NO.	HPCI-CA03-001E-09

HPCI CA

Certification Practice Statement

Ver1.8

March 5th, 2014

HPCI CA 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	In section "9.12.1Procedures for amendment", modified "Approval of the HPCI PMA will not be required for minor modifications … and a new OID not provided" to "… and a new OID provided".
2012.06.19	1.2	1.3.6.1.4.1.32264.2.1.3	In section "4.9.3 Procedure for revocation request, (2)", edited "the HPCI operating office shall send the revocation application or the same content by paper or electronic media to the HPCI CA and …"
2012.08.16	1.3	1.3.6.1.4.1.32264.2.1.4	In sections "3.2.3 Authentication of individual identity" and "5.2.1 Trusted roles, Table 5-1", added the confirmation of the host administrator of the servers in National Institute of Informatics. In section "4.3.1 CA actions during certificate issuance", removed "… online over encrypted channels" In section "5.4.4 Protection of audit log", deleted "lockable" Modified the term "Authentication Portal" to "Certificate Issuing System", the term "HPCI ID" to "HPCI-ID"
2012.08.28	1.4	1.3.6.1.4.1.32264.2.1.5	In section "3.2.3 Authentication of individual identity", removed the official document from the candidates to be presented, and added the case of a non-photo-ID
2013.03.01	1.5	1.3.6.1.4.1.32264.2.1.6	In section "1.1 Overview" and "1.3.5 Other participants", changed the condition of issue of the client certificate. In section "1.4.1" and "6.2.8", changed the condition of use of the client certificate. In section "4.9.2 Who can request revocation", changed "HPCI Account IdP Operating Organization" to "HPCI-ID Management

			Organization". In section "9.6.2 RA representations and warranties", changed "Changes in certificate user name or affiliated organization" to "Changes in certificate user name"
2013.04.01	1.6	1.3.6.1.4.1.32264.2.1.7	In section "4.3.1 (1) Client certificate", deleted "All the above procedures ... online over encrypted channels".
2013.08.16	1.7	1.3.6.1.4.1.32264.2.1.8	In section "5.4.1 Type of events recorded" and "5.5.1 Types of records archived", changed the definition of the records of HPCI-ID Management Organization. In section "8.1 Frequency or circumstances of assessment", changed the definition of the audit. In section "8.3 Assessor's relationship to assessed entity", changed the definition of the auditors. In section "9.6.1CA representations and warranties", changed a part of the responsibilities. In section "9.6.2 RA representations and warranties", changed a part of the obligations.
2014.03.05	1.8	1.3.6.1.4.1.32264.2.1.9	In section "1.3.2 Registration authorities", stated that user's information include the user contact information. Added new sections "1.3.4 Relying parties" and "1.3.5 Other participants". Into section "1.4.1 Appropriate certificate uses", merged the old sections "Certificate types" and "Appropriate certificate uses". In section "2.2 Publication of certification information", changed CRL's publishing site. In section "4.9.3 Procedure for revocation request", added that it is reasonable as a procedure for revocation request even if the user submits the revocation request from the Certificate Issuing System. Into section "5.1.1 Site location and construction",

			merged the old section ″earthquake protection″. In section ″5.5.2 Retention period for archive″, added the explanation of retention period of archive data. In section ″5.6 Key changeover″, changed to describe the CA's lifecycle. In section ″6.2.2 Private key (n out of m) multi-person control″, change the personnel. In section ″6.2.4 Private key backup″, added how to store the Private Key. Into section ″6.3.2 Certificate operational periods and key pair usage periods″, merged the old sections ″Validity period of client certificate″ and ″Validity period of CA certificate″, and in the section changed the expiration date to ″April 24 of each year″. In section ″9.3 Confidentiality of business information″ and ″9.4 Privacy of personal information″, changed URL. In section ″9.6.2 RA representations and warranties″, added about sending the private information over the network. In section ″9.6.3 Subscriber representations and warranties″, changed to apply for revocation within one working day. Modified all section names based on RFC 3647. Unified the terminologies based on section ″1.3 PKI participants″.

Contents

1. INTRODUCTION

This "HPCI Certification Practice Statement" (hereafter referred to as CPS) describes regulations related to operations of the HPCI Certificate Authority.

The structure of this CP/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). The HPCI Certificate Authority Certification Policy (CP) is also covered in this CP/CPS.

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 general users who use HPCI and its associated computing/storage resources but also host and service certificates needed for the HPCI computing 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 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: Allotment rules of "X", see "9.12 Amendments".

1.3 PKI participants

1.3.1 Certification authority

(1) HPCI CA Policy Management Authority

The following decisions concerning operations of the HPCI Certificate Authority shall be made by the HPCI CA Policy Management Authority (hereafter referred to 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. Certificate revocation applications received at RA shall be processed to revoke the appropriate certificates and issue the CRL.

(3) RA

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

RA also confirms that the certificate user is distinguished and authorized by 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 certificates, and registers the CRL issued by the CA to the Certificate Authority Repository.

(4) Certificate Authority Repository

The Certificate Authority Repository registers and publishes CP/CPS, CA Certificates, CRLs and other information to be disclosed to related people.

1.3.2 Registration authorities

(1) HPCI Operating Office

The HPCI Operating Office receives an application from a general user and assigns it an HPCI-ID. It manages the HPCI-ID and other user's information, such as user contact information.

(2) HPCI Account IdP Operating Organization

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

1.3.3 Subscribers

(1) Certificate User

A Certificate User is a user with a certificate issued by the HPCI Certificate

Authority. This includes a general user, a host administrator and a service administrator.

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

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

1.3.4 Relying parties

(1) Relying Party

A Relying Party indicates one who trusts the HPCI Certificate Authority and verifies the certificates.

1.3.5 Other participants

(1) Certificate Management System

The Certificate Management System creates general user key pairs, stores and manages client certificates communicating with RA.

(2) Certificate Issuing System

The Certificate Issuing System is a web system, which offers certificate users an interface for certificate issuance applications.

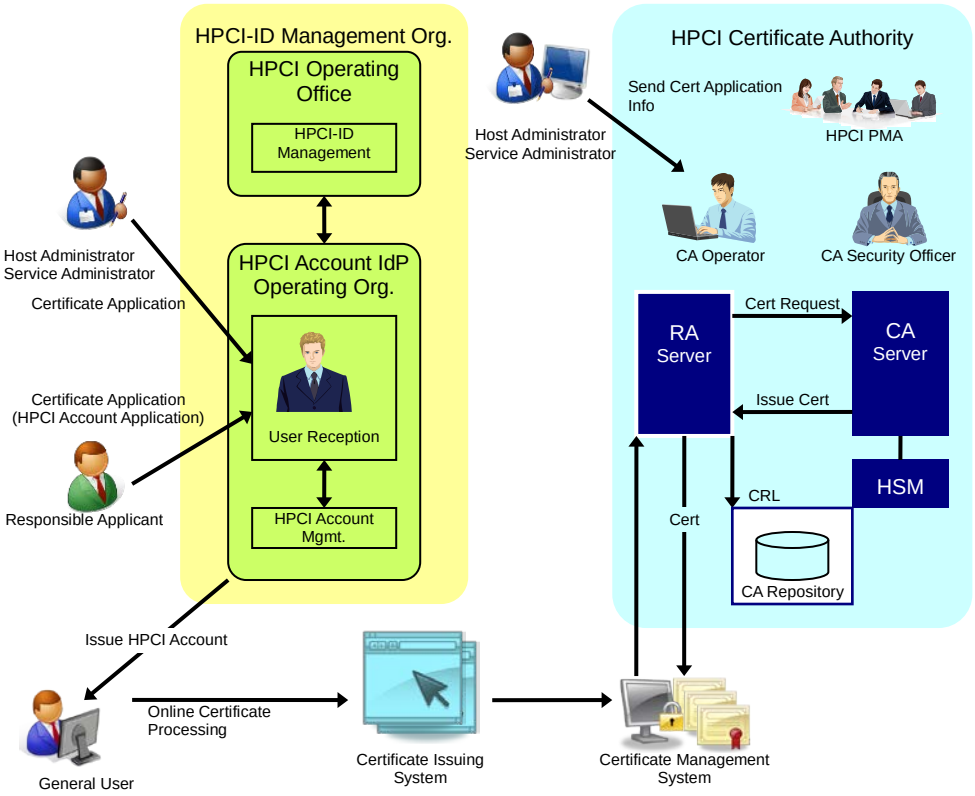

Figure 1-1

1.4 Certificate usage

1.4.1 Appropriate certificate uses

The HPCI Certificate Authority issues the following certificates:

- A Client Certificate
- A Host Certificate
- A Service Certificate

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 and its associated resources
Host Certificate	Server authentication when using HPCI resources
Service Certificate	Service authentication when using HPCI resources

1.4.2 Prohibited certificate uses

Certificates issued by HPCI CA should not be used outside of the scope described in "1.4.1 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: Academic Infrastructure Division
Cyber Science Infrastructure Development Department
National Institute of Informatics
Address: 2-1-2 Hitotsubashi, Chiyoda-ku, 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 require approval of the HPCI PMA or the CA security officer. The approval will be sought following examination by the Member Integrated X.509 PKI Credential Services (MICS) of The Asia Pacific Grid Policy Management Authority (APGrid PMA), when the HPCI PMA determines it is necessary,

1.6 Definitions and acronyms

・Certificate Authority (CA)

An organization that issues, revokes, or suspends public key certificates for key pair (private and public key) owners.

・Certificate Policy (CP)

An applicable policy of certificates for particular communities or applications with general security requirements.

・Certificate Practices Statement (CPS)

A document, which precisely stipulates the procedure to apply the policy defined in CP to the CA operation, external relationships, and general contractual conditions.

・Certificate Revocation List (CRL)

A list, which identifies certificates revoked before the term of validity expires. It is digitally signed by the CA.

・Federal Information Processing Standards (FIPS)

Standardizations developed by the US government for use in computer systems. 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 the user changes affiliation.

・HPCI Account

An account for Single-Sign-On on the HPCI environment. Users will use the HPCI account to apply for certificates via the Certificate Issuing System.

・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, which ensure the validity of the public

keys. It enables stricter (more reliable) identity authentication on the Internet.

・Registration Authority (RA)

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. It 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 Holidays

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

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

Certificate Authority Repository

- The Certificate Authority Repository shall disclose information stipulated in "2.2 Publication of certification information" and shall enable certificate users to search for pertinent information and the CRL.
- Except temporary shutdowns for scheduled maintenance, the goal for operation of the Certificate Authority Repository shall be 24 hours a day, 365 days a year.
- Advance notification shall be provided if the Certificate Authority Repository is to be shut down for reasons such as scheduled maintenance. In the case of unavoidable circumstances such as emergencies, the operation may be shut down without advance notification.
- It shall not be guaranteed that the CRLs stored in the Certificate Authority Repository are the latest available at the point in time in which they are requested.
- Information registered in the Certificate Authority Repository shall be protected.

2.2 Publication of certification information

The following information is published in the Certificate Authority 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	http://www.hpci.nii.ac.jp/ca/hpcica_crl.der
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 Time or frequency of publication

The frequency of information publication is as follows:

- The CA certificate and the CA certificate fingerprint will be published in the Certificate Authority Repository whenever issued.
- The CRL published in the Certificate Authority 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 Certificate Authority Repository whenever updated.

2.4 Access controls on repositories

There is 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 Certificate Issuing System having retrieved the HPCI-ID and the alphabet name from the HPCI Operating 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

The distinguished name given on the certificate will include the unique HPCI-ID issued to the general user. RA will confirm that there is not any overlapping distinguished name 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 identification and authentication when a client certificate, a host certificate, and a service certificate are newly issued.

3.2.1 Method to prove possession of private key

(1) Client certificate

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

(2) Host certificate and service certificate

The 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

The confirmation of the (valid) existence of the certificate user's organization is done by the HPCI Operating Office in the HPCI system usage application procedure.

3.2.3 Authentication of individual identity

(1) Authentication of general user

The reception staff of the HPCI-ID Management Organization shall vet the user identity during user registration. The responsible applicant shall present the user list with copies of their photo-IDs face-to-face to the reception staff. The reception staff will confirm the responsible applicants' own photo-ID and shall confirm that each user on the list matches the given photo-ID. It is assumed that the responsible applicant has confirmed beforehand the validity of all applicants' photo-ID. In cases where the

responsible applicants' own ID does not include the photo, it should be considered acceptable if the reception staff can confirm that the responsible applicant own official document that does include the photo. In the same way, a copy of any user's ID on the list that does not include a photo should be considered acceptable if the responsible applicant can confirm that user's official document that does include a photo.

(2) Authentication of host administrator and service administrator

The reception staff 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 reception staff. The reception staff shall confirm the host administrator's or service administrator's photo-ID and if the host name or service name in the FQDN matches with information provided. If the host administrator or service administrator's own ID does not include a photo, it shall be considered acceptable if the reception staff can confirm that the host administrator's or service administrator's own official document that does include a photo.

The CA security officer is responsible for confirming the identities of host administrators of servers that are part of the HPCI CA system.

3.2.4 Non-verified subscriber information

Only a name and an 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 Operating 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

Face-to-face confirmation at the user reception desk for renewing certificate can be omitted if all of the following conditions are met.

- It is within 5 years from the last certificate application with face-to-face confirmation.
- When there is no change in the certificate user's affiliated organization and subjects written in the certificate.
- The HPCI account will be continued.

If the above is not applicable, the procedure shall follow the registration procedure stipulated 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

Identification and authentication during key renewal after revocation shall 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 presenting the photo-ID. In the case of e-mail, it shall be confirmed that the application is received from the e-mail address registered in the HPCI Operating Office.

However, applications for client, host, or service certificate revocation 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 client certificates, host certificates, and service 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.

Official application form provided by the HPCI Certificate Authority should be used for application for a host or service certificate.

4.1.1 Who can submit a certificate application

Certificate applications will be submitted to the HPCI-ID Management Organization by responsible applicants, host or service administrators.

Online certificate issuance from the HPCI Certificate Authority shall be done by general users, host or service administrators.

4.1.2 Enrollment process and responsibilities

(1) Client certificate

General users shall submit copies of their photo-IDs to the responsible applicant. The responsible applicant shall confirm the legitimacy of the photo-IDs and submit the documents to the user reception desk. The responsible applicant must present accurate information to the HPCI-ID Management Organization.

(2) Host certificates and service certificates

Host administrators and service administrators shall submit copies of photo-IDs, the host name or service name list to the HPCI-ID Management Organization's user reception desk. 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

The examination by the HPCI Operating Office and the HPCI Account IdP Operating 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 the contents of the application submitted by the responsible applicant and host or service administrator do not include any problem.

When the HPCI Certificate Authority confirms that the examination results reported by HPCI-ID Management Organization do not include any problem, it will accept the request for online certificate issuance from the certificate user.

4.2.3 Time to process certificate applications

(1) Client certificates

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

(2) Host certificates and service certificates

Within 5 days (excluded holidays) from the day after the HPCI Account IdP Operating 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

A general user will login to the Certificate Issuing System with the HPCI account, and fill in information required for certificate issuance application. The information for user authentication will be sent to the Certificate Management System from the Certificate Issuing System, and the corresponding key pair will be created within the Certificate Management System. 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

A host or service administrator will create a key pair for the server and then send CSR to the HPCI Certificate Authority. After the HPCI Certificate Authority receives the CSR, it will issue the host and service certificate after verification stipulated in 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.

4.3.2 Notification to subscriber by the CA of issuance of certificate

(1) Client certificate

After a client certificate is issued, the Certificate Management System will send the notification to the user's e-mail address obtained from the HPCI-ID Management Organization.

(2) Host certificate and service certificate

The HPCI Certificate Authority will send the notification by sending the host or service certificate 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 Management System by the user will be acknowledged as "received". If not downloaded, the certificate is counted as "received" when the client certificate is stored in the Certificate Management System.

(2) Host certificate and service certificate

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

4.4.2 Publication of the certificate by the 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

The subscriber shall use the private key and the certificate for the usage stipulated in "1.4.1 Appropriate certificate uses".

4.5.2 Relying party public key and certificate usage

The relying party shall use the public key and the certificate for the usage stipulated in "1.4.1 Appropriate certificate uses".

4.6 Certificate renewal

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:

- The validity of a client certificate has expired.
- When a certificate is reissued after certificate revocation due to the compromise of the user private key, the change in the information contained in the certificate, 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 responsible applicant or the host/service administrator.

4.7.3 Processing certificate re-keying requests

(1) When validity of a client certificate has expired

The renewal process of client certificates, host certificates, and service certificates shall follow procedures stipulated in CP/CPS "4.1 Certificate Application -- 4.4 Certificate acceptance". Note that "4.2.1 Performing identification and authentication functions" shall follow "3.3.1 Identification and authentication for routine re-key".

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

Certificate 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

Acceptance of re-keyed certificates shall be done in accordance with "4.4.1 Conduct constituting certificate acceptance".

4.7.6 Publication of the re-keyed certificate by the CA

Re-keyed certificates shall be done in accordance with "4.4.2 Publication of the certificate by the 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

- The certificate content, such as change in the name, is changed.
- The private key is compromised or suspected to be compromised.

(2) Revocation initiated by HPCI-ID Management Organization

- The existence of the certificate user cannot be confirmed.
- The eligibility of the user is lost.

(3) Revocation initiated by the HPCI CA

- The certificate use violates the CP/CPS or user regulations.
- The private key stored in the Certificate Management System is leaked or compromised.
- It is determined that the HPCI CA wrongly issued a certificate.
- The CA private key in the HPCI CA is leaked or compromised.
- The HPCI CA ceases authentication operations.

4.9.2 Who can request revocation

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

Revocation applications shall be submitted to the HPCI-ID Management Organization by the responsible applicant, the host administrator, or the service administrator. In the case of emergency, revocation applications directly submitted by the certificate user may be accepted at the discretion of the HPCI CA.

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

Revocation applications will be submitted to the HPCI CA by the HPCI Operating Office.

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

Revocation shall be done at the discretion of the CA security officer 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 fill in the application sheet as soon as possible and submit the sheet to the responsible applicant. The responsible applicant should verify the user's identity and the reason for revocation, and then submit the application to the user reception desk. In an emergency, the user can submit the application directly to the user reception desk either in person or by e-mail.

The user reception desk shall perform examinations of the responsible applicant or the user in accordance with "3.4 Identification and authentication for revocation request".

The user reception desk shall send revocation application to the HPCI CA and request the revocation of the appropriate certificate.

The user can also request certificate revocation through the Certificate Issuing

System with the authentication by the user's HPCI account. The HPCI CA regards that the request through the Certificate Issuing System is equivalent for the request through the above procedure.

- 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 the user reception desk.

The user reception desk shall perform examinations of the host or service administrator in accordance with "3.4 Identification and authentication for revocation request".

The user reception desk shall send the revocation application to the HPCI CA and request the revocation of the appropriate certificate.

(2) Procedures for revocation by the HPCI-ID Management Organization

When conditions stipulated in CP/CPS "4.9.1 Circumstances for revocation" are met, the HPCI Operating Office shall send the revocation application, or other documents containing the same content, by the paper or digital media to the HPCI CA and request the revocation of the appropriate certificate.

(3) Procedures for revocation by the HPCI CA

When conditions stipulated in CP/CPS "4.9.1 Circumstances for revocation" are met, the CA security officer or HPCI PMA shall determine the revocation of the appropriate certificate.

After the revocation process, the HPCI CA will notify the HPCI-ID Management Organization the completion of the revocation process.

4.9.4 Revocation request grace period

When there is cause for revocation, the certificate user, the 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 the revocation is approved, the HPCI CA will promptly proceed with the revocation within 1 day excluding the prescribed holidays.

4.9.6 Revocation checking requirement for relying parties

Relying parties shall confirm the validity of certificates by obtaining the latest CRL

published in the Certificate Authority Repository.

4.9.7 CRL issuance frequency

The HPCI CA will issue a 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.

In the normal operation, CRLs will be issued every 24 hours.

4.9.8 Maximum latency for CRLs

After CA issues a new CRL, it will be published in the Certificate Authority Repository within 12 hours.

4.9.9 On-line revocation/status checking availability

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

4.9.10 On-line revocation 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 a CRL in the Certificate Authority Repository.

4.10.2 Service availability

Service usage time shall be as stipulated in ″2.3 Time 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

The HPCI CA facility shall be setup in a place not easily subject to damage due to disasters such as flooding, earthquakes and fire. Safety measures shall be incorporated into the building structure to prevent unauthorized access and withstand earthquakes and fire. Names that explicitly or implicitly indicate the location of the HPCI CA shall not be included on signs or labels inside or outside the building. CA machineries etc., will be set in a dedicated rack complete with safety devices against falling.

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 the authority to access the room to be identified and authenticated by 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 the access authorization are to enter the facilities, those individuals must be accompanied by multiple individuals having the authorization to access the facilities. The purpose for entry will be confirmed, when the room is to be accessed by an unauthorized individual or individuals. A record of accompaniment of two personnel with the authorization to access the room will be kept and periodically reviewed.

When exiting the machine room, the number of people leaving will be checked against the number of people who entered.

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 have water leakage alarms installed, and be in a location that has a

low risk of water damage.

5.1.5 Fire prevention and protection

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

5.1.6 Media storage

Media will be stored in a lockable 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.

5.2 Procedural Controls

5.2.1 Trusted roles

The following show the HPCI CA operation systems and roles:

Table 5-1 HPCI CA Operation Systems and Roles

Person in charge / Agency	Primary Role
CA Security Officer	・Authentication Operations Headquarters ・Management of CA private key ・Management of (physical) keys for the dedicated rack for CA machineries ・Identification of the host administrator of the servers related to the authentication infrastructure operated by the National Institute of Informatics, and the confirmation of their relationship to the FQDN
CA Operator	・Activation/Deactivation of CA private key ・Operation and maintenance management of the CA system (CA server, RA server, and Certificate Authority Repository)
Log Manager	・Management of backup logs 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 followings show the HPCI-ID Management Organization operation systems and roles:

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

Person in charge / Agency	Primary role
HPCI Account IdP Operating Organization User Reception Desk	・Confirmation of identifications of responsible applicants and photo-IDs of applicants ・ Identification of host administrators or service administrators, and their relationship to the FQDN ・Confirmation of user qualifications ・Storage of documents submitted by the certificate users, examination results etc.
HPCI Operating Office	・ Confirmation of the existence of a 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 personnel will be allocated for the following work from the perspective of privilege separation and mutual supervision.

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

Job	Personnel (required number)
Authentication Operations Headquarters	CA Security Officer (1)
Operation and management of CA private key	CA Security Officer (1), CA Operator (1)
Activation/Deactivation of CA private key	CA Operator (2)
management of CA server and RA server	CA Operator (2)
Maintenance and management of CA system	CA Operator (2)
Management of physical key to safe, etc.	Log Manager (1)
Management of audit log and archive media	Log Manager (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 CA Security Officer, the CA Operator, and the Log Manager is not allowed.

5.3 Personnel Controls

5.3.1 Qualifications, experience, and clearance requirements

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

5.3.2 Background check procedures

No stipulation.

5.3.3 Training requirements

Education and training for the operation staff 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

The operation staff will receive education and training for staff reshuffling or changes in work procedures at the discretion of the CA 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 operation 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 appropriately 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 audit logs 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 an event, the date and the time of an event, and the event source information (the system name, the operator's name, etc.).

- CA log
  - CA access log
  - Certificate issue/revocation log and CRL issue log
  - Error log
- RA log
  - RA access log
  - Certificate issue/revocation log
  - Error log
- OS login/logout/reboot log
- Hardware security module (hereafter HSM) log
- Machine room access record
- Machine room work record
- Key lending administration log
- Education and training history
- Record of the work assessment (checklist) of the HPCI-ID Management Organization

5.4.2 Frequency of processing log

Verification of the audit log will be based on instructions of the CA 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 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 Type of events recorded"
- Operation personnel charts
- Explanatory documents to users
- The CP/CPS, certificate and CRL profiles and operation procedures
- Other important documents pertaining to HPCI PMA decisions

(Storage in the HPCI-ID Management Organization)

- Applications received from certificate users, copies of photo-IDs along with their examination results, etc.
- Operation assessment records (checklists)

5.5.2 Retention period for archive

Audit logs will be stored for the period stipulated in "5.4.3 Retention period for audit log". Records of every type of application form, copies of photo-ID, and examination results, etc. will be stored for 5 years in the HPCI-ID Management Organization. Other archive data will be stored for 3 years.

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

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 CRL.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

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

- If an HSM is stolen or the CA private key compromised, the operation will be halted after notifying all related parties.

- If the CA private key is compromised, the key will be used to deactivate the system that verifies the trust of the HPCI CA, in accordance with defined procedures, 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 will be 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 from backup hardware, software and data as soon as possible.

5.7.3 Entity private key compromise procedures

When a user private key has been compromised or there is a possibility of compromise, the user must apply to the HPCI CA for revocation as soon as possible. Also, when a user private key stored in the CA has been compromised or there is a possibility of compromise, the CA 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, the operation can be resumed as stipulated in ″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 CA 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 in the HSM by the CA security officer and the CA operator.

(2) User key

A certificate user key pair will be generated within the Certificate Management System during online certificate issuing.

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

6.1.2 Private key delivery to subscriber

(1) User private key

- When client certificates are stored only in the Certificate Management System
  User private keys are stored only within the Certificate Management System, and not distributed to users.
- When client certificates are downloaded by the user
  User private keys are downloaded in PKCS#12 form by users through the Certificate Management System when they download client certificates.

(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

General user public keys are generated within the Certificate Management System and transmitted to the RA server. The RA server then sends keys to the CA server as certificate issue requests.

Host or service public keys are generated by host administrators or service administrators and transmitted as CSRs to the HPCI CA.

6.1.4 CA public key delivery to relying parties

The CA certificate will be published in the Certificate Authority Repository and distributed.

6.1.5 Key sizes

The algorithm and key length are as follows:

Table 6-1 Key Length Used

Types		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)

Key usages for CA, user, host, and service public keys is configured in the following extensions of X.509 v3:

Table 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

This section stipulates the regulation regarding the CA private key and user private keys. Host and service private keys are managed by the host and service administrators, respectively.

6.2.1 Cryptographic module standards and controls

(1) CA private key

Protected by a FIPS140-2 level 3 HSM or its equivalent.

(2) User private key

・When client certificates are stored only within the Certificate Management System

User private keys will be encrypted when they are stored in the Certificate

Management System. Access the Certificate Management System within the machine room will be restricted to the authorized managers or the authorized servers.

・When users download client certificates

General users will download private keys in the PKCS#12 from the Certificate Management System. The users are responsible for protecting the downloaded certificates and keys.

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

Operations using CA private key will be conducted by the CA Security Officer and the CA Operator.

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 the CA private key shall be carried out by the CA Security Officer and the CA Operator. The backed up CA private key will be saved in an HSM token and stored in a fireproof safe. The HSM physical keys and its PINs must not be stored in places where are managed in the same key.

(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 system backup. The backup media 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 users must be backed up by users, and the backup media 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

The CA private key is generated within an HSM module located in the machine room of the 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 a key is generated and during recovery from backup media. In either case, the process is conducted by the CA Security Officer and the 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 encryption module in the Certificate Management System will be done when a keys is generated during the online certificate issue procedures by the user. A password over 12 characters long will be necessary for authentication.

・When client certificates are downloaded by users

After certificates are download, each private key will be registered 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 two CA Operators within an 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 during authentication for use of resources. Authentication with a password, which is at least 12 characters long, is required for activating private keys.

・When client certificates are downloaded by users

Each certificate user key is activated within the user's computer when authenticating for resource use. Authentication with a password, which is at least 12 characters long, is required for activating private keys.

6.2.9 Method of deactivating private key

CA private keys will be deactivated by two CA Operators within an HSM.

6.2.10 Method of destroying private key

(1) CA private key

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

When backup media containing discarded CA private keys are to be taken out of the room, they must be physically destroyed.

(2) User private key

・When client certificate is stored only within the Certificate Management System

Destruction of user private keys in the Certificate Management System or backup media will be done by the person in charge at the Certificate Management System using designated procedures to ensure the keys cannot be reused.

・When client certificates are downloaded by users

Users will take responsibility for destruction of downloaded certificates and backup media.

6.2.11 Cryptographic Module Rating

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

6.3 Other aspects of key pair management

6.3.1 Public key archival

Public keys are included within archived 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

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

Table 6-3 Validity period of certificate

Types	Expiration date (The validity period not exceeding 13 months in each case)
Client certificate	April 24 of each year
Host certificate	April 24 of each year
Service certificate	April 24 of each year

The validity period of the CA Certificate will not exceed ten years.

6.4 Activation data

6.4.1 Activation data generation and installation

(1) CA private key

The CA private key will be activated using both a password and an HSM physical key. The password will consist of at least 15 characters decided by the CA Operator and inputted into an HSM.

(2) User private key

User private key activation data is a password consisting of over 12 characters input by the user during online certificate issue procedures. This password will be set as the user access password to the private key.

6.4.2 Activation data protection

(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 CA 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 dedicated machine with only the functions needed for the HPCI CA, and only used for the limited operations 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 a firewall.

Connection between CA and RA servers, and between the RA server and the Certificate Management System, will be restricted to the designated communication port, and security measures will be taken to prevent unauthorized access. The communication route between the CA server and the RA server, and the RA server and the Certificate Management System will be encrypted.

6.8 Time-stamping

The HPCI CA will synchronize with a time server in order to accurately record the day and the time for certificates issuance, logs, etc.

7. CERTIFICATE, CRL, AND OCSP PROFILES

The certificate and CRL profile is based on RFC5280 and follows the separately set design specifications for certificate and CRL profiles. 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 in compliance with the CP/CPS.

The HPCI-ID Management Organization performs an internal assessment every year according to the assessment checklist presented by the HPCI CA, and the results are reported to the HPCI CA.

8.2 Identity/qualifications of assessor

Auditors should be familiar with auditing and authentication operations.

8.3 Assessor's relationship to assessed entity

The internal audit of the HPCI CA is made by its personnel. The internal assessment of the HPCI-ID Management Organization is made by its personnel.

Any governmental organization or academic institution with the appropriate jurisdiction can perform an external audit.

If other trusted CAs or relying parties request an external assessment, the costs of the assessment must be paid by the requesting party, except for the costs of HPCI CA and the HPCI-ID Management Organization personnel and infrastructure.

8.4 Topics covered by assessment

The audit will cover whether authentication operations of the HPCI CA are carried out in accordance with the CP/CPS and other operation procedure documents.

8.5 Actions taken as a result of deficiency

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

8.6 Communication of results

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

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

Fees will be determined by the usage regulations of the HPCI Consortium.

9.2 Financial responsibility

No stipulation.

9.3 Confidentiality of business information

Protection and handling of confidential information by the HPCI CA will be stipulated in the following regulations of the National Institute of Informatics:

Research Organization of Information and Systems of Security Policy

http://www.rois.ac.jp/pdf/security_policy.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 not be used except where required. Information designated as confidential will be safely stored under the administration of a designated person in charge.

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 client 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 use personal information provided by users to the HPCI-ID Management Organization for anything other than issuing or revoking certificates.

If there is a request from the user, the following information may be disclosed after confirming the user's identity:

- Application to issue a certificate submitted to the HPCI CA or the HPCI-ID Management Organization
- Certificate contents
- Certificate status

Apart from the above, the following regulations regarding handling of personal information stipulated by the National Institute of Informatics will be followed:

- Research Organization of Information and Systems Personal Information Protection Regulations
  http://www.rois.ac.jp/pdf/3-10.pdf
- For NII Personal Information Protection Disclosure Requests:
  http://www.nii.ac.jp/disclosure/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 CA representations and warranties

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

- Certificate issuance and validation will be based on the CP/CPS.
- Excluding times of system emergency or maintenance, CA certificate information and CRL will be published to the Certificate Authority Repository.
- Applicable CP/CPS will be specified when certificates are issued.
- Authentication operations are performed in accordance with the CP/CPS, and the HPCI CA has full responsibility for the credibility of certificates or CRL from the point they are issued. However, even though HPCI CA adds signatures to this information, it can't guarantee credibility when the data is falsified by a third person (found by attacks), or the signature algorithm becomes obsolete.
- Appropriate authentication operations are done in accordance with CP/CPS to protect the HPCI CA private key from compromise due to theft and/or loss.
- Approval of cooperative applications from the HPCI-ID Management Organization.
- Identification and authentication of the certificate user and/or organization will be done with cooperation of the HPCI-ID Management Organization.
- Operation requirements will be presented to the HPCI-ID Management Organization in the form of an assessment checklist, and everything done to

ensure that the requirements are being fulfilled.

- All communication lines between the HPCI-ID Management Organization and the Certificate Management System will be encrypted for safe and reliable transmission.

9.6.2 RA representations and warranties

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

- Processing of applications for certificate issue, renewal and revocation, including identification and authentication of certificate users and/or organizations will be done in accordance with the CP/CPS.
- Changes in certificate user name and loss of usage qualification should be detected as soon as possible, and a revocation application will be sent to the HPCI CA.
- Send user's certificate information (HPCI-ID, roman alphabet name) safely by coordinating with the Certificate Issuing System of the HPCI CA.
- Cooperate with the Certificate Management System to notify the user of the completion of issuance of their certificate.
- Certificate user information used for each application will be safely stored for the period stipulated in the CP/CPS.
- Regular internal assessments are conducted to ensure the HPCI CA operation requirements are being fulfilled, and the results are reported to the HPCI PMA.
- Identity assertions made by the HPCI-ID Management Organization to any system must occur over encrypted channel.

9.6.3 Subscriber representations and warranties

The certificate user will have the following obligations and responsibilities:

- Present accurate information when applying for certificate issue or revocation to the HPCI-ID Management Organization and HPCI CA.
- Acquire certificates using the procedure provided by the HPCI CA.
- Do not use certificates for purposes other than those stipulated in the CP/CPS, and do not use certificates that have expired.
- Store the activation password of the private key in a safe place.
- Assume the responsibility to manage the private key so as to avoid compromising the key and certificate due to theft or loss.

- Apply for revocation within one working day in the event 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 administrators and service administrators 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:

- Relying Parties must understand and agree with the CP/CPS in the Certificate Authority Repository of the HPCI CA.
- Certificates should not be used for purpose other than what is stipulated in the CP/CPS "4.5.2 Relying party public key and certificate usage".
- Relying Parties should confirm that the target certificate is a valid certificate issued by the HPCI CA and is not falsified.

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. However, the HPCI CA will assume no responsibility for damages that may result.

The HPCI CA will provide certificate users and/or relying parties with the necessary information concerning the CP/CPS, and recommend the contents to be strictly observed, but does not guarantee to other concerned parties that certificate 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 Limitations of liability

The HPCI CA will take no responsibility concerning damages to concerned parties resulting from a certificate 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

Certificate 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". Relying parties 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 will become invalid immediately following the HPCI CA ceasing operations.

9.11 Individual notices and communications with participants

No stipulation.

9.12 Amendments

9.12.1 Procedures for amendment

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

Modified content will be decided on and approved by the HPCI PMA. Also, re-approval will be needed when CP/CPS changes have been approved by the APGrid PMA for MICS compliance.

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. In this case the document will be modified at the discretion of the CA Security Officer, and 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 Certificate Authority Repository without delay. Publishing in the Certificate Authority Repository will serve as notice of the new CP/CPS certificate users and relying parties.

9.12.3 Circumstances under which OID must be changed

OID will be modified in accordance with "9.12.1 Procedures for amendment".

9.13 Dispute resolution provisions

No stipulation.

9.14 Governing law

Any dispute that arises 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 cannot be transferred to or inherited by 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 or any 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 or other contract or agreement have not been fulfilled, or if a question arises concerning interpretation of matters stipulated in the CP/CPS, other contract or agreement, or the documents themselves, the HPCI CA can terminate the CP/CPS or other contract or agreement without the consent of the other party or parties.

Certificate users and/or relying parties may be requested to pay legal fees incurred by the HPCI CA when settling a dispute with certificate users and/or relying parties.

9.16.5 Force Majeure

The HPCI CA and all concerned parties bear no responsibility to certificate 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.