NO.	HPCI-CA03-001E-17

HPCI CA
Certification Practice Statement
Ver8.0

June 30, 2021

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 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".

2015.11.30	1.9	1.3.6.1.4.1.32264.2.1.10	In section "9.12.1 Procedures for amendment", deleted " Also, re-approval will be needed ... APGrid PMA for MICS compliance." because we are approved by the APGrid PMA to be compliant with MICS.
2016.06.15	2.0	1.3.6.1.4.1.32264.2.1.11	In sections "1.1 Overview", "1.3.1 Certification authority", "1.4.1 Appropriate certificate uses", "1.6 Definitions and acronyms", "2.1 Repositories", "2.2 Publication of certification information", "4.9.6 Revocation checking requirement for relying parties", "4.9.9 On-line revocation/status checking availability", "4.10.1 Operational characteristics", "6.1.5 Key sizes", "6.1.7 Key usage purposes (as per X.509 v3 key usage field)", "6.3.2 Certificate operational periods and key pair usage periods", "7 . CERTIFICATE AND CRL PROFILES", "9.6.1 CA representations and warranties" and Figure 1-1, added about OCSP Responder.
2016.08.16	3.0	1.3.6.1.4.1.32264.2.1.12	In section "9.6.3 Subscriber representations and warranties", added "Any user certificates must not be shared".
2016.11.11	4.0	1.3.6.1.4.1.32264.2.1.13	In section "1. INTRODUCTION", added the explanation of HPCI. In section "3.3.1 Identification and authentication for routine re-key", modified the procedure for renewing the HPCI account. In sections "4.9.1 Circumstances for revocation" and "4.9.3 Procedure for revocation request", modified the procedure for the certificate revocation. Replace the term 'Certificate Authority' with 'Certification Authority', and the term

			'Certification Policy' with 'Certificate Policy'.
2017.06.01	5.0	1.3.6.1.4.1.32264.2.1.14	In section "3.1.2 Need for names to be meaningful", added that the commonName in the subject DN for client certificate shall contain at least the first name in full and the full family name of the user.
2017.09.25	6.0	1.3.6.1.4.1.32264.2.1.15	In section "6.3.2 Certificate operational periods and key pair usage periods", modified expiration date of client certificate to "395 days after the certificate issued".
2020.10.02	7.0	1.3.6.1.4.1.32264.2.1.16	In section "3.2.3(1)Authentication of general user ", added video conference as a method of vetting of the identity of the responsible applicant of a research project. In section "5.5.1 Types of records archived", added the snapshots taken during a video conference for remote identity vetting, to the "Storage in the HPCI-ID Management Organization".
2021.06.30	8.0	1.3.6.1.4.1.32264.2.1.17	In section “1.3 PKI participants”, modified the structure to comply with RFC 3647. In section " 1.3.5 Other participants", modified the decision about the HPCI Account IdP Operating Organization. In section "1.3.2 Registration authorities", modified the decision about the Registration Authority. In section "1.3.2 Registration authorities", added the "1.3.2(4)HPCI Cooperative Service Organizing and Working Group" In section "1.5.2 Contact person", added period until response to received e-mail. Modified the department and the telephone number. In section "3.1.2 Need for names to be meaningful", added about the service name of the commonName in the subject DN for

			service certificates. In section "3.1.2 Need for names to be meaningful, Table 3-1", modified the values of the 'Description' and 'Set point' corresponding to commonName. In sections "3.2.3 Authentication of individual identity", modified the description of the identification method for host administrator and service administrator. In sections "3.3.2 Identification and authentication for re-key after revocation" and "3.4 Identification and authentication for revocation request", added Shibboleth authentication. In section "4.1.1 Who can submit a certificate application", replace the term 'issuance' with 'application'. In section "4.1.2 Enrollment process and responsibilities (2)", removed copies of photo-IDs from submission. In section "4.2.3 Time to process certificate applications", modified the description of time to process certificate applications. In section "4.9.1 Circumstances for revocation", added change of certificate users' affiliated organization. In section "5.1.1 Site location and construction", removed the description of indication of the location of the HPCI CA. In sections "5.1.2 Physical access" and "5.2.2 Number of persons required per task", modified the number of personnel for required. In section "5.2.1 Trusted roles", modified personnel managing of physical keys for the dedicated rack for CA equipment.

			In section "5.2.1 Trusted roles", described that "The operation members list of the HPCI CA is updated once a year". In section "5.2.1 Trusted roles", described that "The operation members list of the HPCI-ID management organization is reviewed once a year". In section "5.5.2 Retention period for archive", revised the storage period of "Records of various applications, copies of photo IDs and examination results, etc. from certificate subscribers" stored at the HPCI-ID management organization. In section "5.7.2 Computing resources, software, and/or data are corrupted", added about HSM device recovery training. In section "6.1.5 Key sizes", described that RSA 2048bit key strength is equivalent to 112-bit security. In section "6.2.4 Private key backup", added "The PINs must be kept on an offline medium." In section "6.2.9 Method of deactivating private key", added about deactivation of user private key. In section "6.7 Network security controls", added the cipher strength is 112-bit security or higher. In section "7. CERTIFICATE AND CRL PROFILES", added the RFC6818 as the base profile for the certificate and CRL. In section "8.3 Assessor's relationship to assessed entity", described that "When an external audit is performed, the auditee, the HPCI CA, shall present audit logs in response

			to a request from a governmental organization or an academic institution, the auditor.". In sections "9.3 Confidentiality of business information" and "9.4 Privacy of personal information", modified the issuer of the regulation. In section "9.4 Privacy of personal information", modified the hyperlinks of references. In section "9.6.1 CA representations and warranties", modified the task of identifying and authenticating is delegated to the HPCI Management Organization, replaced the stipulation of the operational requirements with the periodically verification whether requirements are guaranteed. On the whole corrected the English expression. In section "9.6.3 Subscriber representations and warranties", described that "If a user uses a client certificate, host certificate, or service certificate signed by the HPCI Certificate Authority, the user must comply with this CP / CPS".

Contents

1. INTRODUCTION 17

1.1 Overview 17
1.2 Document name and identification 17
1.3 PKI participants 18
1.3.1 Certification authority 18
1.3.2 Registration authorities 18
1.3.3 Subscribers 19
1.3.4 Relying parties 19
1.3.5 Other participants 19
1.4 Certificate usage 20
1.4.1 Appropriate certificate uses 20
1.4.2 Prohibited certificate uses 21
1.5 Policy administration 21
1.5.1 Organization administering the document 21
1.5.2 Contact person 21
1.5.3 Person determining CPS suitability for the policy 21
1.5.4 CPS approval procedures 22
1.6 Definitions and acronyms 22

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES 24

2.1 Repositories 24
2.2 Publication of certification information 24
2.3 Time or frequency of publication 25
2.4 Access controls on repositories 25

3. IDENTIFICATION AND AUTHENTICATION 26

3.1 Naming 26
3.1.1 Types of names 26
3.1.2 Need for names to be meaningful 26
3.1.3 Anonymity or pseudonymity of subscribers 26

3.1.4 Rules for interpreting various name forms 27
3.1.5 Uniqueness of names 27
3.1.6 Recognition, authentication, and role of trademarks 27
3.2 Initial identity validation 27
3.2.1 Method to prove possession of private key 27
3.2.2 Authentication of organization identity 27
3.2.3 Authentication of individual identity 27
3.2.4 Non-verified subscriber information 29
3.2.5 Validation of authority 29
3.2.6 Criteria for interoperation 29
3.3 Identification and authentication for re-key requests 29
3.3.1 Identification and authentication for routine re-key 29
3.3.2 Identification and authentication for re-key after revocation 30
3.4 Identification and authentication for revocation request 30

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 31

4.1 Certificate Application 31
4.1.1 Who can submit a certificate application 31
4.1.2 Enrollment process and responsibilities 31
4.2 Certificate application processing 31
4.2.1 Performing identification and authentication functions 31
4.2.2 Approval and rejection of certificate applications 32
4.2.3 Time to process certificate applications 32
4.3 Certificate issuance 32
4.3.1 CA actions during certificate issuance 32
4.3.2 Notification to subscriber by the CA of issuance of certificate 33
4.4 Certificate acceptance 33
4.4.1 Conduct constituting certificate acceptance 33
4.4.2 Publication of the certificate by the CA 33
4.4.3 Notification of certificate issuance by the CA to other entities 33
4.5 Key pair and certificate usage 34
4.5.1 Subscriber private key and certificate usage 34
4.5.2 Relying party public key and certificate usage 34
4.6 Certificate renewal 34

4.7 Certificate re-key 34
4.7.1 Circumstance for certificate re-key 34
4.7.2 Who may request certification of a new public key 34
4.7.3 Processing certificate re-keying requests 34
4.7.4 Notification of new certificate issuance to subscriber 35
4.7.5 Conduct constituting acceptance of a re-keyed certificate 35
4.7.6 Publication of the re-keyed certificate by the CA 35
4.7.7 Notification of certificate issuance by the CA to other entities 35
4.8 Certificate modification 35
4.9 Certificate revocation and suspension 35
4.9.1 Circumstances for revocation 35
4.9.2 Who can request revocation 36
4.9.3 Procedure for revocation request 36
4.9.4 Revocation request grace period 37
4.9.5 Time within which CA must process the revocation request 38
4.9.6 Revocation checking requirement for relying parties 38
4.9.7 CRL issuance frequency 38
4.9.8 Maximum latency for CRLs 38
4.9.9 On-line revocation/status checking availability 38
4.9.10 On-line revocation checking requirements 38
4.9.11 Other forms of revocation advertisements available 38
4.9.12 Special requirements re-key compromise 38
4.9.13 Circumstances for suspension 38
4.9.14 Who can request suspension 39
4.9.15 Procedure for suspension request 39
4.9.16 Limits on suspension period 39
4.10 Certificate status services 39
4.10.1 Operational characteristics 39
4.10.2 Service availability 39
4.10.3 Optional features 39
4.11 End of subscription 39
4.12 Key escrow and recovery 39

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 40

5.1 Physical controls 40
5.1.1 Site location and construction 40
5.1.2 Physical access 40
5.1.3 Power and air conditioning 40
5.1.4 Water exposures 40
5.1.5 Fire prevention and protection 41
5.1.6 Media storage 41
5.1.7 Waste disposal 41
5.1.8 Off-site backup 41
5.2 Procedural Controls 41
5.2.1 Trusted roles 41
5.2.2 Number of persons required per task 42
5.2.3 Identification and authentication for each role 43
5.2.4 Roles requiring separation of duties 43
5.3 Personnel Controls 43
5.3.1 Qualifications, experience, and clearance requirements 43
5.3.2 Background check procedures 43
5.3.3 Training requirements 44
5.3.4 Retraining frequency and requirements 44
5.3.5 Job rotation frequency and sequence 44
5.3.6 Sanctions for unauthorized actions 44
5.3.7 Independent contractor requirements 44
5.3.8 Documentation supplied to personnel 44
5.4 Audit logging procedures 44
5.4.1 Type of events recorded 44
5.4.2 Frequency of processing log 45
5.4.3 Retention period for audit log 45
5.4.4 Protection of audit log 45
5.4.5 Audit log backup procedures 45
5.4.6 Audit collection system 46
5.4.7 Notification to event-causing subject 46
5.4.8 Vulnerability assessments 46
5.5 Records archival 46
5.5.1 Types of records archived 46
5.5.2 Retention period for archive 46

5.5.3 Protection of archive 47
5.5.4 Archive backup procedures 47
5.5.5 Requirements for time-stamping of records 47
5.5.6 Archive collection system 47
5.5.7 Procedures to obtain and verify archive information 47
5.6 Key changeover 47
5.7 Compromise and disaster recovery 47
5.7.1 Incident and compromise handling procedures 47
5.7.2 Computing resources, software, and/or data are corrupted 48
5.7.3 Entity private key compromise procedures 48
5.7.4 Business continuity capabilities after a disaster 48
5.8 CA termination 48

6. TECHNICAL SECURITY CONTROLS 49

6.1 Key pair generation and installation 49
6.1.1 Key pair generation 49
6.1.2 Private key delivery to subscriber 49
6.1.3 Public key delivery to certificate issuer 49
6.1.4 CA public key delivery to relying parties 49
6.1.5 Key sizes 50
6.1.6 Public key parameters generation and quality checking 50
6.1.7 Key usage purposes (as per X.509 v3 key usage field) 50
6.2 Private Key Protection and Cryptographic Module Engineering Controls 50
6.2.1 Cryptographic module standards and controls 51
6.2.2 Private key (n out of m) multi-person control 51
6.2.3 Private key escrow 51
6.2.4 Private key backup 51
6.2.5 Private key archival 52
6.2.6 Private key transfer into or from a cryptographic module 52
6.2.7 Private key storage on cryptographic module 52
6.2.8 Method of activating private key 53
6.2.9 Method of deactivating private key 53
6.2.10 Method of destroying private key 53
6.2.11 Cryptographic Module Rating 54

6.3 Other aspects of key pair management 54
6.3.1 Public key archival 54
6.3.2 Certificate operational periods and key pair usage periods 54
6.4 Activation data 54
6.4.1 Activation data generation and installation 54
6.4.2 Activation data protection 55
6.4.3 Other aspects of activation data 55
6.5 Computer security controls 55
6.5.1 Specific computer security technical requirements 55
6.5.2 Computer security rating 55
6.6 Life cycle technical controls 55
6.6.1 System development controls 55
6.6.2 Security management controls 55
6.6.3 Life cycle security controls 56
6.7 Network security controls 56
6.8 Time-stamping 56

7. CERTIFICATE AND CRL PROFILES 57

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS 58

8.1 Frequency or circumstances of assessment 58
8.2 Identity/qualifications of assessor 58
8.3 Assessor's relationship to assessed entity 58
8.4 Topics covered by assessment 58
8.5 Actions taken as a result of deficiency 58
8.6 Communication of results 59

9. OTHER BUSINESS AND LEGAL MATTERS 60

9.1 Fees 60
9.2 Financial responsibility 60
9.3 Confidentiality of business information 60
9.3.1 Scope of confidential information 60
9.3.2 Information not within the scope of confidential information 60

9.4 Privacy of personal information 60
9.5 Intellectual property rights 61
9.6 Representations and warranties 61
9.6.1 CA representations and warranties 61
9.6.2 RA representations and warranties 62
9.6.3 Subscriber representations and warranties 62
9.6.4 Relying party representations and warranties 63
9.7 Disclaimers of warranties 63
9.8 Limitations of liability 63
9.9 Indemnities 64
9.10 Term and termination 64
9.11 Individual notices and communications with participants 64
9.12 Amendments 64
9.12.1 Procedures for amendment 64
9.12.2 Notification mechanism and period 64
9.12.3 Circumstances under which OID must be changed 65
9.13 Dispute resolution provisions 65
9.14 Governing law 65
9.15 Compliance with applicable law 65
9.16 Miscellaneous provisions 65
9.16.1 Entire agreement 65
9.16.2 Assignment 65
9.16.3 Severability 65
9.16.4 Enforcement (attorneys' fees and waiver of rights) 66
9.16.5 Force Majeure 66
9.17 Other provisions 66

1. INTRODUCTION

This "HPCI CA Certificate Policy and Certification Practice Statement" (hereafter, CP/CPS) describes regulations related to operations of the HPCI Certification Authority (CA). HPCI stands for High Performance Computing Infrastructure and is a distributed supercomputing infrastructure in Japan.
The structure of this CP/CPS conforms to the Request For Comments (RFC) 3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" advocated by the Public-Key Infrastructure Working Group (PKIX) of the Internet Engineering Task Force (IETF). The HPCI Certification Authority Certificate Policy (CP) is covered in this CP/CPS.

1.1 Overview

The CP/CPS provides information regarding certificate issuance, revocation, and other authentication related procedures managed by the HPCI CA.
The HPCI CA issues the certificates listed below. Certificates are only issued to users who meet the necessary qualifications set out in the "HPCI Consortium Usage Statements" (referred to as "usage statements").

- Client certificates for authentication of users who use HPCI and its associated computing/storage resources
- Host and service certificates needed for access to the computing and storage environment
- OCSP responder certificates for signing OCSP responses

1.2 Document name and identification

The following policy IDs are used by the HPCI CA to distinguish CP/CPS content and certificate policy.

Table 1-1 OIDs and Objects

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

Note: For allotment rules of "X", see "9.12 Amendments".

1.3 PKI participants

1.3.1 Certification authority

(1) CA

The CA issues certificates upon request from RA. Certificate revocation applications received at RA is processed to revoke the appropriate certificates and issue the CRL.

1.3.2 Registration authorities

(1) Registration Authority

The RA receives online certificate issuance requests from certificate users and requests the CA to issue the certificates.
In cooperation with the HPCI-ID Management Organization, the RA also confirms those who was distinguished and authenticated certificate user by the HPCI Account IdP Operating Organization. The RA also receives certificate revocation applications and requests the CA to revoke the certificates and registers the CRL issued by the CA to the Certification Authority Repository.

(2) HPCI Operating Office

The HPCI Operating Office receives applications from users to which HPCI-IDs are assigned. It manages the HPCI-ID and other user information, such as user contact information. It is an external agency different from the Certification authority.

(3) HPCI Account IdP Operating Organization

The 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 approved. It is an external agency different from the Certification authority.

(4) HPCI Cooperative Service Organizing and Working Group

Accepts registration / change requests for host or service managers from organizations that require host or service certificates. Identifies and authenticates the host administrator and service administrator, and registers the authorized host administrator or service administrator on "Administrator list of the HPCI authentication infrastructure". It is an external organization separate from the certificate authority.

1.3.3 Subscribers

(1) Certificate User

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

A 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 service administrator are administrators of hosts and services necessary for usage of HPCI resources. The administrators 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 CA and verifies the certificates.

1.3.5 Other participants

(1) HPCI CA Policy Management Authority

The following decisions concerning operations of the HPCI CA is made by the HPCI CA Policy Management Authority (hereafter, HPCI PMA):

- Decisions regarding and approval of CP/CPS
- Handling CA private key compromise
- Handling of emergencies such as disasters
- Authorization of the HPCI Account IdP Operating Organization
- Other important matters concerning CA operations

(2) Certification Authority Repository

The CA Repository registers and provides information that HPCI CA discloses to concerned personnel, such as CP/CPS, CA Certificates, CRLs, and OCSP responder.

(3) Certificate Management System

The Certificate Management System works in tandem with the RA to create user key pairs, store and manage client certificates.

(4) Certificate Issuing System

The Certificate Issuing System is a web system, which offers certificate users an interface

for certificate issuance applications.

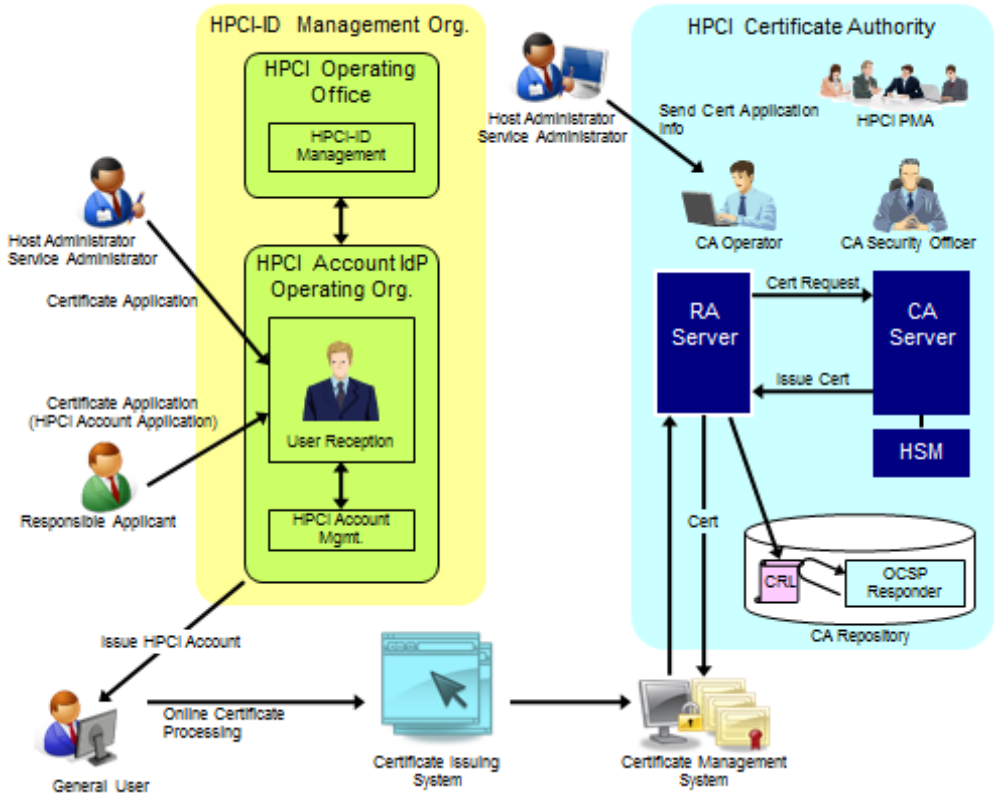

Figure 1-1 Structure of HPCI CA

1.4 Certificate usage

1.4.1 Appropriate certificate uses

The HPCI CA issues the following certificates:

- Client certificates
- Host certificates
- Service certificates
- OCSP responder certificates

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

Table 1-2 Types and Application of Certificates

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
OCSP Responder Certificate (*)	Signing OCSP Responses

(*) The targets are servers operated by HPCI authentication infrastructure only.

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 CP/CPS is maintained and administrated by the HPCI PMA.

1.5.2 Contact person

Contact the following for questions regarding the CP/CPS:

Department: Academic Infrastructure Division
Cyber Science Infrastructure Development Department
Inter-University Reseach Institute Corporation
Research Organization of Information and Systems
National Institute of Informatics

Address: 2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430

Tel: +81-3-4212-2858

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

For inquiries received at this email address, we aim to reply within one business day in principle.

1.5.3 Person determining CPS suitability for the policy

No stipulation.

1.5.4 CPS approval procedures

Establishment of and modifications to the CP/CPS require approval of the HPCI PMA or the CA Security Officer. When the HPCI PMA deems it necessary, approval is sought following screening by the Member Integrated X.509 PKI Credential Services (MICS) of the Asia Pacific Grid Policy Management Authority (APGrid PMA).

1.6 Definitions and acronyms

- Certification Authority (CA)

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

- Certificate Policy (CP)

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

- Certification Practices Statement (CPS)

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

- Certificate Revocation List (CRL)

A list, which identifies certificates revoked before the expiration date. It is digitally signed by the CA.

- Federal Information Processing Standards (FIPS)

Standards developed by the US federal government for use in computer systems. FIPS140-2 is the standard for evaluating cryptographic modules.

- High Performance Computing Infrastructure (HPCI)

An innovative high performance computing infrastructure. The CP/CPS refers to all computing and storage systems linked to the HCPI, and any other systems operating as part of the HPCI environment as the HPCI System.

- HPCI-ID

A unique ID issued to each HPCI user. HPCI-ID does not change even after the user transfers to a different organization.

- HPCI Account

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

- OCSP (Online Certificate Status Protocol)

A protocol for acquiring the revocation status of the certificate

- Object Identifier (OID)

Identifiers allotted to reciprocally distinguish data regardless of its meaning. They are managed in tree form to uniquely specify the data.

- Public Key Cryptography Standards (PKCS)

Industry standards proposed by the USA RSA Laboratories aimed at achieving portability and interconnectivity of applications associated with cryptographic algorithms and other cryptographic calculations.
PKCS#12: Standards concerning personal information

- Public Key Infrastructure (PKI)

Infrastructure to enable the use of public key certificates, which ensures the validity of the public keys. It enables stricter (more reliable) identity authentication on the Internet.

- Registration Authority (RA)

RA registers users with the PKI system, issues public key certificates and examines revocation applications.

- Rivest-Shamir-Adleman (RSA)

Currently the most common form of public key cryptography. This cryptosystem is based on the practical difficulty of factoring the product of two large prime numbers.

- Statutory 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

The CA Repository is responsible for the following:

- Disclosing information stipulated in "2.2 Publication of certification information" and enabling certificate users and relying parties to search for pertinent information and the CRL.
- Except temporary shutdowns for scheduled maintenance, the goal for operation of the CA Repository is 24 hours a day, 365 days a year.
- Providing advance notice if the CA Repository is to be shut down for reasons such as scheduled maintenance. In the case of emergencies and other unforeseen circumstances, operations may be shut down without advance notice.
- It is not guaranteed that the CRLs stored in the CA Repository have been updated at the point at which they are requested.
- It is not guaranteed that the revocation status of the certificate provided by OCSP responder has been updated at the point at which they are requested.
- Protecting information registered in the CA Repository.

2.2 Publication of certification information

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

Table 2-1 Information published by HPCI CA

Document	Site Published (URL)
Fingerprint of CA Certificate, and other information concerning the HPCI CA	https://www.hpci.nii.ac.jp/ca/
CA certificate of the HPCI CA	https://www.hpci.nii.ac.jp/ca/hpcica.cer
CRL	http://www.hpci.nii.ac.jp/ca/hpcica_crl.der
OCSP responder	http://ocsp.hpci.nii.ac.jp
CP/CPS	https://www.hpci.nii.ac.jp/ca/hpcicacps.pdf

The various application procedures and usage regulations of the HPCI system are in

accordance with the HPCI consortium public information.

2.3 Time or frequency of publication

Publication frequency is as follows:

- The CA certificate and the CA certificate fingerprint is published in the CA Repository whenever issued.
- The CRL published in the CA Repository whenever the CRL is issued (or certificate is revoked) and during the periodic update as stipulated in "4.9.7 CRL issuance frequency."
- The CP/CPS and information concerning the HPCI CA is published in the CA 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 CA 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 CA are provided in Table 3-1.

Table 3-1 Naming attributes of certificates

Attributes used	Description	Set point
commonName	User identifier (client certificate)	[User name HPCI-ID]
	Host identifier (host certificate)	[FQDN]
	Service identifier (service certificate)	[Service name/FQDN]
organizationalUnitName	Organizational unit name	HPCI (fixed)
organizationName	Organizational name	NII (fixed)
countryName	Country name	JP (fixed)

The commonName in the subject DN for client certificate is in alphabet and shall contain at least the first name in full and the full family name of the user. The client certificate commonName is set by the Certificate Issuing System having retrieved the HPCI-ID and the alphabet name from the HPCI Operating Office based on attributes received by the SAML assertion from the HPCI Account IdP Operating Organization.
The commonName in the subject DN for service certificate contains only the FQDN unless the software requires the service name.

3.1.3 Anonymity or pseudonymity of subscribers

No stipulation.

3.1.4 Rules for interpreting various name forms

Distinguished names used will be set according to rules stipulated in 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 user. RA checks for duplicate distinguished name to ensure the uniqueness of each 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 certificates

As the private keys for client certificates are created in the Certificate Management System, users do not possess private keys.

(2) Host certificates and service certificates

The HPCI CA confirms the ownership of a 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 existence of the certificate user 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 per research project. Vetting of the identity of the responsible applicant of a research

project shall be based on a face-to-face meeting or a video conference.

- Face-to-face meeting

  The responsible applicant shall present a project members list with copies of their photo-IDs face-to-face to the reception staff.

  The reception staff shall confirm the identity of the responsible applicant in person via photo-ID. The reception staff shall also confirm each member's identity via the copy of the photo-ID concerned. The reception staff shall make a copy of the responsible applicant's own photo-ID.

- Video conference

  The reception staff and the responsible applicant shall obey the manual, "Procedure for remote ID vetting using a live view of video conference system".The reception staff shall take a snapshot containing the face of the responsible applicant and the applicant's own photo-ID during the video conference.

In either case, it is assumed that the responsible applicant has confirmed beforehand the identities of all project members via their photo-IDs. In a case where theresponsible applicant's own ID does not include the photo, it should be considered acceptable if the reception staff can confirm the identity of the responsible applicant via the other official document that includes the photo, in addition to the ID. In the same way, the copy of any member's ID that does not include the photo should be considered acceptable if the responsible applicant can confirm the member identity via the other official document that includes the photo, together with the ID.

(2) Authentication of host administrator and service administrator

"HPCI Cooperative Service Organizing and Working Group" identifies the host administrator and service administrator. The organization that requires a host certificate or service certificate applies to "HPCI Cooperative Service Organizing and Working Group" for registration of a host administrator or service administrator who is recognized within the applying organization. After confirming the application, "HPCI Cooperative Service Organizing and Working Group" approves the registration as a host administrator or service administrator, and registers the host administrator or service administrator on "Administrator list of the HPCI authentication infrastructure".
The HPCI CA authenticates the applicant according to the method of applying for issuance of the host certificate or service certificate.

(A) Online application

In the case of applying for issuance using the certificate issuing system, the applicant shall be authenticated with an HPCI account. In addition, the system authorizes the applicant to use the service by confirming the attribute of a host or service administrator.

(B) E-mail application

In the case of applying for issuance by e-mail, the HPCI CA checks the applicant information of the received e-mail with the "Administrator list of the HPCI authentication infrastructure" and confirms that they match.

The HPCI CA phones to "host certificate administrator phone number" registered in the "Administrator list of the HPCI authentication infrastructure" to authenticate the host administrator or service administrator.

3.2.4 Non-verified subscriber information

Information other than name and affiliation is not used for the screening.

3.2.5 Validation of authority

The HPCI-ID Management Organization confirms whether the user is eligible to use 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

This section describes the regulations for identification and authentication when a client certificate, a host certificate, and a service certificate is renewed or reissued.

3.3.1 Identification and authentication for routine re-key

The HPCI CA will confirm whether the certificate user has been approved by the HPCI-ID Management Organization to renew the certificate by checking to see that the user has a valid HPCI account.

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

- Not more than 5 years have passed since 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 is continued.

If the HPCI-ID Management Organization confirms that the above is not applicable, registration is carried out according to the procedures described in CP/CPS "3.2.2 Authentication of organization identity" and "3.2.3 Authentication of individual identity" of the CP/CPS.

3.3.2 Identification and authentication for re-key after revocation

Identification and authentication during key renewal after revocation will follow the registration procedure described in "3.2.2 Authentication of organization identity" and "3.2.3 Authentication of individual identity" of the CP/CPS.
In lieu of the above procedure, the user can log into the Certificate Issuing System via the HPCI account and enter the necessary information into the Certificate Issue application form.

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.
In lieu of the above procedure, the user can log into the Certificate Issuing System via the HPCI account and enter the necessary information into the Certificate Revocation application form.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

Operation requirements for client certificates, host certificates, and service certificates are stipulated below.

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 forms provided by the HPCI CA should be used for application for a host or service certificate.

4.1.1 Who can submit a certificate application

Certificate applications can be submitted to the HPCI-ID Management Organization by the applicant's supervisor, or host or service administrators.
Online certificate application from the HPCI CA can be carried out by the user, or host or service administrators.

4.1.2 Enrollment process and responsibilities

(1) Client certificates

Users must submit a copy of their photo-ID to their supervisor. The responsible supervisor will confirm the validity of the photo-ID and submit the document to the user reception desk of the HPCI-ID Management Organization. The supervisor must present accurate information to the HPCI-ID Management Organization.

(2) Host certificates and service certificates

Host administrators and service administrators must submit host and service name list to the user reception desk of the HPCI-ID Management Organization. Host 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

Screening by the HPCI Operating Office and the HPCI Account IdP Operating Organization is conducted according to CP/CPS "3.2.2 Authentication of organization

identity" and "3.2.3 Authentication of individual identity."
The HPCI CA will confirm that the certificate user has undergone screening and has been approved for certificate issuance by the HPCI-ID Management Organization.

4.2.2 Approval and rejection of certificate applications

Applications are accepted only after the HPCI-ID Management Organization has confirmed that there are no problems with the contents of the application submitted by the applicant's supervisor, host administrator, or service administrator.
When the HPCI CA confirms that there are no problems with the screening results reported by HPCI-ID Management Organization, it will accept the request for online certificate issuance from the certificate user.

4.2.3 Time to process certificate applications

(1) Client certificates

Application of the client certificates to the HPCI Issuing System is immediately processed.

(2) Host certificates and service certificates

Application of the host or service certificates to the HPCI CA is processed within 5 days (excluding statutory holidays) from the day after the HPCI CA accepts the application.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

(1) Client certificate

The user will use their HPCI account to access the certificate issuance system to enter information required for certificate issuance application. The information for user authentication is sent to the Certificate Management System from the Certificate Issuing System, and the corresponding key pair is created within the Certificate Management System. The Certificate Management System sends the certificate issuance application to the RA server. The RA server requests certificate issuance to the CA server, where the client certificate is created.
The client certificate issued by the HPCI CA 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 each server and then send CSR to the HPCI CA. After the HPCI CA receives the CSR, it will issue the host and service certificates after undertaking verification in accordance with "3.2.1 Method to prove possession of private key" of the CP/CPS.
Host and service certificates issued by the HPCI CA is sent online to the host and service administrators.

4.3.2 Notification to subscriber by the CA of issuance of certificate

(1) Client certificates

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 certificates and service certificates

The host or service certificate sent from the HPCI CA serves as notice of issuance to the host or service administrator.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

(1) Client certificates

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 certificates and service certificates

After receiving the host or service certificate, on-screen confirmation of the certificate content by the host or service administrator is regarded as proof of receipt.

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 certificate has expired.
- When a certificate is reissued after certificate revocation due to the compromise of the user private key, changes in the information contained in the certificate, and so on.

4.7.2 Who may request certification of a new public key

Applications for certificate renewal can be made to the HPCI-ID Management Organization by the applicant's supervisor or the host or service administrator.
Applying for an online certificate to the HPCI CA can be carried out by the user, or host or service administrators.

4.7.3 Processing certificate re-keying requests

(1) When the certificate has expired

The renewal of client certificates, host certificates, and service certificates are processed according to procedures described in "4.1 Certificate Application -- 4.4 Certificate acceptance" of the CP/CPS. Note that "4.2.1 Performing identification and authentication functions" follow procedures described in "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 described in "4.1 Certificate Application -- 4.4 Certificate acceptance" when applying for a reissuance after revocation.

4.7.4 Notification of new certificate issuance to subscriber

As described in "4.3.2 Notification to subscriber by the CA of issuance of certificate" of the CP/CPS.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

As described in "4.4.1 Conduct constituting certificate acceptance" of the CP/CPS.

4.7.6 Publication of the re-keyed certificate by the CA

As described in "4.4.2 Publication of the certificate by the CA" of the CP/CPS.

4.7.7 Notification of certificate issuance by the CA to other entities

As described in"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

The HPCI CA will revoke certificates under the following conditions:

(1) Revocation initiated by certificate user

- The certificate content is changed (e.g. change in the name) or the certificate users' affiliation organization is changed.
- The private key is compromised or suspected to be compromised.

(2) Revocation initiated by the HPCI-ID Management Organization

- The existence of the certificate user cannot be confirmed.

- Loss of qualification by user.

(3) Revocation initiated by the HPCI CA

- The certificate user violates the CP/CPS or user regulations.
- The private key stored in the Certificate Management System is leaked or suspected of being compromised.
- It is determined that the HPCI CA mistakenly issued a certificate.
- The HPCI CA decides that the certificate revocation is necessary; in this case, the HPCI CA must obtain the approval from the HPCI PMA.
- The CA private key in the HPCI CA is leaked or suspected of being compromised.
- The HPCI CA ceases authentication operations.

4.9.2 Who can request revocation

(1) When cause for revocation is due to the certificate user

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

(2) When cause for revocation is due to the HPCI-ID Management Organization

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

(3) When cause for revocation is due to the HPCI CA

Revocation is carried out at the discretion of the CA Security Officer or HPCI PMA.

4.9.3 Procedure for revocation request

(1) Revocation by certificate user

- Client certificates

If a cause for revocation arises, the user must complete the revocation application form and submit it to their supervisor as soon as possible. The supervisor must verify the user's identity and the reason for revocation, and submit the revocation 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 must perform a screening of the applicant's supervisor or the user

in accordance with "3.4 Identification and authentication for revocation request" of the CP/CPS.
The user reception desk sends the revocation application to the HPCI CA to request the revocation of the applicable certificate.
In lieu of the above procedure, the user can log into the Certificate Issuing System via the HPCI account and enter the necessary information into the Certificate Revocation application form.

- Host certificates and service certificates

If a cause for revocation arises, the host or service administrator must complete the revocation application and submit it to the user reception desk as soon as possible.
The user reception desk must perform a screening of the host or service administrator in accordance with "3.4 Identification and authentication for revocation request".
The user reception desk sends the revocation application to the HPCI CA to request the revocation of the applicable certificate.

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

When circumstances arise as described in CP/CPS "4.9.1 Circumstances for revocation" of the CP/CPS, the HPCI Operating Office sends the revocation application, or equivalent content in either paper or digital form to the HPCI CA to request the revocation of the applicable certificate.

(3) Procedure for revocation by the HPCI CA

When circumstances arise as described in CP/CPS "4.9.1 Circumstances for revocation" of the CP/CPS, the applicable certificate will be revoked at the discretion of the CA Security Officer or HPCI PMA.

After the revocation process, the HPCI CA will notify the certificate user regarding the completion of the process. If necessary, the HPCI-ID Management Organization will also be notified of the completion of the revocation process.

4.9.4 Revocation request grace period

If a cause for revocation arises, 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 decide promptly on the validity of the revocation request. When the revocation is approved, the HPCI CA will promptly proceed with the revocation within a day not counting statutory holidays.

4.9.6 Revocation checking requirement for relying parties

Relying parties confirm the validity of certificates by obtaining the latest CRL published in the CA Repository or checking the OCSP responder.

4.9.7 CRL issuance frequency

The HPCI CA issues a CRL with every revocation and also periodically. The valid term of the CRL is 30 days and a new CRL is issued at the latest 7 days before expiration.
During normal operation, CRLs are issued every 24 hours.

4.9.8 Maximum latency for CRLs

After the CA issues a CRL, it is published in the CA Repository within 12 hours.

4.9.9 On-line revocation/status checking availability

The HPCI CA provides certificate validity information via OCSP. It does not handle queries regarding the validity of expired certificates.

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 provides certificate revocation information by publishing a CRL and OCSP responder in the CA Repository.

4.10.2 Service availability

Service usage time is as described in "2.3 Time or frequency of publication" of the CP/CPS.

4.10.3 Optional features

No stipulation.

4.11 End of subscription

Certificate users can withdraw from the service by following the steps described in "4.9.3 Procedure for revocation request" of the CP/CPS.

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 is setup in a place not easily subject to damage due to disasters such as flooding, earthquakes and fire. Safety measures are incorporated into the building structure to prevent unauthorized access and withstand earthquakes and fire.
The CA equipment etc., is 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 advance to receive authorization to enter the room containing the HPCI CA system. Every time the room is accessed, it is necessary for personnel with the authority to access the room to be identified and authenticated by authentication equipment. Entry and exit logs are recorded, managed, and checked periodically. If unauthorized individuals are to enter the room, they must be accompanied by personnel with proper authorization. Unauthorized individuals must state their purpose for entering the room. Authorized personnel must sign a log to indicate that they had accompanied the individual, and this record must be periodically reviewed. When exiting the machine room, confirm that the number of people leaving match the number of people who entered.
The CA system is housed in a dedicated, lockable rack in the machine room.

5.1.3 Power and air conditioning

Ensure sufficient power is supplied to the CA equipment through a dedicated power line connected to a distribution board.
The machine room is equipped with air-conditioning to maintain the proper operation of the CA system and provide an appropriate working environment for the personnel.

5.1.4 Water exposures

The machine room is located in an area with a low risk of water damage and equipped with a flood warning system.

5.1.5 Fire prevention and protection

The building hosting the HPCI CA is fireproofed, and equipped with fire alarm system and fire extinguishing equipment.

5.1.6 Media storage

Media is stored in a lockable storage cabinet in a room with appropriate entry control.

5.1.7 Waste disposal

When disposing of HPCI CA documents or storage media with important personal information pertaining to 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 does not offer offsite backups.

5.2 Procedural Controls

5.2.1 Trusted roles

The following describes 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 keys ● Identification of the host administrator of the servers related to the authentication infrastructure system operated by the National Institute of Informatics, and the confirmation of relationship to the FQDN
CA Operator	● Activation/Deactivation of CA private key ● Operation and maintenance of the CA system (CA server, RA server, and repository)

Log Manager	● Management of media containing backup data, logs and archives ● Management of physical keys for fire proof safes and cabinets ● Examination of system logs and reports (security audit) ● Management of physical keys for the dedicated rack for CA equipment
CA help desk	● Contact point for questions from the HPCI help desk regarding certificate usage

* The list of the HPCI CA personnel shall be updated once a year.

The following describes 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 identification of applicant's supervisor and the photo-IDs of applicant ● Confirmation of identification of host or service administrators, and their relationship to the FQDN ● Confirmation of user qualifications ● Storage of applications submitted by certificate users, screening results etc.
HPCI Operating Office	● Confirmation of the existence of certificate users' affiliated organization, and storage of the confirmation results ● Submission of revocation applications to the HPCI CA after loss of user qualification

* The list of the HPCI-ID management organization personnel shall be reviewed once a year.

5.2.2 Number of persons required per task

In accordance with "5.2.1 Trusted roles" of the CP/CPS, the required number of personnel is allocated for the following work from the perspective of authorization level and mutual

check and balance system.

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 (1)
Maintenance and management of CA system	CA Operator (1)
Management of physical keys 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 the system is operated by the CA Operator, the system identifies/authenticates that the operator has proper authority to operate the system.

5.2.4 Roles requiring separation of duties

Concurrent duties 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 screening, staff reshuffling, etc., for the HPCI CA operation staff are carried out in accordance with the 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 equipment in order to operate the HPCI CA is provided. The history of education and training provided is stored.

5.3.4 Retraining frequency and requirements

Staff will receive education and training in response to 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 staff violate the policy or procedures stipulated or other procedures of the HPCI CA, appropriate penalties are applied, regardless of whether the violation was or was not intentional.

5.3.7 Independent contractor requirements

No stipulation.

5.3.8 Documentation supplied to personnel

The staff is provided with CP/CPS-based, operations and other related manuals that are necessary in order to operate the HPCI CA in a way that is appropriate to their roles.

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 CA, RA, and operation procedures.

5.4.1 Type of events recorded

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

- CA log

CA server access log
Certificate issue/revocation log and CRL issue log
Error log

- RA log

RA server 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

The log administrator will verify of the audit log based on instructions from the CA Security Officer.

5.4.3 Retention period for audit log

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

5.4.4 Protection of audit log

Access to the CA, RA and HSM logs are controlled by the OS function.
Audit logs are kept in a cabinet within a room with proper access control to prevent unauthorized browsing or tampering.

5.4.5 Audit log backup procedures

The CA Operator periodically obtains various types of logs recorded in the CA, etc., and stores them in 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 data below is archived All versions of documents including revision history is stored.

(Storage in the HPCI CA)

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

(Stored in the HPCI-ID Management Organization)

- Applications received from certificate users, copies of photo-IDs along with screening results, the snapshots taken during a video conference for remote identity vetting, etc.
- Operation assessment records (checklists)

5.5.2 Retention period for archive

Audit logs are 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 screening results, etc. from certificate subscribers stored at the HPCI-ID management organization shall be stored until one of the following conditions is satisfied.

(a) The HPCI account has been expired and one year has passed from the start date of the research project that started last.
(b) When five years have passed since the previous face-to-face identity verification, face-to-face identity verification will be performed again.
(c) Six years have passed since the identity verification was completed.

Other archive data is stored for 3 years.

5.5.3 Protection of archive

As described in "5.4.4 Protection of audit log" of the CP/CPS.

5.5.4 Archive backup procedures

As described in "5.4.5 Audit log backup procedures" of the CP/CPS.

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

A new CA private key is created before the time at which the expiration period for the CA private key is shorter than the expiration period for the user certificate. After the new private key is created, it is used to issue certificates and CRL. The old private key will only be used to issue CRLs and not certificates.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

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

- If an HSM is stolen or the CA private key compromised, work will be halted after all concerned personnel are notified.

- If the CA private key is compromised, the key is used to revoke all certificates, including CA certificates according to defined procedures to ensure that trusted HPCI CA systems cannot be operated.
- As soon as safety of the HPCI CA is confirmed, a new HPCI CA key pair is generated and the system reconfigured.

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

If hardware, software and data become damaged or destroyed, it is restored from backup hardware, software and data as soon as possible. In particular, assuming that the HSM device has been damaged or destroyed, training of the recovery procedure from the HSM backup must be performed once a year.

5.7.3 Entity private key compromise procedures

When a user private key has been compromised or compromise is suspected, 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 HPCI 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 compromise has not occurred, the operation can be resumed in accordance to "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 notifies all concerned parties in advance and carries 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 is generated in the HSM by the CA Security Officer and the CA Operator.

(2) User key

A certificate user key pair is generated within the Certificate Management System during online certificate issuing.
Host and service key pairs are generated by host or service administrators of 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 in the Certificate Management System, and not distributed to users.

- When client certificates are downloaded by users

User private keys are downloaded in the PKCS#12 format by users through the Certificate Management System when client certificates are downloaded.

(2) Host and service private keys

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

6.1.3 Public key delivery to certificate issuer

User public keys are generated within the Certificate Management System and sent 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 or service administrators and sent as CSRs to the HPCI CA.

6.1.4 CA public key delivery to relying parties

The CA certificate is published in the CA Repository and distributed.

6.1.5 Key sizes

The algorithm and key length of the generated keys 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
	OCSP responder certificate	RSA 2048bit

* RSA 2048bit key strength is equivalent to 112-bit security.

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 are configured in the following extensions of X.509 v3:

Table 6-2 Purpose of Key Use

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

6.2 Private Key Protection and Cryptographic Module Engineering Controls

This section stipulates the regulation regarding CA private keys 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 in the Certificate Management System

User private keys are encrypted and stored in the Certificate Management System. Access to the Certificate Management System within the machine room is restricted to authorized managers or servers.

- When client certificates are downloaded by users

Users will download private keys in the PKCS#12 format 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 keys are conducted by the CA Security Officer and the CA Operator.

6.2.3 Private key escrow

The HPCI CA does not perform escrow of private keys.

6.2.4 Private key backup

(1) CA private keys

Backup of CA private keys is carried out by the CA Security Officer and the CA Operator. The backed up CA private key is maintained in an HSM token and stored in a fireproof safe. The HSM physical keys and PINs (passwords) of private keys needed for operation must not be stored in the same place as where they are managed with the same key. The PINs must be kept on an offline medium.

(2) User private key

- When client certificates are stored only in the Certificate Management System

System backup is carried out by the manager of the Certificate Management System. The backup media is stored in a lockable safe box in a room with appropriate access control.

- When client certificates are downloaded by users

The user is responsible for backing up the certificates they download, 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 is not transferred.

(2) User private key

- When client certificates are stored only in the Certificate Management System

User private keys are generated and controlled within the Certificate Management System, and not transferred.

- When client certificates are downloaded by users

User private keys are downloaded in the PKCS#12 format.

6.2.7 Private key storage on cryptographic module

(1) CA private key

Registration to the HSM cryptographic module is 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 is required.

(2) User private key

- When client certificates are stored only in the Certificate Management System

Registration to the cryptographic module in the Certificate Management System is carried out when a key is generated during the online certificate issue procedures by the user. A password 12 characters or more is necessary for authentication.

- When client certificates are downloaded by users

After certificates are downloaded, each private key is registered to the cryptographic

module within the user terminal.

6.2.8 Method of activating private key

(1) CA private key

CA private keys are activated by two CA Operators within an HSM.

(2) User private key

- When client certificates are stored only in the Certificate Management System

Activation is carried out within the Certificate Management System during authentication for use of resources. Authentication with a password, which is 12 characters or more, is required for activating private keys.

- When client certificates are downloaded by users

Each key is activated within the user terminal when authenticating for resource use. Authentication with a password, which is 12 characters or more, is required for activating private keys.

6.2.9 Method of deactivating private key

(1) CA private key

CA private keys are deactivated by two CA Operators within an HSM.

(2) User private key

User private keys are deactivated with protection by password of 12 or more characters etc., except when authenticating to use resources.

6.2.10 Method of destroying private key

(1) CA private key

CA private keys within an HSM are destroyed through the initialization of 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 certificates are stored only in the Certificate Management System

Destruction of user private keys in the Certificate Management System or backup media is carried out 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 are responsible for destroying downloaded certificates and backup media.

6.2.11 Cryptographic Module Rating

HSM containing CA private keys must 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 is as stipulated in "5.5.2 Retention period for archive" of the CP/CPS.

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

Type	Expiration date
Client certificate	395 days after the certificate issued
Host certificate	April 24 of each year
Service certificate	April 24 of each year
OCSP responder certificate	April 24 of each year

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

6.4 Activation data

6.4.1 Activation data generation and installation

(1) CA private key

The CA private key is activated using both a password and an HSM physical key. The password must consist of at least 15 characters decided by the CA Operator and entered

into HSM.

(2) User private key

User private key activation data is a password consisting of 12 characters or more entered by the user during online certificate issue procedures. This password is set as the user access password to the private key.

6.4.2 Activation data protection

(1) CA private key

The CA Operator uses and modifies CA private key activation data in accordance with established regulations. The HSM physical key is kept by the CA Security Officer in a locked cabinet.

(2) User private key

The user is responsible for storing the activation data entered by the user.

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 prevents unauthorized access from outside networks using a firewall. Connection between CA and RA servers, and between the RA and the Certificate Management System is restricted to the designated communication port, and security measures are taken to prevent unauthorized access. The communication route between the CA server and the RA server, and the RA and the Certificate Management System are encrypted. The cipher strength is 112-bit security or higher.

6.8 Time-stamping

A time server is used to accurately synchronize the time and date recorded onto for certificates, logs and other documents issued by HPCI CA.

7. CERTIFICATE AND CRL PROFILES

The certificate and CRL profile is based on RFC5280 and RFC6818 and follows the separately set certificate and CRL profile design specifications. The attributes pertinent to OCSP are based on RFC6960.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

The 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

Internal audits of the HPCI CA is performed by the HPCI CA personnel. Internal assessments of the HPCI-ID Management Organization are performed by its personnel.

External audits are performed by governmental organizations or academic institutions with the appropriate jurisdiction.
When an external audit is performed, the auditee, the HPCI CA, shall present audit logs in response to a request from a governmental organization or an academic institution, the auditor.

If other trusted CAs or relying parties request an external assessment, the costs will be incurred 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

Audits are mainly focused on whether authentication operations of the HPCI CA are in compliance with the CP/CPS and other operation procedure documents.

8.5 Actions taken as a result of deficiency

The HPCI PMA quickly examines corrective measures for matters pointed out by the audit and decides on a course of action. After deciding on the course of action, a plan is presented to the auditor and the situation is monitored until the HPCI CA completes the measures.

8.6 Communication of results

All operation members of the HPCI PMA and HPCI CA are informed of the audit results. The HPCI PMA considers whether or not to disclose the audit results to other concerned parties.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

Fees are 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 are stipulated in the following regulations of the Research Organization of Information and Systems:

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 in "2.2 Publication of certification information" of the CP/CPS, all pertinent information is confidential. Confidential information must not be disclosed or leaked to any third party or used beyond the defined scope of use. Information deemed confidential is safely stored under the administration of a designated person in charge of this and other documents and storage medium.

9.3.2 Information not within the scope of confidential information

Information included in "2.2 Publication of certification information" is not deemed confidential.
In the case of a revoked client certificate, the reason for revocation is also published in the CRL. The date and reason for revocation contained in the CRL is not deemed confidential information. Other information concerning revocation is not disclosed to the public.

9.4 Privacy of personal information

The HPCI CA does 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 can be disclosed after confirming the user's identity face-to-face:

- Application to issue a certificate submitted to the HPCI CA or the HPCI-ID

Management Organization
- Certificate contents
- Certificate status

Apart from the above, regulations regarding handling of personal information stipulated by the Research Organization of Information and Systems are contained in the following:

- Research Organization of Information and Systems Personal Information Protection Regulations (in Japanese)
  http://www.rois.ac.jp/pdf/kojinkitei.pdf

- Research Organization of Information and Systems Information Disclosure:
  http://www.rois.ac.jp/en/open/

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 is responsible for the following CA operations:
- Issuing and revoking certificates based on the CP/CPS.
- Registering and publishing the issued CA certificate information, CRL and OCSP responder in the CA Repository, excluding at times of temporary suspension or emergency suspension due to system maintenance.
- Specifying applicable CP/CPS when certificates are issued.
- Performing authentication operations in accordance with the CP/CPS, and taking responsibility for the credibility of certificates and 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 (due to discovery of an attack method, etc.), or the signature algorithm becomes obsolete.
- Performing appropriate authentication operations in accordance with CP/CPS to ensure the HPCI CA private key is not compromised due to theft and/or loss.
- Approving cooperative applications from the HPCI-ID Management Organization.
- Delegating the work related to the identification and authentication of certificate users and/or organizations to the HPCI-ID Management Organization. When the

HPCI CA delegates to the HPCI-ID Management Organization, the HPCI CA selects an organization that guarantees all requirements of the following identity verification procedures as HPCI-ID Management Organization:

(1) Identity verification shall be based on a photo-ID.

(2)Identity verification shall be based on a face-to-face meeting or a video conference.

- Verifying periodically whether the HPCI-ID Management Organization meet the above requirements.
- Encrypting all communication with the HPCI-ID Management Organization and the Certificate Management System to ensure safe and reliable transmission.

9.6.2 RA representations and warranties

The following are the duties and responsibilities of the HPCI-ID Management Organization:

- Accepting applications and identifying and authenticating certificate users and organizations when processing applications for certificate issuance, renewal and revocation in accordance with the CP/CPS.
- Enabling rapid detection of changes in certificate user names or loss of user qualification, and upon detection, applying to the HPCI CA for certificate revocation.
- Working in coordination with the Certificate Issuing System to send user certificate information (HPCI-ID, Alphabet name) safely to the HPCI CA.
- Working in coordination with the Certificate Management System to notify the user of the completion of issuance of their certificate.
- Safely storing certificate user information obtained during the application process for a period stipulated in the CP/CPS.
- Performing regular internal assessments and reporting results to the HPCI PMA to ensure compliance to HPCI CA operation requirements.
- Identity assertions made by the HPCI-ID Management Organization to any system must be conducted via an encrypted network.

9.6.3 Subscriber representations and warranties

The following are the duties and responsibilities of certificate users:

- Presenting accurate information when applying for certificate issuance or revocation to the HPCI-ID Management Organization and HPCI CA.
- Acquiring certificates using procedures provided by the HPCI CA.
- Not using certificates for purposes other than those stipulated in the CP/CPS, and not

using expired certificates.

- Client certificates must not be shared.
- Assumes responsibility for the safe management of activation passwords of private keys.
- Assumes responsibility for the management of private keys so as to prevent the compromising of keys and certificates due to theft or loss.
- Applying for revocation within one working day in the event the private key is stolen, lost (when the private key is compromised or is suspected of being compromised), or the usage of the certificate is terminated.
- Host administrators and service administrators must associate the host/service certificate to one network entity.
- If a user uses a client certificate, host certificate, or service certificate signed by the HPCI Certificate Authority, the user must comply with this CP / CPS.

9.6.4 Relying party representations and warranties

The following are the duties and responsibilities of certificate relying parties:

- Relying Parties must understand and agree with the CP/CPS in the CA Repository of the HPCI CA.
- Certificates should not be used for purposes other than what is stipulated in "4.5.2 Relying party public key and certificate usage" of the CP/CPS.
- Confirming 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 strictly observes the content of the CP/CPS and sees to it that the HPCI CA is operated in accordance with the CP/CPS. However, the HPCI CA assumes no responsibility for damages that may result.

The HPCI CA provides certificate users and/or relying parties with the necessary information contained in the CP/CPS, and recommends the content to be strictly observed, but does not guarantee to other concerned parties that certificate users and/or relying parties will strictly observe the content 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 assumes 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 must 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 becomes invalid immediately following the termination of HPCI CA operations.

9.11 Individual notices and communications with participants

No stipulation.

9.12 Amendments

9.12.1 Procedures for amendment

The HPCI CA modifies the CP/CPS as needed.
Modified content is decided on and approved by the HPCI PMA.
The major version No. of the modified CP/CPS is 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 is modified at the discretion of the CA Security Officer, and the minor version No. is updated and a new OID provided.

9.12.2 Notification mechanism and period

When the CP/CPS is modified, it is published in the CA Repository without delay. Publishing in the CA Repository will serve as notice to certificate users and relying parties.

9.12.3 Circumstances under which OID must be changed

OID is 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 is settled in accordance with Japanese laws.

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 in a separate section in the CP/CPS.

9.16.2 Assignment

Rights and/or obligations stipulated in the CP/CPS 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 is interpreted to correspond most closely to the purpose intended by the HPCI CA.

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 assume no responsibility to certificate users or relying parties in the event of the following:

(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.