JPRS CA Certification Practice Statement Version 1.12

April 01, 2022

Japan Registry Services Co., Ltd.

Version History		
Version Number	Date	**Description**
1.00	2019.06.17	Publication of the first version
1.10	2020.04.01	Revision due to Mozilla Root Store Policy (v2.7)
1.11	2021.04.01	Revision of the date and version
1.12	2022.04.01	Revision of the date and version

*Note
This "JPRS CA Certification Practice Statement" of Japan Registry Services Co., Ltd. (hereinafter referred to as the "JPRS") is an unofficial translation provided as reference, and only the Japanese texts of the statement have legal effect. Please kindly note that JPRS does not guarantee the accuracy of this English translation in comparison to the original statement in the Japanese language. JPRS may provide the revised English translation with the date of revision for the same version of "JPRS CA Certification Practice Statement." If the new version of "JPRS CA Certification Practice Statement" is published, please stop referencing/using this document.

Table of Contents

1. Introduction

1.1 Overview

This document, the JPRS CA Certification Practice Statement (hereinafter referred to as "this CPS"), stipulates policies regarding the operation of a Certification Authority (hereinafter referred to as the "CA") established by Japan Registry Services Co., Ltd. (hereinafter referred to as "JPRS") for the purpose of providing the JPRS Digital Certificate Issuance Services.

The CA conforms to the "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" (hereinafter referred to as the "Baseline Requirements") published by CA/Browser Forum at https://www.cabforum.org/. Various rules regarding the types, usages, operation, and others of certificates to be issued by the CA are stipulated in the JPRS CA Certificate Policy (hereinafter referred to as the "CP").
If any inconsistency is found among the provisions of this CPS, the Terms and Conditions, and the CP, the provisions of the Terms and Conditions shall prevail over those of the CP and this CPS, and the provisions of the CP shall prevail over those of this CPS.

This CPS conforms to the RFC 3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" advocated by the IETF as a framework for the operation of Certification Authorities.

With any developments or improvements pertaining to the certification operations in terms of technologies or services, this CPS shall be revised, as needed, in order to reflect such developments or improvements.

1.2 Document Name and Identification

The official name of this CPS is the "JPRS CA Certification Practice Statement." Following are an Object Identifier (hereinafter referred to as "OID") assigned by the CA under this CPS, and an OID of the CP referenced by this CPS:

Name	OID
JPRS CA Certification Practice Statement (CPS)	1.3.6.1.4.1.53827.1.2.4
JPRS CA Certificate Policy (CP)	1.3.6.1.4.1.53827.1.1.4

1.3 PKI Participants

1.3.1 CA

"CA" stands for "Certification Authority," an entity that mainly issues and revokes certificates, discloses revocation information, provides and stores information on the certificate status using the OCSP (Online Certificate Status Protocol) server, generates and protects the CA's own Private Keys, and registers Subscribers.

1.3.2 RA

"RA" stands for "Registration Authority," an entity that mainly performs reviews to verify the existence and validate the identities of applicants who apply for the issuance or revocation of certificates, registers information necessary for issuing certificates, and requests the CA to issue certificates, among the operations of the CA. The CA acts as an RA.

1.3.3 Subscriber

"Subscriber" means an individual, corporation or organization that has been issued a certificate by the CA and uses the certificate.

1.3.4 Relying Parties

A "Relying Party" means an individual, corporation, or organization that verifies the validity of certificates issued by the CA.

1.3.5 Other Participants

No stipulation.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

Stipulated in the CP.

1.4.2 Prohibited Certificate Uses

Stipulated in the CP.

1.5 Policy Administration

1.5.1 Organization Administering the Document

This CPS shall be maintained and administered by the CA.

1.5.2 Contact Information

Inquiries concerning this CPS should be directed to:

Contact: Inquiries contact office, Japan Registry Services Co., Ltd.
Address: Chiyoda First Bldg. East 13F, 3-8-1 Nishi-Kanda, Chiyoda-ku, Tokyo 101-0065 JAPAN
E-mail: info@jprs.jp

If a compromise or unauthorized use of any Private Key or any other trouble pertaining to a server certificate issued by the CA is revealed, please notify the following party:
Dedicated contact, https://jprs.jp/pubcert/f_mail/

1.5.3 Person Determining CPS Suitability as Policy

The details of this CPS shall be determined by the CA's Certificate Operation Conference.

1.5.4 Approval Procedures

This CPS shall come into effect upon approval of the CA's Certificate Operation Conference.

1.6 Definitions and Acronyms

(1) "あ" ～ "ん"

アーカイブ（Archive)

"Archive" means information acquired for the purpose of keeping a history for any legal or other reason.

エスクロー（Escrow)

"Escrow" means the placement (entrustment) of an asset in the control of an independent third party.

鍵ペア（Key Pair)

A "Key Pair" means a pair consisting of a Private Key and Public Key in a public key cryptosystem.

監査ログ（Audit Log)

An "Audit Log" is a log of actions, accesses, and other histories pertaining to Certification Authority systems that are recorded for the purpose of monitoring accesses to, and unauthorized operations of, Certification Authority systems.

公開鍵（Public Key)

A "Public Key" means a key of a Key Pair used in a public key cryptosystem. A Public

Key corresponds to a certain Private Key and is disclosed to the other party to communication.

私有鍵（Private Key）

A “Private Key” means a key of a Key Pair used in a public key cryptosystem. A Private Key corresponds to a certain Public Key and is possessed only by the person in question. A Private Key may be referred to as a “secret key.”

指定事業者（JPRS Partners）

“JPRS Partners” mean business enterprises authorized by JPRS in connection with the Digital Certificate Issuance Services to be provided by JPRS.

タイムスタンプ（Time Stamp）

“Time Stamp” means recorded data indicating dates and times when, for example, electronic files have been prepared and a system has performed processing.

電子証明書（Digital Certificates）

A “Digital Certificate” means digital data certifying that a Public Key is possessed by the party specified in the data. The validity of a Digital Certificate is assured by a digital signature of the relevant CA affixed to the Digital Certificate.

リポジトリ（Repository）

The “Repository” means the database in which CA certificates, CRLs, and others are stored and published.

(2) “A” ～ “Z”

CA (Certification Authority)

“CA” stands for “Certification Authority,” an entity that mainly issues, renews, and revokes certificates, discloses information on certificate revocation, provides and stores information on the status of certificates using the OCSP (Online Certificate Status Protocol) server, generates and protects the CA’s own Private Keys, and registers Subscribers.

CAA (Certificate Authority Authorization)

“CAA” stands for “Certificate Authority Authorization,” a function to prevent unintended erroneous issuance of certificates from unauthorized Certification

Authorities in connection with the authority to use a domain by adding information to the DNS record in order to specify the Certification Authority authorized to issue a certificate for the domain. This function is stipulated in RFC 6844.

CP (Certificate Policy)

"CP" stands for "Certificate Policy," a document that sets forth policies regarding certificates to be issued by the CA, such as the types of certificates, the servers for which certificates may be issued, the usages of certificates, procedures for applying for the issuance of certificates, and the criteria for such issuance.

CPS (Certification Practices Statement)

A "CPS" stands for "Certification Practice Statement," a document that sets forth provisions to be followed in operating the CA, such as various operational procedures and security standards.

CRL (Certificate Revocation List)

"CRL" stands for "Certificate Revocation List," a list of information about certificates revoked during their period of validity for any reason, including changes in the particulars described in the certificates or the compromise of any Private Keys.

CT (Certificate Transparency)

"CT" stands for "Certificate Transparency," a scheme stipulated in RFC 6962 to register and publish information about certificates on a log server (CT log server) for the purpose of monitoring and auditing information about issued certificates.

FIPS 140-2

"FIPS 140-2" are a set of security accreditation criteria for cryptographic modules developed by the United States NIST (National Institute of Standards and Technology). Four levels, from Level 1 (the lowest) to Level 4 (the highest), have been defined.

HSM (Hardware Security Module)

"HSM" stands for "Hardware Security Module," a tamper-resistant encryption device to be used for generating, storing, using, or otherwise handling Private Keys for the purpose of maintaining security.

NTP (Network Time Protocol)

"NTP" stands for "Network Time Protocol," a protocol designed to synchronize the internal clocks of computers over a network.

OID (Object Identifier)

"OIDs" stands for "Object Identifiers," numerals registered in international registration institutions as unique IDs among global networks, within a framework for maintaining and administering the connectivity of networks and the uniqueness of services or the like.

OCSP (Online Certificate Status Protocol)

"OCSP" stands for "Online Certificate Status Protocol," a protocol for providing information on the status of a certificate in real time.

PKI (Public Key Infrastructure)

"PKI" stands for "Public Key Infrastructure," an infrastructure for using the encryption technology known as a public key cryptosystem to realize security technologies such as digital signatures, encryption, and certification.

RA (Registration Authority)

"RA" stands for "Registration Authority," an entity that mainly performs reviews to verify the existence and validate the identities of applicants who apply for the issuance or revocation of certificates, registers information necessary for issuing certificates, and requests the CA to issue certificates, among the operations of the CA.

RFC 3647 (Request for Comments 3647)

"RFC 3647" stands for "Request for Comments 3647," a document defining the framework for CP and CPS published by the IETF (Internet Engineering Task Force), an industry group that establishes technical standards for the Internet.

RFC 5280 (Request for Comments 5280)

"RFC 5280" stands for "Request for Comments 5280," a document defining the public key infrastructure published by the IETF (Internet Engineering Task Force), an industry group that establishes technical standards for the Internet.

RSA

"RSA" is one of the most standard encryption technologies. RSA is widely used as a

public key cryptosystem.

SHA-1 (Secure Hash Algorithm 1)

"SHA-1" stands for "Secure Hash Algorithm 1," one of the hash functions (summarization functions) used in digital signing. A hash function is a computation technique for generating a fixed-length bit string from a given text. The bit length is one hundred sixty (160) bits. The algorithm works to detect any alterations in an original message during its transmission by comparing the hash values transmitted and received.

SHA-256 (Secure Hash Algorithm 256)

"SHA-256" stands for "Secure Hash Algorithm 256," one of the hash functions (summarization functions) used in digital signing. The bit length is two hundred fifty-six (256) bits. The algorithm works to detect any alterations in an original message during its transmission by comparing the hash values transmitted and received.

2. Publication and Responsibilities for Repository

2.1 Repository

The CA shall maintain and manage the Repository to allow access to the same twenty-four (24) hours a day, three hundred sixty-five (365) days a year. Note, however, that the Repository may be temporarily unavailable at times for system maintenance or other reasons.

2.2 Publication of Information

The CA shall publish the CRLs, this CPS, and the CP on the Repository to allow online access by Subscribers and Relying Parties.

2.3 Time or Frequency of Publication

This CPS shall be published on the Repository as revised.

2.4 Access Controls on Repositories

Stipulated in the CP.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

Stipulated in the CP.

3.1.2 Need for Names to Be Meaningful

Stipulated in the CP.

3.1.3 Anonymity or Pseudonymity of Subscribers

Stipulated in the CP.

3.1.4 Rules for Interpreting Various Name Forms

Stipulated in the CP.

3.1.5 Uniqueness of Names

Stipulated in the CP.

3.1.6 Recognition, Authentication, and Roles of Trademarks

Stipulated in the CP.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of a Private Key

Stipulated in the CP.

3.2.2 Authentication of Organization and Domain Identity

Stipulated in the CP.

3.2.3 Authentication of Individual Identity

Stipulated in the CP.

3.2.4 Non-Verified Subscriber Information

Stipulated in the CP.

3.2.5 Validation of Authority

Stipulated in the CP.

3.2.6 Criteria for Interoperation

Stipulated in the CP.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

Stipulated in the CP.

3.3.2 Identification and Authentication for Re-key after Revocation

Stipulated in the CP.

3.4 Identification and Authentication for Revocation Request

Stipulated in the CP.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Stipulated in the CP.

4.1.2 Enrollment Process and Responsibilities

Stipulated in the CP.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Stipulated in the CP.

4.2.2 Approval or Rejection of a Certificate Application

Stipulated in the CP.

4.2.3 Time to Process Certificate Application

Stipulated in the CP.

4.2.4 Check of CAA Records

Stipulated in the CP.

4.3 Certificate Issuance

4.3.1 CA Actiond during Certificate Issuance

Stipulated in the CP.

4.3.2 Notification to Subscriber of Certificate Issuanc

Stipulated in the CP.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Stipulated in the CP.

4.4.2 Publication of the Certificates by the CA

Stipulated in the CP.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Stipulated in the CP.

4.5 Key Pair and Certificate Usage

4.5.1 Use of a Private Key and Certificate by a Subscriber

Stipulated in the CP.

4.5.2 Relying Party Public Key and Certificate Usage

Stipulated in the CP.

4.6 Certificate Renewal

4.6.1 Circumstances for Certificate Renewal

Stipulated in the CP.

4.6.2 Who May Request Renewal

Stipulated in the CP.

4.6.3 Processing Certificate Renewal Requests

Stipulated in the CP.

4.6.4 Notification of New Certificate Issuance to Subscriber

Stipulated in the CP.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Stipulated in the CP.

4.6.6 Publication of the Renewal Certificate by the CA

Stipulated in the CP.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Stipulated in the CP.

4.7 Certificate Re-key

4.7.1 Circumstances for Certificate Re-key

Stipulated in the CP.

4.7.2 Who May Request Certification of a New Public Key

Stipulated in the CP.

4.7.3 Processing Certificate Re-keying Requests

Stipulated in the CP.

4.7.4 Notification of New Certificate Issuance to Subscriber

Stipulated in the CP.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

Stipulated in the CP.

4.7.6 Publication of the Re-keyed Certificates by the CA

Stipulated in the CP.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Stipulated in the CP.

4.8 Certificate Modification

4.8.1 Circumstances for Certificate Modification

Stipulated in the CP.

4.8.2 Who May Request Certificate Modification

Stipulated in the CP.

4.8.3 Processing Certificate Modification Requests

Stipulated in the CP.

4.8.4 Notification of New Certificate Issuance to Subscriber

Stipulated in the CP.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Stipulated in the CP.

4.8.6 Publication of the Modified Certificate by the CA

Stipulated in the CP.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Stipulated in the CP.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Certificate Revocation

Stipulated in the CP.

4.9.2 Who Can Request Revocation

Stipulated in the CP.

4.9.3 Procedures for Revocation Request

Stipulated in the CP.

4.9.4 Revocation Request Grace Period

Stipulated in the CP.

4.9.5 Time within Which the CA Shall Process the Revocation Request

Stipulated in the CP.

4.9.6 Revocation Checking Requirement for Relying Parties

Stipulated in the CP.

4.9.7 CRL Issuance Frequency

Stipulated in the CP.

4.9.8 Maximum Latency for CRLs

Stipulated in the CP.

4.9.9 On-line Revocation/Status Checking Availability

Stipulated in the CP.

4.9.10 On-line Revocation/Status Checking Requirements

Stipulated in the CP.

4.9.11 Other Forms of Revocation Advertisements Available

Stipulated in the CP.

4.9.12 Special Requirements Regarding Key Compromise

Stipulated in the CP.

4.9.13 Circumstances for Suspension

Stipulated in the CP.

4.9.14 Who Can Request Suspension

Stipulated in the CP.

4.9.15 Procedures for Suspension Request

Stipulated in the CP.

4.9.16 Limits on Suspension Period

Stipulated in the CP.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

Stipulated in the CP.

4.10.2 Service Availability

Stipulated in the CP.

4.10.3 Optional Features

Stipulated in the CP.

4.11 End of Subscription (Registration)

Stipulated in the CP.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

Stipulated in the CP.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Stipulated in the CP.

5. Facility, Management, and Operational Controls

5.1 Physical Security Controls

5.1.1 Site Location and Construction

JPRS shall install the CA's system within a secure data center. The data center will be located in place less vulnerable to damage from floods, earthquakes, fires, or any other disaster. Regarding the construction of the building, JPRS has taken measures to prevent and protect the said system against such disasters.

5.1.2 Physical Access

JPRS shall combine physical and electronic access controls to establish security controls of a level appropriate according to the importance of the CA's system. JPRS shall install surveillance cameras and various sensors to monitor access to the certification infrastructure system.

5.1.3 Power and Air Conditioning

JPRS shall secure a stable power supply for the data center by installing an uninterruptible power supply system and independent power generator to ensure that the CA may operate its system even during sudden interruptions in the power supply or during long-lasting power outages.
Further, JPRS shall install the CA's system in an environment where the optimum temperature and humidity may be constantly maintained using air conditioners.

5.1.4 Water Exposures

In the building where the CA's system is installed, JPRS shall locate the system on the second floor or above to prevent flood damage. Further, JPRS shall deploy water leakage detectors in the rooms where the CA's system is installed as a measure for leakage control.

5.1.5 Fire Prevention and Protection

The rooms where the CA's system is installed shall be structured with fireproof compartments partitioned off by firewalls and equipped with fire alarms and fire-extinguishing equipment.

5.1.6 Media Storage

The CA shall store information necessary for performing certification operations, including archival and backup data, in a depository within a room secured by an

appropriate level of entry-exit controls, and shall also take measures to prevent any damage to or loss of such information.

5.1.7 Waste Disposal

The CA shall dispose of documents and electronic media containing confidential information by initializing the media on which the information is stored, by shredding paper documents, and by other appropriate means.

5.1.8 Off-Site Backup

The CA shall store data, equipment, and other materials and facilities necessary for operating the CA's system at a remote site, or otherwise take available means to protect the same.

5.2 Procedural Controls

5.2.1 Trusted Roles

The roles of the personnel involved in the operation of the CA's system shall be as follows:

(1) Service Manager
- Supervise the whole CA.
- Appoint a Service Administrator.

(2) Service Administrator
- Appoint a CA Operation Manager and an RA Operation Manager.

(3) CA Operation Manager
- Supervise operations as the CA.
- Approve alterations in the CA's system or operational procedures.

(4) CA Operation Administrator(s)
- Give work instructions to the Person or Persons in Charge of CA Operations.
- Stand by during work related to the CA's Private Keys.
- Generally manage operations as the CA.

(5) Person(s) in Charge of CA Operations
- Maintain and manage the components of the CA's system, such as the CA server and Repository server.
- Activate and deactivate the CA's Private Keys, and otherwise handle the same.

(6) RA Operation Manger
- Supervise operations as the RA.

(7) RA Operation Administrator(s)
- Give work instructions to the Person or Persons in Charge of RA Operations.

・ Manage the performance of operations as the RA.

(8) Person(s) in Charge of RA Operations

・ Verify information in procedures for certificate applications.
・ Approve, refuse, and otherwise process applications for the issuance, revocation, and renewal of certificates.
・ Perform other review procedures for certificate issuance under the instructions of the RA Operation Administrator.

(9) Log Inspector(s)

・ Inspect logs of entries and exits to and from rooms, system logs, and the like.

5.2.2 Number of Persons Required per Task

The CA shall assign one (1) or more persons for each of the roles listed in "5.2.1 Trusted Roles" of this CPS, excluding the Service Manager, Service Administrator, CA Operation Manager, and RA Operation Manager. The CA shall have more than one (1) person perform important operations such as the handling of the CA's Private Keys.

5.2.3 Identification and Authentication for Trusted Roles

The CA shall identify and authenticate persons seeking to access the CA's system by physical or logical means, in order to confirm that they are authorized persons.

5.2.4 Roles Requiring Separation of Duties

The rules listed in "5.2.1 Trusted Roles" of this CPS shall be assumed by different persons, in principle. Notwithstanding the foregoing, the (a) CA Operation Administrator(s) and (a) RA Operation Administrator(s) may serve concurrently as (a) Log Inspector(s).

5.3 Personnel Controls

5.3.1 Qualification, Experience, and Clearance Requirements

Individuals assuming any of the roles listed in "5.2.1 Trusted Roles" of this CPS shall be employees and the like hired by JPRS under the hiring criteria prescribed by JPRS.
As persons in charge of the direct operation of the CA's system, individuals who have received specialized training and understand the general outline of the PKI and the methods of PKI system operation shall be assigned.

5.3.2 Background Check Procedures

The CA shall assess the reliability and aptitude of individuals assuming the respective roles listed in "5.2.1 Trusted Roles" of this CPS, at the time of their appointment and at regular intervals thereafter.

5.3.3 Training Requirements and Procedures

Individuals assuming the respective roles listed in “5.2.1 Trusted Roles” of this CPS shall receive training necessary for operating the CA’s system before undertaking their respective roles, and thereafter receive training and exercises according to their respective roles, as needed. In addition, if JPRS makes any change in operating procedures, the foregoing individuals shall receive training and exercises in connection with the change.

5.3.4 Retraining Frequency and Requirements

Individuals assuming the respective roles listed in "5.2.1 Trusted Roles" of this CPS shall receive refresher training as needed.

5.3.5 Job Rotation Frequency and Requirements

The CA shall rotate the jobs of the personnel, as needed to maintain and improve the quality of service and prevent misconduct.

5.3.6 Sanctions for Unauthorized Actions

JPRS shall impose a penalty for any unauthorized action of a relevant individual in accordance with JPRS's work rules.

5.3.7 Independent Contractor Controls

If JPRS outsources any part of the operations of the CA’s system to any external organization, JPRS shall confirm that the outsourced contractor is performing the operations appropriately pursuant to an agreement between JPRS and the outsourced contractor.

5.3.8 Documentation Supplied to Personnel

Each personnel member may only have access to the documents necessary for the performance of his/her duties.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

The CA shall collect the following records as Audit Logs:

(1) Logs related to the CA’s system

・handling of the CA’s Private Keys;

・startup and shutdown of the CA’s system;

・database operation;

・history of authority setting;

・history of the processing of the issuance and revocation of certificates; and
・history of the processing of the issuance of CRLs
(2) Logs related to entries and exits to and from rooms and to and from the network
・records of entries and exits to and from rooms where the CA's system is installed; and
・records of unauthorized accesses to the CA's system

An Audit Logs shall include the following items:
・date;
・time of day;
・event-causing subject; and
・description of the event

5.4.2 Frequency of Processing Audit Log

The CA shall check the Audit Logs at regular intervals.

5.4.3 Retention Period for Audit Log

The CA shall archive Audit Logs related to the CA's system for at least ten (10) years. Logs related to entries and exits to and from rooms and to and from the network shall be retained for at least one (1) year.

5.4.4 Protection of Audit Log

The CA shall adopt appropriate controls on access to Audit Logs so as to restrict access to authorized persons only and to make the Audit Logs unavailable to unauthorized persons.

5.4.5 Audit Logs Backup Procedure

The CA shall create a backup of Audit Logs on offline recording media and store the backup in a secure location.

5.4.6 Audit Log Collection System

A collection system for Audit Logs shall be included in the CA's system as a function of the system.

5.4.7 Notification to Event-causing Subject

The CA shall collect Audit Logs without notifying the person, system, or application that has caused the relevant event.

5.4.8 Vulnerability Assessments

The CA shall assess security vulnerabilities by clarifying the operation and system

behavior based on the inspection results of Audit Logs, review security measures, and then introduce the latest implementable security technologies and otherwise, as needed.

5.5 Records Archival

5.5.1 Types of Records Archived

The CA shall archive the following information in addition to logs related to the CA's system as prescribed in "5.4.1 Types of Events Recorded" of this CPS:

- issued certificates and CRLs;
- this CPS;
- documents prepared under this CPS stipulating the business operations of the Certification Authority;
- documents related to an outsourcing agreement, if any part of the certification operations is outsourced; and
- records and audit reports on the results of audits

5.5.2 Retention Period for Archive

The CA shall keep archives for at least ten (10) years.

5.5.3 Protection of Archive

The CA shall keep archives in access-restricted facilities to which unauthorized persons have no access.

5.5.4 Archive Backup Procedures

If important data concerning the CA's system is changed due to the issuance or revocation of certificates, the issuance of CRLs, or other events, the CA shall create a backup of the archived data in a timely manner.

5.5.5 Requirements for Time-Stamping of Records

The CA shall time synchronize the CA's system and put Time Stamps on important information recorded within the CA's system, by using the NTP (Network Time Protocol).

5.5.6 Archive Collection System

A collection system for Archives shall be included in the CA's system as a function thereof.

5.5.7 Procedures to Obtain and Verify Archive Information

Archives shall be available from a secure depository to persons authorized to access the same. The CA shall check the storage condition of the media at regular intervals and copy Archives to fresh media, for the purpose of maintaining the integrity and confidentiality of the Archives, as needed.

5.6 Key Changeover

Stipulated in the CP.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

The CA shall develop procedures for addressing incidents and compromises of the following types to enable the CA's system and related operations to recover if an incident or compromise occurs:

・compromises of the CA's Private Keys;

・damage to or failures in hardware, software, data, or the like; or

・fires, earthquakes, or other disasters

5.7.2 Recovery Procedures if Computing Resources, Software, and/or Data Are Corrupted

If any hardware, software, or data of the CA's system is damaged, the CA shall promptly undertake efforts to recover the CA's system using the relevant hardware, software, or data retained for backup.

5.7.3 Recovery Procedures After Key Compromise

If the CA determines that the CA's Private Key has been or may be compromised, or if there occurs any disaster or the like that may lead to a suspension or discontinuance of the operation of the CA's system, the CA shall resume the operation in a safe manner pursuant to predetermined plans and procedures.

5.7.4 Business Continuity Capabilities after a Disaster

The CA shall take measures in advance to restore the CA's system as rapidly as possible, so as to undertake recovery efforts promptly in a contingency, by procuring an alternative system to use in place of the CA's system, ensuring backup data for recovery, developing recovery procedures, and the like.

5.8 CA or RA Termination

Stipulated in the CP.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

This paragraph of this CPS stipulates policies on the management of the CA's keys. Policies on the management of the keys of Subscribers and other persons involved are stipulated in the CP.

6.1.1 Key Pair Generation

In generating Key Pairs of the CA, the CA shall use a hardware security module compliant with the FIPS 140-2 Level 3 standards (hereinafter referred to as "HSM"). In generating Key Pairs, the CA shall have two (2) or more authorized persons conduct the work.

6.1.2 Private Key Delivery to Subscriber

Stipulated in the CP.

6.1.3 Public Key Delivery to the Certificate Issuer

A Subscriber may deliver his/her/its Public Key to the CA online when applying for his/her/its certificate. Communication pathways for such delivery shall be encrypted by the TLS.

6.1.4 CA Public Key Delivery to Relying Parties

Stipulated in the CP.

6.1.5 Key Sizes

Stipulated in the CP.

6.1.6 Public Key Parameters Generation and Quality Checking

An HSM to be used in the CA's system shall be equipped with a feature to inspect the quality of the cryptographic functions. The parameters of Public Keys shall be generated using cryptographic functions that have been inspected for quality.

6.1.7 Key Usage Purposes

Stipulated in the CP.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The CA shall generate and store its Private Keys and conduct signing operations related

to its Private Keys using an HSM compliant with the FIPS 140-2 Level 3 standards.

6.2.2 Private Key Multi-Person Control

The CA shall have two (2) or more authorized persons activate, deactivate, back up and otherwise handle the CA's Private Keys in a secure environment.

6.2.3 Private Key Escrow

The CA does not Escrow its Private Keys.

6.2.4 Private Key Backup

The CA shall have two (2) or more authorized persons back up the CA's Private Keys. The backups shall be stored in an encrypted form in a secure room.

6.2.5 Private Key Archival

The CA does not archive its Private Keys.

6.2.6 Private Key Transfer into or from a Cryptographic Module

In transferring the CA's Private Keys to or from an HSM, the CA shall transfer the keys in an encrypted form in a secure room.

6.2.7 Private Key Strorge on Cryptographic Module

The CA shall store its Private Keys in an encrypted form in an HSM.

6.2.8 Method for Activating Private Keys

The CA shall have two (2) or more authorized persons activate the CA's Private Keys in a secure room.

6.2.9 Method for Deactivating Private Keys

The CA shall have two (2) or more authorized persons deactivate the CA's Private Keys in a secure room.

6.2.10 Method for Destroying Private Keys

The CA shall destroy its Private Keys by having two (2) or more authorized persons completely initialize or physically destroy the Private Keys. The foregoing shall also apply to backups of the Private Keys.

6.2.11 Cryptographic Module Capabilities

The quality standards of an HSM to be used in the CA's system shall be as set forth in "6.2.1 Standards and Management of Cryptographic Modules" of this CPS.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Archives of the CA's Public Keys shall be stored pursuant to the provisions of "5.5.1 Types of Archives" of this CPS.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The validity period of the CA's Private Keys shall be twenty (20) years or less.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The CA shall have two (2) or more authorized persons generate activation data necessary for handling the CA's Private Keys and store the data in electronic media.

6.4.2 Activation Data Protection

The CA shall store and manage the electronic media in which the data necessary for activating the CA's Private Keys is stored, in a secure room.

6.4.3 Other Aspects of Activation Data

The generation and setting of activation data for the CA's Private Keys shall be managed by the persons described in "5.2.1. Trusted Roles" of this CPS.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

After due consideration of the quality, stability, safety, and other features and conditions of the hardware and software to be introduced into the CA's system, the CA shall resolve to introduce the same.

6.5.2 Computer Security Rating

The CA shall endeavor to ensure the reliability of the CA's system by conducting system tests of all software and hardware to be used in the CA's system in advance. In addition, the CA shall constantly collect and assess information on security vulnerabilities of the CA's system, and promptly take necessary actions if any vulnerability is found.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The CA shall establish and maintain its system in a secure environment. If the CA is to modify its system, the CA shall fully assess and verify the safety of the modified system.

Further, the CA shall check the security of the CA's system in order to implement the latest security technologies at an appropriate cycle, and thereby ensure the security.

6.6.2 Security Management Controls

The CA shall ensure the security by conducting such operational management as information asset management, personnel management, and authority management, as well as by promptly updating security software such as anti-hacking and anti-virus applications.

6.6.3 Life Cycle Security Controls

The CA shall promptly assess whether the CA's system is properly developed, operated and maintained, and improve the same, as needed.

6.7 Network Security Controls

The CA shall set up a firewall, an IDS, and the like as measures to prevent unauthorized access to the CA's system from the network.

6.8 Time Stamping

Requirements related to Time Stamps shall be similar to those set forth in "5.5.5 Requirements of Time-Stamping on Records."

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

7.1.1 Version Number(s)

Stipulated in the CP.

7.1.2 Certificate Consent and Extensions

Stipulated in the CP.

7.1.3 Algorithm Object Identifier

Stipulated in the CP.

7.1.4 Name Forms

Stipulated in the CP.

7.1.5 Name Constraints

Stipulated in the CP.

7.1.6 Certificate Policy Object Identifier

Stipulated in the CP.

7.1.7 Usage of Policy Constraints Extension

Stipulated in the CP.

7.1.8 Policy Qualifiers Syntax and Semantics

Stipulated in the CP.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Stipulated in the CP.

7.2 CRL Profile

7.2.1 Version Number(s)

Stipulated in the CP.

7.2.2 CRL and CRL Entry Extensions

Stipulated in the CP.

7.3 OCSP Profile

7.3.1 Version Number(s)

Stipulated in the CP.

7.3.2 OCSP Extensions

Stipulated in the CP.

8. Compliance Audit and Other Assessments

8.1 Frequency and Circumstances of Assessment

JPRS shall perform audits at least once a year to verify whether or not the CA is operated in compliance with this CPS.

8.2 Identity/Qualifications of Assessor

Compliance audits shall be performed by auditors who are adequately experienced in auditing.

Audits required for obtaining the WebTrust certification shall be performed by audit corporations.

8.3 Assessor's Relationship to Assessed Entity

Auditors shall be operationally independent of the auditee divisions, except in matters related to the audits. The auditee divisions shall cooperate with auditors in performing audits.

8.4 Topics Covered by Assessment

Audits shall be performed mainly to verify whether or not the CA is operated in compliance with this CPS, based on the WebTrust for CA and the WebTrust for BR, the criteria for Certification Authorities.

8.5 Actions Taken as a Result of Deficiency

The CA shall promptly take necessary corrective actions with respect to any deficiencies pointed out in an audit report.

8.6 Communication of Results

Auditors shall report the audit results to the CA.

The CA will not externally disclose the audit results unless the CA is required to disclose the same under any law, or by an associated organization based on an agreement with JPRS, or unless such disclosure has been approved by the CA's Certificate Operation Conference.

Reports on validation under the WebTrust for CA and the WebTrust for BR shall be made referable in a specific site according to the provisions of the respective guidelines of the WebTrust for CA and the WebTrust for BR.

8.7 Self-Audits

The CA shall perform regular internal audits to verify and validate whether or not the CA is operated in compliance with this CPS, the CP, and the Baseline Requirements

through the random sampling of certificates under the requirements stipulated in the Baseline Requirements.

9. Other Business and Legal Matters

9.1 Fees

Stipulated in the CP.

9.2 Financial Responsibility

The CA shall maintain a sufficient financial foundation required for operating and maintaining the CA.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

Information possessed by the CA on individuals and organizations shall be treated as confidential, with the exception of information explicitly published as a part of a certificate, a CRL, this CPS, or the CP.

9.3.2 Information not within the Scope of Confidential Information

Information described in certificates and CRLs shall not be treated as confidential. In addition, information falling under any of the following items shall not be treated as confidential:

- information that is or comes to be known through no fault of the CA;
- information that has been or is made known to the CA by a source other than the CA without confidentiality restriction;
- information independently developed by the CA; or
- information whose disclosure has been approved by the relevant Subscriber

9.3.3 Responsibility to Protect Confidential Information

The CA may disclose confidential information as required by any legal provision. In such a case, the CA may not permit any party that comes to acquire the information to disclose the said information to any third party, due to contractual or legal constraints.

9.4 Privacy of Personal Information

JPRS has made its Privacy Policy public on its Web site.

9.5 Intellectual Property Rights

Stipulated in the CP.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

Stipulated in the CP.

9.6.2 RA Representations and Warranties

Stipulated in the CP.

9.6.3 Subscriber Representations and Warranties

Stipulated in the CP.

9.6.4 Relying Party Representations and Warranties

Stipulated in the CP.

9.6.5 Representations and Warranties of Other Participants

Stipulated in the CP.

9.7 Disclaimer of Warranties

Stipulated in the CP.

9.8 Limitations of Liability

Stipulated in the CP.

9.9 Indemnities

Stipulated in the CP.

9.10 Term and Termination

9.10.1 Term

This CPS shall come into effect upon approval by the CA's Certificate Operation Conference. This CPS shall not lose its effect under any circumstances before its termination stipulated in "9.10.2 Termination" herein.

9.10.2 Termination

This CPS shall lose its effect upon termination of the CA, except as provided in "9.10.3 Effect of Termination and Survival" herein.

9.10.3 Effect of Termination and Survival

Even in the event of termination of a usage agreement between a Subscriber and the CA, or termination of the CA itself, any provisions that should survive such termination, by the nature thereof, shall continue to apply to Subscribers, Relying Parties, and the CA, regardless of the reason for such termination.

9.11 Individual Notices and Communications with Participants

JPRS shall provide necessary notices to Subscribers and Relying Parties on its Web site, by e-mail, in writing, or by other means.

9.12 Amendments

9.12.1 Procedure for Amendment

This CPS may be revised at the discretion of the CA, as appropriate, and the revised version hereof shall come into effect upon approval of the CA's Certificate Operation Conference.

9.12.2 Notification Mechanizm and Period

If the CA amends this CPS, the CA shall promptly publish the amended version of this CPS, which shall be deemed to be a notification thereof to Subscribers.

9.12.3 Circumstances under Which OID Must Be Changed

No stipulation.

9.13 Dispute Resolution Provisions

Stipulated in the CP.

9.14 Governing Law

Stipulated in the CP.

9.15 Compliance with Applicable Laws

Stipulated in the CP.

9.16 Miscellaneous Provisions

Not applicable.

9.17 Other Provisions

Stipulated in the CP.