

JPRS CA Certificate Policy Version 3.40

June 08, 2023

Japan Registry Services Co., Ltd.

Version History		
Version Number	Date	Description
1.00	2019.06.17	Publication of the first version
1.10	2019.09.25	Revision of “3.2.2.4 Validation of Domain Authorization or Control” (adding the additional information of “general e-mail address indicating an administrator”
1.20	2020.04.01	Revision due to Mozilla Root Store Policy (v2.7)
1.30	2020.07.10	Revision of “7.1.2 Subordinate CA Certificate Profile”
2.00	2020.07.22	Revision of “7. Certificate, CRL, and OCSP Profiles”
2.10	2020.08.20	Revision of the maximum validity period of certificate
2.20	2020.10.06	Revision of “3.2.2.4 Validation of Domain Authorization or Control”
2.21	2021.04.01	Revision of the date and version
2.22	2021.04.28	Revision due to Mozilla Root Store Policy (v2.7.1)
2.23	2021.05.27	<ul style="list-style-type: none"> · Clarification of “3.2.2.4 Validation of Domain Authorization or Control” · Delete the description of invalid Subordinate CAs from “7. Certificate, CRL, and OCSP Profiles”.
2.30	2021.11.18	<ul style="list-style-type: none"> · Revision of “3.2.2.4.18 Agreed-Upon Change to Website v2” · Sunset of “subject:organizationalUnitName”
3.00	2021.12.08	Revisions due to new service provision
3.10	2022.03.02	Add a reference to the new terms and conditions
3.11	2022.04.01	Revision of the date and version
3.20	2022.09.30	<ul style="list-style-type: none"> · Revision of “6.3 Other Aspects of Key Pair Management” · Add description of Revocation Reason Code to be applied in this CA.
3.30	2023.04.24	· Revision of the maximum validity period of certificate
3.40	2023.06.08	<ul style="list-style-type: none"> · Revision of “1.1 Overview” · Revision of “7.3 OCSP Profile”

*Note

This “JPRS CA Certificate Policy” 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 Certificate Policy.” If the new version of “JPRS CA Certificate Policy” is published, please stop referencing/using this document.

Table of Contents

1. Introduction.....	10
1.1 Overview	10
1.2 Document Name and Identification.....	11
1.3 PKI Participants.....	11
1.3.1 CA	11
1.3.2 RA	11
1.3.3 Subscribers.....	11
1.3.4 Relying Parties	12
1.3.5 Other Participants.....	12
1.4 Certificate Usage.....	12
1.4.1 Appropriate Certificate Uses	12
1.4.2 Prohibited Certificate Uses.....	12
1.5 Policy Administration	12
1.5.1 Organization Administering the Document	12
1.5.2 Contact Information	12
1.5.3 Person Determining CP Suitability as Policy.....	12
1.5.4 Approval Procedures.....	12
1.6 Definitions and Acronyms.....	13
2. Publication and Repository Responsibilities.....	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
3.1.4 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.....	20
3.2.2.1 Authentication of Organization Identity.....	20
3.2.2.2 DBA/Tradenname.....	20
3.2.2.3 Verification of a Country	20

3.2.2.4 Validation of Domain Authorization or Control.....	20
3.2.3 Authentication of Individual Identity	23
3.2.4 Non-Verified Subscriber Information.....	23
3.2.5 Validation of Authority.....	23
3.2.6 Criteria for Interoperation.....	24
3.3 Identification and Authentication for Re-key Requests	24
3.4 Identification and Authentication for Revocation Request	24
4. Certificate Life-Cycle Operational Requirements	25
4.1 Certificate Application	25
4.1.1 Who Can Submit a Certificate Application.....	25
4.1.2 Enrollment Process and Responsibilities.....	25
4.2 Certificate Application Processing	25
4.2.1 Performing Identification and Authentication Functions	25
4.2.2 Approval or Rejection of a Certificate Application	25
4.2.3 Time to Process Certificate Applications	25
4.2.4 Check of CAA Records.....	26
4.3 Certificate Issuance.....	26
4.3.1 CA Actions during Certificate Issuance	26
4.3.2 Notification to Subscriber of Certificate Issuance	26
4.4 Certificate Acceptance.....	26
4.4.1 Conduct Constituting Certificate Acceptance.....	26
4.4.2 Publication of the Certificates by the CA	26
4.4.3 Notification of Certificate Issuance by the CA to Other Entities.....	26
4.5 Key Pair and Certificate Usage.....	26
4.5.1 Subscriber Private Key and Certificate Usage.....	27
4.5.2 Relying Party Public Key and Certificate Usage	27
4.6 Certificate Renewal.....	27
4.6.1 Circumstances for Certificate Renewal	27
4.6.2 Who May Request Renewal	27
4.6.3 Processing Certificate Renewal Requests.....	27
4.6.4 Notification of New Certificate Issuance to Subscriber.....	27
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate.....	27
4.6.6 Publication of the Renewal Certificate by the CA.....	27
4.6.7 Notification of Certificate Issuance by the CA to Other Entities.....	28
4.7 Certificate Re-key.....	28
4.7.1 Circumstances for Certificate Re-key	28

4.7.2 Who May Request Certification of a New Public Key.....	28
4.7.3 Processing Certificate Re-keying Requests	28
4.7.4 Notification of New Certificate Issuance to Subscriber.....	28
4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate.....	28
4.7.6 Publication of the Re-keyed Certificates by the CA.....	28
4.7.7 Notification of Certificate Issuance by the CA to Other Entities.....	28
4.8 Certificate Modification	28
4.8.1 Circumstances for Certificate Modification.....	28
4.8.2 Who May Request Certificate Modification.....	29
4.8.3 Processing Certificate Modification Requests	29
4.8.4 Notification of New Certificate Issuance to Subscriber.....	29
4.8.5 Conduct Constituting Acceptance of Modified Certificate.....	29
4.8.6 Publication of the Modified Certificate by the CA	29
4.8.7 Notification of Certificate Issuance by the CA to Other Entities.....	29
4.9 Certificate Revocation and Suspension	29
4.9.1 Circumstances for Certificate Revocation	29
4.9.2 Who Can Request Revocation.....	30
4.9.3 Procedures for Revocation Request.....	30
4.9.5 Time within Which the CA Shall Process the Revocation Request	30
4.9.6 Revocation Checking Requirement for Relying Parties.....	30
4.9.7 CRL Issuance Frequency	30
4.9.8 Maximum Latency for CRLs.....	31
4.9.9 On-line Revocation/Status Checking Availability	31
4.9.10 On-line Revocation/Status Checking Requirements.....	31
4.9.11 Other Forms of Revocation Advertisements Available.....	31
4.9.12 Special Requirements Regarding Key Compromise	31
4.9.13 Circumstances for Suspension.....	31
4.9.14 Who Can Request Suspension	31
4.9.15 Procedures for Suspension Request	31
4.9.16 Limits on Suspension Period	32
4.10 Certificate Status Services	32
4.10.1 Operational Characteristics.....	32
4.10.2 Service Availability.....	32
4.10.3 Optional Features.....	32
4.11 End of Subscription (Registration).....	32
4.12 Key Escrow and Recovery.....	32

4.12.1 Key Escrow and Recovery Policy and Practices	32
4.12.2 Session Key Encapsulation and Recovery Policy and Practices	32
5. Facility, Management, and Operational Controls.....	33
5.1 Physical Security Controls	33
5.2 Procedural Controls	33
5.3 Personnel Controls	33
5.4 Audit Logging Procedures.....	33
5.4.1 Types of Events Recorded	33
5.4.2 Frequency of Processing Audit Log	33
5.4.3 Retention Period for Audit Log.....	33
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	34
5.7 Compromise and Disaster Recovery	34
5.8 CA or RA Termination.....	35
6. Technical Security Controls	36
6.1 Key Pair Generation and Installation	36
6.1.1 Key Pair Generation.....	36
6.1.2 Private Key Delivery to Subscriber.....	36
6.1.3 Public Key Delivery to the Certificate Issuer.....	36
6.1.4 CA' Public Key Delivery to Relying Parties	36
6.1.5 Key Sizes	36
6.1.6 Public Key Parameters Generation and Quality Checking.....	36
6.1.7 Key Usage Purposes	36
6.2 Private Key Protection and Cryptographic Module Engineering Controls	37

6.3 Other Aspects of Key Pair Management	37
6.3.1 Public key archival	37
6.3.2 Certificate operational periods and key pair usage periods.....	37
6.4 Activation Data.....	37
6.5 Computer Security Controls.....	37
6.6 Life Cycle Technical Controls	37
6.7 Network Security Controls	37
6.8 Time Stamping	37
7. Certificate, CRL, and OCSP Profiles.....	38
7.1 Certificate Profile	38
7.1.1 Subscriber Certificate Profile	38
7.1.2 Subordinate CA Certificate Profile.....	41
7.2 CRL Profile	42
7.3 OCSP Profile.....	44
7.3.1 Version Number(s).....	45
7.3.2 OCSP Extensions.....	45
8. Compliance Audit and Other Assessments.....	46
8.1 Frequency and Circumstances of Assessment	46
8.2 Identity/Qualifications of Assessor	46
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	46
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	48
9.5 Intellectual Property Rights.....	48
9.6 Representations and Warranties	48
9.6.1 CA Representations and Warranties.....	48
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.....	50
9.10 Term and Termination	50
9.10.1 Term.....	50
9.10.2 Termination.....	50
9.10.3 Effect of Termination and Survival.....	51
9.11 Individual Notices and Communications with Participants.....	51
9.12 Amendments.....	51
9.12.1 Procedure for Amendment	51
9.12.2 Notification Mechanism and Period.....	51
9.12.3 Circumstances under Which OID Must Be Changed	51
9.13 Dispute Resolution Provisions	51
9.14 Governing Law	51
9.15 Compliance with Applicable Laws	51
9.16 Miscellaneous Provisions.....	52
9.17 Other Provisions.....	52

1. Introduction

1.1 Overview

This document, the JPRS CA Certificate Policy (hereinafter referred to as “this CP”), stipulates policies regarding the usages, purposes of use, scope of application, etc. of Digital Certificates to be issued by Japan Registry Services Co., Ltd. (hereinafter referred to as “JPRS”) as a Certification Authority (hereinafter referred to as the “CA”), for the purpose of providing the JPRS Digital Certificate Issuance Services (hereinafter referred to as the “Services”).

Various procedures regarding the operation and maintenance of the CA are stipulated in the JPRS CA Certification Practice Statement (hereinafter referred to as the “CPS”).

A certificate for one-way and mutual certification has been issued to the CA by Security Communication RootCA2, a Certification Authority operated by SECOM Trust Systems Co., Ltd. (hereinafter referred to as “SECOM Trust Systems”), and the CA is authorized to issue certificates to Subscribers.

Certificates issued by the CA are used for encrypting information for server authentication and on communication pathways. “The Terms and Conditions of JPRS Digital Certificate Issuance Services” and “The Terms and Conditions of JPRS Digital Certificate Issuance Services for ACME” (hereinafter, both will be referred to as the “Terms and Conditions”) stipulate the servers to be covered by the issuance of such certificates.

Each person who intends to have a certificate issued by the CA is required to consider the Terms and Conditions, this CP, and the CPS in light of his/her/its own purposes of use, and then to consent to the Terms and Conditions, this CP, and the CPS.

The CA conforms to the current version of “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/>, and RFC 5280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.”

If any inconsistency is found among the provisions of this CP, the Terms and Conditions, and the CPS, the provisions of the Terms and Conditions shall prevail over those of this CP and the CPS, and the provisions of this CP shall prevail over those of the CPS. In the event of any inconsistency between the documents established by the CA (including, but not limited to, this CP, the CPS, the Terms and Conditions, and the related documents)

and Baseline Requirements, Baseline Requirements take precedence over these documents.

This CP 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 CA in terms of technologies or operation, this CP shall be revised, as needed, in order to reflect such developments or improvements.

1.2 Document Name and Identification

The official name of this CP is the “JPRS CA Certificate Policy.”

Following are an Object Identifier (hereinafter referred to as “OID”) assigned by the CA under this CP, and an OID of the CPS referenced by this CP:

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

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 Subscribers

“Subscribers” 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

Certificates issued by the CA are used to encrypt information for server authentication and on communication pathways.

1.4.2 Prohibited Certificate Uses

Certificates issued by the CA may be used solely as set forth in “1.4.1 Appropriate Certificate Uses,” and may not be used for any other purposes.

1.5 Policy Administration

1.5.1 Organization Administering the Document

This CP shall be maintained and administered by the CA.

1.5.2 Contact Information

Inquiries concerning this CP 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 certificate issued by the CA is revealed, please notify via the following webform:

https://jprs.jp/pubcert/f_mail/

1.5.3 Person Determining CP Suitability as Policy

The details of this CP shall be determined by the CA’s Certificate Operation Conference.

1.5.4 Approval Procedures

This CP 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.

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.

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.”

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.

ランダム値 (Random Value)

A value specified by a CA to the Applicant that exhibits at least 112 bits of entropy.

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”

ACME (Automated Certificate Management Environment)

“ACME” stands for “Automated Certificate Management Environment”, a protocol that a CA and an applicant can use to automate the process of verification and certificate issuance. This Protocol is specified in RFC 8555.

Authorization Domain Name

The Domain Name used to obtain authorization for certificate issuance for a given FQDN. The CA may use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. If the FQDN contains a wildcard character, then the CA MUST remove all wildcard labels from the left most portion of requested FQDN. The CA may prune zero or more labels from left to right until encountering a Base Domain Name and may use any one of the intermediate values for the purpose of domain validation.

Base Domain Name

The portion of an applied-for FQDN that is the first domain name node left of a registry-controlled or public suffix plus the registry-controlled or public suffix (e.g. "example.co.uk" or "example.com"). For FQDNs where the right-most domain name node is a gTLD having ICANN Specification 13 in its registry agreement, the gTLD itself may be used as the Base Domain Name.

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)

“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 Repository Responsibilities

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 CP, and the CPS on the Repository to allow online access by Subscribers and Relying Parties.

2.3 Time or Frequency of Publication

This CP and the CPS shall be published on the Repository as revised.

The frequency of CRL issuance is specified in Section 4.9.7.

2.4 Access Controls on Repositories

The CA does not exercise any specific access control over information published on the Repository. The CA's CRLs shall be made available to Subscribers and Relying Parties through the Repository. Access to the Repository shall be granted through a general Web interface.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

The name of each Subscriber to be described in certificates to be issued by the CA shall be configured according to the Distinguished Name (DN) format for the X.500 series recommendations (recommendations formulated by the International Telecommunication Union Telecommunication Standardization Sector (ITU-T)). 3.1.2 Need for Names to Be Meaningful

The information included in certificates issued by the CA and their meanings are specified in Section 7.1.1.3.1.3 Anonymity or Pseudonymity of Subscribers

No name identical to any anonym or pseudonym used in any certificate to be issued by the CA may be registered.

3.1.4 Rules for Interpreting Various Name Forms

The Distinguished Name (DN) format of the X.500 series shall stipulate the rules for interpreting various name forms and shall be complied with accordingly.

3.1.5 Uniqueness of Names

The attribute of a Distinguished Name (DN) to be described in a certificate to be issued by the CA shall be unique to the server covered by the issuance.

3.1.6 Recognition, Authentication, and Roles of Trademarks

The CA does not verify whether an applicant holds any intellectual property right to the name described in a certificate application. No Subscriber may submit to the CA a certificate application with any registered trademark or associated name of any third party. If any dispute arises between a Subscriber and any third party in connection with a registered trademark or the like, the CA will not undertake to arbitrate or settle the dispute. The CA is entitled to reject a Subscriber's certificate application or to revoke an issued certificate on account of such a dispute.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of a Private Key

A Subscriber's possession of a Private Key is proved by verifying the signature on the relevant Certificate Signing Request (hereinafter referred to as "CSR") and confirming that the CSR has been signed with the Private Key corresponding to the Public Key

contained in the CSR.

3.2.2 Authentication of Organization and Domain Identity

3.2.2.1 Authentication of Organization Identity

(1) Domain Validation

The CA does not verify the existence of organizations.

(2) Organization Validation

The CA shall verify the existence of organizations by using public documents issued by, or Web pages or Web page databases of, the relevant country or local public entity, or using inquiries made by any third party that is deemed reliable by the CA, or the databases of any such third party.

3.2.2.2 DBA/Tradename

If a DBA/tradename is described as the “Organization (organization name)” in a certificate to be issued by the CA, the CA shall verify the information same manner as set forth in “3.2.2.1 Authentication of Organization Identity (2) Organization Validation.”

3.2.2.3 Verification of a Country

The CA shall verify the information on the “Country (country name)” in a certificate to in the same manner as set forth in “3.2.2.1 Authentication of Organization Identity.”

3.2.2.4 Validation of Domain Authorization or Control

The CA SHALL confirm that prior to issuance, the CA has validated each Fully-Qualified Domain Name (FQDN) listed in the Certificate using at least one of the methods listed below;

Subsequent sections 3.2.2.4.1-20 correspond to the section numbers of the methods specified by BR.

3.2.2.4.1 Validating the Applicant as a Domain Contact

Not applicable

3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact

Confirming the Applicant's control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value.

The Random Value MUST be sent to an email address listed in the WHOIS record.

The CA does not use fax, SMS, or postal mail to send a Random Values.

The Random Value SHALL be unique in each email. The Random Value SHALL remain valid for use in a confirming response for no more than 25 days from its creation.

3.2.2.4.3 Phone Contact with Domain Contact

Not applicable

3.2.2.4.4 Constructed Email to Domain Contact

Confirm the Applicant's control over the FQDN by

1. Sending an email to one or more addresses created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at-sign ("@"), followed by the Authorization Domain Name; and
2. including a Random Value in the email; and
3. receiving a confirming response utilizing the Random Value.

The Random Value SHALL be unique in each email. The Random Value SHALL remain valid for use in a confirming response for no more than 25 days from its creation.

3.2.2.4.5 Domain Authorization Document

Not applicable

3.2.2.4.6 Agreed-Upon Change to Website

Not applicable

3.2.2.4.7 DNS Change

Confirming the Applicant's control over the FQDN by confirming the presence of a Random Value for either in a DNS TXT record of the Authorization Domain Name that is prefixed with a Domain Label that begins with "_acme-challenge".

The CA MUST provide a Random Value unique to the certificate request. The Random Value MUST remain valid for use in a confirming response for no more than 25 days from its creation.

3.2.2.4.8 IP Address

Not applicable

3.2.2.4.9 Test Certificate

Not applicable

3.2.2.4.10 TLS Using a Random Number

Not applicable

3.2.2.4.11 Any Other Method

Not applicable

3.2.2.4.12 Validating Applicant as a Domain Contact

Confirming the Applicant's control over the FQDN by validating the Applicant is the a registrant of the domain name. This method may only be used if the CA is also the Domain Name Registrar, or an Affiliate of the Registrar, of the Base Domain Name.

3.2.2.4.13 Email to DNS CAA Contact

Not applicable

3.2.2.4.14 Email to DNS TXT Contact

Not applicable

3.2.2.4.15 Phone Contact with Domain Contact

Not applicable

3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact

Not applicable

3.2.2.4.17 Phone Contact with DNS CAA Phone Contact

Not applicable

3.2.2.4.18 Agreed-Upon Change to Website v2

Confirming the Applicant's control over the FQDN by verifying that the Random Value is contained in the contents of a file.

1. The entire Random Value MUST NOT appear in the request used to retrieve the file, and
2. the CA MUST receive a successful HTTP response from the request (meaning a 2xx HTTP status code must be received).

The file containing the Random Value:

1. MUST be located on the Authorization Domain Name, and
2. MUST be located under the "%well-known/pki-validation" directory, and
3. MUST be retrieved via either the "http" or "https" scheme, and
4. MUST be accessed over port 80 (http) or 443 (https).

If the CA follows redirects, the following apply:

1. Redirects MUST be initiated at the HTTP protocol layer.
 - Redirects MUST be the result of a 301, 302, or 307 HTTP status code response, as defined in RFC 7231, Section 6.4, or a 308 HTTP status code response, as defined in RFC 7538, Section 3.
 - Redirects MUST be to the final value of the Location HTTP response header, as defined in RFC 7231, Section 7.1.2.
2. Redirects MUST be to resource URLs with either the "http" or "https" scheme.
3. Redirects MUST be to resource URLs accessed via port 80 (http) or 443 (https).

The CA MUST provide a Random Value unique to the certificate request. The Random Value MUST remain valid for use in a confirming response for no more than 25 days from its creation.

For Certificates issued on or after 2021-11-18, this method is not applicable for

validating Wildcard Domain Names.

3.2.2.4.19 Agreed-Upon Change to Website - ACME

Confirming the Applicant's control over a FQDN by validating domain control of the FQDN using the ACME HTTP Challenge method defined in Section 8.3 of RFC 8555. The following are additive requirements to RFC 8555.

1. The CA MUST receive a successful HTTP response from the request (meaning a 2xx HTTP status code must be received).
2. The CA MUST provide a Random Value unique to the certificate request. The Random Value MUST remain valid for use in a confirming response for no more than 25 days from its creation.
3. If the CA follows redirects, the following apply:
 1. Redirects MUST be initiated at the HTTP protocol layer.
 - Redirects MUST be the result of a 301, 302, or 307 HTTP status code response, as defined in RFC 7231, Section 6.4, or a 308 HTTP status code response, as defined in RFC 7538, Section 3.
 - Redirects MUST be to the final value of the Location HTTP response header, as defined in RFC 7231, Section 7.1.2.
 2. Redirects MUST be to resource URLs with either the "http" or "https" scheme.
 3. Redirects MUST be to resource URLs accessed via port 80 (http) or 443 (https).

This method is not applicable for validating Wildcard Domain Names.**3.2.2.4.20 TLS Using ALPN**

Not applicable

3.2.3 Authentication of Individual Identity

The CA does not issue any certificate to grant certification to any individual.

3.2.4 Non-Verified Subscriber Information

(1) Domain Validation

The CA stipulates no policies on non-verified information on Subscribers.

(2) Organization Validation

The CA stipulates no policies on non-verified information on Subscribers, however, and does not assure the accuracy of information described in the "Organizational Unit (organizational unit name)" (OU).

3.2.5 Validation of Authority

(1) Domain Validation

When issuing a certificate, the CA shall verify that the Subscriber is a registrant of the domain name to be described in the certificate or has been granted an exclusive right to use the domain name by the registrant.

(2) Organization Validation

The CA shall verify that an applicant for a certificate has the legitimate authority to apply for a certificate by making contact with a contact person that may be verified by any document, database, or other information source to be used for “3.2.2. Authentication of an Organization’s Identity and Domain Name” of this CP.

3.2.6 Criteria for Interoperation

A certificate for one-way mutual certification has been issued to the CA by Security Communication RootCA2, a Certification Authority operated by SECOM Trust Systems.

3.3 Identification and Authentication for Re-key Requests

The CA shall perform validate and authenticate the identity of any Subscriber at a rekey in the same manner as set forth in “3.2 Initial Identity Validation” of this CP.

3.4 Identification and Authentication for Revocation Request

The CA shall validate an identity in order to accept Revocation Request by check one of the following;

1. The Revocation Request from any Subscriber through the Designated Business Enterprise that has acted as an agent in the application for issuance of the certificate or use of services.
2. The certificate issued under ACME protocol and the Revocation Request is signed by private key of the account granted to the subscriber.
3. The certificate issued under ACME protocol and the Revocation Request is signed by private key of the certificate.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

(1) Domain Validation

A person who is a registrant of the domain name to be described in a certificate or has been granted an exclusive right to use the domain name by the registrant may apply for the certificate.

(2) Organization Validation

A person who is an individual having his/her address within Japan, or an organization having its head office or principal office, branch office or subdivision, place of business, or other equivalent permanent place to the foregoing within Japan, whether incorporated or unincorporated, may apply for the certificate.

4.1.2 Enrollment Process and Responsibilities

Each person who may apply for a certificate and intends to do so shall apply for the certificate after consenting to the provisions of the Terms and Conditions, this CP, and the CPS. Each person applying for a certificate must assure that the information provided in the Certificate Application submitted to the CA is accurate.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

The CA shall review application information by considering the information in the manner set forth in “3.2 Initial Identity Validation” of this CP.

4.2.2 Approval or Rejection of a Certificate Application

On approving any certificate application as a result of the review, the CA shall proceed to the issuance registration of the certificate.

If any certificate application is not complete, the CA shall reject the application and request the person who has submitted the application to submit an application again after correction or addition.

4.2.3 Time to Process Certificate Applications

After approving a certificate application, the CA shall proceed to the issuance registration of the certificate in a timely manner.

4.2.4 Check of CAA Records

In reviewing the application information, the CA shall check the CAA records in accordance with RFC 6844. The domain of the CA to be described in the CAA records shall be “jprs.jp.”

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

After completing a review of a certificate application, the CA shall register information that is based on the application information and necessary for the issuance of a certificate, on a CT log server operated by a third party and prescribed by the CA, and then issue the certificate. The information to be registered on the CT log server shall be as described in “7.1 Certificate Profile” of this CP.

4.3.2 Notification to Subscriber of Certificate Issuance

The CA shall notify a Subscriber of the issuance of a certificate by sending an e-mail to the Designated Business Enterprise or the Subscriber. However, if the certificate issued under ACME protocol, no notification sending an e-mail.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The Subscriber shall be deemed to have accepted the certificate at any of the following time;

1. When the Subscriber requests to get the certificate from the subscriber-only web page and the CA responses the Certificate.
2. When the subscriber requests to get the certificate under ACME protocol and the CA responses the Certificate. However, only for certificates issued under ACME protocol.
3. When the subscriber installs the certificate obtained by a method other than 1 and 2 into his/her/its server.

4.4.2 Publication of the Certificates by the CA

The CA does not publish certificates of Subscribers.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

The CA does not notify any third party (excluding Designated Business Enterprises) of the issuance of certificates.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Each Subscriber may use his/her/its certificate issued by the CA and the corresponding Private Key solely for encrypting information for server authentication and on communication pathways, and not for any other usage.

4.5.2 Relying Party Public Key and Certificate Usage

Relying Parties may verify the reliability of certificates issued by the CA by using such certificates. Relying Parties shall understand and consent to the provisions of this CP and the CPS before verifying the reliability of certificates issued by the CA and relying on the same.

4.6 Certificate Renewal

A “certificate renewal” means the issuance of a new certificate to a Subscriber without any change in his/her/its Public Key. When a Subscriber has his/her/its certificate renewed, the CA recommends that the Subscriber generate a new Key Pair.

4.6.1 Circumstances for Certificate Renewal

A certificate may be renewed without involving rekey when the certificate is about to expire.

4.6.2 Who May Request Renewal

The provisions of “4.1.1 Who Can Submit a Certificate Application” of this CP shall apply correspondingly.

4.6.3 Processing Certificate Renewal Requests

The provisions of “4.3.1 CA Actions during Certificate Issuance” of this CP shall apply correspondingly.

4.6.4 Notification of New Certificate Issuance to Subscriber

The provisions of “4.3.2 Notification to Subscriber of Certificate Issuance” of this CP shall apply correspondingly.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

The provisions of “4.4.1 Conduct Constituting Certificate Acceptance” of this CP shall apply correspondingly.

4.6.6 Publication of the Renewal Certificate by the CA

The provisions of “4.4.2 Publication of the Certificates by the CA” of this CP shall apply correspondingly.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

The provisions of “4.4.3 Notification of Certificate Issuance by the CA to Other Entities” of this CP shall apply correspondingly.

4.7 Certificate Re-key

A “certificate re-key” means the issuance of a new certificate to a Subscriber after generating a new Key Pair.

4.7.1 Circumstances for Certificate Re-key

A certificate may be renewed without involving re-key when the certificate is about to expire.

4.7.2 Who May Request Certification of a New Public Key

The provisions of “4.1.1 Who Can Submit a Certificate Application” of this CP shall apply correspondingly.

4.7.3 Processing Certificate Re-keying Requests

The provisions of “4.3.1 CA Actions during Certificate Issuance” of this CP shall apply correspondingly.

4.7.4 Notification of New Certificate Issuance to Subscriber

The provisions of “4.3.2 Notification to Subscriber of Certificate Issuance” of this CP shall apply correspondingly.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

The provisions of “4.4.1 Conduct Constituting Certificate Acceptance” of this CP shall apply correspondingly.

4.7.6 Publication of the Re-keyed Certificates by the CA

The provisions of “4.4.2 Publication of the Certificates by the CA” of this CP shall apply correspondingly.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

The provisions of “4.4.3 Notification of Certificate Issuance by the CA to Other Entities” of this CP shall apply correspondingly.

4.8 Certificate Modification

4.8.1 Circumstances for Certificate Modification

If a need arises to modify any registered information in a certificate (excluding the common name used in the certificate), the certificate shall be modified.

4.8.2 Who May Request Certificate Modification

The provisions of “4.1.1 Who Can Submit a Certificate Application” of this CP shall apply correspondingly.

4.8.3 Processing Certificate Modification Requests

The provisions of “4.3.1 CA Actions during Certificate Issuance” of this CP shall apply correspondingly.

4.8.4 Notification of New Certificate Issuance to Subscriber

The provisions of “4.3.2 Notification to Subscriber of Certificate Issuance” of this CP shall apply correspondingly.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

The provisions of “4.4.1 Conduct Constituting Certificate Acceptance” of this CP shall apply correspondingly.

4.8.6 Publication of the Modified Certificate by the CA

The provisions of “4.4.2 Publication of the Certificates by the CA” of this CP shall apply correspondingly.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

The provisions of “4.4.3 Notification of Certificate Issuance by the CA to Other Entities” of this CP shall apply correspondingly.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Certificate Revocation

If any one of the following events occurs, the Subscriber must apply to the CA to have the corresponding certificate revoked:

- the information described in the certificate has changed;
- the Private Key has been or may be compromised for any reason, including theft, loss, leakage, or unauthorized use thereof;
- any of the particulars described in the certificate or its purposes of use are incorrect;
- the Subscriber finds that an improper string has been designated for, or is included in, a value set in any information in the certificate (as set forth in “3.1.1 Types of Names” of this CP) (for Organization Validation only); or
- the Subscriber stops using the certificate.

If any of the following events occurs, the CA may revoke the certificate at the CA's

discretion:

- the Subscriber has not performed any of his/her/its obligations under this CP, the CPS, or any relevant agreement or law;
- the CA determines that the CA's Private Key has been or may be compromised;
- the CA learns that an improper string has been designated for, or is included in, a value set in any information in the certificate (as set forth in "3.1.1 Types of Names" of this CP), on the basis of reasonable evidence (for Organization Validation only);
- any other situation arises that the CA deems to necessitate revocation.

4.9.2 Who Can Request Revocation

The following can request the Revocation Request;

1. The Subscriber
2. Designated Business Enterprise that has acted as an agent in the application for issuance of the certificate or use of services.
3. Owner of the private key for the Certificate.

4.9.3 Procedures for Revocation Request

The CA SHALL accept the Revocation Request received in one of the following way, and revoke the certificate after verification the Revocation Request by section 3.4.

1. Request through Designated Business Enterprise
2. Request under ACME protocol

4.9.4 Revocation Request Grace Period
If someone who can request revocation determines that the Private Key has been or may be compromised, he/she/it must promptly file the Revocation Request of the certificate.

4.9.5 Time within Which the CA Shall Process the Revocation Request

Upon accepting a valid Revocation Request of a certificate, the CA shall promptly process the Revocation Request and reflect the relevant information in the certificate on the CRL.

4.9.6 Revocation Checking Requirement for Relying Parties

A URL in which the CRL is stored shall be described in a certificate to be issued by the CA. Before placing trust in and using a certificate issued by the CA, the Relying Party must verify the validity of the certificate by checking the CRL. CRLs do not contain information on certificates that have expired.

4.9.7 CRL Issuance Frequency

The CA SHALL update and reissue CRLs at least once every seven days, and the value

of the nextUpdate field MUST NOT be more than ten days beyond the value of the thisUpdate field.

4.9.8 Maximum Latency for CRLs

The CA shall forthwith reflect an issued CRL in the Repository.

4.9.9 On-line Revocation/Status Checking Availability

Information on the certificate status shall be provided online via the OCSP server.

4.9.10 On-line Revocation/Status Checking Requirements

Before placing trust and using a certificate issued by the CA, the Relying Party must verify the validity of the certificate. If any Relying Party does not confirm whether or not the revocation of the certificate has been registered by checking the CRL included in the Repository, the Relying Party shall check the information on the certificate status provided through the OCSP server.

4.9.11 Other Forms of Revocation Advertisements Available

Not applicable.

4.9.12 Special Requirements Regarding Key Compromise

If a compromise of any Private Key pertaining to a certificate issued by the CA is revealed, please notify via the following webform:

https://jprs.jp/pubcert/f_mail/

Please include either of the following information in your report.

- The compromised private key itself
- A CSR signed by the compromised private key

(A CSR must contain a string indicating that a private key has been compromised in the "CN" field. e.g. CN="This key is compromised")

The CA shall verify whether any of the certificates issued by the CA use the presented private key. Upon confirmation of a certificate that uses the presented private key, the CA shall revoke the certificate within 24 hours from the time of confirmation.

4.9.13 Circumstances for Suspension

Not applicable.

4.9.14 Who Can Request Suspension

Not applicable.

4.9.15 Procedures for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

Subscribers and Relying Parties may check information on the status of a certificate through the OCSP server.

4.10.2 Service Availability

The CA shall manage the OCSP server to allow Subscribers and Relying Parties to check information on the status of a certificate twenty-four (24) hours a day, three hundred sixty-five (365) days a year. However, the OCSP server may be temporarily unavailable at times for maintenance or other reasons.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription (Registration)

If a Subscriber ceases to use his/her/its certificate, or cancels the Services, the Subscriber shall request for revocation of his/her/its certificate. If a Subscriber fails to carry procedures for certificate renewal and his/her/its certificate expires, the certificate registration shall terminate.

However, the CA may treat a Subscriber who has been issued a certificate under ACME protocol differently from the above. Other details regarding the cancellation of the Service by the Subscriber are specified in the Term and Conditions.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

The CA does not escrow the Private Keys of Subscribers.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5. Facility, Management, and Operational Controls

5.1 Physical Security Controls

Stipulated in the CPS.

5.2 Procedural Controls

Stipulated in the CPS.

5.3 Personnel Controls

Stipulated in the CPS.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

Stipulated in the CPS.

5.4.2 Frequency of Processing Audit Log

Stipulated in the CPS.

5.4.3 Retention Period for Audit Log

Stipulated in the CPS. Audit Logs on the RA system shall be archived for at least seven (7) years.

5.4.4 Protection of Audit Log

Stipulated in the CPS.

5.4.5 Audit Logs Backup Procedure

Stipulated in the CPS.

5.4.6 Audit Log Collection System

Stipulated in the CPS.

5.4.7 Notification to Event-Causing Subject

Stipulated in the CPS.

5.4.8 Vulnerability Assessments

Stipulated in the CPS.

5.5 Records Archival

5.5.1 Types of Records Archived

The CA shall archive the following information in addition to the information prescribed

in “5.5 Records Archival” of the CPS:

- this CP;
- documents prepared under this CP stipulating the business operations of the Certification Authority;
- records and audit reports on the results of audits; and
- information on applications from Subscribers and the histories thereof.

5.5.2 Retention Period for Archive

Stipulated in the CPS. The CA shall archive the following information for at least seven (7) years:

- this CP;
- documents prepared under this CP stipulating the business operations of the Certification Authority;
- records and audit reports on the results of audits; and
- information on applications from Subscribers and the histories thereof.

5.5.3 Protection of Archive

Stipulated in the CPS.

5.5.4 Archive Backup Procedures

Stipulated in the CPS.

5.5.5 Requirements for Time-Stamping of Records

Stipulated in the CPS.

5.5.6 Archive Collection System

Stipulated in the CPS.

5.5.7 Procedures to Obtain and Verify Archive Information

Stipulated in the CPS.

5.6 Key Changeover

Before the validity period of a certificate relevant to the CA’s own Private Key becomes shorter than the maximum validity period of certificates issued to Subscribers, a new Private Key for the CA shall be generated and a certificate relevant thereto shall be issued. Once the new Private Key has been generated, the CA shall issue certificates and CRLs using the new Private Key.

5.7 Compromise and Disaster Recovery

Stipulated in the CPS.

5.8 CA or RA Termination

If the CA is required to suspend its operations as a Certification Authority or Registration Authority, the CA shall notify Subscribers to that effect in advance by any of the means set forth in “9.11 Individual Notices and Communications with Participants.”

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

“6.1.1 Generation of Key Pairs” of the CPS stipulates a policy on Private Keys of the CA.

6.1.2 Private Key Delivery to Subscriber

Each Subscriber’s Private Key shall be generated by the Subscriber himself/herself/itself. The CA does not generate or deliver the Private Keys of Subscribers to Subscribers.

6.1.3 Public Key Delivery to the Certificate Issuer

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

6.1.4 CA’ Public Key Delivery to Relying Parties

Relying Parties may obtain Public Keys of the CA by accessing the CA’s Repository.

6.1.5 Key Sizes

Key Pairs of the CA shall have a key length of 2048 bits in the RSA cryptosystem.

Key Pairs of Subscribers shall have a key length of 2048 bits in the RSA cryptosystem.

6.1.6 Public Key Parameters Generation and Quality Checking

Stipulated in the CPS. No policy is stipulated on the generation and quality inspection of the Public Key parameters of Subscribers.

6.1.7 Key Usage Purposes

The following table summarizes the usages of keys intended by the CA and by certificates issued by the CA :

Table 6.1 Key Usage Purposes

	the CA	Certificates issued by the CA
digitalSignature	—	yes
nonRepudiation	—	—
keyEncipherment	—	yes
dataEncipherment	—	—

keyAgreement	—	—
keyCertSign	yes	—
cRLSign	yes	—
encipherOnly	—	—
decipherOnly	—	—

6.2 Private Key Protection and Cryptographic Module Engineering Controls

Stipulated in the CPS.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archival

Stipulated in the CPS.

6.3.2 Certificate operational periods and key pair usage periods

The Validity period of the key pair and CA certificate of the CA is stipulated in the CPS. Subscriber Certificates issued on or after 1 September 2020 MUST NOT have a validity period greater than 398 days. Subscriber Certificates issued prior to 1 September 2020 have a validity period of 825 days or less.

6.4 Activation Data

Stipulated in the CPS.

6.5 Computer Security Controls

Stipulated in the CPS.

6.6 Life Cycle Technical Controls

Stipulated in the CPS.

6.7 Network Security Controls

Stipulated in the CPS.

6.8 Time Stamping

Stipulated in the CPS.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

7.1.1 Subscriber Certificate Profile

The profile of digital certificates to be issued by the CA shall be as described in the following table.

After registering the information necessary for issuing a certificate on the CT log server operated by a third party and prescribed by the CA, the CA shall issue a certificate compliant with the CT.

Table 7.1.1.1 (Deleted)

Table 7.1.1.2 Subscriber Certificate Profile (applicable to certificates issued on or after July 29, 2020)

Basic field		Description of setting	critical
Version		Version 3	-
Serial Number		An integral serial number to be assigned by the CA to the certificate	-
Signature Algorithm		sha256 with RSA Encryption	-
Issuer	Country	C=JP	-
	Organization	O=Japan Registry Services Co., Ltd.	-
	Common Name	(1) Domain Validation CN=JPRS Domain Validation Authority - G4 (2) Organization Validation CN=JPRS Organization Validation Authority - G4	-
Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-
	NotAfter	E.g.) 2009/3/1 00:00:00 GMT	-
Subject	Country	(1) Domain Validation No description (2) Organization Validation C=JP as the address of the organization or individual (country)	-
	State or Province	(1) Domain Validation No description	-

		(2) Organization Validation Address of the organization or individual (prefecture name) (mandatory)	
	Locality	(1) Domain Validation No description (2) Organization Validation Address of the organization or individual (city, town, or village name) (mandatory)	-
	Organization	(1) Domain Validation No description (2) Organization Validation Name of the Subscriber or the Subscriber's organization (mandatory)	-
	Organizational Unit	(1) Domain Validation No description (2) Organization Validation Business division name of the Subscriber (voluntary). However, this item will not be included in certificates issued on or after 18 November 2021. ● A string comprising symbols only or spaces only may not be designated, and any of the following strings may not be included: <ul style="list-style-type: none"> • any name, company name, trade name, or trademark that is likely to cause others to misconstrue that the relevant information is the information of any organization other than the applicant organization; • any string indicating a legal personality, such as “Co., Ltd”; • any string referring to a specific natural person; 	-

		<ul style="list-style-type: none"> • any string indicating an address; • any phone number; • any domain name or IP address; or • any string meaning “blank”, “not applicable” or the like (“null”, “N/A” or the like) 	
	Common Name	A host name used in the DNS of the server in which the certificate is scheduled to be installed (mandatory)	-
Subject Public Key Info		The subject’s Public Key (2048 bits)	-
Extended field		Description of setting	critical
KeyUsage		digitalSignature, keyEncipherment	y
ExtendedKeyUsage		TLS Web Server Authentication	n
Subject Alt Name		dNSName= name(s) of the server(s)	n
CertificatePolicies		[1] Certificate Policy 1.3.6.1.4.1.53827.1.1.4 CPS http://jprs.jp/pubcert/info/repository/ [2] Certificate Policy (1) Domain Validation 2.23.140.1.2.1 (2) Organization Validation 2.23.140.1.2.2	n
CRL Distribution Points		(1) Domain Validation http://repo.pubcert.jprs.jp/sppca/jprs/dvca_g4/fullcr1.crl (2) Organization Validation http://repo.pubcert.jprs.jp/sppca/jprs/ovca_g4/fullcr1.crl	n
Authority Information Access		[1] ocsf (1.3.6.1.5.5.7.48.1) (1) Domain Validation http://dv.g4.ocsf.pubcert.jprs.jp (2) Organization Validation http://ov.g4.ocsf.pubcert.jprs.jp [2] ca issuers (1.3.6.1.5.5.7.48.2)	n

	(1) Domain Validation http://repo.pubcert.jprs.jp/sppca/jprs/dvca_g4/JPRS_DVCA_G4_DER.cer (2) Organization Validation http://repo.pubcert.jprs.jp/sppca/jprs/ovca_g4/JPRS_OVCA_G4_DER.cer	
Authority Key Identifier	SHA-1 hash for the issuer's Public Key (160 bits)	n
Subject Key Identifier	SHA-1 hash for the subject's Public Key (160 bits)	n
Certificate Transparency Timestamp (*) (1.3.6.1.4.1.11129.2.4.2)	Value of SignedCertificateTimestampList	n

*: A Certificate Transparency Timestamp is not registered on the CT log server operated by a third party and prescribed by the CA at the time of certificate issuance. Other information in the profile of certificates shall be registered on the CT log server.

7.1.2 Subordinate CA Certificate Profile

The profile of intermediate certificates to be issued by the CA shall be as described in the following table:

Table 7.1.2.1 (Deleted)

Table 7.1.2.2 (Deleted)

Table 7.1.2.3 Subordinate CA Certificate Profile (applicable to certificates issued on or after July 29, 2020)

Basic field		Description of setting	critical
Version		Version 3	-
Serial Number		An integral serial number to be assigned by the CA to the certificate	-
Signature Algorithm		sha256 With RSA Encryption	-
Issuer	Country	C=JP	-
	Organization	O=SECOM Trust Systems CO.,LTD.	-
	Common Name	OU=Security Communication RootCA2	-
Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-
	NotAfter	E.g.) 2009/3/1 00:00:00 GMT	-

Subject	Country	C=JP	-
	Organization	O=Japan Registry Services Co., Ltd.	-
	Common Name	(1) Organization Validation CN=JPRS Organization Validation Authority - G4 (2) Domain Validation CN=JPRS Domain Validation Authority - G4	-
Subject Public Key Info		The subject's Public Key (2048 bits)	-
Extended field		Description of setting	critical
Authority Key Identifier		SHA-1 hash for the issuer's Public Key (160 bits)	n
Subject Key Identifier		SHA-1 hash for the subject's Public Key (160 bits)	n
KeyUsage		Certificate Signing Off-line CRL Signing CRL Signing (06)	y
CertificatePolicies		Certificate Policy 1.2.392.200091.100.901.4 CPS http://repository.secomtrust.net/SC-Root2/	N
Basic Constraints		Subject Type=CA Path Length Constraint=0	y
ExtendedKeyUsage		TLS Web Server Authentication	n
CRL Distribution Points		http://repository.secomtrust.net/SC-Root2/SCRoot2CRL.crl	n
Authority Information Access		[1] ocsp (1.3.6.1.5.5.7.48.1) http://scrootca2.ocsp.secomtrust.net [2] ca issuers (1.3.6.1.5.5.7.48.2) http://repository.secomtrust.net/SC-Root2/SCRoot2ca.cer	n

7.2 CRL Profile

The profile of CRLs to be issued by the CA shall be as described in the following table:

Table 7.2.1 (Deleted)

Table 7.2.2 CRL Profile (applicable to certificates issued on or after July 29, 2020)

Basic field		Description of setting	critical
Version		Version 2	-
Signature Algorithm		SHA256 with RSAEncryption	-
Issuer	Country	C=JP	-
	Organization	O= Japan Registry Services Co., Ltd.	-
	Common Name	(1) Domain Validation CN=JPRS Domain Validation Authority - G4 (2) Organization Validation CN=JPRS Organization Validation Authority – G4	-
This Update		E.g.) 2008/3/1 00:00:00 GMT	-
Next Update		E.g.) 2008/3/5 00:00:00 GMT	-
Revoked Certificate s	Serial Number	E.g.) 0123456789	-
	Revocation Date	E.g.) 2008/3/1 00:00:00 GMT	-
	Reason Code	Revocation Reason Code (*)	-
Extended field		Description of setting	critical
CRL Number		CRL number	n
Authority Key Identifier		SHA-1 hash for the issuer's Public Key (160 bits)	n

*: The “Reason Code” field is set one of the Revocation Reason code specified in the following table. If the Revocation Reason Code is “#0 unspecified”, the “Reason Code” field does not appear in the CRL profile.

Table 7.2.3 Revocation Reason Code

Revocation Reason Code	Circumstances for setting this Revocation Reason Code
#0 unspecified	When the reason codes below do not apply to the revocation request.
#1 keyCompromise	When the Subscriber have reasons to believe that the private key of their certificate has been or may be compromised,
#3 affiliationChanged	When the name of subscriber's organization or other organizational information in the certificate has

	changed.
#4 superseded	When the Subscriber requests a new certificate to replace their existing certificate.
#5 cessationOfOperation	When the Subscriber no longer owns all of the domain names in the certificate or when they will no longer be using the certificate because they are discontinuing their website.
#9 privilegeWithdrawn	When the Subscriber has not upheld their material obligations under the Terms and Conditions.

7.3 OCSP Profile

The profile of the OCSP to be issued by the CA shall be as described in the following table:

Table 7.3.1 (Deleted)

Table 7.3.2 OCSP Profile (Applicable to certificates issued on or after July 29, 2020)

Basic field		Description of setting	critical
Version		Version 3	-
Serial Number		An integral serial number to be assigned by the CA	-
Signature Algorithm		sha256 With RSA Encryption	-
Issuer	Country	C=JP	-
	Organization	O= Japan Registry Services Co., Ltd.	-
	Common Name	(1) Domain Validation CN=JPRS Domain Validation Authority - G4 (2) Organization Validation CN=JPRS Organization Validation Authority – G4	-
Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-
	NotAfter	E.g.) 2008/3/5 00:00:00 GMT	-
Subject	Country	C=JP (fixed value)	-
	Organization	Japan Registry Services Co., Ltd. (fixed value)	-
	Common Name	Name of the OCSP server (mandatory)	-
Subject Public Key Info		The subject's Public Key (2048 bits)	-

Extended field	Description of setting	critical
Authority Key Identifier	SHA-1 hash for the issuer's Public Key (160 bits)	n
Subject Key Identifier	SHA-1 hash for the subject's Public Key (160 bits)	n
KeyUsage	digitalSignature	y
CertificatePolicies (*)	Certificate Policy 1.3.6.1.4.1.53827.1.1.4 CPS http://jprs.jp/pubcert/info/repository/	n
ExtendedKeyUsage	OCSPSigning	n
OCSP No Check	null	n

*: The "CertificatePolicies" field appears in the OCSP profile if the CA required.
However, this field does not appear in the OCSP profile on or after 15 September 2023.

7.3.1 Version Number(s)

The CA shall apply OCSP Version 1.

7.3.2 OCSP Extensions

No stipulation.

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 CP and the 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.

8.4 Topics Covered by Assessment

Audits shall be performed mainly to verify whether or not the CA is operated in compliance with this CP and the 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 CP, the CPS, and the Baseline Requirements through random sampling of certificates under the requirements stipulated in the

Baseline Requirements.

9. Other Business and Legal Matters

9.1 Fees

To be separately stipulated.

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

Stipulated in the CPS.

9.3.2 Information not within the Scope of Confidential Information

Stipulated in the CPS.

9.3.3 Responsibility to Protect Confidential Information

Stipulated in the CPS.

9.4 Privacy of Personal Information

Stipulated in the CPS.

9.5 Intellectual Property Rights

Unless separately agreed, all intellectual property rights pertaining to the following information shall belong to JPRS:

- certificates and site seals issued by the CA, as well as information on certificate revocation;
- this CP, the CPS, and related documents;
- Public Keys and Private Keys of the CA; and
- software provided by JPRS.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

The CA shall bear the following obligations in performing its business operations as the CA:

- securely generate and manage the CA's Private Keys;
- accurately manage certificate issuance and revocation based on applications from the RA;

- monitor and operate the CA's system at work; and
- issue and publish the CRLs.

9.6.2 RA Representations and Warranties

The CA shall bear the following obligations in performing its business operations as an RA:

- install registration terminals in a secure environment and operate them;
- accurately communicate information to the CA in processing applications for certificate issuance and revocation;
- promptly communicate information to the CA during operating hours in processing applications for certificate revocation; and
- maintain and administer the Repository.

9.6.3 Subscriber Representations and Warranties

Each Subscriber warrants that he/she/it will comply with the provisions of the Terms and Conditions and this CP. If any Subscriber fails to comply with any provision of the Terms and Conditions or this CP, the Subscriber shall assume all responsibilities therefor.

9.6.4 Relying Party Representations and Warranties

Each Relying Party warrants that he/she/it will comply with the provisions of this CP. If any Relying Party fails to comply with any provision of this CP, the Relying Party shall assume all responsibilities therefor.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimer of Warranties

The CA is not liable for any indirect, special, incidental, or consequential damage arising in connection with any of the warranties stipulated in “9.6.1 CA Representations and Warranties” of this CP, or for lost profits, loss of data, or any other indirect or consequential damage whatsoever.

9.8 Limitations of Liability

The CA is not liable for the provisions of “9.6.1 CA Representations and Warranties” of this CP if damage falling under any of the following occurs:

- any or all damage arising from any unlawful conduct, unauthorized use, negligence, or any other cause not attributable to the CA;
- any damage resulting from a failure of a Subscriber to perform any of his/her/its

obligations;

- any or all damage arising from any cause attributable to a Subscriber's system;
- any damage arising from any defect or malfunction, or operation, of the hardware or software of the CA or a Subscriber;
- any damage caused by any information published in a certificate or the CRL, for any reason not attributable to the CA;
- any or all damage incurred by a failure in normal communication caused by any reason not attributable to the CA;
- any or all damage arising in connection with the use of a certificate, such as business debts;
- any damage caused by an improvement, beyond expectations at this point in time, in the cryptographic algorithm decoding capabilities of hardware or software;
- any or all damage caused by the suspension of the CA's business operations due to a force majeure event, including, but not limited to, any act of God, earthquake, volcanic eruption, fire, tsunami, flood disaster, lightning strike, war, civil commotion or terrorism; or
- any or all damage arising concomitantly with, or in connection with, registration and publication on the CT log server of information necessary for certificate issuance.

9.9 Indemnities

Each Subscriber shall become liable to indemnify and hold harmless the CA or any organizations or other entities related to the CA, upon applying for, receiving, and trusting certificates issued by the CA. The events to be covered by the foregoing liabilities include any loss, damage, lawsuit, mistake, omission, act, delay of, or failure in performance, or any other event that may incur cost burdens of any kind. The Terms and Conditions stipulate a policy on indemnification to Subscribers for damage.

9.10 Term and Termination

9.10.1 Term

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

9.10.2 Termination

This CP 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 an agreement on use or the like between a Subscriber and the CA, or termination of the CA itself, any provisions of this CP that should survive such termination, by the nature thereof, shall continue to apply to Subscribers, Relying Parties, and the CA, regardless of the reason of 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 CP 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 CP, the CA shall promptly publish the amended version of this CP, 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

If any party, for the purpose of resolving a dispute over the use of a certificate, seeks to file a lawsuit, refer the dispute to arbitration, or take any other legal action against the CA, such party shall notify the CA to that effect in advance. The Tokyo District Court shall have the agreed exclusive jurisdiction over all disputes involving the Services in the first instance.

9.14 Governing Law

Regardless of the respective addresses of the CA and Subscribers, the laws of Japan shall apply to any dispute over the interpretation or validity of this CP, or the use of a certificate.

9.15 Compliance with Applicable Laws

No stipulation.

9.16 Miscellaneous Provisions

Stipulated in the CPS.

9.17 Other Provisions

Not applicable.