HPCI CA

Certification Practice Statement

Ver1.1

2012 May 29th

HPCI Policy Management Authority

Revision History

Date issued	Ver.	OID	Description
2011.12.28	1.0	1.3.6.1.4.1.32264.2.1.1	First Release
2012.05.29	1.1	1.3.6.1.4.1.32264.2.1.2	Under the title “ 9.12.1 Procedure for amendment ”, was changed to “ For the changes of small misprint revisions…new OID will be distributed”

Contents

1. INTRODUCTION

This “HPCI Certification Practice Statement” (Referred as CPS) describes regulations related to operations of the HPCI Certificate Authority.

The CPS conforms to the Request For Comments(RFC) 3647 “Internet X.509 Public Key Infrastructure Certificate Policy and Certificate Practices Framework” advocated by the Public-Key Infrastructure Working Group(PKIX) of the Internet Engineering Task Force(IETF).

1.1 Overview

The CPS provides information regarding certificate issuance, revocation, and other authentication related procedures managed by the HPCI Certificate Authority.

The HPCI Certificate Authority issues not only client certificates for authentication of users that use HPCI calculation/storage resources but also host and service certificates needed for HPCI calculation and storage environment. Certificates are only issued to users who meet the necessary qualifications set out in the “HPCI Consortium Usage Statements” (referred to as “usage statements”).

1.2 Document name and identification

The following policy IDs are used in the HPCI Certification Authority to distinguish CP/CPS contents and certificate policy.

Table 1-1 Object OIDs

OID	Object
1.3.6.1.4.1.32264.2	HPCI Certificate Authority
1.3.6.1.4.1.32264.2.1.X (*1)	HPCI CA Certification Practice Statements
1.3.6.1.4.1.32264.2.2.1	HPCI CA Certificate and CRL Profile

1: “X” is allotted for each CPS major version upgrade.

1.3 PKI participants

1.3.1 HPCI Certificate Authority (CA)

(1) HPCI Policy Management Authority

The following decisions concerning operations of the HPCI Certificate Authority shall be made by the HPCI Policy Management Authority (referred as “HPCI PMA”)

・Decisions regarding and approvals of CP/CPS

・Handling CA private key compromise

・Handling of emergencies such as disasters

・Approval of applications to federate from the HPCI Account IdP Operating Organization

・Other important matters concerning CA operations

(2) CA

CA shall issue certificates upon request from RA. Also, certificate revocation applications received at RA shall be processed to revoke the appropriate certificate and issue the CRL.

(3) RA

RA receives online certificate issuance requests from users and requests the CA to issue the certificate.

RA also confirms the distinguished and authorized certificate users of the HPCI Account IdP Operating Organization via the HPCI ID Management Organization. It also receives certificate revocation applications and requests the CA to revoke the certificate, and registers the CRL issued by the CA to the Certificate Authority Repository.

(4)Certificate Authority Repository

Registers and offers CP/CPS, CA Certificates, CRL's and other information to be disclosed to related people.

1.3.2 HPCI ID Management Organization

(1) HPCI Operating Office

HPCI Operating Office receives an application from the user and assigns it a HPCI ID. It manages the HPCI ID and other user's information.

(2) HPCI Accout IdP Operating Organization

HPCI Account IdP Operating Organization accepts applications for Certificate Issuance as part of user registration procedures. It distinguishes and authorizes users and issues HPCI accounts to those permitted.

1.3.3 Other parties

(1) Certificate User

Certificate User is a user with a certificate issued by the HPCI Certificate Authority. This includes general users, host administrators and service administrators.

A general user is someone who uses the client certificate to access HPCI resources via single sign on (SSO). A user representative can assume responsibility for applying for certificates for users.

The host administrator and service administrator are administrators of hosts and services necessary for usage of HPCI resources, shall individually apply for certificates through user registration.

(2) Relying Party

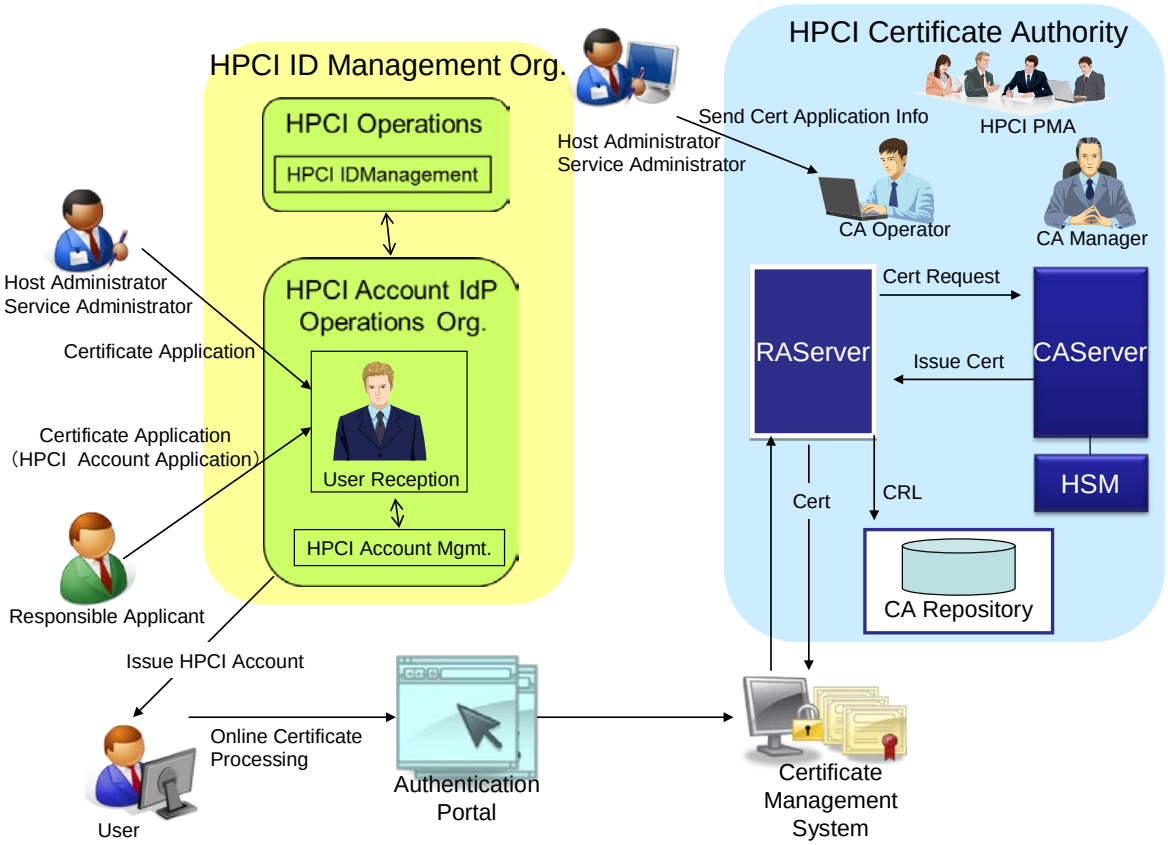
Indicates one who trusts the HPCI Certificate Authority and verifies certificates.

(3) Certificate Management System

In tandem with the RA, a system, which creates user's key pairs, and stores and manages client certificates.

(4) Authentication Portal

A web system, which offers users an interface for certificate issuance applications.



1.4 Certificate usage

1.4.1 Certificate types

The following are certificates issued by the HPCI Certificate Authority

・Client Certificate

・Host Certificate

・Service Certificate

1.4.2 Appropriate certificate uses

Certificates issued by the HPCI Certificate Authority are expected to be for the following usage or application:

Table 1-2 Types and Application of Certificate

Type	Application
Client Certificate	Client authentication when using HPCI resources
Host Certificate	Server authentication when using HPCI resources
Service Certificate	Service authentication when using HPCI resources

1.4.3 Prohibited certificate usage

Other uses of HPCI CA certificates are prohibited other than described in “1.4.2 Appropriate

certificate uses."

1.5 Policy administration

1.5.1 Organization administering the document

The CPS shall be maintained and administrated by the HPCI PMA.

1.5.2 Contact person

Contacts for questions regarding the CPS

Department: National Institute of Informatics, Cyber Science Infrastructure Development Department, Academic Infrastructure Division

Address:

2-1-2 Hitotsubashi, Chidaku, Tokyo 101-8430

Tel:＋81-3-4212-2226

e-mail: hpci-ca-support@nii.ac.jp

1.5.3 Person determining CPS suitability for the policy

No stipulation.

1.5.4 CPS approval procedures

Establishment and modifications to the CP/CPS shall require approval of the HPCI PMA or the security officer. When the HPCI PMA determines it is necessary, approval will be sought following examination by the Member Intergrated X.509 PKI Credential Services (MICS) of The Asia Pacific Grid Policy Management Authority (ApGridPMA).

1.6 Definitions and acronyms

・Certificate Authority(CA)

Issues, revokes or suspends public key certificates for key pair (private and public key) owners.

・ Certificate Policy (CP)

Applicable policy pertaining to certificates for particular communities or applications having accompanying general security requirements.

・ Certificate Practices Statement (CPS)

Document that precisely stipulates external relationships, general contractual conditions, and procedures for applying the policies stipulated in the CP to the operation of the CA.

・ Certificate Revocation List (CRL)

List that identifies certificates that have been revoked before the term of validity expires. It is digitally signed by the CA.

・ FIPS

Federal Information Processing Standards (USA). FIPS140-2 is the standards for encryption module assessment.

・High Performance Computing Infrastructure (HPCI)

Innovative high performance computing infrastructure. This document refers to all computing and storage systems linking to the HCPI, and any other systems operating as part of the HPCI environment as the HPCI System.

・HPCI ID

A unique ID for HPCI users. HPCI ID will not change even after transfer between departments.

・HPCI Account

An account for Single-Sign-On on the HPCI environment. Users will use the HPCI account to apply for certificates via the authentication portal.

・Object Identifier (OID)

Identifiers allotted to reciprocally distinguish data regardless of its meaning. They are managed in tree form to ensure uniqueness.

・Public Key Cryptography Standards (PKCS)

Industry standards proposed by the USA RSA Laboratories governing encryption algorithms and encryption calculations aimed at interconnectivity and portability between applications.
PKCS#12: Standards concerning personal information

・ Public Key Infrastructure (PKI)

Infrastructure to enable public key certificates that ensure the validity of the public key. It enables stricter (more reliable) identity authentication on the Internet.

・ Registration Authority (RA)

Registers users with PKI system, issues public key certificates and examines revocation applications.

・ Rivest-Shamir-Adleman (RSA)

Currently the most common form of public key encryption. Utilizes the fact that factorization of the value derived by multiplication of two sufficiently large prime factors is difficult as the foundation for encryption technology.

・ Designated holiday

Day established by Article 8, Section 1 of the regulations concerning working hours, holidays and breaks.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Certificate Authority Repository

Repository

・ The repository shall disclose information stipulated in "2.2 Publication of certificate information" and shall enable users to search for pertinent information and CRL.

・ With the exception of temporary shutdowns for periodic maintenance, the goal for operation of the repository shall be 24 hours a day, 365 days a year.

・ Advance notification shall be provided if the repository is to be shut down for reasons such as periodic maintenance. In the case of unavoidable circumstances such as emergencies, operation may be shut down without advance notification.

・ It shall not be guaranteed that the CRLs stored in the repository are the latest available at the point in time in which they are requested.

・ Information registered in the repository shall be protected.

2.2 Publication of certification information

The following information is published in the CA repository managed by the HPCI CA:

Table 2-1 Publication information of HPCI Certificate Authority

Document	Publishing Site(URL)
Fingerprint of CA Certificate, and other information concerning the HPCI Certificate Authority	https://www.hpci.nii.ac.jp/ca/
CA certificate of the HPCI Certificate Authority	https://www.hpci.nii.ac.jp/ca/hpcica.cer
CRL	https://www.hpci.nii.ac.jp/ca/hpcica.crl
CP/CPS	https://www.hpci.nii.ac.jp/ca/hpcicacps.pdf

The various application procedures and usage regulations of the HPCI system is in accordance with the HPCI consortium public information.

2.3 Timing and frequency of publication

Frequency of information publication is as follows:

・ CA certificates and CA certificate fingerprints will be published in the repository whenever issued.

・ The CRL published in the repository will be periodically updated as stipulated in "4.9.7 CRL issuance frequency" .

・ The CP/CPS and information concerning the HPCI Certificate Authority will be published in the repository whenever updated.

2.4 Access controls on repositories

There will be no restriction concerning access to information stipulated in “2.2 Publication of certification information” .

The ability to update disclosed information is restricted to authorized parties at the HPCI CA.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

The DN of certificates issued by the HPCI Certificate Authority is determined according to the format of X.500 DN (DN: Distinguished name).

3.1.2 Need for names to be meaningful

Attributes used as names of certificates issued by the HPCI Certificate Authority are provided in Table 3-1.

Table 3-1 Attributes use by certificates

Attributes used	Description	Set point
commonName	User name and HPCI ID (Client certificate)	[User's full name (Hepburn style Roman alphabet) HPCI ID]
	Host name(Host Certificate)	[FQDN]
	Service name (Service Certificate)	[Service name/FQDN]
organizationalUnitName	Organizational unit name	HPCI(fixed)
organizationName	Organizational name	NII (fixed)
countryName	Country name	JP (fixed)

The client certificate commonName will be set by the Authentication Portal having retrieved the HPCI ID and alphabet name from the HPCI Operations office using the attributes received in the SAML assertion from the HPCI Account IdP Operating Organization.

3.1.3 Anonymity or pseudonymity of subscribers

No stipulation..

3.1.4 Rules for interpreting various name forms

Distinguished names used will obey rules from Table 3-1.

3.1.5 Uniqueness of names

Distinguished name given on the certificate is a unique name allotted to each certificate issued by the HPCI ID. RA will confirm if there any overlapping distinguished names to ensure the uniqueness of the name.

3.1.6 Recognition, authentication, and role of trademarks

No stipulation..

3.2 Initial identity validation

This section describes regulations for when confirming a newly issued client certificate, host certificate, and service certificate.

3.2.1 Method to prove possession of private key

(1) Client certificate

As the private key for client certificates is created and stored in the Certificate Management System, users do not possess their private key.

(2) Host certificate, Service certificate

HPCI Certificate Authority confirms the ownership of the private key by examining the public key within the CSR signature to confirm that it is signed with the private key.

3.2.2 Authentication of organization identity

Confirmation of the (valid) existence of certificate user's organization is done by the HPCI Operations office during the HPCI system usage application procedure.

3.2.3 Authentication of individual identity

(1) User confirmation

The user reception of the HPCI ID Management Organization shall confirm the user identity during user registration. The applicant's supervisor shall present the user list with copies of a photo-identification (or similar valid official documents) face-to-face to the user reception. The user reception, having confirmed the applicants own picture ID, shall confirm that each user on the list matches the given picture IDs. It should be noted that it is assumed that the applicant's supervisor has confirmed beforehand the validity of all applicants' photo-identifications.

(2) Confirmation of host manager, service manager

The user reception of the HPCI ID Management Organization shall confirm Host administrators' and Service administrators' identities during user registration. The Host administrator or Service administrator shall present the host name or service name face-to-face to the user reception. The user reception shall confirm the host administrator or service administrator's photo-identifications and if the host name or service name in the FQDN matches with information provided.

3.2.4 Non-verified subscriber information

Only name, affiliation will be used and All other information will be not used for the examination..

3.2.5 Validation of authority

The HPCI ID Management Organization will confirm whether the user is eligible using the information managed by the HPCI Operations office.

3.2.6 Criteria for interoperation

No stipulation..

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key (renewal of expired certificate)

It is possible to omit face-to-face confirmation at the user reception when renewing expired certificates in the following cases:

・ It is within 5 years from issuance of a new certificate

・ When there is no change in the user's affiliated organization and subjects written in the certificate

・ The HPCI account will be continued

If the above is not applicable, follow the registration procedure mentioned in CP/CPS "3.2.2 Authentication of organization identity" and "3.2.3 Authentication of individual identity".

3.3.2 Identification and authentication for re-key after revocation

For identification and authentication during key renewal after revocation, follow the registration procedure mention in CP/CPS "3.2.2 Authentication of organization identity" and "3.2.3 Authentication of individual identity".

3.4 Identification and authentication for revocation request

Identification and authentication when applying to revoke a certificate shall follow the registration procedure mention in CP/CPS "3.2.2 Authentication of organization identity" and "3.2.3 Authentication of individual identity".

In the case of an emergency, however, application for revocation may be accepted from the certificate user in person or by e-mail . If presented in person, the user shall be confirmed by presentation of a photo-identification. In the case of e-mail, it shall be confirmed that the application is received from an e-mail address registered in the user administration system.

However, client, host, or service certificate revocation applications by parties other than the above will be accepted when it can be determined that the private key has been disclosed or the encryption algorithm used is confirmed to be compromised.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

Operation requirements for user certificates and grid host certificates are as follows:

4.1 Certificate application

Application for a client certificate is included in the application for an HPCI account necessary for using the HPCI system. Application for an HPCI account means a client certificate application is also submitted.

Host and service certificates will require submitting an HPCI Certificate Authority official application.

4.1.1 Who can submit a certificate application

Cerficate applications will be submitted to the HPCI ID Management Organization shall be done by the applicant's supervisor, host or service administrator.

HPCI Certificate Authority online certificate issuance shall be done by users, host or service administrators.

4.1.2 Enrollment process and responsibility

(1) Client Certificate

Users shall submit a copy of a photo-identification to the applicant's supervisor. The supervisor shall confirm the legitimacy of the photo-identification and submit the documents to the user reception. The applicant's supervisor must present accurate information to the HPCI ID Management Organization.

(2) Host certificates and service certificates

Host administrators and service administrators shall submit a copy of a photo-identification, host name or service name list to the HPCI ID Management Organization's user reception. Host administrators and service administrators must present accurate information to the HPCI ID Management Organization.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

Examination by the HPCI Operations office and HPCI Account IdP Operations Organization will be conducted according to CP/CPS "3.2.2 Authentication of organization identity" and "3.2.3 Authentication of individual identity".

The HPCI Certificate Authority will confirm that the certificate user has passed examination by the HPCI ID Management Organization.

4.2.2 Approval and rejection of certificate applications

Applications will be accepted only after the HPCI ID Management Organization has confirmed that there are no problems with contents of the application submitted by the applicant's supervisor, host

or service administrator.

When the HPCI Certificate Authority judges that there are no problems with the HPCI ID Management Organization examination results, it will accept online certificate issuance requests from the certificate user.

4.2.3 Time to process certificate application

(1) Client certificates

Within 5 days (holidays excluded) from the day after the HPCI Account IdP Operations Organization accepts the application, the HPCI account will issued and the user will be notified.

(2) Host certificates and service certificates

Within 5 days (holidays excluded) from the day after the HPCI Account IdP Operations Organization accepts the application, information required for application to the HPCI Certificate Authority will be notified to the host or service administrator.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

(1) Client certificate

Users will use HPCI account to input certificate issuance application information into the authentication portal. User authentication information will be sent to the certificate management system from the authentication portal and corresponding keys pairs within the system will be created. The certificate management system will send the certificate issuance application to the RA server. Certificate issuance will be requested to the CA server and the client certificate will be created at the CA server. The client certificate issued by the HPCI Certificate Authority will be stored in the certificate management system.

(2) Host certificate and service certificate

Host administrator or service administrator will create keys pairs for the servers and then send CSR's to the HPCI Certificate Authority. After the HPCI Certificate Authority receives the CSR, it will issue the host and service certificate after verification by the CP/CPS "3.2.1 Method to prove possession of private key".

Host and service certificates issued by the HPCI Certificate Authority will be sent online to the host administrator or service administrator.

Procedures between the user, host administrator or service administrator and the HPCI Certificate Authority will be done online over encrypted channels.

4.3.2 Notification to subscriber by the CA of issuance of certificate

(1) Client Certificate

After the client certificate is issued, notification mails will be sent by the certificate management system to the users address obtained from the HPCI ID Management Organization.

(2) Host certificate and service certificate

Host or service certificate sent from the HPCI Certificate Authority will serve as notification to the host or service administrator.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

(1) Client certificate

A download of the client certificate from the certificate manager system by the user will be acknowledged as "received". If not downloaded, the certificate is counted as "received" at the point when the client certificate is stored in the certificate management system.

(2) Host certificate and service certificate

After receiving the host or service certificate, confirmation of the certificate content is done by the host or service administrator.

4.4.2 Publication of the certificates by CA

Client, host and service certificates are not published.

4.4.3 Notification of certificate issuance by the CA to other entities

No stipulation.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

Used for applications stipulated in "1.4.2 Appropriate certificate uses".

4.5.2 Relying party public key and certificate usage

Used for applications stipulated in "1.4.2 Appropriate certificate uses".

4.6 Certificate renewal without re-key

HPCI CA renews key pairs when renewing certificates in all cases. Certificates cannot be renewed without renewing key pairs.

4.7 Certificate re-key

4.7.1 Circumstance for certificate re-key

Certificates are renewed in the following cases:

- Validity of a user certificate has expired.
- When reissued after certificate revocation due to compromise of user private key, etc.

4.7.2 Who may request certification of a new public key

Certificate renewal applications shall be submitted to the HPCI ID Management Organization by the applicant's supervisor or host/service administrator.

4.7.3 Processing certificate re-keying requests

(1) When validity of a user certificate has expired

Renewal process of client certificates, host certificates, and service certificates shall follow procedures stipulated in CP/CPS "4.1 Certificate application". However, "4.2.1 Performing identification and authentication functions" shall follow "3.3.1 Identification and authentication for routine re-key (renewal of expired certificate)".

Renewal applications can be submitted beginning 1 month prior to the expiration date.

(2) Reissuing after certificate revocation

Refer to procedures "4.1 Certificate application ～4.4 Certificate acceptance" for applying for a reissue after revocation.

4.7.4 Notification of new certificate issuance to subscriber

Users shall be notified of certificate renewal in accordance with "4.3.2 Notification to subscriber by the CA of issuance of certificate."

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Users shall be notified of certificate reception in accordance with "4.4.1 Conduct constituting certificate acceptance".

4.7.6 Publication of the new certificate by the CA

Renewed certificates shall be disclosed in accordance with "4.4.2 Publication of the certificate by CA."

4.7.7 Notification of certificate issuance by the CA to other entities

Notification of certificate issuance to other concerned parties shall be carried out in accordance with "4.4.3 Notification of certificate issuance by the CA to other entities."

4.8 Certificate modification

No stipulation.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

HPCI CA will revoke certificates under the following conditions:

(1) Revocation initiated by certificate user

・Change of certificate content (such as change in the name, etc.)

・The private key is reported or suspected to be compromised

(2) Revocation initiated by HPCI ID Management Organization

・Certificate user's existence confirmation could not be done

・Loss of eligibility

(3) Revocation initiated by the HPCI CA

・Violation of the CP/CPS or user regulations by the certificate user

・Leakage or compromise of private key stored in the certificate management system

・It is determined that the HPCI CA wrongly issued a certificate

・Leakage or compromise of the CA private key in the HPCI CA

・The HPCI CA ceases authentication operations

4.9.2 Who can request revocation

(1) If there is cause for revocation from the user

Revocation applications shall be handled by the applicant's supervisor, host administrator, or service administrator. In the case of emergency, revocation applications may be accepted from the certificate user at the discretion of the HPCI CA.

(2) If there is cause for revocation from the HPCI CA Management Organization

Revocation application will be submitted to the HPCI CA by the HPCI Operations office.

(3) If there is cause for revocation from the HPCI CA

Revocation shall be done at the discretion of a responsible person at the CA manager or HPCI PMA.

4.9.3 Procedure for revocation request

(1) Revocation by certificate user

・Client Certificate

If the user has cause for a client certificate to be revoked, the user should immediately fill out the necessary forms and submit them to the applicant's supervisor. The applicant's supervisor should verify user's identity and reason for revocation, and then submit the application to the user reception. In an emergency, the user can submit an application directly to the user reception either in person or by email.

User reception shall perform examinations of the applicant's supervisor or user in accordance with "3.4 Identification and Authentication for Revocation".

User reception shall send revocation applications to the HPCI CA and request revocation of the appropriate certificate.

・Host certificate, service certificate

When there is cause for revocation, the host or service administrator should fill in application sheet as soon as possible and submit it to user reception.

User reception shall perform examinations of the host or service administrator in accordance with "3.4 Identification and Authentication for Revocation".

User reception shall send revocation applications to the HPCI CA and request revocation to the appropriate certificate.

(2) Revocation procedures for the HPCI ID Management Organization

When conditions mentioned in CP/CPS "4.9.1 Reasons for Revocation" are met, the HPCI Operations

office shall send the revocation application to the HPCI CA and request revocation of the appropriate certificate.

(3) Revocation procedures for the HPCI CA

When conditions mentioned in CP/CPS "4.9.1 Reasons for Revocation" are met, the CA manager or HPCI PMA shall determine revocation to the appropriate certificate.

After the revocation process, the HPCI CA will notify the HPCI ID Management Organization that the revocation has been completed.

4.9.4 Revocation request grace period

When there is cause for revocation, the user, HPCI ID Management Organization or HPCI CA must request revocation to the HPCI CA as soon as possible.

4.9.5 Time within which CA must process the revocation request

The HPCI CA will determine revocation promptly when a revocation request is received. When revocation is approved, the HPCI CA will promptly proceed with revocation within 1 day excluding prescribed holidays.

4.9.6 Revocation checking requirement for relying parties

Related parties shall confirm validity of certificates by obtaining the latest CRL published in the repository.

4.9.7 CRL issuance frequency

The HPCI CA will issue the CRL with every revocation, and also periodically. The valid term of the CRL is 30 days and a new CRL will be issued at the latest 7 days before expiration.

During normal operations, CRLs will be issued every 24 hours.

4.9.8 Maximum latency for CRLs

After the CRL is issued by the CA, it will take a maximum of 12 hours to publish it in the CA repository.

4.9.9 On-line revocation/status (OCSP) checking availability

The HPCI CA does not provide certificate validity information by OCSP.

4.9.10 On-line revocation/status (OCSP) checking requirements

No stipulation.

4.9.11 Other forms of revocation advertisements available

No stipulation.

4.9.12 Special requirements re key compromise

No stipulation.

4.9.13 Circumstances for suspension

The HPCI CA does not suspend certificates.

4.9.14 Who can request suspension

No stipulation.

4.9.15 Procedure for suspension request

No stipulation.

4.9.16 Limits on suspension period

No stipulation.

4.10 Certificate status services

4.10.1 Operational characteristics

The HPCI CA shall provide certificate revocation information by publishing the CRL in the repository.

4.10.2 Service availability

Service usage time shall be as stipulated in “2.3 Timing or frequency of publication”.

4.10.3 Optional features

No stipulation.

4.11 End of subscription

Certificate users may quit according to “4.9.3 Procedure for revocation request”.

4.12 Key escrow and recovery

The HPCI CA does not offer key escrow service.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

5.1.1 Site location and construction

Equipment shall be setup in a place within the HPCI CA facilities not easily subject to damage due to disasters such as flooding, earthquake and fire. Safety measures shall be incorporated into the building structure to prevent unauthorized access and withstand earthquakes and fire. Names that expressly or implicitly indicate the location of the HPCI CA shall not be included on signs or labels inside or outside the building.

5.1.2 Physical access

It is necessary to register with the security system in advanced to receive authorization to enter the room containing the machines set up in the HPCI CA. Every time the room is accessed, it is necessary for multiple persons with authority to access the room to be identified and authenticated by biometric authentication equipment. Entry and exit logs will be recorded and managed. Entry and exit logs will be checked periodically. If an individual or individuals without access authorization are to enter the facilities, those individuals must be accompanied by multiple individuals having authorization to access the facilities. The purpose for entry will be confirmed if the room is to be accessed by an unauthorized individual or individuals. A record of accompaniment of two personnel with authorization to access the room will be kept and periodically reviewed.

When exiting the machine room, both the person who entered and the accompanying person will be confirmed.

CA machineries will be housed in a dedicated, lockable rack in the machine room.

5.1.3 Power and air conditioning

CA equipment will be powered by a dedicated power line from the power distribution board with sufficient capacity.

The machine room will be equipped with air-conditioning equipment to maintain the proper service environment and appropriate working environment for the personnel.

5.1.4 Water exposures

The machine room will be set in a place not easily damaged by water disasters, and water leakage alarms put in place.

5.1.5 Fire prevention and protection

The HPCI CA building will be fireproofed, and prepared with automatic fire alarm and fire extinguishing equipment.

5.1.6 Media storage

Media will be stored in a locked storage cabinet within a room with appropriate entry control.

5.1.7 Waste disposal

When disposing of HPCI CA documents or storage media with important personal information of certificate users and private keys, it must be completely physically destroyed or otherwise made impossible to recover the data.

5.1.8 Off-site backup

The HPCI CA will not engage in offsite backups.

5.1.9 Earthquake protection

CA machineries etc., will be set in a dedicated rack with complete with safety devices against falling.

5.2 Procedural Controls

5.2.1 Trusted roles

The following show the HPCI CA operation systems and roles:

Chart 5-1 HPCI CA Operation Systems and Roles

Operation System	Primary Role
Security Officer	・Authentication Operations Headquarters ・Management of CA private key ・Management of CA machinery dedicated rack (physical) keys
CA Operator	・Activation/ Deactivation of CA private key ・Operation and maintenance management of CA system (CA server/ RA server/ repository)
Log Administrator	・Management of back-up, log and archive media ・Management of (physical) keys for fire proof safes and cabinets ・Examination of system logs and reports (security audit)
CA help desk	・Answer questions regarding certificate usage from the HPCI help desk

The following show the HPCI ID Management Organization operation systems and roles:

Chart 5-2 HPCI ID Management Organization operation systems and roles

Operation System	Primary role
HPCI Account IdP Management Organization User Reception	・Confirmation of identification of the applicant's supervisor, and confirmation of photo-identifications of applicants ・Identification of host administrator or service administrator, and confirmation of their relationship to the FQDN ・Confirmation of user qualifications ・Storage of documents submitted by the certificate users, examination results etc.
HPCI Operations Office	・Confirmation of existence of the certificate users affiliated organization, and storage of the confirmation results ・Submission of revocation applications to the HPCI CA after loss of user qualifications

5.2.2 Number of persons required per task

In accordance with "5.2.1 Trusted roles", the required number of workers will be allocated for the following work from the perspective of privilege separation and mutual supervision.

Chart 5-3 Required number of personnel in the CA management service

Job	Personnel (required number)
Authentication Operations Headquarters	Security Officer (1)
Operation and management of CA private key	Security Officer (1), CA Operator (1)
Activation/ Deactivation of CA private key	CA Operator (2)
CA server, management of RA server	CA Operator (2)
Maintenance management of CA system	CA Operator (2)
Management of physical key of safe, etc.	Log Administrator (1)
Management of audit log and archive media	Log Administrator (1)
CA help desk	CA help desk (1)

5.2.3 Identification and authentication for each role

When operation is done by the CA Operator, the system identifies/authenticates if the operator has proper authority to operate the system.

5.2.4 Roles requiring separation of duties

Concurrency between the Security Officer, the CA Operator, and the Log Administrator is not allowed.

5.3 Personnel Controls

5.3.1 Qualifications, experience, and clearance requirements

Contract requirements, penalties, competence examination, staff reshuffling, etc., for HPCI CA operation staff will be done in accordance with a separately established personnel regulations.

5.3.2 Background check procedures

No stipulation.

5.3.3 Training requirements

Education and training in the techniques, knowledge, and operations of machines in order to operate the HPCI CA will be provided. The history of education and training provided will be stored.

5.3.4 Retraining frequency and requirements

Staff will receive education and training for staff reshuffling or changes in work procedure at the discretion of the Security Officer.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

If a member or members of the staff violate the policy or procedures stipulated or other procedures of the HPCI CA, appropriate penalties will be applied, regardless of whether the violation was intended or not.

5.3.7 Independent contractor requirements

No stipulation.

5.3.8 Documentation supplied to personnel

The staff will be provided with all documents, based on this CP/CPS, necessary in order to operate the HPCI CA appropriate to their role including operation procedures and related operation manuals, etc..

5.4 Audit logging procedures

In order to ensure a safe environment, the HPCI CA will keep an audit log of all events that occur in

RA, CA and operation procedures.

5.4.1 Type of events recorded

The HPCI CA will record the following information: Each record includes the type of event, date and time of event, and event source information (system name, operator's name, etc.).

- CA log
  - CA access log
  - Certificate and CRL issue/revocation log
  - Error log
- RA log
  - RA access log
  - Certificate issue/revocation log
  - Error log
  - RA server CRL Publisher operation log
  - CRL Publisher error log
  - RA access log
  - Certificate issue/revocation log
  - Error log
- OS login/logout/reboot log
- Hardware security module (so called HSM) log
- Machine room access record
- Machine room work record
- Key lending administration log
- Education and training history
- Record of work audit (check list) of the HPCI ID management institution

5.4.2 Frequency of audit log

Verification of the audit log will be based on instructions of the Security Officer.

5.4.3 Retention period for audit log

Auditing logs will be kept for a period of three years. However, CA logs and HSM logs will be stored for 10 years.

5.4.4 Protection of audit log

Access control by OS function shall be implemented for CA, RA and HSM logs. Audit logs will be kept in a locked cabinet within a room with proper access administration to prevent unauthorized browsing or tampering.

5.4.5 Audit log backup procedures

The CA Operator will periodically acquire various types of logs recorded in the CA, etc., and shall maintain a safe environment.

5.4.6 Audit collection system

No stipulation.

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability assessments

No stipulation.

5.5 Records archival

5.5.1 Types of records archived

The following information will be stored as archive data: Each version of documents including revision history will be kept.

(Storage in the HPCI CA)

- All certificates and CRLs issued by the HPCI CA
- Notification documents to the certificate users
- Work records concerning CA keys
- Audit logs stipulated in "5.4.1 Types of events recorded"
- Operation personnel chart
- Explanatory documents to users
- The CP/CPS, profile design and operation procedures
- Other important documents pertaining to HPCI PMA decisions

(Storage in the HPCI ID Management Organization)

- Record of every type of application form, copy of photo-identifications, and examination results, etc.
- Record of work audit (check list)

5.5.2 Retention period for archive

Archive data will be kept as stipulated in "5.4.3 Retention period for audit log". However, "Record of every type of application form, copy of photo-identifications, and examination results, etc." will be stored for 5 years in the HPCI ID Management Organization.

5.5.3 Protection of archive

Archive data will be protected as stipulated in "5.4.4 Protection of audit log".

5.5.4 Archive backup procedures

Archive data will be backed up as stipulated in “5.4.5 Audit log backup procedures”.

5.5.5 Requirements for time-stamping of records

Archive data stored in electronic form will include time stamps.

5.5.6 Archive collection system

No stipulation.

5.5.7 Procedures to obtain and verify archive information

No stipulation.

5.6 Key changeover

5.6.1 Validity of user certificate

Validity of the certificate issued by the HPCI CA is as follows:

Chart 5-4 Validity of certificate

Types	Validity
Client certificate	The end of the academic year of issuance + one month
Host certificate	The end of the academic year of issuance + one month
Service certificate	The end of the academic year of issuance + one month

5.6.2 Validity of CA certificates

CA certificates are valid for 10 years.

Before the term of validity of the CA private key becomes shorter than that of the user certificate, the HPCI CA shall stop issuing new client certificates, host certificates and service certificates with the existing private key.

5.7 Compromise and disasters recovery

5.7.1 Restoration procedure for CA private key compromise

The following procedure will be carried out based on the decision of the HPCI PMA:

- If an HSM is stolen of the CA private key compromised, operations will be halted after notifying all related parties.
- If the CA private key is compromised, prescribed procedures are followed to use the key to deactivate the system that verifies the trust of the HPCI CA, and all certificates, including the CA certificates will be revoked.
- As soon as safety of the HPCI CA is confirmed, a new key pair will be generated and the system reconfigured.

5.7.2 Computing resources, software, and/or data are corrupted

When hardware, software and data has been damaged or destroyed, it will be restored as soon as possible from backup hardware, software and data.

5.7.3 Entity private key compromise procedures

When user private key compromise has been found or there is a possibility of compromise, the user must apply to the HPCI CA for revocation as soon as possible. Also, when user private key compromise has been found or there is a possibility of compromise, the Security Officer must apply for revocation as soon as possible.

5.7.4 Business continuity capabilities after a disaster

When the CA private key has not been compromised and there is no doubt that it may have been compromised, it shall be restored in accordance with "5.7.2 Computing resources, software, and/or data are corrupted".

5.8 CA termination

Concerning cessation of authentication operations by the HPCI CA and accompanied storage of backup data, etc., the Security Officer will notify all concerned parties in advance and will carry out the stipulated procedures for shutting down operations.

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 Security Officer and CA Operator in the HSM.

(2) User key

The certificate user key pair will be generated within the certificate management system when the online certificate issue is proceeding.

Host and service key pairs are generated by the host managers or service managers within each host or service.

6.1.2 Private key delivery to subscriber

(1) User private key

・When client certificates are stored only within the certificate management system

User private keys are stored only in the certificate management system, and not distributed to users.

・When users download the client certificate

User keys are downloaded by users through the certificate management system in the PKCS#12 form.

(2) Host and service private keys

Private keys are generated within each host or service and are not distributed.

6.1.3 Public key delivery to certificate issuer

User public keys are generated within the certificate management system and transmitted by the RA server. The RA server then transmits to the CA server as a certificate issue request.

Host or service public keys are generated by the host managers or service managers and transmitted as a Certificate Signing Request (CSR) to the HPCI CA.

6.1.4 CA public key delivery to relying party

CA certificates will be published in the repository and distributed.

6.1.5 Algorithm and key sizes

The algorithm and key length generation are as follows:

Chart 6-1 Key Length Used

Types	Key algorithm and key length
CA key	RSA 2048bit

User key	Client certificate	RSA 2048bit
	Host certificate	RSA 2048bit
	Service certificate	RSA 2048bit

6.1.6 Public key parameters generation and quality checking

No stipulation.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

The objective of CA, user, host, and service public keys is the usage of territorial expansion of X.509 v3 and to set the following contents：

Chart 6-2 Objective of Key Use

Target	Objective of key use
CA certificate	keyCertSign, cRLSign
Client certificate	digitalSignature ,keyEncipherment
Host certificate	digitalSignature ,keyEncipherment
Service certificate	digitalSignature ,keyEncipherment

6.2 Private key protection and Cryptographic Module Engineering controls

It is to stipulate the CA private key and user private key. Host and service private keys are managed by the host or service managers.

6.2.1 Cryptographic module standards and controls

(1) CA private keys

Protected by HSM equivalent of FIPS140-2 level 3.

(2) User private key

・When client certificates are stored only within the certificate management system

Encryption will be needed in order to be stored in the certificate management system. Only authorized manager or server has access to the certificate management system within the machine room

・When users download the client certificate

Users will download in the form of PKCS#12 from the certificate management system. Downloaded certificates and keys are in the responsibility of the user to save it.

6.2.2 Private key (n out of m) multi-person control

Operations using CA private key will be conducted by the Security Officer and multiple of CA Operators.

6.2.3 Private key escrow

The HPCI CA will not deposit private keys.

6.2.4 Private key backup

(1) CA private keys

Backup of CA private key shall be carried out by the Security Officer and CA Operator. Backed up CA private keys will be saved by HSM token and stored in a safe place.

(2) User private key

・When client certificate is stored only within the certificate management system

The manager of the certificate management system will carry out the system backup. Backup medium will be stored in a lockable safe box within a room with appropriate access management.

・ When client certificates are downloaded by users

Certificates downloaded by the user must be backed up by the user and the backup medium must be stored in a safe place.

6.2.5 Private key archival

Private keys are not archived.

6.2.6 Private key transfer into or from a cryptographic module

(1) CA private key

CA private keys are generated within the HSM module located in the machine room of HPCI CA and are not transmitted.

(2) User private key

・When client certificate is stored only within the certificate management system

Private keys will be generated and controlled within the certificate management system, and transmission will not be done.

・When client certificates are downloaded by users

Users will download in the form of PKCS#12.

6.2.7 Private key storage on cryptographic module

(1) CA private key

Registration to the HSM encryption module will be conducted when keys are generated and recovery from backup mediums. In either case, the process is conducted by the Security Officer and CA Operator. A password consisting of at least 15 characters will be required.

(2) User private key

・When client certificate is stored only within the certificate management system

Registration to the encrypted module in the certificate management system will be done when the user generates the key within the online certificate issuance procedure. Over 12 charactered password will be needed in order to generate the key confirmation.

・When client certificates are downloaded by users

After the certificate download, registration will be proceeded to the encrypted module within the user's computer.

6.2.8 Method of activating private key

(1) CA private key

CA private keys will be activated by 2 CA Operators within the HSM.

(2) User private key

・When client certificate is stored only within the certificate management system

Activation will be done within the certificate management system, when authentication of the resource use in the HPCI.

Activation of the private keys are required for at least 12 characters password needed to authenticate.

・When client certificates are downloaded by users

Certificate user keys are activated within the user computer when authenticating resource use within the HPCI. When activating keys, password consisting of at least 12 digits will be required when authenticating.

6.2.9 Method of deactivating private key

CA private keys will be deactivated by 2 CA Operators within the HSM.

6.2.10 method of destroying private key

(1) CA private key

CA private keys within the HSM will be discarded by the Security Officer and CA Operator whom initializes the HSM. If the HSM cannot be initialized and is to be taken out of the room, it must be physically destroyed.

Also when backup mediums of discarded CA private key is to be taken out of the room, it also must be physically destroyed.

(2) User private key

・When client certificate is stored only within the certificate management system

The manager of the certificate management system will discards the user private key within the backup medium of the certificate management system according to the procedures predetermined to make the key not to be reused.

・When client certificates are downloaded by users

Users will take responsibility of discard for the certificate downloads and backup mediums created.

6.2.11 Cryptographic Module rating

HSM containing CA private keys will meet criterias equivalent to FIPS140-2 level 3.

6.3 Other aspects of key pair management

6.3.1 Public key archival

Public keys are stored within the archive data. The storage period will be as stipulated in “5.5.2 Retention period for archive”.

6.3.2 Certificate operational periods and key pair usage periods

Follow the CP/CPS “5.6.1 Validity of user certificate” and “5.6.2 Validity of CA certificates”.

6.4 Private key activation data

6.4.1 Activation data generation and installation

(1) CA private key

CA private keys will be activated by password and HSM physical key. The password will consist of at least 15 characters decided by the CA Operator and input it in the HSM.

(2) User private key

User private key activation data is the password with over 12 characters inputted by the user when online certificate issue procedure is being done. This password would be set as the user access password to the private key.

6.4.2 Security management controls

(1) CA private key

The CA Operator will use and modify CA private key activation data in accordance with established regulations. The HSM physical key will be kept by the Security Officer in locked cabinet.

(2) User private key

It is the user’s responsibility to store the activation data that the user inputted.

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 a special machine that have functions only needed for the HPCI CA, and only used for limited works regulated in the 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 controls

No stipulation.

6.7 Network security controls

The HPCI CA will prevent unauthorized access from outside networks by firewall. Connection between CA and RA servers, and between RA and the certificate management system will be limited to a certain communication port; security measures will be taken to prevent unauthorized access. The communication route between CA and RA, and RA and certificate management system will be encrypted.

6.8 Time-stamping

The HPCI CA will execute time synchronization by time server to record the accurate day and time for certificates and logs, etc.

7. CERTIFICATE, CRL, AND OCSP PROFILES

The certificate and CRL profile is based on the RFC5280 and follows the separately set design specifications of certificate and CRL profile. OCSP profile is not stipulated.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

HPCI CA performs an internal audit every year to check if operations are complied according to the CP/CPS.

The HPCI ID Management Organization performs an internal audit every year according to the audit check list presented by the HPCI CA, and results are reported to the HPCI CA.

8.2 Identify/qualifications of assessment

Auditors should be familiar with auditing and authentication work.

8.3 Assessor's relationship to assessed entity

Auditor is person whom is not involved in operation of the HPCI CA and have no interest in the HPCI CA.

8.4 Topics covered by assessment

Auditing will concern whether authentication work of the HPCI CA is carried out in according to the CP/CP and operation procedures, etc.

8.5 Actions taken as a result of deficiency

The HPCI PMA should study corrective measures for matters pointed out by audit and decide a course of action without delay. After deciding the course of action, the HPCI CA will present the action plan to the auditor and the situation will be monitored until the HPCI CA completes the measures.

8.6 Disclosure of auditing results

All operation staff members of the HPCI PMA and HPCI CA will be informed of auditing results. The HPCI PMA will consider whether or not to disclose auditing results to others.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

It will follow the usage regulations by the HPCI Consortium

9.2 Financial responsibility

No stipulation.

9.3 Confidentiality of business information

Protection and service of confidential information of the HPCI CA will be stipulated with the following regulations of the National Institute of Informatics:

Security Policy of Research Organization of Information and Systems
http://nsin.op.nii.ac.jp/NII_staff/plan/lan/pdf/K1001.pdf

9.3.1 Scope of confidential information

With the exception of information indicated in "2.2 Publication of certification information", all pertinent information is to be confidential. Confidential information will not be disclosed or leaked to any third party and furthermore not be used except where required. Information treated as confidential will be safely stored under administration of a person in charge of documents and recording media containing information.

9.3.2 Information not within the scope of confidential information

Information given in "2.2 Publication of certification information" is not treated as confidential.
In the case of a revoked user certificate, the reason the certificate was revoked is also published in the CRL. The date and reason for revocation contained in the CRL will not be considered as confidential information. Other information concerning revocation will not be disclosed to the public.

9.4 Privacy of personal information

The HPCI CA will not exceed the required range for personal information presented by the person in charge of applications or user for issue or revocation of certificates.
If there is a request from the user, the following information may be disclosed after confirming face-to-face the user's identity:

- Issue application to HPCI CA or HPCI ID Management Organization
- Certificate contents
- Certificate status

Other personal information is stipulated in the regulations of the National Institute of Informatics from the following cites:

- Personal Information Protection Regulations of Research Organization of Information and

Systems'

http://www.rois.ac.jp/pdf/30-10.pdf

・For NII Personal Information Protection Disclosure Requests:

http://www.nii.ac.jp/top/diclosure/privacy/

9.5 Intellectual property rights

The HPCI CA will not claim any IPR for certificates issued.

9.6 Representations and warranties

9.6.1 Representations and warranties of the HPCI CA

The HPCI CA will have the following responsibilities concerning CA work:

・ Certificate issuance and validation will be based on the CP/CPS.

・Excluding times of emergency and system maintenance, CA certificate information and CRL will be recorded to the CA repository and published.

・When certificates are issued, applied CP/CPS can be specified

・Follow appropriate authentic work based on the CP/CPS, and have the responsibility of credibility at the point when certificates or CRL's are issued. HPCI CA put signatures to these information, however, when falsification by a third person (found by attacks), or obsolesce of algorithm signature occurred, there is no guarantee of credibility.

・Appropriate authentic work is done, based on CP/CPS to protect the HPCI CA private key from compromising due to theft and/or loss.

・Approval of cooperative application from the HPCI ID Management Organization

・Identification and authentication work of the certificate user/organization will be done with cooperation of the HPCI ID Management Organization

・Present the operation requirements as the audit checklist to the HPCI ID Management Organization and perceive requirement compliance situations

・All communication lines between the HPCI ID Management Organization and certificate management system will be encrypted for safe and reliable send/receive

9.6.2 Representations and warranties of the HPCI ID Management Organization

The HPCI ID Management Organization will have the following obligations and responsibilities:

・Identification and authentication of certificate user and organization, information desk work, should be ensured when certificate issue, renewal, and validation is done by the certificate users, based on the CP/CPS

・Detects change of the certificate user name or change in the affiliated organization, loss of usage qualification as soon as possible, and when detected, validation application will be done to the HPCI CA

・Sends user's certificate information (HPCI ID, roman alphabet name) safely by cooperating

with the authentication portal to the HPCI CA

・Cooperate with the certificate management system to notify the user for the completion of certificate issue

・Certificate user information used for each application procedure will be safely stored within the period mentioned in the CP/CPS

・To keep the HPCI CA operation requirements, internal audit is put into practice, periodically and results are reported to the HPCI PMA

9.6.3 Subscriber representations and warranties

The certificate user will have the following obligations and responsibilities:

・Present accurate information on request for certificate issuance or revoke to the HPCI ID Management Organization or the HPCI CA

・Implement according to the procedure manuals provided by the HPCI CA for certificate acquisitions

・Not to use the certificate for purpose of usage other than what is stipulated in this CP/CPS. Also, do not use after expiration date

・Safely protect the activation password of the private key on user's own risponsibility

・Have the responsibility not to compromise the private key and certificate due to theft and loss

・Submit a revocation request as soon as the private key has been stolen, lost (when the private key has a possibility of compromise or is compromised), or the suspension of the usage of the certificate

・Host manager and service managers must associate the host/service certificate to one network entity

9.6.4 Relying party representations and warranties

The relying party will have the following obligations and responsibilities:

・Certificate verifier has to understand and agree with CP/CPS in the CA repository of the HPCI CA

・Certificates must not be used other than what is stipulated in this CP/CPS "4.5.2 Relying party public key and certificate usage"

・The relying party should confirm if the target certificate issued by the HPCI CA is not falsified and valid

9.7 Disclaimers of warranties

The HPCI CA will strictly observe the contents of the CP/CPS and see to it that the HPCI CA is operated in accordance with the CP/CPS. The HPCI CA however will have no responsibility for damages that may result.

The HPCI CA will provide users and/or relying parties required information concerning the CP/CPS, and recommend the contents to be strictly observed, but does not guarantee to other concerned parties

that users and/or relying parties will strictly observe the contents of “9.6.3 Subscriber representations and warranties” and “9.6.4 Relying party representations and warranties.”

9.8 Limitation of liability (breach of obligation)

The HPCI CA will take no responsibility concerning damages to concerned parties resulting from a user being in violation of “9.6.3 Subscriber representations and warranties” or a party being in violation of “9.6.4 Relying party representations and warranties”.

9.9 Indemnities

Users will be obligated to provide compensation for damages suffered by a third party or parties as a result of failure to comply with “9.6.3 Subscriber representations and warranties.” Verifiers will be obligated to provide compensation for damages suffered by a third party or parties as a result of failure to comply with “9.6.4 Relying party representations and warranties.” Any dispute that may occur between or among concerned parties will be settled between or among said concerned parties.

9.10 Term and termination

The CP/CPS becomes invalid as soon as the HPCI CA completes its work.

9.11 Individual notices and Communications with participants

No stipulation.

9.12 Amendments

9.12.1 Procedure for amendment

The HPCI CA will modify the CP/CPS as needed.

Modified content will be decided and approved by the HPCI PMA. Also, re-approval will be needed when approval was made by the CP/CPS MICS compliance of the APGrid PMA.

The major version No. of the modified CP/CPS will be updated and provided with a new OID.

Approval of the HPCI PMA will not be required for minor modifications such as correction of typographical errors; the document will be modified at the discretion of the Security Officer. At this time, the minor version No. will be updated and a new OID provided.

9.12.2 Notification mechanism and period

When the CP/CPS is modified, it will be published in the CA repository without delay. Users and verifiers will be notified in this way.

9.12.3 Circumstances under which OID must be changed

OID will be modified in accordance with “9.12.1 Revision Procedures”.

9.13 Dispute resolutions provisions

No stipulation.

9.14 Governing law

Any dispute that arise between the HPCI CA and concerned party or parties will be settled in accordance with Japanese domestic law.

9.15 Compliance with applicable law

No stipulation.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

Stipulations of the CP/CPS or any other contract or agreement that directly affect the rights and/or obligations of concerned parties cannot be revised, discarded, added, modified, deleted or ended in writing or orally, unless otherwise stipulated.

9.16.2 Assignment

Rights and/or obligations stipulated or by other contract or agreement will not be transferred or succeeded to any third party without the advance consent of the HPCI CA.

9.16.3 Severability

Even if a portion of the CP/CPS or other contract or agreement becomes invalid or cannot be executed to any degree, it does not affect the validity of the CP/CPS, other contract or agreement, and will be interpreted to match the purpose intended by the HPCI CA as much as rationally possible.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

If it is determined that rights/obligations stipulated in the CP/CPS, other contract or agreement have not been fulfilled, or if a question arises concerning interpretation matters stipulated in the CPS, other contract or agreement, or the documents themselves, the HPCI CA can terminate the CP/CPS, other contract or agreement without the consent of the other party or parties.

Users and/or relying parties may be requested to pay legal fees that result for the HPCI CA to settle a dispute with users and/or relying parties.

9.16.5 Force majeure

The HPCI CA and all concerned parties bear no responsibility to users or relying parties in the event of the followings:

(1) Damage due to natural disaster such as earthquake, flood or volcanic eruption

(2) Damage due to disasters such as fire or power failure

(3) Damage resulting from war, strife or other force majeure

9.17 Other provisions

No stipulation.