JPRS CA Certificate Policy/Certification Practice Statement Version 2.00

August 22, 2025

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
1.51	2024.06.05	Revision of “1.6 Definitions and Acronyms”
1.52	2024.08.26	Revision of “5.4 Audit Logging Procedures”
1.53	2024.11.07	Revision of “ 6.1.1 Key Pair Generation”, “ 8.4 Topics Covered by Assessment”
1.54	2025.05.20	Revision of “5.4.1 Types of Events Recorded”, “8.7 Self-Audits”
2.00	2025.08.22	Integrated CPS Version 1.54 and CP Version 3.80 and revised as CP/CPS Version 2.00. Revision of description to clarify compliance with Baseline Requirements.

Table of Contents

1. Introduction

1.1 Overview

This document, the JPRS CA Certificate Policy/Certification Practice Statement (hereinafter referred to as "this CP/CPS"), 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"), and various procedures regarding the operation and maintenance of the CA, for the purpose of providing the JPRS Digital Certificate Issuance Services (hereinafter referred to as the "Services").

A certificate for one-way and mutual certification has been issued to the CA by Security Communication RootCA2, Security Communication ECC RootCA1 or SECOM TLS RSA Root CA 2024, 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/CPS in light of his/her/its own purposes of use, and then to consent to the Terms and Conditions and this CP/CPS.

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

If any inconsistency is found among the provisions of this CP/CPS and the Terms and Conditions, the provisions of the Terms and Conditions shall prevail over those of this CP/CPS. Also, if any inconsistency is found among the provisions of the Japanese version and the English version of this CP/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 CP/CPS , the Terms and Conditions, and the related documents) and Baseline Requirements, Baseline Requirements take precedence over these documents.

This CP/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 CA or certification operations in terms of technologies, operation or services, this CP/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 CP/CPS is the "JPRS CA Certificate Policy/ Certification Practice Statement."

The following is the Object Identifier (hereinafter referred to as "OID") assigned by the CA under this CP/CPS used when issuing certificates:

Name	OID
JPRS CA Certificate Policy	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 Subscribers

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

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" of this CP/CPS, and may not be used for any other purposes.

1.5 Policy Administration

1.5.1 Organization Administering the Document

This CP/CPS shall be maintained and administered by the CA.

1.5.2 Contact Information

Inquiries concerning this CP/CPS should be directed to:
Contact: Inquiries contact office, Japan Registry Services Co., Ltd.

Address: Chiyoda First Bldg. East, 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 CPS Suitability as Policy

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

1.5.4 Approval Procedures

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

1.6 Definitions and Acronyms

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.

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.

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 8659.

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.

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.

DNS TXT Record Email Contact

The email address included in the TXT resource record in the DNS zone of the FQDN prefixed with the "_validation-contactemail" label, as defined in Appendix A.2.1 of Baseline Requirements.

ECDSA（Elliptic Curve Digital Signature Algorithm）

"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.

FQDN（Fully-Qualified Domain Name）

A Domain Name that includes the Domain Labels of all superior nodes in the Internet Domain Name System.

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.

Linting

A process in which the content of digitally signed data such as a Precertificate [RFC 6962], Certificate, Certificate Revocation List, or OCSP response, or data-to-be-signed object such as a tbsCertificate (as described in RFC 5280, Section 4.1.1.1) is checked for conformance with the profiles and requirements defined in these Requirements.

Multi-Perspective Issuance Corroboration (MPIC)

A process by which the determinations made during domain validation and CAA checking by the Primary Network Perspective are corroborated by other Network Perspectives before Certificate issuance.

Network Perspective

Related to Multi-Perspective Issuance Corroboration. A system (e.g., a cloud-hosted server instance) or collection of network components (e.g., a VPN and corresponding infrastructure) for sending outbound Internet traffic associated with a domain control validation method and/or CAA check. The location of a Network Perspective is determined by the point where unencapsulated outbound Internet traffic is typically first handed off to the network infrastructure providing Internet connectivity to that perspective.

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.

Primary Network Perspective

The Network Perspective used by the CA to make the determination of 1) the CA’s authority to issue a Certificate for the requested domain(s) or IP address(es) and 2) the Applicant’s authority and/or domain authorization or control of the requested domain(s) or IP address(es).

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.

Random Value

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

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.

Wildcard Certificate
A Certificate containing at least one Wildcard Domain Name in the Subject Alternative Names in the Certificate.

Wildcard Domain Name
A string starting with "*." (U+002A ASTERISK, U+002E FULL STOP) immediately followed by a Fully-Qualified Domain Name.

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

2.3 Time or Frequency of Publication

This CP/CPS shall be revised at least once every 365 days and published on the Repository as revised. The CA describes to the CP/CPS in detail how the CA implements the latest version of Baseline Requirements.

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

The CA SHALL inspect any document relied upon under this Section for alteration or falsification.

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 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.

The CA doesn’t issue certificates if "RFC 7686 - The ".onion" Special-Use Domain Name" is included in the certificates.

The CA SHALL maintain a record of which domain validation method, including relevant BR version number, they used to validate every domain.

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.

For certificates issued on or after 2025-7-10, this method will no longer be applicable.

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 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.

The CA performing validations using this method MUST implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. To count as corroborating, a Network Perspective MUST observe the same Random Value as the Primary Network Perspective.

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 Value

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 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

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 a DNS TXT Record Email Contact for the Authorization Domain Name selected to validate the FQDN.

Each email MAY confirm control of multiple FQDNs, provided that each email address is DNS TXT Record Email Contact for each Authorization Domain Name being validated. The same email MAY be sent to multiple recipients as long as all recipients are DNS TXT Record Email Contacts for each Authorization Domain Name being validated.

The Random Value SHALL be unique in each email. The email MAY be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient(s) SHALL remain unchanged. The Random Value SHALL remain valid for use in a confirming response for no more than 25 days from its creation.

This method will be applicable for certificates issued on or after 2025-5-29.

The CA performing validations using this method MUST implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. To count as corroborating, a Network Perspective MUST observe the same selected contact address used for domain validation as the Primary Network Perspective.

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.

Except for Onion Domain Names, the CA performing validations using this method MUST implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. To count as corroborating, a Network Perspective MUST observe the same Random Value as the Primary Network Perspective.

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.
Except for Onion Domain Names, the CA performing validations using this method MUST implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. To count as corroborating, a Network Perspective MUST observe the same Random Value as the Primary Network Perspective.

3.2.2.4.20 TLS Using ALPN

Not applicable

3.2.2.4.21 DNS Labeled with Account ID - ACME

Not applicable

3.2.2.5 Authentication for an IP Address

The CA does not issue any certificate to grant certification to any IP Address.

3.2.2.6 Wildcard Domain Validation

Before issuing a Wildcard Certificate, the CA MUST establish and follow a documented procedure that determines if the FQDN portion of any Wildcard Domain Name in the Certificate is “registry-controlled” or is a “public suffix” (e.g. “*.com”, “*.co.uk”, see RFC 6454 Section 8.2 for further explanation).

If the FQDN portion of any Wildcard Domain Name is "registry-controlled" or is a "public suffix", CAs MUST refuse issuance unless the Applicant proves its rightful control of the entire Domain Namespace. (e.g. CAs MUST NOT issue "*.co.uk" or "*.local", but MAY issue "*.example.com" to Example Co.).

Determination of what is "registry-controlled" versus the registerable portion of a Country Code Top-Level Domain Namespace is accordance with Baseline Requirements.

3.2.2.7 Data Source Accuracy

Prior to using any data source as a Reliable Data Source, the CA SHALL evaluate the source for its reliability, accuracy, and resistance to alteration or falsification. The CA considers the following during its evaluation:

1. The age of the information provided,
2. The frequency of updates to the information source,
3. The data provider and purpose of the data collection,
4. The public accessibility of the data availability, and
5. The relative difficulty in falsifying or altering the data.

3.2.2.8 CAA Records

As part of the Certificate issuance process, the CA MUST retrieve and process CAA records in accordance with RFC 8659 for each dNSName in the subjectAltName extension that does not contain an Onion Domain Name. If the CA issues, they MUST do so within the TTL of the CAA record, or 8 hours, whichever is greater.

Some methods relied upon for validating the Applicant's ownership or control of the subject domain(s) (see Section 3.2.2.4 of this CP/CPS) to be listed in a certificate require CAA records to be retrieved and processed from additional remote Network Perspectives before Certificate issuance (see Section 3.2.2.9 of this CP/CPS). To corroborate the Primary Network Perspective, a remote Network Perspective's CAA check response MUST be interpreted as permission to issue, regardless of whether the responses from both Perspectives are byte-for-byte identical. Additionally, the CA MAY consider the response from a remote Network Perspective as corroborating if one or both of the Perspectives experience an acceptable CAA record lookup failure, as defined in this section.

When processing CAA records, the CA MUST process the issue, issuewild, and iodef property tags as specified in RFC 8659, although the CA does not act on the contents of the iodef property tag. Where are additional property tags are supported, the CA MUST NOT conflict with or supersede the mandatory property tags set out in Baseline Requirements.

The CA MUST respect the critical flag and not issue a certificate if they encounter an unrecognized property tag with this flag set.

The CA is permitted to treat a record lookup failure as permission to issue if:

- the failure is outside the CA's infrastructure; and
- the lookup has been retried at least once; and
- the domain's zone does not have a DNSSEC validation chain to the ICANN root.

The CA shall log any actions taken as part of its processing practices.

3.2.2.9 Multi-Perspective Issuance Corroboration

On or after 2025-3-15, the CA implements Multi-Perspective Issuance Corroboration in accordance with section 3.2.2.9 of the Baseline Requirements.

Before Certificate issuance, the CA will corroborate the following determinations made by the Primary Network Perspective from multiple remote Network Perspectives:

- the presence of the expected 1) Random Value, 2) Request Token, 3) Contact Address as specified in this CP/CPS “3.2.2.4 Domain Authentication”
- the CA’s authority to issue to the requested domain(s), as specified in this CP/CPS “3.2.2.8 CAA Records”

The "Quorum Requirements" Table describes quorum requirements related to Multi-Perspective Issuance Corroboration. If the CA does NOT rely on the same set of Network Perspectives for both Domain Authorization or Control and CAA Record checks, the quorum requirements MUST be met for both sets of Network Perspectives (i.e.,the Domain Authorization or Control set and the CAA record check set). Network Perspectives are considered distinct when the straight-line distance between them is at least 500 km. Network Perspectives are considered "remote" when they are distinct from the Primary Network Perspective and the other Network Perspectives represented in a quorum.

The CA MAY reuse corroborating evidence for CAA record quorum compliance for a maximum of 398 days. After issuing a Certificate to a domain, remote Network Perspectives MAY omit retrieving and processing CAA records for the same domain or its subdomains in subsequent Certificate requests from the same Applicant for up to a maximum of 398 days.

Table 3.2.2.9-1 Quorum Requirements

# of Distinct Remote Network Perspectives Used	# of Allowed non-Corroborations

2-5	1
6+	2

Phased Implementation Timeline:

- On or after 2025-3-15, the CA implements Multi-Perspective Issuance Corroboration using at least two (2) remote Network Perspectives. The CA MAY proceed with certificate issuance if the number of remote Network Perspectives that do not corroborate the determinations made by the Primary Network Perspective ("non-corroborations") is greater than allowed in the Quorum Requirements table.

- On or after 2025-09-15, the CA MUST implement Multi-Perspective Issuance Corroboration using at least five (5) remote Network Perspectives. The CA MUST ensure that the requirements defined in the Quorum Requirements Table are satisfied, and the remote Network Perspectives that corroborate the Primary Network Perspective fall within the service regions of at least two (2) distinct Regional Internet Registries. If the requirements are not satisfied, then the CA MUST NOT proceed with issuance of the Certificate.

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.

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/CPS.

3.2.6 Criteria for Interoperation

A certificate for one-way mutual certification has been issued to the CA by Security Communication RootCA2, Security Communication ECC RootCA1 or SECOM TLS RSA Root CA 2024, a Certification Authority operated by SECOM Trust Systems.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

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/CPS.

3.3.2 Identification and Authentication for Re-key after Revocation

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/CPS.

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 a sole proprietor 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/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/CPS.

The certificate request MAY include all factual information about the Applicant to be included in the Certificate, and such additional information as is necessary for the CA to obtain from the Applicant in order to comply with these Requirements and this CP/CPS. In cases where the certificate request does not contain all the necessary information about the Applicant, the CA SHALL obtain the remaining information from the Applicant or, having obtained it from a reliable, independent, third-party data source, confirm it with the Applicant. The CA SHALL establish and follow a documented procedure for verifying all data requested for inclusion in the Certificate by the Applicant.

Applicant information MUST include, but not be limited to, at least one Fully-Qualified Domain Name or IP address to be included in the Certificate's subjectAltName extension.

Section 6.3.2 of this CP/CPS limits the validity period of Subscriber Certificates.
The CA MAY use the documents and data provided in Section 3.2 of this CP/CPS to verify certificate information, or may reuse previous validations themselves, provided that the CA obtained the data or document from a source specified under Section 3.2 of this CP/CPS or completed the validation itself no more than 825 days prior to issuing the Certificate.

For validation of Domain Names according to Section 3.2.2.4 of this CP/CPS, any data, document, or completed validation used MUST be obtained no more than 398 days prior to issuing the Certificate.
In no case may a prior validation be reused if any data or document used in the prior validation was obtained more than the maximum time permitted for reuse of the data or document prior to issuing the Certificate.

After the change to any validation method specified in the Baseline Requirements, the CA may continue to reuse validation data or documents collected prior to the change, or the validation itself, for the period stated in this section unless otherwise specifically provided in a ballot.

The CA SHALL develop, maintain, and implement documented procedures that identify and require additional verification activity for High Risk Certificate Requests prior to the Certificate's approval, as reasonably necessary to ensure that such requests are properly verified under these Requirements.

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 8659. The domain name of the CA to be described in the CAA records shall be “jprs.jp” or “acme.jprs.jp”.

The Certificate Subscribers who want to grant the authority to issue certificates to the FQDN must include one of the following domain names in the property "issue" or “issuewild” of the CAA record for each DNS zone.

- jprs.jp (for certificates issued without using the ACME protocol)
- acme.jprs.jp (for certificates issued using the ACME protocol)

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/CPS.

4.3.1.1 Manual authorization of certificate issuance for Root CAs

No stipulation.

4.3.1.2 Linting of to-be-signed Certificate content

The CA confirms whether the certificate to be issued technically conforms to Baseline Requirements for some items by the pre-certificate linting function and refuses to issue if it does not meet the requirements.

4.3.1.3 Linting of issued Certificates

The CA MAY use a Linting process to test each issued Certificate.

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/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/CPS shall apply correspondingly.

4.6.3 Processing Certificate Renewal Requests

The provisions of "4.3.1 CA Actions during Certificate Issuance" of this CP/CPS 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/CPS 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/CPS 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/CPS 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/CPS 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/CPS 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/CPS 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/CPS 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/CPS 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/CPS 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/CPS 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/CPS shall apply correspondingly.

4.8.3 Processing Certificate Modification Requests

The provisions of “4.3.1 CA Actions during Certificate Issuance” of this CP/CPS 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/CPS 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/CPS 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/CPS 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/CPS 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/CPS) (for Organization Validation only); or
- the Subscriber stops using the certificate.

The CA SHALL revoke a Certificate within 24 hours and use the corresponding CRLReason if one or more of the following occurs:

1. The Subscriber requests in writing, without specifying a CRLreason, that the CA revoke the Certificate (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL);
2. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization (CRLReason #9, privilegeWithdrawn);
3. The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise (CRLReason #1, keyCompromise);
4. The CA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate , including but not limited to those identified in the Baseline Requirements Section 6.1.1.3(5), and “6.1.1 Key Pair Generation” of this CP/CPS (CRLReason #1, keyCompromise);
5. The CA obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon (CRLReason #4, superseded).

The CA SHOULD revoke a certificate within 24 hours and MUST revoke a Certificate within 5 days and use the corresponding CRLReason if one or more of the following occurs:

6. The Certificate no longer complies with the requirements of Section 6.1.5 and Section 6.1.6 of Baseline Requirements (CRLReason #4, superseded);
7. The CA obtains evidence that the Certificate was misused (CRLReason #9, privilegeWithdrawn);
8. The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use (CRLReason #9, privilegeWithdrawn);
9. The CA is made aware of any circumstance indicating that use of a FQDN in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name) (CRLReason #5, cessationOfOperation);
10. The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate FQDN (CRLReason #9, privilegeWithdrawn);
11. The CA is made aware of a material change in the information contained in the Certificate (CRLReason #9, privilegeWithdrawn);
12. The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's CP/ CPS (CRLReason #4, superseded);
13. The CA determines or is made aware that any of the information appearing in the Certificate is inaccurate (CRLReason #9, privilegeWithdrawn);
14. The CA's right to issue Certificates under Baseline Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL);
15. Revocation is required by this CP/CPS for a reason that is not otherwise required to be specified by this section 4.9.1.1 of Baseline Requirements (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL); or
16. The CA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed (CRLReason #1, keyCompromise).

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. The CA SHALL maintain a continuous 24x7 ability to accept and respond to revocation requests and Certificate Problem Reports.

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. Within 24 hours after receiving a Certificate Problem Report, the CA SHALL investigate the facts and circumstances related to a Certificate Problem Report and provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report.

After reviewing the facts and circumstances, the CA SHALL work with the Subscriber and any entity reporting the Certificate Problem Report or other revocation-related notice to establish whether or not the certificate will be revoked, and if so, a date which the CA will revoke the certificate. The period from receipt of the Certificate Problem Report or revocation-related notice to published revocation MUST NOT exceed the time frame set forth in Section 4.9.1.1 of this CP/CPS.

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

The validity interval of an OCSP response is the difference in time between the thisUpdate and nextUpdate field, inclusive. For purposes of computing differences, a difference of 3,600 seconds shall be equal to one hour, and a difference of 86,400 seconds shall be equal to one day, ignoring leap-seconds.

A certificate serial is "assigned" if:

- a Certificate or Precertificate [RFC 6962] with that serial number has been issued by the Issuing CA; or
- a Precertificate with that serial number has been issued by a Precertificate Signing Certificate, as defined in Section 7.1.2.4 of the Baseline Requirements, associated with the Issuing CA.

A certificate serial is "unassigned" if it is not "assigned".

The following SHALL apply for communicating the status of Certificates and Precertificates which include an Authority Information Access extension with an id-ad-ocsp accessMethod.

OCSP responders operated by the CA SHALL support the HTTP GET method, as described in RFC 6960 and/or RFC 5019. The CA MAY process the Nonce extension (1.3.6.1.5.5.7.48.1.2) in accordance with RFC 8954.

For the status of a Subscriber Certificate or its corresponding Precertificate:

- Effective 2025-01-15, an authoritative OCSP response MUST be available (i.e. the responder MUST NOT respond with the "unknown" status) starting no more than 15 minutes after the Certificate or Precertificate is first published or otherwise made available.
- For OCSP responses with validity intervals less than sixteen hours, the CA SHALL provide an updated OCSP response prior to one-half of the validity period before the nextUpdate.

- For OCSP responses with validity intervals greater than or equal to sixteen hours, the CA SHALL provide an updated OCSP response at least eight hours prior to the nextUpdate, and no later than four days after the thisUpdate.

For the status of a Subordinate CA Certificate, the CA SHALL provide an updated OCSP response at least every twelve months, and within 24 hours after revoking the Certificate.

The following SHALL apply for communicating the status of *all* Certificates for which an OCSP responder is willing or required to respond.

OCSP responses MUST conform to RFC 6960 and/or RFC 5019. OCSP responses MUST either:

1. be signed by the CA that issued the Certificates whose revocation status is being checked, or
2. be signed by an OCSP Responder which complies with the OCSP Responder Certificate Profile in Section 7.1.2.8.

OCSP responses for Subscriber Certificates MUST have a validity interval greater than or equal to eight hours and less than or equal to ten days.

If the OCSP responder receives a request for the status of a certificate serial number that is "unassigned", then the responder SHOULD NOT respond with a "good" status. If the OCSP responder is for a CA that is not Technically Constrained in line with Section 7.1.2.3 or Section 7.1.2.5 of the Baseline Requirements, the responder MUST NOT respond with a "good" status for such requests.

4.9.10 On-line Revocation/Status Checking Requirements

No Stipulation.

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.
Revocation entries on a CRL or OCSP Response MUST NOT be removed until after the Expiry Date of the revoked Certificate.

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.
The CA SHALL operate and maintain its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

The CA SHALL maintain an online 24x7 Repository that application software can use to automatically check the current status of all unexpired Certificates issued by the CA.

The CA SHALL maintain a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint.

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 Terms 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

The CA/Browser Forum's "Network and Certificate System Security Requirements" 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 CP/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 CP/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 CP/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 CP/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 CP/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/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 CP/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 CP/CPS "5.3.3 Training Requirements" and this CP/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 ;
    6. Signing of OCSP Responses; and
    7. 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 this CP/CPS;

    3. Approval and rejection of certificate requests;
    4. Issuance of Certificates;
    5. Generation of Certificate Revocation Lists.; and
    6. Signing of OCSP Responses.
    7. Multi-Perspective Issuance Corroboration attempts from each Network Perspective, minimally recording the following information:
        a. an identifier that uniquely identifies the Network Perspective used;
        b. the attempted domain name and
        c. the result of the attempt (e.g., "domain validation pass/fail", "CAA permission/prohibition").
    8. Multi-Perspective Issuance Corroboration quorum results for each attempted domain name represented in a Certificate request.
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. Relevant router and firewall 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.

5.4.1.1 Router and firewall activities logs

Logging of router and firewall activities necessary to meet the requirements of this CP/CPS "5.4.1 Types of Events Recorded", Subsection 3.6 MUST at a minimum include:

1. Successful and unsuccessful login attempts to routers and firewalls; and
2. Logging of all administrative actions performed on routers and firewalls, including configuration changes, firmware updates, and access control modifications; and
3. Logging of all changes made to firewall rules, including additions, modifications, and deletions; and
4. Logging of all system events and errors, including hardware failures, software crashes, and system restarts.

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 CP/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 CP/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 CP/CPS "5.4.1 Types of Events Recorded") after the event occurred.

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

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 CP/CPS:

- issued certificates and CRLs;
- processing history related to CRL issuance;
- this CP/CPS;
- documents prepared under this CP/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 CP/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 CP/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

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

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.

Beginning 2025-09-01, the CA shall prepare and maintain comprehensive and actionable plans to address mass revocation events in accordance with the provisions of the Mozilla Root Store Policy.

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

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" of this CP/CPS.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

This paragraph stipulates policies on the management of the keys of Subscribers, other persons involved and the CA's keys.

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/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/CPS. The key pair of the 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 this CP/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/CPS "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 notified that the Applicant's Private Key has suffered a Key Compromise using the CA's procedure for revocation request as described in the CP/CPS "4.9.3 Procedure for Revocation Request" and the CP/CPS "4.9.12 Special Requirements Regarding Key Compromise".
5. The Public Key corresponds to an industry-demonstrated weak Private Key. For requests submitted on or after November 15, 2024, at least the following precautions SHALL be implemented by the CA:
    1. In the case of Debian weak keys vulnerability (https://wiki.debian.org/SSLkeys), the CA SHALL reject all keys found at https://github.com/cabforum/Debianweak-keys/ for each key type (e.g. RSA, ECDSA) and size listed in the repository. For all other keys meeting the requirements of this CP/CPS "6.1.5 Key Sizes", with the exception of RSA key sizes greater than 8192 bits, the CA SHALL reject Debian weak keys.
    2. In the case of ROCA vulnerability, the CA SHALL reject keys identified by the tools available at https://github.com/crocs-muni/roca or equivalent.
    3. In the case of Close Primes vulnerability (https://fermatattack.secvuln.info/), the CA SHALL reject weak keys which can be factored within 100 rounds using Fermat's factorization method.

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 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

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

6.1.5 Key Sizes

When issuing a TLS server certificate that complies with Baseline Requirements, the following confirmation need to be done:

For RSA key pairs the CA SHALL:

- Ensure that the modulus size, when encoded, is at least 2048 bits, and;
- Ensure that the modulus size, in bits, is evenly divisible by 8.

For ECDSA key pairs the CA SHALL:

- Ensure that the key represents a valid point on the NIST P-256 or NIST P-384 elliptic curve.

No other algorithms or key sizes are permitted.

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]
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 (except for certificates issued by using ECDSA key)

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

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 CP/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 CP/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.

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.

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 CP/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

The CA SHALL meet the technical requirements set forth in Section 2.2 - Publication of Information, Section 6.1.5 - Key Sizes, and Section 6.1.6 - Public Key Parameters Generation and Quality Checking of this CP/CPS.

The CA SHALL generate non-sequential Certificate serial numbers greater than zero (0) and less than 2^159 containing at least 64 bits of output from a CSPRNG.

Certificates issued by the CA conform to RFC 5280, the profile of which are indicated in the tables below.

Table 7.1-1 Subscriber Certificate Profile (applicable to certificates issued by JPRS Domain Validation Authority – G4 or JPRS Organization Validation Authority – G4)

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 Subscriber (country)	-
	State or Province	(1) Domain Validation No description	-

		(2) Organization Validation Address of the Subscriber (prefecture name) (mandatory)	
	Locality	(1) Domain Validation No description (2) Organization Validation Address of the Subscriber (city, town, or village name) (mandatory)	-
	Organization	(1) Domain Validation No description (2) Organization Validation Name of the Subscriber (mandatory)	-
	Organizational Unit	(1) Domain Validation No description (2) Organization Validation Business division name of the Subscriber (optional). 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: ・ 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; ・ 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) - The value must be encoded as a character-for-character copy of the dNSName entry value from the Subject Alternative Name extension. Specifically.	-
Subject Public Key Info		The subject's Public Key (RSA 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/fullcrl.crl (2) Organization Validation http://repo.pubcert.jprs.jp/sppca/jprs/ovca_g4/fullcrl.crl	n
Authority Information Access		[1] ocsp (1.3.6.1.5.5.7.48.1) (1) Domain Validation http://dv.g4.ocsp.pubcert.jprs.jp	n

	(2) Organization Validation http://ov.g4.ocsp.pubcert.jprs.jp [2] ca issuers (1.3.6.1.5.5.7.48.2) (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 List （1.3.6.1.4.1.11129.2.4.2)	Value of an OCTET STRING containing the encoded SignedCertificateTimestampList	n

Table 7.1-2 Subscriber Certificate Profile (applicable to certificates issued by JPRS DV RSA CA 2024 G1 or JPRS OV RSA CA 2024 G1)

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 DV RSA CA 2024 G1
		(2) Organization Validation
		CN= JPRS OV RSA CA 2024 G1
			-

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 Subscriber	-

		(country)	
	State or Province	(1) Domain Validation No description (2) Organization Validation Address of the Subscriber (prefecture name) (mandatory)	-
	Locality	(1) Domain Validation No description (2) Organization Validation Address of the Subscriber (city, town, or village name) (mandatory)	-
	Organization	(1) Domain Validation No description (2) Organization Validation Name of the Subscriber (mandatory)	-
	Common Name	A host name used in the DNS of the server in which the certificate is scheduled to be installed (mandatory) - The value must be encoded as a character-for-character copy of the dNSName entry value from the Subject Alternative Name extension. Specifically.	-
Subject Public Key Info		The subject's Public Key (RSA 4096 bits, RSA3072 bits or RSA 2048 bits)	-
Extended field		Description of setting	critical
KeyUsage		digitalSignature, keyEncipherment	y
ExtendedKeyUsage		TLS Web Server Authentication, TLS Web Client Authentication (optional)	n
Subject Alt Name		dNSName= name(s) of the server(s)	n
CertificatePolicies		Certificate Policy (1) Domain Validation 2.23.140.1.2.1 (2) Organization Validation	n

	2.23.140.1.2.2	
CRL Distribution Points	(1) Domain Validation http://repo.pubcert.jprs.jp/sppca/jprs/dvca_rsa2024g1/fullcrl.crl (2) Organization Validation http://repo.pubcert.jprs.jp/sppca/jprs/ovca_rsa2024g1/fullcrl.crl	n
Authority Information Access	[1] ocsp (1.3.6.1.5.5.7.48.1) (1) Domain Validation http://dv.rsa2024g1.ocsp.pubcert.jprs.jp (2) Organization Validation http://ov.rsa2024g1.ocsp.pubcert.jprs.jp [2] ca issuers (1.3.6.1.5.5.7.48.2) (1) Domain Validation http://repo.pubcert.jprs.jp/sppca/jprs/dvca_rsa2024g1/JPRS_DVCA_RSA2024G1_DER.cer (2) Organization Validation http://repo.pubcert.jprs.jp/sppca/jprs/ovca_rsa2024g1/JPRS_OVCA_RSA2024G1_DER.cer	n
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 List （1.3.6.1.4.1.11129.2.4.2）	Value of an OCTET STRING containing the encoded SignedCertificateTimestampList(optional).	n

Table 7.1-3 Subscriber Certificate Profile (applicable to certificates issued by JPRS DV ECC CA 2024 G1 or JPRS OV ECC CA 2024 G1)

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		ecdsa-with-SHA384	-
Issuer	Country	C=JP	-
	Organization	O=Japan Registry Services Co., Ltd.	-

	Common Name	(1) Domain Validation
		CN= JPRS DV ECC CA 2024 G1
		(2) Organization Validation
		CN= JPRS OV ECC CA 2024 G1
			-

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 Subscriber (country)	-
	State or Province	(1) Domain Validation No description (2) Organization Validation Address of the Subscriber (prefecture name) (mandatory)	-
	Locality	(1) Domain Validation No description (2) Organization Validation Address of the Subscriber (city, town, or village name) (mandatory)	-
	Organization	(1) Domain Validation No description (2) Organization Validation Name of the Subscriber (mandatory)	-
	Common Name	A host name used in the DNS of the server in which the certificate is scheduled to be installed (mandatory) - The value must be encoded as a character-for-character copy of the dNSName entry value from the Subject Alternative Name extension.	-

		Specifically.	
Subject Public Key Info		The subject's Public Key (RSA 4096 bits, RSA 3072 bits, RSA 2048 bits, P-256 or P-384)	-
Extended field		Description of setting	critical
KeyUsage		digitalSignature, keyEncipherment (except for certificates issued by using ECDSA key)	y
ExtendedKeyUsage		TLS Web Server Authentication, TLS Web Client Authentication (optional)	n
Subject Alt Name		dNSName= name(s) of the server(s)	n
CertificatePolicies		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_ecc2024g1/fullcrl.crl (2) Organization Validation http://repo.pubcert.jprs.jp/sppca/jprs/ovca_ecc2024g1/fullcrl.crl	n
Authority Information Access		[1] ocsp (1.3.6.1.5.5.7.48.1) (1) Domain Validation http://dv.ecc2024g1.ocsp.pubcert.jprs.jp (2) Organization Validation http://ov.ecc2024g1.ocsp.pubcert.jprs.jp [2] ca issuers (1.3.6.1.5.5.7.48.2) (1) Domain Validation http://repo.pubcert.jprs.jp/sppca/jprs/dvca_ecc2024g1/JPRSDVCA_ECC2024G1_DER.cer (2) Organization Validation http://repo.pubcert.jprs.jp/sppca/jprs/ovca_ecc2024g1/JPRS_OVCA_ECC2024G1	n

	_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 List (1.3.6.1.4.1.11129.2.4.2)	Value of an OCTET STRING containing the encoded SignedCertificateTimestampList (optional)	n

Table 7.1-4 Subordinate CA Certificate Profile (applicable to certificates issued by Security Communication RootCA2)

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 (RSA 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	n

	(160 bits)	
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

Table 7.1-5 Subordinate CA Certificate Profile (applicable to certificates issued by SECOM TLS RSA Root CA 2024)

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		Sha384 With RSA Encryption	-
Issuer	Country	C=JP	-
	Organization	O=SECOM Trust Systems Co., Ltd.	-
	Common Name	CN= SECOM TLS RSA Root CA 2024	-
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 OV RSA CA 2024 G1
		(2) Domain Validation
		CN= JPRS DV RSA CA 2024 G1	

Subject Public Key Info		The subject’s Public Key (RSA 4096 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		[1] Certificate Policy （1） Domain Validation 2.23.140.1.2.1 （2） Organization Validation 2.23.140.1.2.2 [2] Certificate Policy 1.2.392.200091.100.901.11	n
Basic Constraints		Subject Type=CA Path Length Constraint=0	y
ExtendedKeyUsage		TLS Web Server Authentication TLS Web Client Authentication	n
CRL Distribution Points		http://repo1.secomtrust.net/root/tlsrsa/tlsrsarootca2024.crl	n
Authority Information Access		[1] ocsp（1.3.6.1.5.5.7.48.1） http://tlsrsarootca2024.ocsp.secom-cert.jp [2] ca issuers（1.3.6.1.5.5.7.48.2） http://repo2.secomtrust.net/root/tlsrsa/tlsrsarootca2024.cer	n

Table 7.1-6 Subordinate CA Certificate Profile (applicable to certificates issued by Security Communication ECC RootCA1)

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		ecdsa-with-SHA384	-
Issuer	Country	C=JP	-
	Organization	O=SECOM Trust Systems CO.,LTD.	-
	Common Name	CN=Security Communication ECC RootCA1	-
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 OV ECC CA 2024 G1
		(2) Domain Validation
		CN= JPRS DV ECC CA 2024 G1
			-

Subject Public Key Info		The subject's Public Key (384 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		[1] Certificate Policy （1）Domain Validation 2.23.140.1.2.1 （2）Organization Validation 2.23.140.1.2.2 [2] Certificate Policy 1.2.392.200091.100.902.1	n
Basic Constraints		Subject Type=CA Path Length Constraint=0	y
ExtendedKeyUsage		TLS Web Server Authentication TLS Web Client Authentication	n

CRL Distribution Points	http://repository.secomtrust.net/SC-ECC-Root1/SCECCRoot1CRL.crl	n
Authority Information Access	[1] ocsp（1.3.6.1.5.5.7.48.1） http://sceccrootca1.ocsp.secomtrust.net [2] ca issuers（1.3.6.1.5.5.7.48.2） http://repository.secomtrust.net/SC-ECC-Root1/SCECCRoot1ca.cer	n

Table 7.1-7 Precertificate Profile (applicable to certificates issued on or after July 29, 2020)

Basic field		Description of setting	critical
Version		Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate.	-
Serial Number		Same as above	-
Signature Algorithm		Same as above	-
Issuer	Country	Same as above	-
	Organization	Same as above	-
	Common Name	Same as above	-
Validity	NotBefore	Same as above	-
	NotAfter	Same as above	-
Subject	Country	Same as above	-
	State or Province	Same as above	-
	Locality	Same as above	-
	Organization	Same as above	-
	Organizational Unit	Same as above	-
	Common Name	Same as above	-
Subject Public Key Info		Same as above	-
Extended field		**Description of setting**	**critical**
Precertificate Poison		extnValue OCTET STRING which is exactly the hex-encoded bytes 0500, the encoded representation of the ASN.1 NULL value, as specified in RFC 6962, Section 3.1.	y

KeyUsage	Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate.	y
ExtendedKeyUsage	Same as above	n
Subject Alt Name	Same as above	n
CertificatePolicies	Same as above	n
CRL Distribution Points	Same as above	n
Authority Information Access	Same as above	n
Authority Key Identifier	Same as above	n
Subject Key Identifier	Same as above	n

※If the Precertificate Poison extension is removed from the Precertificate, and the Signed Certificate Timestamp List is removed from the Subscriber certificate, the contents of the extensions field MUST be byte-for-byte identical to the Subscriber Certificate.

Table 7.1-8 OCSP Responder Certificate Profile (Applicable to certificates issued by JPRS Domain Validation Authority – G4 or JPRS Organization Validation Authority – G4)

Basic field		Description of setting	critical
Version		Version 3	-
Serial Number		Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG	-
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 (RSA 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
ExtendedKeyUsage		OCSPSigning	n
OCSP No Check		null	n

Table 7.1-9 OCSP Responder Certificate Profile (Applicable to certificates issued by JPRS DV RSA CA 2024 G1 or JPRS OV RSA CA 2024 G1)

Basic field		Description of setting	critical
Version		Version 3	-
Serial Number		Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG	-
Signature Algorithm		sha256 With RSA Encryption	-
Issuer	Country	C=JP	-
	Organization	O= Japan Registry Services Co., Ltd.	-

	Common Name	(1) Domain Validation
		CN=JPRS DV RSA CA 2024 G1
		(2) Organization Validation
		CN= JPRS OV RSA CA 2024 G1
			-

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 (RSA 4096 bits , RSA 3072 bits or RSA 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
ExtendedKeyUsage	OCSPSigning	n
OCSP No Check	null	n

Table 7.1-10 OCSP Responder Certificate Profile (Applicable to certificates issued by JPRS DV ECC CA 2024 G1 or JPRS OV ECC CA 2024 G1)

Basic field		Description of setting	critical
Version		Version 3	-
Serial Number		Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG	-
Signature Algorithm		ecdsa-with-SHA384	-
Issuer	Country	C=JP	-
	Organization	O= Japan Registry Services Co., Ltd.	-

	Common Name	(1) Domain Validation
		CN=JPRS DV ECC CA 2024 G1
		(2) Organization Validation
		CN= JPRS OV ECC CA 2024 G1
			-

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 (256 bits or 384 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	n

	(160 bits)	
KeyUsage	digitalSignature	y
ExtendedKeyUsage	OCSPSigning	n
OCSP No Check	null	n

7.1.1 Version Number(s)

The CA applies version 3.

7.1.2 Certificate Content and Extensions

Extensions of the Certificate issued by the CA is specified Section 7.1 of this CP/CPS.

7.1.3 Algorithm Object Identifier

The algorithm OID used in this service is as follows:

Algorithm	Object Identifier
sha256 With RSA Encryption	1.2.840.113549.1.1.11
RSA Encryption	1.2.840.113549.1.1.1
sha384 With RSA Encryption	1.2.840.113549.1.1.12
id-ecPublicKey	1.2.840.10045.2.1
ecdsa-with-SHA384	1.2.840.10045.4.3.3

7.1.4 Name Forms

The CA uses the Distinguished Name specified in RFC 5280.

For every valid Certification Path (as defined by RFC 5280, Section 6), for each Certificate in the Certification Path, the encoded content of the Issuer Distinguished Name field of a Certificate SHALL be byte-for-byte identical with the encoded form of the Subject Distinguished Name field of the Issuing CA certificate.

By issuing the Certificate, the CA represents that it followed the procedure set forth in its CP/CPS to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate. The CA SHALL NOT include a Domain Name in a Subject attribute except as specified in Baseline Requirements Section 3.2.2.4.

Distinguished Names MUST NOT contain only metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.

The CA will not issue a certificate with a Subject Alternative Name extension or "common name" field that contains a reserved IP address or internal name.

If the "common name" value is a fully qualified domain name or a wildcard domain name, the "common name" value is encoded as a character-for-character copy of the dNSName entry value in the Subject Alternative Name extension. Specifically, all Domain Labels in the FQDN part of a fully qualified domain name or wildcard domain name are encoded as LDH Labels, and P-Labels does not convert to Unicode.

7.1.5 Name Constraints

Not set in the CA.

7.1.6 Certificate Policy Object Identifier

The OID of the certificate issued by the CA is as described in this CP/CPS "1.2 Document Name and Identification".
The following Certificate Policy identifiers are reserved for use by the CA as an optional means of assertaing that a Certificate complies with Baseline Requirements.

【For DV certificate】 {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificatepolicies(1) baseline-requirements(2) domain-validated(1)} (2.23.140.1.2.1)

【For OV certificate】 {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificatepolicies(1) baseline-requirements(2) organization-validated(2)} (2.23.140.1.2.2)

7.1.7 Usage of Policy Constraints Extension

Not set.

7.1.8 Policy Qualifiers Syntax and Semantics

For the policy qualifier, the URI of the Web page that publishes this CP/CPS is stored.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Not set.

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 by JPRS DV RSA CA 2024 G1 or JPRS OV RSA CA 2024 G1)

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 Certificates	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 table 7.2.2.1. If the Revocation Reason Code is "#0 unspecified", the "Reason Code" field does not appear in the CRL profile.

Table 7.2.3 CRL Profile (applicable to certificates issued by JPRS DV RSA CA 2024 G1 or JPRS OV RSA CA 2024 G1)

Basic field		Description of setting	critical
Version		Version 2	-
Signature Algorithm		SHA384 with RSAEncryption	-
Issuer	Country	C=JP	-
	Organization	O= Japan Registry Services Co., Ltd.	-

	Common Name	(1) Domain Validation
		CN= JPRS DV RSA CA 2024 G1
		(2) Organization Validation
		CN=JPRS OV RSA CA 2024 G1
			-

This Update		E.g.) 2008/3/1 00:00:00 GMT	-
Next Update		E.g.) 2008/3/5 00:00:00 GMT	-

Revoked Certificates	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 table 7.2.2.1. If the Revocation Reason Code is "#0 unspecified", the "Reason Code" field does not appear in the CRL profile.

Table 7.2.4 CRL Profile (applicable to certificates issued by JPRS DV ECC CA 2024 G1 or JPRS OV ECC CA 2024 G1)

Basic field		Description of setting	critical
Version		Version 2	-
Signature Algorithm		ecdsa-with-SHA384	-
Issuer	Country	C=JP	-
	Organization	O= Japan Registry Services Co., Ltd.	-

	Common Name	(1) Domain Validation
		CN= JPRS DV ECC CA 2024 G1
		(2) Organization Validation
		CN=JPRS OV ECC CA 2024 G1
			-

This Update		E.g.) 2008/3/1 00:00:00 GMT	-
Next Update		E.g.) 2008/3/5 00:00:00 GMT	-
Revoked Certificates	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 table 7.2.2.1. If the Revocation Reason Code is "#0 unspecified", the "Reason Code" field does not appear in the CRL profile.

7.2.1 Version Number(s)

The CA applies CRL version 2.

7.2.2 CRL and CRL Entry Extensions

Use the CRL extension field issued by the CA.

reasonCode (OID 2.5.29.21)

CRLReason must be included in the reasonCode extension of the CRL entry corresponding to a Subscriber Certificate that is revoked after July 15, 2023, unless the CRLReason is “unspecified (0)”.

The CA set one of the Revocation Reason Code specified in the following table, with the exception of “unspecified (0)”.

Table 7.2.2.1 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

7.3.1 Version Number(s)

The CA shall apply OCSP Version 1.

7.3.2 OCSP Extensions

Refer to Section 7.1 of this CP/CPS.

The singleExtensions of an OCSP response MUST NOT contain the reasonCode (OID 2.5.29.21) CRL entry extension.

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/CPS.

Certificates that are capable of being used to issue new certificates must either be Technically Constrained in line with "7.1.5 Name Constraints" of this CP/CPS and audited in line with "8.7 Self-Audit" of this CP/CPS 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 CP/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 CP/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 CP/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 CP/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 CP/CPS. The CA shall undergo WebTrust in accordance with one of the following schemes:

- WebTrust for CAs
- WebTrust for CAs - SSL Baseline
- WebTrust for CAs - 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 CP/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 CP/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/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 CP/CPS 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.

Effective 2025-03-15, the CA uses a Linting process to verify the technical accuracy of Certificates within the selected sample set independently of previous linting performed on the same Certificates.

Except for Delegated Third Parties that undergo an annual audit that meets the criteria specified in this CP/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/CPS. The CA shall internally audit each Delegated Third Party's compliance with these Requirements on an annual basis. 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/CPS are met.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

To be separately stipulated in the Terms and Conditions.

9.1.2 Certificate Access Fees

No stipulation.

9.1.3 Revocation or Status Information Access Fees

No stipulation.

9.1.4 Fees for Other Services

To be separately stipulated in the Terms and Conditions.

9.1.5 Refund Policy

To be separately stipulated in the Terms and Conditions.

9.2 Financial Responsibility

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

9.2.1 Insurance Coverage

No stipulation.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

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 or this CP/CPS.

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

9.4.1 Privacy Plan

JPRS has published its Privacy Policy on its Web site (https://jprs.jp/privacy.html) .

9.4.2 Information Treated as Private

Stipulated in the Privacy Policy published on JPRS's Web site (https://jprs.jp/privacy.html) .

9.4.3 Information not Deemed Private

JPRS does not deem any information other than the information stipulated in the Privacy Policy published on JPRS's Web site (https://jprs.jp/privacy.html) to be personal information.

9.4.4 Responsibility to Protect Private Information

Stipulated in the Privacy Policy published on JPRS's Web site (https://jprs.jp/privacy.html).

9.4.5 Notice and Consent to Use Private Information

Stipulated in the Privacy Policy published on JPRS's Web site (https://jprs.jp/privacy.html).

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Stipulated in the Privacy Policy published on JPRS's Web site (https://jprs.jp/privacy.html).

9.4.7 Other Information Disclosure Circumstances

Stipulated in the Privacy Policy published on JPRS's Web site (https://jprs.jp/privacy.html).

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/CPS and related documents;
- Public Keys and Private Keys of the CA; and
- software provided by JPRS.

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

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

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

The CA SHALL require, as part of the Subscriber Agreement or Terms of Use, that the Applicant make the commitments and warranties in this section for the benefit of the CA and the Certificate Beneficiaries.

The Subscriber Agreement or Terms of Use MUST contain provisions imposing on the Applicant itself (or made by the Applicant on behalf of its principal or agent under a subcontractor or hosting service relationship) the following obligations and warranties:

1. **Accuracy of Information**: An obligation and warranty to provide accurate and complete information at all times to the CA, both in the certificate request and as otherwise requested by the CA in connection with the issuance of the Certificate(s) to be supplied by the CA;

2. **Protection of Private Key**: An obligation and warranty by the Applicant to take all reasonable measures to assure control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token);

3. **Acceptance of Certificate**: An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy;

4. **Use of Certificate**: An obligation and warranty to install the Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate, and to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use;

5. **Reporting and Revocation**: An obligation and warranty to: a. promptly request revocation of the Certificate, and cease using it and its associated Private Key, if

there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate, and b. promptly request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate;

6. **Termination of Use of Certificate**: An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise.

7. **Responsiveness**: An obligation to respond to the CA's instructions concerning Key Compromise or Certificate misuse within a specified time period.

8. **Acknowledgment and Acceptance**: An acknowledgment and acceptance that the CA is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber Agreement or Terms of Use or if revocation is required by the CA's CP/CPS or these Baseline Requirements.

9.6.4 Relying Party Representations and Warranties

Each Relying Party warrants that he/she/it will comply with the provisions of this CP/CPS. If any Relying Party fails to comply with any provision of this CP/CPS, 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/CPS, 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/CPS 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/CPS shall come into effect upon approval by the CA's Certificate Operation Conference. This CP/CPS shall not lose its effect under any circumstances before its termination stipulated in "9.10.2 Termination" herein.

9.10.2 Termination

This CP/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 CP/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 CP/CPS, the CA shall promptly publish the amended version of this CP/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

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/CPS, or the use of a certificate.

9.15 Compliance with Applicable Laws

The CA SHALL issue Certificates and operate its PKI in accordance with all law applicable to its business and the Certificates it issues in every jurisdiction in which it operates.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

To be separately stipulated in the Terms and Conditions.

9.16.3 Severability

In the event of a conflict between these Requirements and a law, regulation or government order (hereinafter 'Law') of any jurisdiction in which the CA operates or issues certificates, the CA MAY modify any conflicting requirement to the minimum extent necessary to make the requirement valid and legal in the jurisdiction. This applies only to operations or certificate issuances that are subject to that Law. In such event, the CA SHALL immediately (and prior to issuing a certificate under the modified requirement) include in Section 9.16.3 of the CA's CP/CPS a detailed reference to the Law requiring a modification of these Requirements under this section, and the specific modification to these Requirements implemented by the CA.

The CA MUST also (prior to issuing a certificate under the modified requirement) notify the CA/Browser Forum of the relevant information newly added to its CP/CPS by sending a message to questions@cabforum.org and receiving confirmation that it has been posted to the Public Mailing List and is indexed in the Public Mail Archives available at https://cabforum.org/pipermail/public/ (or such other email addresses and links as the Forum may designate), so that the CA/Browser Forum may consider possible revisions to these Requirements accordingly.

Any modification to the CA practice enabled under this section MUST be discontinued if and when the Law no longer applies, or these Requirements are modified to make it possible to comply with both them and the Law simultaneously. An appropriate change in practice, modification to the CA's CP/CPS and a notice to the CA/Browser Forum, as outlined above, MUST be made within 90 days.

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

Stipulated in Section 9.13 of this CP/CPS, “Dispute Resolution Provisions,” and in the Terms and Conditions.

9.16.5 Force Majeure

To be separately stipulated in the Terms and Conditions.

.

9.17 Other Provisions

Not applicable.