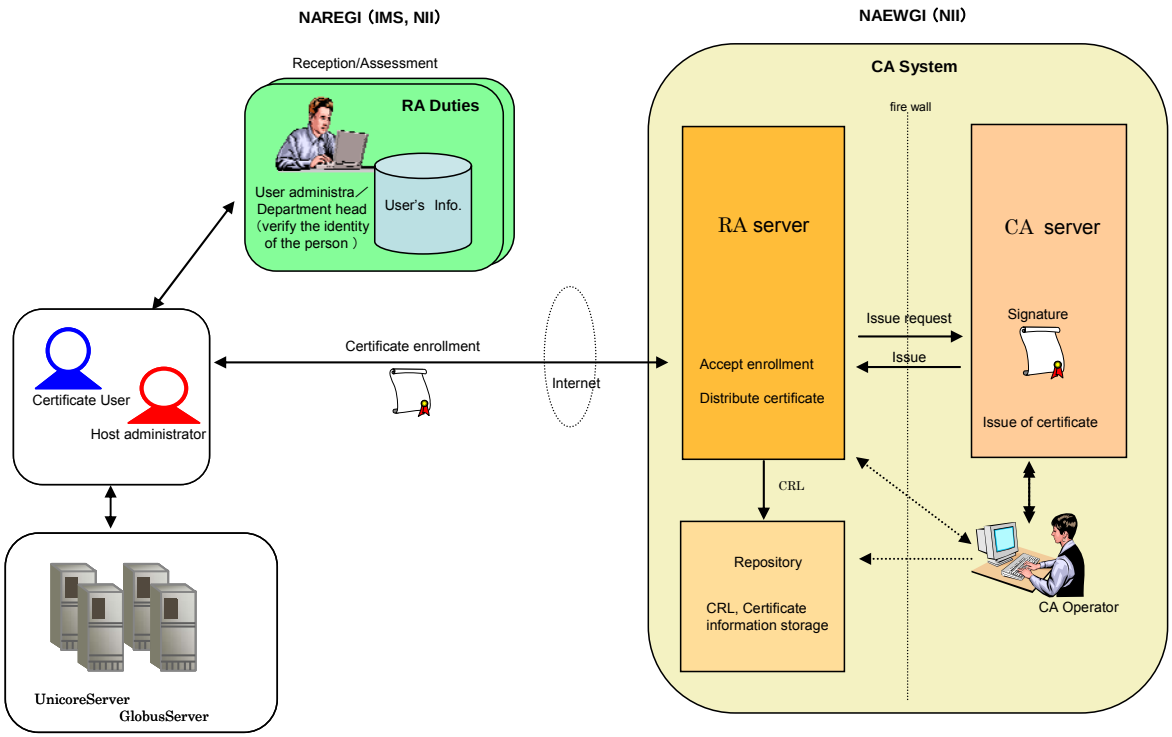

Fig.1-2 NAREGI CA System conceptual diagram

1.3.3 Applicability of Certificates

Certificates issued by the NAREGI CA are applicable as indicated in the Table 1-3 below. They should not be used outside of the scope indicated in the table.

Table1-3 Certificate types and their use

Type		Use
Client Certificate		・Client authentication when using grid computing environments ・Client authentication (SSL) when issuing and revoking certificates
Server Certificate	Globus Server Certificate	Server certification when accessing Globus
	Unicore Server Certificate	Server certification when accessing Unicore
	LDAP Server Certificate (SSL)	Certificate to access LDAP
	Web Server Certificate (SSL) (Note)	Server certification end encryption for issuing and revoking certificates.

(Note) Only applies to the NAREGI web server

1.4 Contacts related to CP/CPS

1.4.1 Administration organization

This CP/CPS is maintained and managed by the NAREGI PMA.

1.4.2 Contact Information

For inquiries regarding this CP/CPS, please contact:

Center for GRID Research and Development, National Institute of Informatics,
2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430
Phone: +81-3-4212-2857
e-mail: naregi-ca@grid.nii.ac.jp

2. General Provisions

2.1 Obligations

2.1.1 Certification Authority obligations

The CA will undertake the following obligations:

To create and manage the CA private key in a secure environment.

To verify the user administrators of the operating organization, NAREGI (IMS, NII), and generate and distribute the required license IDs.

To issue certificates reflecting the enrollment information from certificate users and host administrators (hereafter users), based on issue requests from the Registration Authority (RA).

To revoke user certificates and issue a revocation list (CRL) based on revocation requests from the RA.

To publish the CRL and certificate-related information in the repository promptly.

To specify which CP/CPS was applied upon issue of a certificate.

To make reasonable effort to ensure that users realize the importance of protecting their private data.

2.1.2 Registration Authority obligations

The RA will undertake the following obligations:

To confirm the identity of the applicant

To validate enrollment requests using the license ID, and forward applicable requests to the CA.

To authenticate the origin of revocation requests, and forward applicable requests to the CA.

To distribute certificates issued by the CA securely to the users.

To archive enrollment information securely.

2.1.3 Certificate Users, host administrators obligations

Certificate users and host administrators shall undertake the following obligations:

To provide correct information when enrolling.

To carry out enrollment and key-pair creation based on the procedures described in the documentation provided.

To refrain from using the certificate for purposes outside the scope specified in this CP/CPS.

To manage the certificate and its private key securely. To do so, they should not allow the certificate to be used by unauthorized persons. They should use a pass phrase

for the private key that is greater than 12 characters in length, and should not disclose it to persons other than the authorized user.
To instruct the CA to revoke the certificate within one working day in principle upon any actual or suspected loss, disclosure, or other compromise of the private key.
To request that the certificate be revoked within one working day in principle when it is no longer to be used. This obligation covers ownership changes and resignations.
To not share any client certificate.
To associate server certificates with only a single network entity.

2.1.4 Relying party obligations

The relying party will verify the validity of certificates and certificate paths when they are used. Verification of validity determines the following:
The certificate has not been falsified.
It is within its validity period.
It is signed by a trusted CA.
It has not been revoked.

2.1.5 User Administrator obligations

The user administrator will undertake the following obligations:
To accept enrollments from users, evaluate their originator based on previously registered user information, and approve the correct enrollment information.
To obtain the certificate issue information provided by the CA system, and create a grid map file.

2.1.6 Repository Obligations

The repository will undertake the following obligations:
To publish the information as specified in section 2.6.1 “CA Public Information”, and enable users to look-up certificates and CRL information in the repository.
To make efforts to maintain stable operation 24 hours/day and 365 days/year, with the exception of temporary suspensions for maintenance, etc.
To provide adequate protection for the registered information.

2.2 Liability

2.2.1 CA Liability

The NAREGI CA takes on the following liabilities:
To issue certificates based on enrollment information forwarded to it by the RA.
To revoke certificates based on requests forwarded to it by the RA
To register client certificate information in the repository after issue and publish it along

with a CRL, except during temporary suspensions for system maintenance, or when necessary in emergency situations

To carry on appropriate certification duties based on this CP/CPS, and to take responsibility for the authenticity of the certificates and the CRL when they are issued. The NAREGI CA will sign these materials, but if they are falsified by a third party, or the signature algorithm becomes obsolete (e.g. when an attack is discovered, etc.), authenticity cannot be guaranteed.

The NAREGI CA will carry on appropriate practices based on this CP/CPS in order to prevent compromise of private keys through theft or loss.

2.2.2 RA Liability

The NAREGI CA takes on the following liability regarding RA duties:

To forward user enrollment requests to the CA correctly.

To forward user revocation requests to the CA promptly.

To carry out the certification practices appropriately based on this CP/CPS in order to prevent unauthorized access or falsification of the enrollment and other confidential information.

2.2.3 Certificate users and host administrators liability

Certificate Users and host administrators are liable to manage certificates and private keys to prevent compromise through theft or loss.

2.2.4 VA liability

No stipulation.

2.2.5 User administrator liability

User administrator is liable to ensure that NAREGI CA enrollment information is correct by distributing license IDs to users.

2.2.6 Repository liability

The repository has the following liabilities:

To return replies to legitimate requests for repository information during its operating periods as specified in section 2.1.6, “Repository Obligation”, of this CP/CPS.

To ensure that the most-recent version of the CRL is available when it is requested.

2.3 Financial Responsibility

No stipulation.

2.4 Interpretation and Enforcement

No stipulation.

2.5 Fees

No stipulation

2.6 Regulations related to public information

2.6.1 Publication

The following information will be published in the repository operated by the NAREGI CA:

Client certificate information used for the grid map file

Procedures for each type of NAREGI CA enrollment

The CRL issued by the NAREGI CA

The CA certificate

The CA certificate fingerprint

This CP/CPS

Use purpose of personal information

Other information related to the NAREGI CA

2.6.2 Frequency of publication

Information is to be published with frequency as follows:

Client certificate information, the CA certificate, and CA certificate fingerprint will be published in the repository as soon as they are issued.

The CRL will be published in the repository when it is refreshed on the NAREGI CA fixed schedule, and whenever a certificate is revoked.

NAREGI CA enrollment information or this CP/CPS or use purpose of personal information will be published in the repository as they are updated.

2.6.3 Access control

The information regulated in this CP/CPS, section 2.6.1, will be published on the Internet with appropriate access control..

2.6.4 Repository

The repository will store the information, as specified in this CP/CPS, section 2.6.1, and make it public on the Internet.

2.7 Compliance Audit

2.7.1 Frequency of Compliance Audit

The NAREGI CA must accept an audit at least once a year by another accredited CA. An operational audit of the staff will also be performed at least once a year.

2.7.2 Auditor identity and qualifications

Audits will be carried out by a professional auditor or expert in certification.

2.7.3 Relationship of auditor to audited party

The auditor will have no involvement in the operation of the NAREGI CA, or hold any interest in the NAREGI CA.

2.7.4 Topics covered by audit

The audit will focus on whether the NAREGI CA certification duties are compliant to this CP/CPS and the operations procedure manuals.
The NAREGI CA is expected to operate according to the Minimum CA Requirements specified by the Asia Pacific Grid Policy Management Authority (http://www.apgridpma.org/).

2.7.5 Responses to items identified by the audit

The NAREGI PMA will consider corrective steps for any issues identified by the audit in a timely manner. Once a decision has been released, the corrective plan will be submitted to the auditor, to monitor the status until the NAREGI CA measures are completed.

2.7.6 Notification of audit results

The NAREGI PMA and the NAREGI CA operations staff will be informed of the audit results. The NAREGI PMA will consider whether the results can be released to any other parties.

2.8 Confidentiality

2.8.1 Confidential information

Except for that clearly specified in section 2.6.1, “Publication”, of this CP/CPS, all related information is considered confidential. Confidential information will not be disclosed or leaked to any third party, or used outside the necessary scope.
Documents and media which include any applicable confidential information will be

stored safely, and an administrator will be designated to be responsible for them.

2.8.2 Information not considered confidential

The information indicated in section 2.6.1, “Publication” of this CP/CPS is not considered confidential.

2.8.3 Disclosure of certificate revocation or suspension information

When a user certificate is revoked, the revocation date and reason will be included in the information published in the CRL. This information is not considered confidential. Other information regarding the revocation will not be published.

2.8.4 Disclosure to law enforcement officials

No stipulation.

2.8.5 Disclosure as part of civil discovery

No stipulation.

2.8.6 Disclosure upon request by certificate owner or other party

The following information will be disclosed to the certificate owner upon request and upon verification of the owner’s identity:

Enrollment materials submitted to the NAREGI CA

Contents of the certificate

Certificate status

2.8.7 Disclosure in other circumstances

No stipulation.

2.9 Intellectual property rights

The NAREGI CA does not claim any IPR on issued certificates.

3. Identification and Authentication

3.1 Initial registration (application)

3.1.1 Types of names

Certificates issued by the NAREGI CA will be identified by X.500 Distinguished Names.

3.1.2 Requirements related to name meaning

The attributes used for the name of certificates issued by the NAREGI CA are as indicated in Table 3-1.

The CN field of DN in a user certificate must contain the name of the user. The NAREGI CA system checks the DN and will not issue a certificate if the system has already issued a valid certificate for the same DN. In such cases, the user must assign a new and unique CN field by appending any distinguishable two digits to the name.

The CN of DN field in a host certificate must contain the FQDN of the host.

Table 3-1. Attributes used in Certificates

Attribute Used	Description	Value
commonName	User name (client certificate)	Based on application information
	Host name (server certificate)	
organizationalUnitName	Name of organizational unit	CGRD
organizationName	Name of organization	National Research Grid Initiative
countryName	Name of country	JP

3.1.3 Rules for interpreting name forms

Identifiers will be according to those regulated in Table 3-1.

3.1.4 Uniqueness of names

Certificates issued by the NAREGI CA will be distinguished by assigning unique names based on ``Requirements related to name meaning'' in section 3.1.2.

3.1.5 Name claim dispute resolution procedure

No stipulation.

3.1.6 Recognition, authentication and role of trademarks

No stipulation.

3.1.7 Method for proving possession of private keys

The NAREGI CA verifies the signature on a certificate issue request (CSR) by checking that it has been signed using the private key that corresponds to the public key included in the CSR.

3.1.8 Identity of Organizations

The NAREGI CA identifies the organization by comparing it with officially recognized organization information maintained separately by the NAREGI.

3.1.9 User Identity Authentication

(1) Users from NAREGI partner research and development facilities

The user administrator receiving enrollment from certificate users, after checking that it is recognized by the department head from their organization, will verify the identity of the person by comparing the information presented by the user according to section 3.1.8, “Identity of organizations”, with the pre-registered user information. The check will include at least the following items:

User Name

Department

Mail address

For server certificates, FQDN and the administrator name of the server are checked in addition to the above information.

(2) Users from special participating organizations

When users from special participating organizations enroll for a certificate, a “Certificate Issue Enrollment Form” with the required items filled in and the following information must be submitted to the user administrator in-person:

Photo identification from the applicant’s organization (company, association, etc.).

A name card indicating the applicant’s department.

* If photo ID is not available, the above identification and a driver’s license or insurance certificate are required.

The user administrator will check receiving information from users, will verify the identity of the person by comparing this information, with the pre-registered user information.

For server certificates, FQDN and the administrator name of the server are checked in addition to the above information.

3.2 Routine Re-key

When a certificate has expired, its validity date must not be extended. A new certificate must be issued again with a new public key according to resubmission of an enrollment request in section 4.1. ``Application, assessment and issue of certificates''.

3.3 Re-key after revocation

When enrolling for reissue of a certificate after revocation, the user identity and organization will be verified according to the procedures specified in section 3.1, "Initial registration", of this CP/CPS.

3.4 Revocation request

When requesting revocation of a certificate, the user identity and organization shall be verified, in principle, as when issuing a certificate according to section 3.1, "Initial registration", of this CP/CPS.

4. Operational requirements

The operational requirements for client and server certificates are given below. This CP/CPS does not regulate self-signed CA certificates.

Communication among users, the RA sever and the CA server follows ``6.7 Network security controls''.

4.1 Application, assessment and issue of certificates

(1) Certificate application

Users from NAREGI-affiliated research facilities will present the "Certificate issue enrollment form" in-person to their department head with the required items filled in, and after receiving approval with his/her stamp or signature, present it in-person or mail (or FAX) it to the user administrator.

Users from specially participating organizations will present the "Certificate issue enrollment form" with the required items filled in, as well as photo-identification from their own organization (company, association, etc.) and a name card showing the organization and department to the user administrator.

The user administrator will inspect the application according to section 3.1.9, "User confirmation", of this CP/CPS, and if everything is in order, the user will be sent a 24-digit license ID obtained from the CA operations staff, a URL indicating where to get related documentation, and the CA certificate. The license ID and CA certificate will be sent in a manner that is safe and that only the user can receive them, using a procedure that is regulated in a another document.

Issue of the license ID, which is done between the CA operation staff and the user administrator, will be done by storing the license ID on a floppy disk and delivering it in-person or by mail. Notification of each issue will be given orally, or by e-mail.

Status changes of an issued certificate requires a revocation of the certificate and a application of a new certificate with the new, changed status. A change of a certificate is treated as a certificate issue described in ``4.1 Application, assessment and issue of certificates''.

(2) Certificate enrollment

Users will be informed of a URL where the procedure for generating the public and private keys is published, and after generating them, the user will send an online request for enrollment containing the public key to the NAREGI CA (RA server).

4.2 Certificate issuance

The process for the user, from enrolling with the NAREGI CA to obtaining the certificate, will be done on-line using the Lightweight Certificate Management Protocol

(LCMP) provided for the NAREGI CA, or the web enrollment functions provided in the standard Windows environment.

4.2.1 Receipt of Certificate enrollment

After receiving the enrollment from the user, the RA server will perform the following steps on-line:

Prompt the user to enter their license ID.

Verify that the entered license ID is valid.

Prompt the user for the enrollment information (the certificate subject information), once the license ID is verified.

Forward the certificate issue request with the enrollment information entered by the user to the CA server.

4.2.2 Certificate Issuance

The CA server will issue a certificate signed with the CA private key and the user's public key for the issue request received from the RA server.

4.2.3 Certificate delivery

Users retrieve the certificate issued by the CA server via the RA server.

4.3 Certificate Acceptance

Users will register the certificate in the certificate stores of the applicable servers to enable access as required, according to the procedure published at a URL. The user will be notified of this URL.

4.4 Certificate suspension and revocation

The procedure for revocation requests from a user or revocation from the CA can, as for certificate enrollment, be done on-line using the Lightweight Certificate Management Protocol (LCMP), or the web enrollment functions provided in standard Windows environments.

4.4.1 Circumstances for revocation

In any of the following circumstances, a certificate will be revoked due to a user request, or by the CA.

The user's key is compromised or suspected of being compromised.

The user information in the certificate is suspected of being incorrect.

The user violates his/her obligations, as specified in section 2.1.3, "User, host administrator obligations" of this CP/CPS.

When the use of the certificate will stop (including resignation of the user, etc.).
The CA private key is compromised.

4.4.2 Who can request revocation

The user of a certificate can request revocation of the certificate to the CA (RA server).The RA server will forward a revocation request to the CA based on this request.

If, when any of the circumstances specified in section 4.4.1, “Circumstances for revocation”, occurs and the user cannot, or has no intention to request revocation, it will be revoked by the CA operator. The revocation can be also requested by those who admit the certificate application and who can show the invalidation. The revocation request is reviewed according to section 4.1 `` Application, assessment and issue of certificates’’. If the request is accepted, the CA operator will revoke the certificate.

4.4.3 Procedure for revocation request

When one of the revocation situations occurs, the user may send a request revocation to the NAREGI CA (RA server) by using the procedure published at a URL of which the user will be notified.

The RA server will authenticate the user submitting the request as specified in section 3.4, “Revocation request”, of this CP/CPS. After authentication, it will send a revocation request to the CA server for the relevant certificate (the certificate used to authenticate the user).

The CA server, upon receiving the revocation request from the RA server, will revoke the certificate and update the CRL in the repository.

4.4.4 Revocation request grace period

The NAREGI CA will revoke the certificate immediately upon reception of the revocation request by the CA server, and the revocation information will be posted in the repository immediately.

4.4.5 Circumstances for suspension

The NAREGI CA does not support Certificate suspension.

4.4.6 Who can request suspension

The NAREGI CA does not support Certificate suspension.

4.4.7 Procedure for suspension request

The NAREGI CA does not support Certificate suspension.

4.4.8 Limits on suspension period

The NAREGI CA does not support Certificate suspension.

4.4.9 CRL issuance frequency

The NAREGI CA will issue a new CRL and publish it in the repository at fixed intervals in addition to when revoking a certificate.

The CRL is valid for 30 days, and it will be reissued at least seven days before the current one expires.

4.4.10 CRL checking requirements

A relying party will verify a certificate by retrieving the newest CRL published in the repository.

4.4.11 Availability of on-line validity checking

No stipulation (not supported).

4.4.12 Requirements for on-line validity checking

No stipulation.

4.4.13 Other available methods validity checking

No stipulation.

4.4.14 Verification requirements for other available validity checking methods

No stipulation.

4.4.15 Special requirements due to jeopardized private keys

No stipulation.

4.5 Security audit procedures

To promote a safe environment, the NAREGI CA will record an audit log of any incidents related to the CA or RA servers or operational procedures.

4.5.1 Types of event recorded

The following information will be recorded by the NAREGI CA. For each record, the event type, date and time, and occurrence information (system name, operations staff name, etc.) will be included.

CA Server log

CA Server access log

Certificate and CRL issue and revocation log

Error log
OS Login, Logout, Reboot log
RA Server log
CRL Publisher activity log
CRL Publisher error log
RA Server access log
Certificate issue, revocation log
Error log
OS Login, Logout, Reboot log
HSM log
Token access log
Machine room work record
Key sign-out journal

4.5.2 Frequency of log audit

Logs will be audited based on instructions from the CA Officer.

4.5.3 Retention period for audit log

Audit logs will be retained for three years.

4.5.4 Protection of audit logs

Access to the CA server, RA server, and HSM logs will be controlled using OS functions.
The machine room work record, and key sign-out journal will be checked by the CA officer, and each record will be signed-off and given assigning record and page numbers.
Audit logs will be protected in a lockable cabinet in a room with appropriate entry management, with access to the keys managed by the log administrator.

4.5.5 Audit log backup procedures

CA operators will obtain each type of log recorded by the CA server and other systems on external media weekly, and store them monthly.

4.5.6 Audit log collection system

No stipulation.

4.5.7 Recorded event notification

No stipulation.

4.5.8 Vulnerability assessment

No stipulation.

4.6 Records Archival

4.6.1 Types of archive data

The NAREGI CA will store the following archive data. Documents shall be stored by including all versions and their revision history.

All certificates and the CRL issued by the NAREGI CA

All enrollments submitted by users and any notifications sent to users with identity information of users

A record of any work done related to the CA key

The audit logs as specified in section 4.5.1, "Types of event recorded" of this CP/CPS

The operation organization chart

The NAREGI organization chart

Conformance audit and security audit records

Certificate use rules and guides provided to users

This CP/CPS, profile plan, and operational procedures documents

Other important materials related to decisions of the NEREGI PMA

4.6.2 Retention period for archive data

Archived data will be stored for three years. Records related certificate will be stored for three years from the end of the validity.

4.6.3 Protection of archive data

Section 4.5.4, "Protection of audit logs", of this CP/CPS specifies how the archive logs are to be protected.

Archive data will be protected in an indoor, lockable locker with appropriate entry control, and the log administrator will manage sign-out of the locker key.

4.6.4 Archive backup procedures

The CA operations staff will archive the CA server and other data on external storage media weekly, and store this media monthly.

4.6.5 Requirements for time-stamping of records

Archive data stored in electronic form will be time stamped.

4.6.6 Archive collection system

No stipulation.

4.6.7 Procedures to verify archive information

No stipulation.

4.7 Key changeover

4.7.1 User certificate validity period

A list of validity period of user and host certificates is described in Table 4-3.
As described in Section 3.2, renewing of a certificate is not allowed. Re-keying of a certificate is not allowed if the certificate is valid. In order to renewal a certificate, the subscriber must request a new certificate following the procedures described in Section 4.1.

Table 4-3 User certificate validity period

Type		Validity Period
Client certificate		13 months(395days)
Server Certificates	Globus server certificate	13 months(395days)
	Unicore server certificate	13 months(395days)
	LDAP server certificate	13 months(395days)
	Web server certificate	13 months(395days)

4.7.2 CA Certificate validity period

The CA will create a new CA private key before the time at which the validity of user certificates with the old CA private key would go beyond the validity of the CA private key. After the new private key being created, the CA will issue new certificates and CRL with the new key and the old key will be only used to issue ARL and CRL. The validity period of the CA Certificate will not exceed ten years.

4.8 Key compromise and disaster recovery

4.8.1 Recovery procedure for hardware, software or data corruption

If damage to the hardware or corruption of software or data is detected, the system will be recovered by using backup hardware, software, or data as quickly as possible.

4.8.2 Recovery procedure for compromised CA private key

Based on a decision of the NAREGI PMA, the following procedure will be followed:
If the CA private key is compromised through theft of the HSM, loss of the management keys, or other means, all related persons will be notified, and operation will be stopped.
If it is determined that the CA private key has been compromised, all certificates will be revoked. Once the security of the CA is confirmed, a new NAREGI CA key pair will

be generated, and the CA system will be rebuilt.

4.8.3 Procedure for recovering secure facilities after natural or other disaster

The procedure to be followed is given in section 4.8.1, “Recovery procedure for hardware, software or data corruption” in this CP/CPS.

4.9 Termination of CA

The certification officer will inform any related parties ahead of time regarding termination of the CA operations and preservation of related backup data, etc., before the prescribed procedures for termination are carried out.

5. Physical, procedural and personnel-related security controls

5.1 Physical controls

5.1.1 Site location and construction

The NAREGI CA system will be located where it is not easily susceptible to damage from water exposure, earthquake, fire or other disasters. It will be constructed to be earthquake and fire resistant, and with safety measures to prevent unauthorized entry. A safe location shall also be provided to protect CA machinery from damage or unauthorized entry.

5.1.2 Physical access

A machine room will be provided for the CA server and other devices. Entry to the machine room will be restricted to explicitly authorized persons using IC card access control. When performing work in the machine room, only CA operations staff are authorized to enter.

The CA server and other devices will be stored in a special locked cage, with two keys managed by two different CA operations staff members. When work is done in the room, all staff members who entered the room, the start and end time of the work, and a description of what was done will be recorded in the machine-room log book, and the security officer will check and sign-off each record.

5.1.3 Power and air conditioning

The CA server will have a dedicated cable from the power switch-box, ensuring enough power for the server.

The machine room will be equipped with adequate air conditioning to maintain a comfortable environment for the CA server and other devices, and for the CA staff to perform their duties.

5.1.4 Protection from water exposure

Flood warning devices shall be installed to guard against water damage.

5.1.5 Protection from earthquake damage

The CA server and other equipment will be housed in specialized cages, constructed to stay upright at all times. The cages will also be built to resist sliding.

5.1.6 Protection from fire damage

The building housing the NAREGI CA facilities will be constructed to be fire resistant,

and will be equipped with equipment such as sprinklers and automatic fire alarms. The machine room will be equipped with carbon-dioxide fire extinguishers.

5.1.7 Media storage

Media will be stored in a lockable storage cabinet in a room with appropriate access control.

5.1.8 Waste disposal

Any materials or storage media which contain data considered to be confidential will be disposed of appropriately according to the prescribed procedures.

5.2 Procedural security controls

5.2.1 Trusted roles

Operation of NAREGI CA will be carried out by staff whose the roles are defined in section 1.3.2, "Operating structure" of this CP/CPS.

5.2.2 Number of persons required per task

The number of staff required for each of the tasks prescribed in section 1.3.2, "Operating structure", of this CP/CPS, is assigned in order to separate authority and provide mutual checks.

Table 5-1 Required staff by task

Task	No. of persons required
Overall certification duties	One certification officer
Operation and management of the CA private key	One certification and two CA operators
CA private key activation/deactivation	Two CA operators
RA and CA server administration	Two CA operators
License ID generation and distribution	Two CA operators
CA system maintenance, administration	Two CA operators
Audit log, archive media administrator	One log administrator
Help desk	Four operations staff
Receive/assess, approval user enrollments	Four user administrators

5.2.3 Identification and authentication for each role

The system shall identify and verify that the operator has the appropriate authority to carry out the operation when CA system operations are performed.

5.3 Personnel-related security controls

Contract requirements, penalties, aptitude tests, job rotation, and other issues regarding NAREGI CA operations staff will be regulated in separate documentation.

5.3.1 Background check procedures

No stipulation.

5.3.2 Training requirements

Education and training for the knowledge, technology, and equipment operation required to operate the NAREGI CA will be provided.

5.3.3 Retraining frequency and requirements

Education and training required for job rotation and procedural changes will be done at the discretion of the certification officer.

5.3.4 Job rotation frequency and sequence

No stipulation.

5.3.5 Sanctions for unauthorized activity

No stipulation.

5.3.6 Personnel contract requirements

No stipulation.

5.3.7 Documentation supplied to personnel

The procedural manuals and relevant operation manuals required for operation of the NAREGI CA based on this CP/CPS will be provided to staff according to their roles.

6. Technical security controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

(1) CA Key

The CA key pair will be generated by the certification officer and operations staff by using the Hardware Security Module (HSM).

(2) User key

User key pairs are generated by software on each user terminal at the time of enrollment.

6.1.2 Delivery of private key

The user's private key is generated by the user, so it will not be distributed by the NAREGI CA.

6.1.3 Delivery of public key to CA

The user's public key is sent to the NAREGI CA at the time of enrollment as part of the Certificate Issue Request (CSR).

6.1.4 Delivery of CA public key

The CA certificate is published in the repository.

6.1.5 Key length

The key generation algorithms and key lengths are given below.

Table 6-1 Key lengths used

Type		Key algorithm and length
CA Key		RSA 2048 bit
User Key	Client Certificate	RSA 1024 bit
	Server Certificate	RSA 1024 bit

6.1.6 Generation of public key parameters

No stipulation.

6.1.7 Public key parameter quality checking

No stipulation.

6.1.8 Hardware/Software key generation

As defined in section 6.1.1, “Key pair generation”, of this CP/CPS.

6.1.9 Key usage (X.509 v3 KeyUsage Field)

A user private key is used for digital signatures and for shared-key encryption. This usage is specified in the X.509 v3 Extension. The user may use the certificate within the scope of this usage.

6.2 Private key protection

6.2.1 Cryptographic module standards

The CA private key is protected by a FIPS140-1 Level 3 compliant HSM.

6.2.2 Private key multi-person control

Operations using the CA private key will be carried out by the certification officer and CA operations staff.

6.2.3 Private key escrow

CA private key escrow will not be performed.

6.2.4 Private key backup

(1) CA private key

Backup of the CA private key will be performed by certification officer and a CA operations staff member. The backuped CA private key will be saved in an HSM token and stored in a safe place. Physical keys and the PIN of the HSM will be stored in safe places separately.

(2) User private keys.

Individual users will backup and manage their private keys.

6.2.5 Private key archive

The CA private key will not be archived.

6.2.6 Entry of the private key into the cryptographic module

The CA private key into the cryptographic module is entered when the key is generated, and during recovery from backup media. In both cases, it is done by the security officer and CA operations staff, and must be protected by a pass phrase of at least 15 characters.

6.2.7 Method for activating a private key

The CA private key will be activated inside the HSM by two CA operations staff members.

6.2.8 Method for deactivating a private key

The CA private key will be deactivated in the HSM by two CA operations staff members.

6.2.9 Method for destroying a private key

To destroy the CA private key inside the HSM, the HSM is initialized by the security officer and a CA operations staff member. If it is not possible to initialize the HSM, or it is taken outside, the HSM must be physically destroyed.

If the backup media of the destroyed CA private key is to be taken outside, the media should be physically destroyed.

6.3 Other aspects of key management

6.3.1 Public key archive

Public keys are included in the stored archive data. Details such as storage period are specified in section 4.6, “Archives”, of this CP/CPS.

6.3.2 Usage periods for public and private keys

Usage periods for public and private keys are specified in section 4.7.1, “User certificate validity period”, and 4.7.2, “CA certificate validity period”.

6.4 Activation data

6.4.1 Generation and installation of activation data

The CA private key is activated using a password and the HSM physical key. The password is decided by CA operations staff and entered into the HSM.

6.4.2 Protection of activation data

The password must be at least 15 characters long, and is used and modified according to specific regulations. The HSM physical key is protected by the security officer, who will keep it in a lockable cabinet.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

The CA server is to be equipped with only the functionalities required to operate as the NAREGI CA, and is only to be used for the tasks regulated in this CP/CPS.

6.5.2 Computer security rating

No stipulation.

6.6 Life-cycle technical controls

6.6.1 System development controls

No stipulation.

6.6.2 Security management controls

No stipulation.

6.6.3 Life-cycle security ratings

No stipulation.

6.7 Network security controls

The CA server will be placed on an independent network segment, with a dedicated connection to the RA server.

Communication between the CA server and the RA server will be limited to only specific communications ports, and security measures to prevent unauthorized access will be taken. Communications between users and the RA server will be encrypted with SSL.

6.8 Cryptographic module engineering controls

No stipulation.

7. Certificate and CRL Profiles

7.1 Certificate Profiles

Each certificate profile is described in a separate document, “NAREGI CA Certificate Profile”.

7.2 CRL Profiles

The CRL is compliant with RCF3280, X509 version 2. The CRL profile is described in a separate document, “NAREGI CA CRL Profile”.

8. Specification document management

8.1 Specification change procedure

The NAREGI CA will make changes to this document as required.

Changes in content will be decided and approved by the NAREGI PMA. The updated CP/CPS will be given a new major version number, and a new OID will be assigned to it.

Minor corrections such as misprints will not require approval of the NAREGI PMA, and will be done based on a decision of the security officer. In these cases, the minor version number will be updated, but a new OID will not be assigned.

8.2 Publication and notification of policies

Changes to this CP/CPS will be published promptly in the repository. Users and relying parties are notified in this way.

8.3 CP/CPS Approval procedure

This CP/CPS is enacted according to the approval of the NAREGI PMA and the decision of the certification officer.

Changes to the CP/CPS are approved by the NAREGI PMA.

9. Glossary

・Authority Revocation List (ARL)

A list identifying CA certificates that have been revoked before their validity period is expired. Normally, it is signed by the CA.

・Certification Authority (CA)

An organization that issues public key certificates for users of key pairs (a private and a public key), and carries out disclosure, expiry, and suspension of the certificates.

・Certificate Policy (CP)

A policy statement that indicates how a certificate is to be applied to a given community or application, according to its general security requirements.

・Certification Practice Statement (CPS)

Operating regulations for a certification authority. A document which describes the operating procedures of the CA that implement the policy regulated in the CP, regulating in detail the agreements and details of external trust relationships.

・Certificate Revocation List (CRL)

A list of certificates which have been revoked before their normal period of validity. It is normally signed by the CA.

・Certificate User

A person protecting a private key, and using a public key certificate. Besides individual persons, there are other types of users such as server applications.

・Digital Signature

A hash value of the signed data encrypted with the private key. The digital signature can be verified by decrypting the digital signature using the public key and comparing it with the hash value of the original data. The digital signature can only be generated by the holder of the corresponding private key, so it is similar in effect to a written signature.

・FIPS

American Federal Information Processing Standards Publication. FIPS140-1 is a standard for evaluating cryptographic modules.

・Hash

An algorithm for compressing arbitrary-length data to a fixed-length data value. It is not possible to recover the original data from the hash value. One-way hashing algorithms are used as checksums to check that a message has not been damaged or falsified, and as part of digital signatures. SHA-1 and MD5 are examples of hashing algorithms.

・Issuing Authority (IA)

A facility which creates and issues electronic certificates as its main business.

・Message Digest5 (MD5)

A one-way hashing algorithm which creates a 128-bit hash value from data of arbitrary length.

・Object Identifier (OID)

An identifier which is assigned to information objects irrespective to their content in order to distinguish one from another. To specify them uniquely, they are managed in a tree structure.

・Public Key Infrastructure (PKI)

An infrastructure which enables identity authentication (verification) using the Internet in a more rigorous and correct way.

・PKCS

A group of industry standards in the area of encryption algorithms and computations which were proposed by RSA Laboratories of the U.S.A. to promote application portability and compatibility.

PKCS #1: Standards related to RSA encryption. Signature formats, etc.

PKCS #7: Standards related to encrypted message formats.

PKCS #10: Format standards for requesting certificates.

PKCS #12: Standards related to personal and private information

・Registration Authority (RA)

An entity which registers users of a PKI system. It issues public key certificates, and assesses petitions for revocation.

・Request For Comments (RFC)

A series of documents collected by the IETF.

・Rivest-Shamir-Adleman (RSA)

The current, most generally used public-key encryption format. It is an encryption technology based on the difficulty in factoring the product of two sufficiently large prime numbers.

・Repository

Data storage used for storing and distributing public key certificates, CRLs and the like. NAREGI CA uses a web server as a repository.

・Relying Party

A party which receives a certificate, and acts based on its trust in the certificate.

・SHA-1

A one-way hashing algorithm which generates a 160-bit hash value from an arbitrarily long data item.

・Validation Authority (VA)

A facility which determines whether a certificate is valid.

・X.509

The International Telecommunications Union Standardization group (ITU-T) recommendation, which regulates technical standards for authentications derived from technology in the directories field. Regulations related to the role of certification authorities (CA), public key certificates, revocation lists, attributes used, etc.

Appendix A. Revision History

Version 2.1 → Version 3.0

- Major revision

  (1) 3.1 Initial registration (application)

  - ✧ Added: CN of host certificates contains FQDN.（Section 3.1.2）
  - ✧ Added: Uniqueness of names bases CN on.（Section 3.1.4）

  (2) Added: Secure communication is used.（Section 4）

  (3) Added: Communications are encrypted.（Section 6.7）

  (4) Added: procedure of near the end of validity period of cert（Section 4.7.2）

- Minor revision

  (1) 1.3.2 Organization

  - ✧ figure 1-1（Section 1.3.2）
  - ✧ figreue1-2（Section 1.3.2）

  (2) 2.1 Obligations

  - ✧ Changed: CA obligation（Section 2.1.1）
  - ✧ Changed: RA obligation（Section 2.1.2）
  - ✧ Added: condition of ``within one day”（Section 2.1.3）

  (3) Changed: `official’ s to comprehensible words.（Section 3.1.9）

  (4) Added: procedure of Re-new.（Section 3.2）

  (5) Changed: who can request revocation（Section 4.4.2）

  (6) 4.6 Records Archival

  - ✧ Add the identity information to archive data（Section 4.6.1）
  - ✧ Added: a note about archive period of certificates（Section 4.6.2）

  (7) Added: procedure of Re-New in certificate validity period（Section 4.7.1）

  (8) Deleted: too detailed note (Section 6.1.9 Key usage)

  (9) Added: backup of CA private key（Section 6.2.4）

  (10) Added: compliance of CRL profile（Section 7.2）