JPRS CA Certification Practice Statement Version 1.50

February 22, 2024

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
1.20	2022.09.30	Revision of "6.3 Other Aspects of Key Pair Management"
1.30	2023.06.08	Revision of "1.1 Overview"
1.40	2023.08.28	Revision of description to clarify compliance with Baseline Requirements
1.50	2024.02.22	Revision of description regarding the formal name of Baseline Requirements

Table of Contents

1. Introduction 11
1.1 Overview 11
1.2 Document Name and Identification 12
1.3 PKI Participants 12
1.3.1 CA 12
1.3.2 RA 12
1.3.3 Subscriber 12
1.3.4 Relying Parties 13
1.3.5 Other Participants 13
1.4 Certificate Usage 13
1.4.1 Appropriate Certificate Uses 13
1.4.2 Prohibited Certificate Uses 13
1.5 Policy Administration 13
1.5.1 Organization Administering the Document 13
1.5.2 Contact Information 13
1.5.3 Person Determining CPS Suitability as Policy 13
1.5.4 Approval Procedures 13
1.6 Definitions and Acronyms 14
2. Publication and Responsibilities for Repository 18
2.1 Repository 18
2.2 Publication of Information 18
2.3 Time or Frequency of Publication 18
2.4 Access Controls on Repositories 18
3. Identification and Authentication 19
3.1 Naming 19
3.1.1 Types of Names 19
3.1.2 Need for Names to Be Meaningful 19
3.1.3 Anonymity or Pseudonymity of Subscribers 19
3.1.4 Rules for Interpreting Various Name Forms 19
3.1.5 Uniqueness of Names 19
3.1.6 Recognition, Authentication, and Roles of Trademarks 19
3.2 Initial Identity Validation 19
3.2.1 Method to Prove Possession of a Private Key 19
3.2.2 Authentication of Organization and Domain Identity 19
3.2.3 Authentication of Individual Identity 19

3.2.4 Non-Verified Subscriber Information 19
3.2.5 Validation of Authority 19
3.2.6 Criteria for Interoperation 19
3.3 Identification and Authentication for Re-key Requests 20
3.3.1 Identification and Authentication for Routine Re-key 20
3.3.2 Identification and Authentication for Re-key after Revocation 20
3.4 Identification and Authentication for Revocation Request 20
4. Certificate Life-Cycle Operational Requirements 21
4.1 Certificate Application 21
4.1.1 Who Can Submit a Certificate Application 21
4.1.2 Enrollment Process and Responsibilities 21
4.2 Certificate Application Processing 21
4.2.1 Performing Identification and Authentication Functions 21
4.2.2 Approval or Rejection of a Certificate Application 21
4.2.3 Time to Process Certificate Application 21
4.2.4 Check of CAA Records 21
4.3 Certificate Issuance 21
4.3.1 CA Actiond during Certificate Issuance 21
4.3.2 Notification to Subscriber of Certificate Issuanc 21
4.4 Certificate Acceptance 21
4.4.1 Conduct Constituting Certificate Acceptance 21
4.4.2 Publication of the Certificates by the CA 21
4.4.3 Notification of Certificate Issuance by the CA to Other Entities 22
4.5 Key Pair and Certificate Usage 22
4.5.1 Use of a Private Key and Certificate by a Subscriber 22
4.5.2 Relying Party Public Key and Certificate Usage 22
4.6 Certificate Renewal 22
4.6.1 Circumstances for Certificate Renewal 22
4.6.2 Who May Request Renewal 22
4.6.3 Processing Certificate Renewal Requests 22
4.6.4 Notification of New Certificate Issuance to Subscriber 22
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate 22
4.6.6 Publication of the Renewal Certificate by the CA 22
4.6.7 Notification of Certificate Issuance by the CA to Other Entities 22
4.7 Certificate Re-key 22
4.7.1 Circumstances for Certificate Re-key 22

4.7.2 Who May Request Certification of a New Public Key 22
4.7.3 Processing Certificate Re-keying Requests 23
4.7.4 Notification of New Certificate Issuance to Subscriber 23
4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate 23
4.7.6 Publication of the Re-keyed Certificates by the CA 23
4.7.7 Notification of Certificate Issuance by the CA to Other Entities 23
4.8 Certificate Modification 23
4.8.1 Circumstances for Certificate Modification 23
4.8.2 Who May Request Certificate Modification 23
4.8.3 Processing Certificate Modification Requests 23
4.8.4 Notification of New Certificate Issuance to Subscriber 23
4.8.5 Conduct Constituting Acceptance of Modified Certificate 23
4.8.6 Publication of the Modified Certificate by the CA 23
4.8.7 Notification of Certificate Issuance by the CA to Other Entities 23
4.9 Certificate Revocation and Suspension 23
4.9.1 Circumstances for Certificate Revocation 23
4.9.2 Who Can Request Revocation 24
4.9.3 Procedures for Revocation Request 24
4.9.4 Revocation Request Grace Period 24
4.9.5 Time within Which the CA Shall Process the Revocation Request 24
4.9.6 Revocation Checking Requirement for Relying Parties 24
4.9.7 CRL Issuance Frequency 24
4.9.8 Maximum Latency for CRLs 24
4.9.9 On-line Revocation/Status Checking Availability 24
4.9.10 On-line Revocation/Status Checking Requirements 24
4.9.11 Other Forms of Revocation Advertisements Available 24
4.9.12 Special Requirements Regarding Key Compromise 24
4.9.13 Circumstances for Suspension 24
4.9.14 Who Can Request Suspension 24
4.9.15 Procedures for Suspension Request 24
4.9.16 Limits on Suspension Period 25
4.10 Certificate Status Services 25
4.10.1 Operational Characteristics 25
4.10.2 Service Availability 25
4.10.3 Optional Features 25
4.11 End of Subscription (Registration) 25

4.12 Key Escrow and Recovery 25
4.12.1 Key Escrow and Recovery Policy and Practices 25
4.12.2 Session Key Encapsulation and Recovery Policy and Practices 25
5. Facility, Management, and Operational Controls 26
5.1 Physical Security Controls 27
5.1.1 Site Location and Construction 27
5.1.2 Physical Access 27
5.1.3 Power and Air Conditioning 27
5.1.4 Water Exposures 27
5.1.5 Fire Prevention and Protection 28
5.1.6 Media Storage 28
5.1.7 Waste Disposal 28
5.1.8 Off-Site Backup 28
5.2 Procedural Controls 28
5.2.1 Trusted Roles 28
5.2.2 Number of Persons Required per Task 29
5.2.3 Identification and Authentication for Trusted Roles 29
5.2.4 Roles Requiring Separation of Duties 29
5.3 Personnel Controls 30
5.3.1 Qualification, Experience, and Clearance Requirements 30
5.3.2 Background Check Procedures 30
5.3.3 Training Requirements and Procedures 30
5.3.4 Retraining Frequency and Requirements 30
5.3.5 Job Rotation Frequency and Requirements 31
5.3.6 Sanctions for Unauthorized Actions 31
5.3.7 Independent Contractor Controls 31
5.3.8 Documentation Supplied to Personnel 31
5.4 Audit Logging Procedures 31
5.4.1 Types of Events Recorded 31
5.4.2 Frequency of Processing Audit Log 32
5.4.3 Retention Period for Audit Log 32
5.4.4 Protection of Audit Log 33
5.4.5 Audit Logs Backup Procedure 33
5.4.6 Audit Log Collection System 33
5.4.7 Notification to Event-causing Subject 33
5.4.8 Vulnerability Assessments 33

5.5 Records Archival 33
5.5.1 Types of Records Archived 33
5.5.2 Retention Period for Archive 34
5.5.3 Protection of Archive 34
5.5.4 Archive Backup Procedures 34
5.5.5 Requirements for Time-Stamping of Records 34
5.5.6 Archive Collection System 34
5.5.7 Procedures to Obtain and Verify Archive Information 34
5.6 Key Changeover 35
5.7 Compromise and Disaster Recovery 35
5.7.1 Incident and Compromise Handling Procedures 35
5.7.2 Recovery Procedures if Computing Resources, Software, and/or Data Are Corrupted 36
5.7.3 Recovery Procedures After Key Compromise 36
5.7.4 Business Continuity Capabilities after a Disaster 36
5.8 CA or RA Termination 36
6. Technical Security Controls 37
6.1 Key Pair Generation and Installation 37
6.1.1 Key Pair Generation 37
6.1.2 Private Key Delivery to Subscriber 38
6.1.3 Public Key Delivery to the Certificate Issuer 38
6.1.4 CA Public Key Delivery to Relying Parties 38
6.1.5 Key Sizes 38
6.1.6 Public Key Parameters Generation and Quality Checking 38
6.1.7 Key Usage Purposes 38
6.2 Private Key Protection and Cryptographic Module Engineering Controls 39
6.2.1 Cryptographic Module Standards and Controls 39
6.2.2 Private Key Multi-Person Control 39
6.2.3 Private Key Escrow 39
6.2.4 Private Key Backup 39
6.2.5 Private Key Archival 39
6.2.6 Private Key Transfer into or from a Cryptographic Module 39
6.2.7 Private Key Strorge on Cryptographic Module 39
6.2.8 Method for Activating Private Keys 39
6.2.9 Method for Deactivating Private Keys 40
6.2.10 Method for Destroying Private Keys 40

6.2.11 Cryptographic Module Capabilities 40
6.3 Other Aspects of Key Pair Management 40
6.3.1 Public Key Archival 40
6.3.2 Certificate Operational Periods and Key Pair Usage Periods 40
6.4 Activation Data 40
6.4.1 Activation Data Generation and Installation 40
6.4.2 Activation Data Protection 40
6.4.3 Other Aspects of Activation Data 41
6.5 Computer Security Controls 41
6.5.1 Specific Computer Security Technical Requirements 41
6.5.2 Computer Security Rating 41
6.6 Life Cycle Technical Controls 41
6.6.1 System Development Controls 41
6.6.2 Security Management Controls 41
6.6.3 Life Cycle Security Controls 41
6.7 Network Security Controls 41
6.8 Time Stamping 42
7. Certificate, CRL, and OCSP Profiles 43
7.1 Certificate Profile 43
7.1.1 Version Number(s) 43
7.1.2 Certificate Consent and Extensions 43
7.1.3 Algorithm Object Identifier 43
7.1.4 Name Forms 43
7.1.5 Name Constraints 43
7.1.6 Certificate Policy Object Identifier 43
7.1.7 Usage of Policy Constraints Extension 43
7.1.8 Policy Qualifiers Syntax and Semantics 43
7.1.9 Processing Semantics for the Critical Certificate Policies Extension 43
7.2 CRL Profile 43
7.2.1 Version Number(s) 43
7.2.2 CRL and CRL Entry Extensions 43
7.3 OCSP Profile 44
7.3.1 Version Number(s) 44
7.3.2 OCSP Extensions 44
8. Compliance Audit and Other Assessments 45
8.1 Frequency and Circumstances of Assessment 45

8.2 Identity/Qualifications of Assessor 45
8.3 Assessor's Relationship to Assessed Entity 46
8.4 Topics Covered by Assessment 46
8.5 Actions Taken as a Result of Deficiency 46
8.6 Communication of Results 46
8.7 Self-Audits 47
9. Other Business and Legal Matters 48
9.1 Fees 48
9.2 Financial Responsibility 48
9.3 Confidentiality of Business Information 48
9.3.1 Scope of Confidential Information 48
9.3.2 Information not within the Scope of Confidential Information 48
9.3.3 Responsibility to Protect Confidential Information 48
9.4 Privacy of Personal Information 49
9.5 Intellectual Property Rights 49
9.6 Representations and Warranties 49
9.6.1 CA Representations and Warranties 49
9.6.2 RA Representations and Warranties 49
9.6.3 Subscriber Representations and Warranties 49
9.6.4 Relying Party Representations and Warranties 49
9.6.5 Representations and Warranties of Other Participants 49
9.7 Disclaimer of Warranties 49
9.8 Limitations of Liability 49
9.9 Indemnities 49
9.10 Term and Termination 49
9.10.1 Term 49
9.10.2 Termination 50
9.10.3 Effect of Termination and Survival 50
9.11 Individual Notices and Communications with Participants 50
9.12 Amendments 50
9.12.1 Procedure for Amendment 50
9.12.2 Notification Mechanism and Period 50
9.12.3 Circumstances under Which OID Must Be Changed 50
9.13 Dispute Resolution Provisions 50
9.14 Governing Law 50
9.15 Compliance with Applicable Laws 50

9.16 Miscellaneous Provisions 50
9.17 Other Provisions 51

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 current version of "Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates" (hereinafter referred to as the "Baseline Requirements") published by CA/Browser Forum at https://www.cabforum.org/, and the Application Software Supplier Standards published.

Table1.1 List of Standards

Types of certificates issued by the CA	Standards to comply with
TLS Server Certificate	・ Baseline Requirements for the Issuance and Management of Publicly - Trusted TLS Server Certificates ・ Apple Root Certificate Program ・ Chrome Root Program Policy ・ Microsoft Trusted Root Program ・ Mozilla Root Store Policy

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. Also, if any inconsistency is found among the provisions of the Japanese version and the English version of this CPS, the English version shall prevail over the Japanese version.

In the event of any inconsistency between the documents established by the CA (including, but not limited to, this CPS, the CP, the Terms and Conditions, and the related documents) and Baseline Requirements, Baseline Requirements take precedence

over these documents.

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

Archive

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

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.

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.

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.

ECDSA

"ECDSA" is one of the most standard encryption technologies. ECDSA is widely used as a public key cryptosystem.

Escrow

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

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.

JPRS Partners

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

Key Pair

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

NTP (Network Time Protocol)

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

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.

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.

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.

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.”

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.

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.

Repository

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

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.

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.

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

The CA/Browser Forum's "Network and Certificate System Security Requirement" is fully incorporated into this document by reference.

The CA shall develop, implement, and maintain a comprehensive security program designed to:

1. Protect the confidentiality, integrity, and availability of Certificate Data and Certificate Management Processes;
2. Protect against anticipated threats or hazards to the confidentiality, integrity, and availability of the Certificate Data and Certificate Management Processes;
3. Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of any Certificate Data or Certificate Management Processes;
4. Protect against accidental loss or destruction of, or damage to, any Certificate Data or Certificate Management Processes; and
5. Comply with all other security requirements applicable to the CA by law.

The Certificate Management Process must include:

1. Physical security and environmental controls;
2. System integrity controls, including configuration management, integrity maintenance of trusted code, and malware detection/prevention;
3. Network security and firewall management, including port restrictions and IP address filtering;
4. User management, separate trusted-role assignments, education, awareness, and training; and
5. Logical access controls, activity logging, and inactivity time-outs to provide individual accountability.

The CA's security program should include the following annual risk assessments:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;
2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
3. Assesses the sufficiency of the policies, procedures, information systems, technology,

and other arrangements that the CA has in place to counter such threats.

Based on the Risk Assessment, the CA shall develop, implement, and maintain a security plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of the Certificate Data and Certificate Management Processes. The security plan must include administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the Certificate Data and Certificate Management Processes. The security plan must also take into account then-available technology and the cost of implementing the specific measures, and shall implement a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

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.
The CA Private Key shall be backed up, stored, and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment.

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.
The CA shall provide all personnel performing information verification duties with skills-training that covers basic Public Key Infrastructure knowledge, authentication and vetting policies and procedures (including the CA’s CP and/or CPS), common threats to the information verification process (including phishing and other social engineering tactics), and these Requirements.
The CA shall maintain records of such training and ensure that personnel entrusted with Validation Specialist duties maintain a skill level that enables them to perform such duties satisfactorily.
The CA shall document that each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task.
The CA shall require all Validation Specialists to pass an examination provided by the CA on the information verification requirements outlined in these Requirements.

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.
All personnel in Trusted Roles shall maintain skill levels consistent with the CA’s

training and performance programs.

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.

The CA shall verify that the Delegated Third Party's personnel involved in the issuance of a Certificate meet the training and skills requirements of this CPS "5.3.3 Training Requirements" and this CPS "5.4.1 Types of Events Recorded".

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. CA certificate and key lifecycle events, including:
    1. Key generation, backup, storage, recovery, archival, and destruction;
    2. Certificate requests, renewal, and re-key requests, and revocation;
    3. Approval and rejection of certificate requests;
    4. Cryptographic device lifecycle management events;
    5. Generation of Certificate Revocation Lists and OCSP entries;
    6. Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.
2. Subscriber Certificate lifecycle management events, including:
    1. Certificate requests, renewal, and re-key requests, and revocation;
    2. All verification activities stipulated in these Requirements and the CA's Certification Practice Statement;

3. Approval and rejection of certificate requests;
4. Issuance of Certificates; and
5. Generation of Certificate Revocation Lists and OCSP entries.

3. Security events, including:
1. Successful and unsuccessful PKI system access attempts;
2. PKI and security system actions performed;
3. Security profile changes;
4. Installation, update and removal of software on a Certificate System;
5. System crashes, hardware failures, and other anomalies;
6. Firewall and router activities; and
7. Entries to and exits from the CA facility.

Log records MUST include the following elements:

1. Date and time of record;
2. Identity of the person making the journal record; and
3. Description of the record.

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.

However, if related to Baseline Requirements, the CA shall retain the following for at least two years:

1. The CA certificate and key lifecycle management event record (described in this CPS "5.4.1 Types of Events Recorded") shall be retained after any of the following have occurred:
1. The destruction of the CA Private Key; or
2. The revocation or expiration of the final CA Certificate in that set of Certificates that have an X.509v3 basicConstraints extension with the cA field set to true and which share a common Public Key corresponding to the CA Private Key;
2. Subscriber Certificate lifecycle management event records (described in this CPS "5.4.1 Types of Events Recorded") after the revocation or expiration of the Subscriber Certificate;
3. Any security event records (described in this CPS "5.4.1 Types of Events Recorded")

after the event occurred.

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. Additionally, the CA's security program must include an annual Risk Assessment that:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;
2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

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;

- processing history related to CRL issuance;
- 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
- application documents from the subscribers; and
- access logs to OCSP responders (for CAs using OCSP responders).

5.5.2 Retention Period for Archive

The CA shall keep archives for at least ten (10) years.
However, in relation to Baseline Requirements, archived audit logs (as set forth in " 5.5.1 Types of Records Archived " of this CPS) shall be retained for a period of at least two (2) years from their record creation timestamp, or as long as they are required to be retained per "5.4.3 Retention Period for Audit Log" of this CPS, whichever is longer.

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

Should it be determined that CA Private Keys have been or may be compromised or should a disaster or any other unexpected incidents result in a situation that may lead to interruptions or suspensions of the Services, the predetermined plans and procedures are followed to securely resume the Services.

The CA shall have an Incident Response Plan and a Disaster Recovery Plan.

The CA shall document a business continuity and disaster recovery procedures designed to notify and reasonably protect Application Software Suppliers, Subscribers, and Relying Parties in the event of a disaster, security compromise, or business failure. The CA is not required to publicly disclose its business continuity plans but shall make its business continuity plan and security plans available to the CA's auditors upon request.

The CA shall annually test, review, and update these procedures.

The business continuity plan must include:

1. The conditions for activating the plan,
2. Emergency procedures,
3. Fallback procedures,
4. Resumption procedures,
5. A maintenance schedule for the plan;
6. Awareness and education requirements;
7. The responsibilities of the individuals;
8. Recovery time objective (RTO);
9. Regular testing of contingency plans.
10. The CA's plan to maintain or restore the CA's business operations in a timely manner following interruption to or failure of critical business processes.
11. A requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location;
12. What constitutes an acceptable system outage and recovery time
13. How frequently backup copies of essential business information and software are taken;
14. The distance of recovery facilities to the CA's main site; and
15. Procedures for securing its facility to the extent possible during the period of time following a disaster and prior to restoring a secure environment either at the original

or a remote site.

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

The following management is performed for the key pair of the CA's keys:

1. Prepare and follow a Key Generation Script and
2. Have a Qualified Auditor witness the CA Key Pair generation process or record a video of the entire CA Key Pair generation process.

In all cases, the CA shall:

1. Generate the CA Key Pair in a physically secured environment as described in the CA's CP and/or CPS;
2. Generate the CA Key Pair using personnel in trusted roles under the principles of multiple person control and split knowledge;
3. Generate the CA Key Pair within cryptographic modules meeting the applicable technical and business requirements as disclosed in the CA's CP and/or CPS. The key pair of this CA is generated on a hardware security module (hereinafter referred to as "HSM") that has acquired FIPS 140-1 Level 3 certification.
4. Log its CA Key Pair generation activities; and
5. Maintain effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in its CP and/or CPS and (if applicable) its Key Generation Script.

For key pair generation of subscriber certificates for TLS server certificates that complies with Baseline Requirements, the CA must reject the certificate request if one or more of the following conditions are met:

1. The key pair does not meet the requirements described in the CP "6.1.5 Key Sizes" or "6.1.6 Public Key Parameters Generation and Quality Checking";
2. There is clear evidence that the specific method used to generate the Private Key was flawed;
3. The CA is aware of a demonstrated or proven method that exposes the Applicant's

Private Key to compromise;

4. The CA has previously been made aware that the Applicant's Private Key has suffered a Key Compromise, such as through the provisions of the CP "4.9.1 Reason for Certificate Revocation".
5. The CA is aware of a demonstrated or proven method to easily compute the Applicant's Private Key based on the Public Key (such as a Debian weak key, see https://wiki.debian.org/SSLkeys).

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.
For RSA, the CA shall confirm that the value of the public exponent is an odd number equal to 3 or more. Additionally, the public exponent should be in the range between 2^16+1 and 2^256 - 1. The modulus should also have the following characteristics: an odd number, not the power of a prime, and have no factors smaller than 752. [Source: Section 5.3.3, NIST SP 800-89].
For ECDSA, the CA should confirm the validity of all keys using either the ECDSA Full Public Key Validation Routine or the ECDSA Partial Public Key Validation Routine. [Source: Sections 5.6.2.3.2 and 5.6.2.3.3, respectively, of NIST SP800-56A: Revision2]

6.1.7 Key Usage Purposes

Stipulated in the CP.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The CA shall implement physical and logical safeguards to prevent unauthorized certificate issuance. Protection of the CA Private Key outside the validated system or device specified above must consist of physical security, encryption, or a combination of both, implemented in a manner that prevents disclosure of the CA Private Key. The CA shall encrypt its Private Key with an algorithm and key-length that, according to the state of the art, are capable of withstanding cryptanalytic attacks for the residual life of the encrypted key or key part.

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 key pair of the CA is not specified, but the validity period of the certificate is assumed to be 20 years or less.
The validity period of the Subscriber Certificates is stipulated in the CP.

OCSP certificates must not have a Validity Period greater than 125 days.

For the purpose of calculations, a day is measured as 86,400 seconds. Any amount of time greater than this, including fractional seconds and/or leap seconds, shall represent an additional day.

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.
The CA shall enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.

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 conducts audits from time to time to examine if the operations of the Digital Certification Infrastructure are in compliance with this CPS or not.

Certificates that are capable of being used to issue new certificates must either be Technically Constrained in line with the CP "7.1.5 Name Constraints" and audited in line with the CP "8.7 Self-Audit" only, or Unconstrained and fully audited in line with all remaining requirements from this section. A Certificate is deemed as capable of being used to issue new certificates if it contains an X.509v3 basicConstraints extension, with the cA boolean set to true and is therefore by definition a Root CA Certificate or a Subordinate CA Certificate.

The period during which the CA issues Certificates shall be divided into an unbroken sequence of audit periods. An audit period must not exceed one year in duration.

If the CA has a currently valid Audit Report indicating compliance with an audit scheme listed in this CPS, “8.4 Topics Covered by Assessment”, then no pre-issuance readiness assessment is necessary.

If the CA does not have a currently valid Audit Report indicating compliance with one of the audit schemes listed in this CPS, “8.4 Topics Covered by Assessment”, then, before issuing Publicly-Trusted Certificates, the CA shall successfully complete a point-in- time readiness assessment performed in accordance with applicable standards under one of the audit schemes listed in this CPS, “8.4 Topics Covered by Assessment”. The point-in-time readiness assessment shall be completed no earlier than twelve (12) months prior to issuing Publicly-Trusted Certificates and shall be followed by a complete audit under such scheme within ninety (90) days of issuing the first Publicly- Trusted Certificate.

8.2 Identity/Qualifications of Assessor

The CA’s audit shall be performed by a Qualified Auditor. A Qualified Auditor means a natural person, Legal Entity, or group of natural persons or Legal Entities that collectively possess the following qualifications and skills:

1. Independence from the subject of the audit;
2. The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme (see this CPS, “8.4 Topics Covered by Assessment”);
3. Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;

4. (For audits conducted in accordance with the WebTrust standard) licensed by WebTrust;
5. Bound by law, government regulation, or professional code of ethics; and
6. Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage.

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.

The CA shall undergo an audit in accordance with one of the following schemes:

・WebTrust for CAs

・WebTrust for CAs SSL Baseline with Network Security

It must incorporate periodic monitoring and/or accountability procedures to ensure that its audits continue to be conducted in accordance with the requirements of the scheme.

The audit must be conducted by a Qualified Auditor, as specified in this CPS "8.2 Identity/Qualifications of Assessor".

For Delegated Third Parties which are not Enterprise RAs, then the CA shall obtain an audit report, issued under the auditing standards that underlie the accepted audit schemes found in this CPS, "8.4 Topics Covered by Assessment", that provides an opinion whether the Delegated Third Party's performance complies with either the Delegated Third Party's practice statement or the CA's CP and/or CPS. If the opinion is that the Delegated Third Party does not comply, then the CA shall not allow the Delegated Third Party to continue performing delegated functions.

The audit period for the Delegated Third Party shall not exceed one year (ideally aligned with the CA's audit).

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 shall be made referable in a specific site according to the provisions of the respective guidelines of the WebTrust.

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.

During the period in which the CA issues Certificates, the CA shall monitor adherence to its CP, CPS and these Requirements and strictly control its service quality by performing self-audits on at least a quarterly basis against a randomly selected sample of the greater of one certificate or at least three percent of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken. Except for Delegated Third Parties that undergo an annual audit that meets the criteria specified in this CPS, Section 8.4 "Topics Covered by Assessment", the CA SHALL strictly control the service quality of Certificates issued or containing information verified by a Delegated Third Party by having a Validation Specialist employed by the CA perform ongoing quarterly audits against a randomly selected sample of at least the greater of one certificate or three percent of the Certificates verified by the Delegated Third Party in the period beginning immediately after the last sample was taken. The CA shall review each Delegated Third Party's practices and procedures to ensure that the Delegated Third Party is in compliance with these Requirements and the relevant CP and/or CPS. The CA shall internally audit each Delegated Third Party's compliance with these Requirements on an annual basis. During the period in which a Technically Constrained CA issues Certificates that complies with Baseline Requirements, the CA shall monitor adherence to the CA's CP. On at least a quarterly basis, against a randomly selected sample of the greater of one certificate or at least three percent of the Certificates issued by the CA, during the period commencing immediately after the previous audit sample was taken, the CA shall ensure all applicable CP are met.

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.

The CA does not disclose such information externally unless it is required by law or there is a prior consent of the relevant Subscriber. The CA may disclose the information subject to confidentiality to a legal counsel or a financial adviser who provides advice in connection with such legal, judicial, administrative or other procedures required by law. It may also disclose information subject to confidentiality to an attorney, an accountant, a legal institution or any other specialist who provides advice on corporate mergers, acquisitions or restructuring.

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 or there is a prior consent of the relevant Subscriber. 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

This CPS is published under the Creative Commons license Attribution- NoDerivatives (CC-BY-ND) 4.0 International.

（https://creativecommons.org/licenses/by-nd/4.0/）

For other matters, 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 Mechanism 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

Stipulated in the CP.

9.17 Other Provisions

Stipulated in the CP.