| 変更履歴あり | 整形版 | 備考 |
| --- | --- | --- |
| | | 凡例：<br>赤字（下線付き）：追加<br>~~青字（取消線付き）~~：削除 |
| JPRS CA Certificate Policy<br>Version 3.7372 | JPRS CA Certificate Policy<br>Version 3.73 | バージョンの更新 |
| NovemberAugust 726, 2024<br>Japan Registry Services Co., Ltd. | November 7, 2024<br>Japan Registry Services Co., Ltd. | 改訂日の更新 |

## 変更履歴あり

Version History

| Version Number | Date | Description |
|---|---|---|
| 1.00 | 2019.06.17 | Publication of the first version |
| 1.10 | 2019.09.25 | Revision of “3.2.2.4 Validation of Domain Authorization or Control” (adding the additional information of “general e-mail address indicating an administrator” |
| 1.20 | 2020.04.01 | Revision due to Mozilla Root Store Policy (v2.7) |
| 1.30 | 2020.07.10 | Revision of “7.1.2 Subordinate CA Certificate Profile” |
| 2.00 | 2020.07.22 | Revision of “7. Certificate, CRL, and OCSP Profiles” |
| 2.10 | 2020.08.20 | Revision of the maximum validity period of certificate |
| 2.20 | 2020.10.06 | Revision of “3.2.2.4 Validation of Domain Authorization or Control” |
| 2.21 | 2021.04.01 | Revision of the date and version |
| 2.22 | 2021.04.28 | Revision due to Mozilla Root Store Policy (v2.7.1) |
| 2.23 | 2021.05.27 | ・ Clarification of “3.2.2.4 Validation of Domain Authorization or Control”<br>・ Delete the description of invalid Subordinate CAs from “7. Certificate, CRL, and OCSP Profiles”. |
| 2.30 | 2021.11.18 | ・ Revision of “3.2.2.4.18 Agreed-Upon Change to Website v2”<br>・ Sunset of “subject:organizationalUnitName” |
| 3.00 | 2021.12.08 | ・ Revisions due to new service provision |
| 3.10 | 2022.03.02 | ・ Add a reference to the new terms and conditions |
| 3.11 | 2022.04.01 | ・ Revision of the date and version |
| 3.20 | 2022.09.30 | ・ Revision of “6.3 Other Aspects of Key Pair Management”<br>・ Add description of Revocation Reason Code to be applied in this CA. |
| 3.30 | 2023.04.24 | ・ Revision of the maximum validity period of certificate |
| 3.40 | 2023.06.08 | ・Revision of “1.1 Overview”<br>・ Revision of “7.3 OCSP Profile” |
| 3.50 | 2023.08.28 | Revision of description to clarify compliance with Baseline Requirements |
| 3.60 | 2024.02.22 | Revision of “ 7. Certificate, CRL, and OCSP Profiles” |
| 3.70 | 2024.04.11 | Revision of Table 7.1-2 and Table 7.1-3 |
| 3.71 | 2024.06.05 | Revision of “1.6 Definitions and Acronyms” and “4.2.4 Check of CAA Records” |
| 3.72 | 2024.08.26 | Revision of “4.2.1 Performing Identification and Authentication Functions” |
| 3.73 | 2024.11.07 | Revision of ” 4.3.1 CA Actions during Certificate Issuance”, “ 4.9.1 Circumstances for Certificate Revocation” and “ 8.4 Topics Covered by Assessment” |

## 整形版

Version History

| Version Number | Date | Description |
|---|---|---|
| 1.00 | 2019.06.17 | Publication of the first version |
| 1.10 | 2019.09.25 | Revision of “3.2.2.4 Validation of Domain Authorization or Control” (adding the additional information of “general e-mail address indicating an administrator” |
| 1.20 | 2020.04.01 | Revision due to Mozilla Root Store Policy (v2.7) |
| 1.30 | 2020.07.10 | Revision of “7.1.2 Subordinate CA Certificate Profile” |
| 2.00 | 2020.07.22 | Revision of “7. Certificate, CRL, and OCSP Profiles” |
| 2.10 | 2020.08.20 | Revision of the maximum validity period of certificate |
| 2.20 | 2020.10.06 | Revision of “3.2.2.4 Validation of Domain Authorization or Control” |
| 2.21 | 2021.04.01 | Revision of the date and version |
| 2.22 | 2021.04.28 | Revision due to Mozilla Root Store Policy (v2.7.1) |
| 2.23 | 2021.05.27 | ・ Clarification of “3.2.2.4 Validation of Domain Authorization or Control”<br>・ Delete the description of invalid Subordinate CAs from “7. Certificate, CRL, and OCSP Profiles”. |
| 2.30 | 2021.11.18 | ・ Revision of “3.2.2.4.18 Agreed-Upon Change to Website v2”<br>・ Sunset of “subject:organizationalUnitName” |
| 3.00 | 2021.12.08 | ・ Revisions due to new service provision |
| 3.10 | 2022.03.02 | ・ Add a reference to the new terms and conditions |
| 3.11 | 2022.04.01 | ・ Revision of the date and version |
| 3.20 | 2022.09.30 | ・ Revision of “6.3 Other Aspects of Key Pair Management”<br>・ Add description of Revocation Reason Code to be applied in this CA. |
| 3.30 | 2023.04.24 | ・ Revision of the maximum validity period of certificate |
| 3.40 | 2023.06.08 | ・Revision of “1.1 Overview”<br>・ Revision of “7.3 OCSP Profile” |
| 3.50 | 2023.08.28 | Revision of description to clarify compliance with Baseline Requirements |
| 3.60 | 2024.02.22 | Revision of “ 7. Certificate, CRL, and OCSP Profiles” |
| 3.70 | 2024.04.11 | Revision of Table 7.1-2 and Table 7.1-3 |
| 3.71 | 2024.06.05 | Revision of “1.6 Definitions and Acronyms” and “4.2.4 Check of CAA Records” |
| 3.72 | 2024.08.26 | Revision of “4.2.1 Performing Identification and Authentication Functions” |
| 3.73 | 2024.11.07 | Revision of ” 4.3.1 CA Actions during Certificate Issuance”, “ 4.9.1 Circumstances for Certificate Revocation” and “ 8.4 Topics Covered by Assessment” |

## 備考

改訂履歴の追記

| 変更履歴あり | 整形版 | 備考 |
|---|---|---|

# 1. Introduction

## 1.1 Overview

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

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

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

The CA conforms to the current version of “Baseline Requirements for the Issuance and Management of Publicly-Trusted 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<br>・ Apple Root Certificate Program<br>・ Chrome Root Program Policy<br>・ Microsoft Trusted Root Program<br>・ Mozilla Root Store Policy |


# 1. Introduction

## 1.1 Overview

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

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

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

The CA conforms to the current version of “Baseline Requirements for the Issuance and Management of Publicly-Trusted 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<br>・ Apple Root Certificate Program<br>・ Chrome Root Program Policy<br>・ Microsoft Trusted Root Program<br>・ Mozilla Root Store Policy |

| 変更履歴あり | 整形版 | 備考 |
|---|---|---|

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

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

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

## 1.2 Document Name and Identification

The official name of this CP is the “JPRS CA Certificate Policy.”
Following are an Object Identifier (hereinafter referred to as “OID”) assigned by the CA under this CP, and an OID of the CPS referenced by this CP:

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

## 1.3 PKI Participants

### 1.3.1 CA

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

### 1.3.2 RA

“RA” stands for “Registration Authority,” an entity that mainly performs reviews to verify the existence and validate the identities of applicants who apply for the issuance or revocation of certificates, registers information necessary for issuing certificates, and

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

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

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

## 1.2 Document Name and Identification

The official name of this CP is the “JPRS CA Certificate Policy.”
Following are an Object Identifier (hereinafter referred to as “OID”) assigned by the CA under this CP, and an OID of the CPS referenced by this CP:

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

## 1.3 PKI Participants

### 1.3.1 CA

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

### 1.3.2 RA

“RA” stands for “Registration Authority,” an entity that mainly performs reviews to verify the existence and validate the identities of applicants who apply for the issuance or revocation of certificates, registers information necessary for issuing certificates, and

| 変更履歴あり | 整形版 | 備考 |
| --- | --- | --- |
| requests the CA to issue certificates, among the operations of the CA. The CA acts as an RA.<br>### 1.3.3 Subscribers<br>“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.<br>### 1.3.4 Relying Parties<br>A “Relying Party” means an individual, corporation, or organization that verifies the validity of certificates issued by the CA.<br>### 1.3.5 Other Participants<br>No stipulation.<br>## 1.4 Certificate Usage<br>### 1.4.1 Appropriate Certificate Uses<br>Certificates issued by the CA are used to encrypt information for server authentication and on communication pathways.<br>### 1.4.2 Prohibited Certificate Uses<br>Certificates issued by the CA may be used solely as set forth in “1.4.1 Appropriate Certificate Uses,” and may not be used for any other purposes.<br>## 1.5 Policy Administration<br>### 1.5.1 Organization Administering the Document<br>This CP shall be maintained and administered by the CA.<br>### 1.5.2 Contact Information<br>Inquiries concerning this CP should be directed to:<br>Contact: Inquiries contact office, Japan Registry Services Co., Ltd.<br>Address: Chiyoda First Bldg. East, 3-8-1 Nishi-Kanda, Chiyoda-ku, Tokyo 101-0065 JAPAN<br>E-mail: info@jprs.jp<br><br>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:<br>https://jprs.jp/pubcert/f_mail/<br>### 1.5.3 Person Determining CP Suitability as Policy<br>The details of this CP shall be determined by the CA’s Certificate Operation Conference.<br>### 1.5.4 Approval Procedures<br>This CP shall come into effect upon approval of the CA’s Certificate Operation Conference. | requests the CA to issue certificates, among the operations of the CA. The CA acts as an RA.<br>### 1.3.3 Subscribers<br>“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.<br>### 1.3.4 Relying Parties<br>A “Relying Party” means an individual, corporation, or organization that verifies the validity of certificates issued by the CA.<br>### 1.3.5 Other Participants<br>No stipulation.<br>## 1.4 Certificate Usage<br>### 1.4.1 Appropriate Certificate Uses<br>Certificates issued by the CA are used to encrypt information for server authentication and on communication pathways.<br>### 1.4.2 Prohibited Certificate Uses<br>Certificates issued by the CA may be used solely as set forth in “1.4.1 Appropriate Certificate Uses,” and may not be used for any other purposes.<br>## 1.5 Policy Administration<br>### 1.5.1 Organization Administering the Document<br>This CP shall be maintained and administered by the CA.<br>### 1.5.2 Contact Information<br>Inquiries concerning this CP should be directed to:<br>Contact: Inquiries contact office, Japan Registry Services Co., Ltd.<br>Address: Chiyoda First Bldg. East, 3-8-1 Nishi-Kanda, Chiyoda-ku, Tokyo 101-0065 JAPAN<br>E-mail: info@jprs.jp<br><br>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:<br>https://jprs.jp/pubcert/f_mail/<br>### 1.5.3 Person Determining CP Suitability as Policy<br>The details of this CP shall be determined by the CA’s Certificate Operation Conference.<br>### 1.5.4 Approval Procedures<br>This CP shall come into effect upon approval of the CA’s Certificate Operation Conference. | |

| 変更履歴あり | 整形版 | 備考 |
| --- | --- | --- |
| **1.6 Definitions and Acronyms**<br>ACME（Automated Certificate Management Environment）<br>“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.<br><br>Archive<br>“Archive” means information acquired for the purpose of keeping a history for any legal or other reason.<br><br>Audit Log<br>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.<br><br>Authorization Domain Name<br>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.<br><br>Base Domain Name<br>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.<br><br>CA (Certification Authority)<br>“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.<br><br>CAA (Certificate Authority Authorization)<br>“ CAA” stands for “Certificate Authority Authorization,” a function to prevent | **1.6 Definitions and Acronyms**<br>ACME（Automated Certificate Management Environment）<br>“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.<br><br>Archive<br>“Archive” means information acquired for the purpose of keeping a history for any legal or other reason.<br><br>Audit Log<br>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.<br><br>Authorization Domain Name<br>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.<br><br>Base Domain Name<br>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.<br><br>CA (Certification Authority)<br>“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.<br><br>CAA (Certificate Authority Authorization)<br>“ CAA” stands for “Certificate Authority Authorization,” a function to prevent | |

| 変更履歴あり | 整形版 | 備考 |
| --- | --- | --- |
| 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.<br><br>CP (Certificate Policy)<br>“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.<br><br>CPS (Certification Practices Statement)<br>“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.<br><br>CRL (Certificate Revocation List)<br>“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.<br><br>CT (Certificate Transparency)<br>“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.<br><br>Digital Certificates<br>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.<br><br>ECDSA（Elliptic Curve Digital Signature Algorithm）<br>“ECDSA” is one of the most standard encryption technologies. ECDSA is widely used as a public key cryptosystem.<br><br>Escrow<br>“Escrow” means the placement (entrustment) of an asset in the control of an independent third party. | 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.<br><br>CP (Certificate Policy)<br>“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.<br><br>CPS (Certification Practices Statement)<br>“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.<br><br>CRL (Certificate Revocation List)<br>“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.<br><br>CT (Certificate Transparency)<br>“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.<br><br>Digital Certificates<br>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.<br><br>ECDSA（Elliptic Curve Digital Signature Algorithm）<br>“ECDSA” is one of the most standard encryption technologies. ECDSA is widely used as a public key cryptosystem.<br><br>Escrow<br>“Escrow” means the placement (entrustment) of an asset in the control of an independent third party. | |

| 変更履歴あり | 整形版 | 備考 |
| --- | --- | --- |
| FIPS 140-2<br>“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.<br><br>FQDN（Fully-Qualified Domain Name）<br>A Domain Name that includes the Domain Labels of all superior nodes in the Internet Domain Name System.<br><br>HSM (Hardware Security Module)<br>“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.<br><br>JPRS Partners<br>“JPRS Partners” mean business enterprises authorized by JPRS in connection with the Digital Certificate Issuance Services to be provided by JPRS.<br><br>Key Pair<br>A “Key Pair” means a pair consisting of a Private Key and Public Key in a public key cryptosystem.<br><br>Linting<br>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.<br><br>NTP (Network Time Protocol)<br>“NTP” stands for “Network Time Protocol,” a protocol designed to synchronize the internal clocks of computers over a network.<br><br>OCSP (Online Certificate Status Protocol)<br>“OCSP” stands for “Online Certificate Status Protocol,” a protocol for providing information on the status of a certificate in real time.<br><br>OID (Object Identifier)<br>“OIDs” stands for “Object Identifiers,” numerals registered in international registration institutions as unique IDs among global networks within a framework for maintaining | FIPS 140-2<br>“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.<br><br>FQDN（Fully-Qualified Domain Name）<br>A Domain Name that includes the Domain Labels of all superior nodes in the Internet Domain Name System.<br><br>HSM (Hardware Security Module)<br>“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.<br><br>JPRS Partners<br>“JPRS Partners” mean business enterprises authorized by JPRS in connection with the Digital Certificate Issuance Services to be provided by JPRS.<br><br>Key Pair<br>A “Key Pair” means a pair consisting of a Private Key and Public Key in a public key cryptosystem.<br><br>Linting<br>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.<br><br>NTP (Network Time Protocol)<br>“NTP” stands for “Network Time Protocol,” a protocol designed to synchronize the internal clocks of computers over a network.<br><br>OCSP (Online Certificate Status Protocol)<br>“OCSP” stands for “Online Certificate Status Protocol,” a protocol for providing information on the status of a certificate in real time.<br><br>OID (Object Identifier)<br>“OIDs” stands for “Object Identifiers,” numerals registered in international registration institutions as unique IDs among global networks within a framework for maintaining | 用語定義の追加 |

| 変更履歴あり | 整形版 | 備考 |
| --- | --- | --- |
| and administering the connectivity of networks and the uniqueness of services or the like.<br><br>PKI (Public Key Infrastructure)<br>“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.<br><br>Private Key<br>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.”<br><br>Public Key<br>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.<br><br>RA (Registration Authority)<br>“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.<br><br>Random Value<br>A value specified by a CA to the Applicant that exhibits at least 112 bits of entropy.<br><br>Repository<br>The “Repository” means the database in which CA certificates, CRLs, and others are stored and published.<br><br>RFC 3647 (Request for Comments 3647)<br>“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.<br><br>RFC 5280 (Request for Comments 5280)<br>“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. | and administering the connectivity of networks and the uniqueness of services or the like.<br><br>PKI (Public Key Infrastructure)<br>“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.<br><br>Private Key<br>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.”<br><br>Public Key<br>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.<br><br>RA (Registration Authority)<br>“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.<br><br>Random Value<br>A value specified by a CA to the Applicant that exhibits at least 112 bits of entropy.<br><br>Repository<br>The “Repository” means the database in which CA certificates, CRLs, and others are stored and published.<br><br>RFC 3647 (Request for Comments 3647)<br>“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.<br><br>RFC 5280 (Request for Comments 5280)<br>“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. | |

| 変更履歴あり | 整形版 | 備考 |
| --- | --- | --- |
| RSA<br>“RSA” is one of the most standard encryption technologies. RSA IS widely used as a public key cryptosystem.<br><br>SHA-1 (Secure Hash Algorithm 1)<br>“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.<br><br>SHA-256 (Secure Hash Algorithm 256)<br>“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.<br><br>Time Stamp<br>“Time Stamp” means recorded data indicating dates and times when, for example, electronic files have been prepared and a system has performed processing.<br><br>Wildcard Certificate<br>A Certificate containing at least one Wildcard Domain Name in the Subject Alternative Names in the Certificate.<br><br>Wildcard Domain Name<br>A string starting with "*." (U+002A ASTERISK, U+002E FULL STOP) immediately followed by a Fully-Qualified Domain Name.<br><br>## 2. Publication and Repository Responsibilities<br><br>### 2.1 Repository<br>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.<br><br>### 2.2 Publication of Information | RSA<br>“RSA” is one of the most standard encryption technologies. RSA IS widely used as a public key cryptosystem.<br><br>SHA-1 (Secure Hash Algorithm 1)<br>“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.<br><br>SHA-256 (Secure Hash Algorithm 256)<br>“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.<br><br>Time Stamp<br>“Time Stamp” means recorded data indicating dates and times when, for example, electronic files have been prepared and a system has performed processing.<br><br>Wildcard Certificate<br>A Certificate containing at least one Wildcard Domain Name in the Subject Alternative Names in the Certificate.<br><br>Wildcard Domain Name<br>A string starting with "*." (U+002A ASTERISK, U+002E FULL STOP) immediately followed by a Fully-Qualified Domain Name.<br><br>## 2. Publication and Repository Responsibilities<br><br>### 2.1 Repository<br>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.<br><br>### 2.2 Publication of Information | |

| 変更履歴あり | 整形版 | 備考 |
| --- | --- | --- |
| The CA shall publish the CRLs, this CP, and the CPS on the Repository to allow online access by Subscribers and Relying Parties.<br>**2.3 Time or Frequency of Publication**<br>This CP and the CPS shall be revised at least annually and published on the Repository as revised. The CA describes to the CP and the CPS in detail how the CA implements the latest version of Baseline Requirements.<br>The frequency of CRL issuance is specified in Section 4.9.7.<br>**2.4 Access Controls on Repositories**<br>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.<br>**3. Identification and Authentication**<br>**3.1 Naming**<br>**3.1.1 Types of Names**<br>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)).<br>**3.1.2 Need for Names to Be Meaningful**<br>The information included in certificates issued by the CA and their meanings are specified in Section 7.1.1.<br>**3.1.3 Anonymity or Pseudonymity of Subscribers**<br>No name identical to any anonym or pseudonym used in any certificate to be issued by the CA may be registered.<br>**3.1.4 Rules for Interpreting Various Name Forms**<br>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.<br>**3.1.5 Uniqueness of Names**<br>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.<br>**3.1.6 Recognition, Authentication, and Roles of Trademarks**<br>The CA does not verify whether an applicant holds any intellectual property right to the | The CA shall publish the CRLs, this CP, and the CPS on the Repository to allow online access by Subscribers and Relying Parties.<br>**2.3 Time or Frequency of Publication**<br>This CP and the CPS shall be revised at least annually and published on the Repository as revised. The CA describes to the CP and the CPS in detail how the CA implements the latest version of Baseline Requirements.<br>The frequency of CRL issuance is specified in Section 4.9.7.<br>**2.4 Access Controls on Repositories**<br>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.<br>**3. Identification and Authentication**<br>**3.1 Naming**<br>**3.1.1 Types of Names**<br>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)).<br>**3.1.2 Need for Names to Be Meaningful**<br>The information included in certificates issued by the CA and their meanings are specified in Section 7.1.1.<br>**3.1.3 Anonymity or Pseudonymity of Subscribers**<br>No name identical to any anonym or pseudonym used in any certificate to be issued by the CA may be registered.<br>**3.1.4 Rules for Interpreting Various Name Forms**<br>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.<br>**3.1.5 Uniqueness of Names**<br>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.<br>**3.1.6 Recognition, Authentication, and Roles of Trademarks**<br>The CA does not verify whether an applicant holds any intellectual property right to the | |

| 変更履歴あり | 整形版 | 備考 |
| --- | --- | --- |
| 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. | 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 Initial Identity Validation** | |
| **3.2.1 Method to Prove Possession of a Private Key** | **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. | A Subscriber's possession of a Private Key is proved by verifying the signature on the relevant Certificate Signing Request (hereinafter referred to as "CSR") and confirming that the CSR has been signed with the Private Key corresponding to the Public Key contained in the CSR. | |
| **3.2.2 Authentication of Organization and Domain Identity** | **3.2.2 Authentication of Organization and Domain Identity** | |
| The CA SHALL inspect any document relied upon under this Section for alteration or falsification. | The CA SHALL inspect any document relied upon under this Section for alteration or falsification. | |
| **3.2.2.1 Authentication of Organization Identity** | **3.2.2.1 Authentication of Organization Identity** | |
| (1) Domain Validation<br>The CA does not verify the existence of organizations.<br>(2) Organization Validation<br>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. | (1) Domain Validation<br>The CA does not verify the existence of organizations.<br>(2) Organization Validation<br>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** | **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." | 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** | **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." | 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** | **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;<br>Subsequent sections 3.2.2.4.1-20 correspond to the section numbers of the methods specified by BR.<br>The CA doesn't issue certificates if "RFC 7686 - The ".onion" Special-Use Domain Name" is | 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;<br>Subsequent sections 3.2.2.4.1-20 correspond to the section numbers of the methods specified by BR.<br>The CA doesn't issue certificates if "RFC 7686 - The ".onion" Special-Use Domain Name" is | |

| 変更履歴あり | 整形版 | 備考 |
| --- | --- | --- |
| included in the certificates.<br>The CA SHALL maintain a record of which domain validation method, including relevant BR version number, they used to validate every domain.<br>**3.2.2.4.1 Validating the Applicant as a Domain Contact**<br>Not applicable<br>**3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact**<br>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.<br>The CA does not use fax, SMS, or postal mail to send a Random Values.<br>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.<br>**3.2.2.4.3 Phone Contact with Domain Contact**<br>Not applicable<br>**3.2.2.4.4 Constructed Email to Domain Contact**<br>Confirm the Applicant's control over the FQDN by<br>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<br>2. including a Random Value in the email; and<br>3. receiving a confirming response utilizing the Random Value.<br>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.<br>**3.2.2.4.5 Domain Authorization Document**<br>Not applicable<br>**3.2.2.4.6 Agreed-Upon Change to Website**<br>Not applicable<br>**3.2.2.4.7 DNS Change**<br>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”.<br>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.<br>**3.2.2.4.8 IP Address**<br>Not applicable | included in the certificates.<br>The CA SHALL maintain a record of which domain validation method, including relevant BR version number, they used to validate every domain.<br>**3.2.2.4.1 Validating the Applicant as a Domain Contact**<br>Not applicable<br>**3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact**<br>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.<br>The CA does not use fax, SMS, or postal mail to send a Random Values.<br>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.<br>**3.2.2.4.3 Phone Contact with Domain Contact**<br>Not applicable<br>**3.2.2.4.4 Constructed Email to Domain Contact**<br>Confirm the Applicant's control over the FQDN by<br>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<br>2. including a Random Value in the email; and<br>3. receiving a confirming response utilizing the Random Value.<br>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.<br>**3.2.2.4.5 Domain Authorization Document**<br>Not applicable<br>**3.2.2.4.6 Agreed-Upon Change to Website**<br>Not applicable<br>**3.2.2.4.7 DNS Change**<br>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”.<br>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.<br>**3.2.2.4.8 IP Address**<br>Not applicable | |

| 変更履歴あり | 整形版 | 備考 |
| --- | --- | --- |
| **3.2.2.4.9 Test Certificate**<br>Not applicable<br>**3.2.2.4.10 TLS Using a Random Value**<br>Not applicable<br>**3.2.2.4.11 Any Other Method**<br>Not applicable<br>**3.2.2.4.12 Validating Applicant as a Domain Contact**<br>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.<br>**3.2.2.4.13 Email to DNS CAA Contact**<br>Not applicable<br>**3.2.2.4.14 Email to DNS TXT Contact**<br>Not applicable<br>**3.2.2.4.15 Phone Contact with Domain Contact**<br>Not applicable<br>**3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact**<br>Not applicable<br>**3.2.2.4.17 Phone Contact with DNS CAA Phone Contact**<br>Not applicable<br>**3.2.2.4.18 Agreed-Upon Change to Website v2**<br>Confirming the Applicant's control over the FQDN by verifying that the Random Value is contained in the contents of a file.<br>1. The entire Random Value MUST NOT appear in the request used to retrieve the file, and<br>2. the CA MUST receive a successful HTTP response from the request (meaning a 2xx HTTP status code must be received).<br>The file containing the Random Value:<br>1. MUST be located on the Authorization Domain Name, and<br>2. MUST be located under the "/.well-known/pki-validation" directory, and<br>3. MUST be retrieved via either the "http" or "https" scheme, and<br>4. MUST be accessed over port 80 (http) or 443 (https).<br>If the CA follows redirects, the following apply:<br>1. Redirects MUST be initiated at the HTTP protocol layer.<br>・ 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.<br>・ Redirects MUST be to the final value of the Location HTTP response header, as defined in RFC 7231, Section 7.1.2. | **3.2.2.4.9 Test Certificate**<br>Not applicable<br>**3.2.2.4.10 TLS Using a Random Value**<br>Not applicable<br>**3.2.2.4.11 Any Other Method**<br>Not applicable<br>**3.2.2.4.12 Validating Applicant as a Domain Contact**<br>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.<br>**3.2.2.4.13 Email to DNS CAA Contact**<br>Not applicable<br>**3.2.2.4.14 Email to DNS TXT Contact**<br>Not applicable<br>**3.2.2.4.15 Phone Contact with Domain Contact**<br>Not applicable<br>**3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact**<br>Not applicable<br>**3.2.2.4.17 Phone Contact with DNS CAA Phone Contact**<br>Not applicable<br>**3.2.2.4.18 Agreed-Upon Change to Website v2**<br>Confirming the Applicant's control over the FQDN by verifying that the Random Value is contained in the contents of a file.<br>1. The entire Random Value MUST NOT appear in the request used to retrieve the file, and<br>2. the CA MUST receive a successful HTTP response from the request (meaning a 2xx HTTP status code must be received).<br>The file containing the Random Value:<br>1. MUST be located on the Authorization Domain Name, and<br>2. MUST be located under the "/.well-known/pki-validation" directory, and<br>3. MUST be retrieved via either the "http" or "https" scheme, and<br>4. MUST be accessed over port 80 (http) or 443 (https).<br>If the CA follows redirects, the following apply:<br>1. Redirects MUST be initiated at the HTTP protocol layer.<br>・ 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.<br>・ Redirects MUST be to the final value of the Location HTTP response header, as defined in RFC 7231, Section 7.1.2. | |

| 変更履歴あり | 整形版 | 備考 |
| --- | --- | --- |
| 2. Redirects MUST be to resource URLs with either the "http" or "https" scheme.<br>3. Redirects MUST be to resource URLs accessed via port 80 (http) or 443 (https).<br>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.<br>For Certificates issued on or after 2021-11-18, this method is not applicable for validating Wildcard Domain Names.<br>**3.2.2.4.19 Agreed-Upon Change to Website - ACME**<br>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.<br>1. The CA MUST receive a successful HTTP response from the request (meaning a 2xx HTTP status code must be received).<br>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.<br>3. If the CA follows redirects, the following apply:<br>1. Redirects MUST be initiated at the HTTP protocol layer.<br>・ 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.<br>・ Redirects MUST be to the final value of the Location HTTP response header, as defined in RFC 7231, Section 7.1.2.<br>2. Redirects MUST be to resource URLs with either the "http" or "https" scheme.<br>3. Redirects MUST be to resource URLs accessed via port 80 (http) or 443 (https).<br>This method is not applicable for validating Wildcard Domain Names.<br>**3.2.2.4.20 TLS Using ALPN**<br>Not applicable<br>**3.2.2.5 Authentication for an IP Address**<br>The CA does not issue any certificate to grant certification to any IP Address.<br>**3.2.2.6 Wildcard Domain Validation**<br>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 | 2. Redirects MUST be to resource URLs with either the "http" or "https" scheme.<br>3. Redirects MUST be to resource URLs accessed via port 80 (http) or 443 (https).<br>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.<br>For Certificates issued on or after 2021-11-18, this method is not applicable for validating Wildcard Domain Names.<br>**3.2.2.4.19 Agreed-Upon Change to Website - ACME**<br>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.<br>1. The CA MUST receive a successful HTTP response from the request (meaning a 2xx HTTP status code must be received).<br>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.<br>3. If the CA follows redirects, the following apply:<br>1. Redirects MUST be initiated at the HTTP protocol layer.<br>・ 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.<br>・ Redirects MUST be to the final value of the Location HTTP response header, as defined in RFC 7231, Section 7.1.2.<br>2. Redirects MUST be to resource URLs with either the "http" or "https" scheme.<br>3. Redirects MUST be to resource URLs accessed via port 80 (http) or 443 (https).<br>This method is not applicable for validating Wildcard Domain Names.<br>**3.2.2.4.20 TLS Using ALPN**<br>Not applicable<br>**3.2.2.5 Authentication for an IP Address**<br>The CA does not issue any certificate to grant certification to any IP Address.<br>**3.2.2.6 Wildcard Domain Validation**<br>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 | |

| 変更履歴あり | 整形版 | 備考 |
| --- | --- | --- |
| 6454 Section 8.2 for further explanation).<br><br>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.).<br><br>Determination of what is "registry-controlled" versus the registerable portion of a Country Code Top-Level Domain Namespace is accordance with Baseline Requirements.<br><br>**3.2.2.7 Data Source Accuracy**<br>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:<br><br>1. The age of the information provided,<br>2. The frequency of updates to the information source,<br>3. The data provider and purpose of the data collection,<br>4. The public accessibility of the data availability, and<br>5. The relative difficulty in falsifying or altering the data.<br><br>**3.2.2.8 CAA Records**<br>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.<br><br>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.<br><br>The CA MUST respect the critical flag and not issue a certificate if they encounter an unrecognized property tag with this flag set.<br><br>The CA permitted to treat a record lookup failure as permission to issue if:<br>- the failure is outside the CA's infrastructure; and<br>- the lookup has been retried at least once; and<br>- the domain's zone does not have a DNSSEC validation chain to the ICANN root. | 6454 Section 8.2 for further explanation).<br><br>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.).<br><br>Determination of what is "registry-controlled" versus the registerable portion of a Country Code Top-Level Domain Namespace is accordance with Baseline Requirements.<br><br>**3.2.2.7 Data Source Accuracy**<br>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:<br><br>1. The age of the information provided,<br>2. The frequency of updates to the information source,<br>3. The data provider and purpose of the data collection,<br>4. The public accessibility of the data availability, and<br>5. The relative difficulty in falsifying or altering the data.<br><br>**3.2.2.8 CAA Records**<br>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.<br><br>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.<br><br>The CA MUST respect the critical flag and not issue a certificate if they encounter an unrecognized property tag with this flag set.<br><br>The CA permitted to treat a record lookup failure as permission to issue if:<br>- the failure is outside the CA's infrastructure; and<br>- the lookup has been retried at least once; and<br>- the domain's zone does not have a DNSSEC validation chain to the ICANN root. | |

| 変更履歴あり | 整形版 | 備考 |
| --- | --- | --- |
| The CA shall log any actions taken as part of its processing practices.<br>**3.2.3 Authentication of Individual Identity**<br>The CA does not issue any certificate to grant certification to any individual.<br>**3.2.4 Non-Verified Subscriber Information**<br>(1) Domain Validation<br>The CA stipulates no policies on non-verified information on Subscribers.<br>(2) Organization Validation<br>The CA stipulates no policies on non-verified information on Subscribers.<br>**3.2.5 Validation of Authority**<br>(1) Domain Validation<br>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.<br>(2) Organization Validation<br>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.<br>**3.2.6 Criteria for Interoperation**<br>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.<br>**3.3 Identification and Authentication for Re-key Requests**<br>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.<br>**3.4 Identification and Authentication for Revocation Request**<br>The CA shall validate an identity in order to accept Revocation Request by check one of the following;<br>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.<br>2. The certificate issued under ACME protocol and the Revocation Request is signed by private key of the account granted to the subscriber.<br>3. The certificate issued under ACME protocol and the Revocation Request is signed by private key of the certificate. | The CA shall log any actions taken as part of its processing practices.<br>**3.2.3 Authentication of Individual Identity**<br>The CA does not issue any certificate to grant certification to any individual.<br>**3.2.4 Non-Verified Subscriber Information**<br>(1) Domain Validation<br>The CA stipulates no policies on non-verified information on Subscribers.<br>(2) Organization Validation<br>The CA stipulates no policies on non-verified information on Subscribers.<br>**3.2.5 Validation of Authority**<br>(1) Domain Validation<br>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.<br>(2) Organization Validation<br>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.<br>**3.2.6 Criteria for Interoperation**<br>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.<br>**3.3 Identification and Authentication for Re-key Requests**<br>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.<br>**3.4 Identification and Authentication for Revocation Request**<br>The CA shall validate an identity in order to accept Revocation Request by check one of the following;<br>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.<br>2. The certificate issued under ACME protocol and the Revocation Request is signed by private key of the account granted to the subscriber.<br>3. The certificate issued under ACME protocol and the Revocation Request is signed by private key of the certificate. | |

| 変更履歴あり | 整形版 | 備考 |
| --- | --- | --- |
| # 4. Certificate Life-Cycle Operational Requirements<br><br>## 4.1 Certificate Application<br><br>### 4.1.1 Who Can Submit a Certificate Application<br><br>(1) Domain Validation<br>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.<br>(2) Organization Validation<br>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.<br><br>### 4.1.2 Enrollment Process and Responsibilities<br><br>Each person who may apply for a certificate and intends to do so shall apply for the certificate after consenting to the provisions of the Terms and Conditions, this CP, and the CPS. Each person applying for a certificate must assure that the information provided in the Certificate Application submitted to the CA is accurate.<br><br>## 4.2 Certificate Application Processing<br><br>### 4.2.1 Performing Identification and Authentication Functions<br><br>The CA shall review application information by considering the information in the manner set forth in “3.2 Initial Identity Validation” of this CP.<br>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 the CA's Certificate Policy and/or Certification Practice Statement. 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.<br><br>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.<br><br>Section 6.3.2 of this CP limits the validity period of Subscriber Certificates.<br>The CA MAY use the documents and data provided in Section 3.2 of this CP to verify | # 4. Certificate Life-Cycle Operational Requirements<br><br>## 4.1 Certificate Application<br><br>### 4.1.1 Who Can Submit a Certificate Application<br><br>(1) Domain Validation<br>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.<br>(2) Organization Validation<br>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.<br><br>### 4.1.2 Enrollment Process and Responsibilities<br><br>Each person who may apply for a certificate and intends to do so shall apply for the certificate after consenting to the provisions of the Terms and Conditions, this CP, and the CPS. Each person applying for a certificate must assure that the information provided in the Certificate Application submitted to the CA is accurate.<br><br>## 4.2 Certificate Application Processing<br><br>### 4.2.1 Performing Identification and Authentication Functions<br><br>The CA shall review application information by considering the information in the manner set forth in “3.2 Initial Identity Validation” of this CP.<br>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 the CA's Certificate Policy and/or Certification Practice Statement. 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.<br><br>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.<br><br>Section 6.3.2 of this CP limits the validity period of Subscriber Certificates.<br>The CA MAY use the documents and data provided in Section 3.2 of this CP to verify | |

| 変更履歴あり | 整形版 | 備考 |
| --- | --- | --- |
| 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 or completed the validation itself no more than 825 days prior to issuing the Certificate.<br><br>For validation of Domain Names according to Section 3.2.2.4 of this CP, any data, document, or completed validation used MUST be obtained no more than 398 days prior to issuing the Certificate.<br>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.<br><br>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.<br><br>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. | 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 or completed the validation itself no more than 825 days prior to issuing the Certificate.<br><br>For validation of Domain Names according to Section 3.2.2.4 of this CP, any data, document, or completed validation used MUST be obtained no more than 398 days prior to issuing the Certificate.<br>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.<br><br>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.<br><br>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**<br>On approving any certificate application as a result of the review, the CA shall proceed to the issuance registration of the certificate.<br><br>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. | **4.2.2 Approval or Rejection of a Certificate Application**<br>On approving any certificate application as a result of the review, the CA shall proceed to the issuance registration of the certificate.<br><br>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**<br>After approving a certificate application, the CA shall proceed to the issuance registration of the certificate in a timely manner. | **4.2.3 Time to Process Certificate Applications**<br>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**<br>In reviewing the application information, the CA shall check the CAA records in accordance with RFC 8659. The domain of the CA to be described in the CAA records shall be “jprs.jp.”<br>The Certificate Subscribers who want to grant the authority to issue certificates to the FQDN must include the value of "jprs.jp" in the property "issue" of the CAA record for each DNS zone. | **4.2.4 Check of CAA Records**<br>In reviewing the application information, the CA shall check the CAA records in accordance with RFC 8659. The domain of the CA to be described in the CAA records shall be “jprs.jp.”<br>The Certificate Subscribers who want to grant the authority to issue certificates to the FQDN must include the value of "jprs.jp" in the property "issue" of the CAA record for each DNS zone. | |
| **4.3 Certificate Issuance** | **4.3 Certificate Issuance** | |

| 変更履歴あり | 整形版 | 備考 |
| --- | --- | --- |
| ### 4.3.1 CA Actions during Certificate Issuance<br>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.<br>#### 4.3.1.1 Manual authorization of certificate issuance for Root CAs<br>No stipulation.<br>#### 4.3.1.2 Linting of to-be-signed Certificate content<br>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.<br>#### 4.3.1.3 Linting of issued Certificates<br>The CA MAY use a Linting process to test each issued Certificate.<br>### 4.3.2 Notification to Subscriber of Certificate Issuance<br>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.<br>## 4.4 Certificate Acceptance<br>### 4.4.1 Conduct Constituting Certificate Acceptance<br>The Subscriber shall be deemed to have accepted the certificate at any of the following time;<br>1. When the Subscriber requests to get the certificate from the subscriber-only web page and the CA responses the Certificate.<br>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.<br>3. When the subscriber installs the certificate obtained by a method other than 1 and 2 into his/her/its server.<br>### 4.4.2 Publication of the Certificates by the CA<br>The CA does not publish certificates of Subscribers.<br>### 4.4.3 Notification of Certificate Issuance by the CA to Other Entities<br>The CA does not notify any third party (excluding Designated Business Enterprises) of the issuance of certificates.<br>## 4.5 Key Pair and Certificate Usage | ### 4.3.1 CA Actions during Certificate Issuance<br>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.<br>#### 4.3.1.1 Manual authorization of certificate issuance for Root CAs<br>No stipulation.<br>#### 4.3.1.2 Linting of to-be-signed Certificate content<br>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.<br>#### 4.3.1.3 Linting of issued Certificates<br>The CA MAY use a Linting process to test each issued Certificate.<br>### 4.3.2 Notification to Subscriber of Certificate Issuance<br>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.<br>## 4.4 Certificate Acceptance<br>### 4.4.1 Conduct Constituting Certificate Acceptance<br>The Subscriber shall be deemed to have accepted the certificate at any of the following time;<br>1. When the Subscriber requests to get the certificate from the subscriber-only web page and the CA responses the Certificate.<br>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.<br>3. When the subscriber installs the certificate obtained by a method other than 1 and 2 into his/her/its server.<br>### 4.4.2 Publication of the Certificates by the CA<br>The CA does not publish certificates of Subscribers.<br>### 4.4.3 Notification of Certificate Issuance by the CA to Other Entities<br>The CA does not notify any third party (excluding Designated Business Enterprises) of the issuance of certificates.<br>## 4.5 Key Pair and Certificate Usage | Baseline Requirementsへの準拠を明確にするための追記 |

| 変更履歴あり | 整形版 | 備考 |
| --- | --- | --- |
| **4.5.1 Subscriber Private Key and Certificate Usage**<br>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.<br>**4.5.2 Relying Party Public Key and Certificate Usage**<br>Relying Parties may verify the reliability of certificates issued by the CA by using such certificates. Relying Parties shall understand and consent to the provisions of this CP and the CPS before verifying the reliability of certificates issued by the CA and relying on the same.<br>**4.6 Certificate Renewal**<br>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.<br>**4.6.1 Circumstances for Certificate Renewal**<br>A certificate may be renewed without involving rekey when the certificate is about to expire.<br>**4.6.2 Who May Request Renewal**<br>The provisions of “4.1.1 Who Can Submit a Certificate Application” of this CP shall apply correspondingly.<br>**4.6.3 Processing Certificate Renewal Requests**<br>The provisions of “4.3.1 CA Actions during Certificate Issuance” of this CP shall apply correspondingly.<br>**4.6.4 Notification of New Certificate Issuance to Subscriber**<br>The provisions of “4.3.2 Notification to Subscriber of Certificate Issuance” of this CP shall apply correspondingly.<br>**4.6.5 Conduct Constituting Acceptance of a Renewal Certificate**<br>The provisions of “4.4.1 Conduct Constituting Certificate Acceptance” of this CP shall apply correspondingly.<br>**4.6.6 Publication of the Renewal Certificate by the CA**<br>The provisions of “4.4.2 Publication of the Certificates by the CA” of this CP shall apply correspondingly.<br>**4.6.7 Notification of Certificate Issuance by the CA to Other Entities**<br>The provisions of “4.4.3 Notification of Certificate Issuance by the CA to Other Entities” of this CP shall apply correspondingly. | **4.5.1 Subscriber Private Key and Certificate Usage**<br>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.<br>**4.5.2 Relying Party Public Key and Certificate Usage**<br>Relying Parties may verify the reliability of certificates issued by the CA by using such certificates. Relying Parties shall understand and consent to the provisions of this CP and the CPS before verifying the reliability of certificates issued by the CA and relying on the same.<br>**4.6 Certificate Renewal**<br>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.<br>**4.6.1 Circumstances for Certificate Renewal**<br>A certificate may be renewed without involving rekey when the certificate is about to expire.<br>**4.6.2 Who May Request Renewal**<br>The provisions of “4.1.1 Who Can Submit a Certificate Application” of this CP shall apply correspondingly.<br>**4.6.3 Processing Certificate Renewal Requests**<br>The provisions of “4.3.1 CA Actions during Certificate Issuance” of this CP shall apply correspondingly.<br>**4.6.4 Notification of New Certificate Issuance to Subscriber**<br>The provisions of “4.3.2 Notification to Subscriber of Certificate Issuance” of this CP shall apply correspondingly.<br>**4.6.5 Conduct Constituting Acceptance of a Renewal Certificate**<br>The provisions of “4.4.1 Conduct Constituting Certificate Acceptance” of this CP shall apply correspondingly.<br>**4.6.6 Publication of the Renewal Certificate by the CA**<br>The provisions of “4.4.2 Publication of the Certificates by the CA” of this CP shall apply correspondingly.<br>**4.6.7 Notification of Certificate Issuance by the CA to Other Entities**<br>The provisions of “4.4.3 Notification of Certificate Issuance by the CA to Other Entities” of this CP shall apply correspondingly. | |

| 変更履歴あり | 整形版 | 備考 |
| --- | --- | --- |
| **4.7 Certificate Re-key**<br>A “certificate re-key” means the issuance of a new certificate to a Subscriber after generating a new Key Pair.<br>**4.7.1 Circumstances for Certificate Re-key**<br>A certificate may be renewed without involving re-key when the certificate is about to expire.<br>**4.7.2 Who May Request Certification of a New Public Key**<br>The provisions of “4.1.1 Who Can Submit a Certificate Application” of this CP shall apply correspondingly.<br>**4.7.3 Processing Certificate Re-keying Requests**<br>The provisions of “4.3.1 CA Actions during Certificate Issuance” of this CP shall apply correspondingly.<br>**4.7.4 Notification of New Certificate Issuance to Subscriber**<br>The provisions of “4.3.2 Notification to Subscriber of Certificate Issuance” of this CP shall apply correspondingly.<br>**4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate**<br>The provisions of “4.4.1 Conduct Constituting Certificate Acceptance” of this CP shall apply correspondingly.<br>**4.7.6 Publication of the Re-keyed Certificates by the CA**<br>The provisions of “4.4.2 Publication of the Certificates by the CA” of this CP shall apply correspondingly.<br>**4.7.7 Notification of Certificate Issuance by the CA to Other Entities**<br>The provisions of “4.4.3 Notification of Certificate Issuance by the CA to Other Entities” of this CP shall apply correspondingly.<br>**4.8 Certificate Modification**<br>**4.8.1 Circumstances for Certificate Modification**<br>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.<br>**4.8.2 Who May Request Certificate Modification**<br>The provisions of “4.1.1 Who Can Submit a Certificate Application” of this CP shall apply correspondingly.<br>**4.8.3 Processing Certificate Modification Requests**<br>The provisions of “4.3.1 CA Actions during Certificate Issuance” of this CP shall apply | **4.7 Certificate Re-key**<br>A “certificate re-key” means the issuance of a new certificate to a Subscriber after generating a new Key Pair.<br>**4.7.1 Circumstances for Certificate Re-key**<br>A certificate may be renewed without involving re-key when the certificate is about to expire.<br>**4.7.2 Who May Request Certification of a New Public Key**<br>The provisions of “4.1.1 Who Can Submit a Certificate Application” of this CP shall apply correspondingly.<br>**4.7.3 Processing Certificate Re-keying Requests**<br>The provisions of “4.3.1 CA Actions during Certificate Issuance” of this CP shall apply correspondingly.<br>**4.7.4 Notification of New Certificate Issuance to Subscriber**<br>The provisions of “4.3.2 Notification to Subscriber of Certificate Issuance” of this CP shall apply correspondingly.<br>**4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate**<br>The provisions of “4.4.1 Conduct Constituting Certificate Acceptance” of this CP shall apply correspondingly.<br>**4.7.6 Publication of the Re-keyed Certificates by the CA**<br>The provisions of “4.4.2 Publication of the Certificates by the CA” of this CP shall apply correspondingly.<br>**4.7.7 Notification of Certificate Issuance by the CA to Other Entities**<br>The provisions of “4.4.3 Notification of Certificate Issuance by the CA to Other Entities” of this CP shall apply correspondingly.<br>**4.8 Certificate Modification**<br>**4.8.1 Circumstances for Certificate Modification**<br>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.<br>**4.8.2 Who May Request Certificate Modification**<br>The provisions of “4.1.1 Who Can Submit a Certificate Application” of this CP shall apply correspondingly.<br>**4.8.3 Processing Certificate Modification Requests**<br>The provisions of “4.3.1 CA Actions during Certificate Issuance” of this CP shall apply | |

| 変更履歴あり | 整形版 | 備考 |
| --- | --- | --- |
| correspondingly.<br>**4.8.4 Notification of New Certificate Issuance to Subscriber**<br>The provisions of “4.3.2 Notification to Subscriber of Certificate Issuance” of this CP shall apply correspondingly.<br>**4.8.5 Conduct Constituting Acceptance of Modified Certificate**<br>The provisions of “4.4.1 Conduct Constituting Certificate Acceptance” of this CP shall apply correspondingly.<br>**4.8.6 Publication of the Modified Certificate by the CA**<br>The provisions of “4.4.2 Publication of the Certificates by the CA” of this CP shall apply correspondingly.<br>**4.8.7 Notification of Certificate Issuance by the CA to Other Entities**<br>The provisions of “4.4.3 Notification of Certificate Issuance by the CA to Other Entities” of this CP shall apply correspondingly.<br>**4.9 Certificate Revocation and Suspension**<br>**4.9.1 Circumstances for Certificate Revocation**<br>If any one of the following events occurs, the Subscriber must apply to the CA to have the corresponding certificate revoked:<br>・ the information described in the certificate has changed;<br>・ the Private Key has been or may be compromised for any reason, including theft, loss, leakage, or unauthorized use thereof;<br>・ any of the particulars described in the certificate or its purposes of use are incorrect;<br>・ the Subscriber finds that an improper string has been designated for, or is included in, a value set in any information in the certificate (as set forth in “3.1.1 Types of Names” of this CP) (for Organization Validation only); or<br>・ the Subscriber stops using the certificate.<br><br>The CA SHALL revoke a Certificate within 24 hours and use the corresponding CRLReason if one or more of the following occurs:<br><br>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);<br>2. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization (CRLReason #9, privilegeWithdrawn);<br>3. The CA obtains evidence that the Subscriber's Private Key corresponding to the | correspondingly.<br>**4.8.4 Notification of New Certificate Issuance to Subscriber**<br>The provisions of “4.3.2 Notification to Subscriber of Certificate Issuance” of this CP shall apply correspondingly.<br>**4.8.5 Conduct Constituting Acceptance of Modified Certificate**<br>The provisions of “4.4.1 Conduct Constituting Certificate Acceptance” of this CP shall apply correspondingly.<br>**4.8.6 Publication of the Modified Certificate by the CA**<br>The provisions of “4.4.2 Publication of the Certificates by the CA” of this CP shall apply correspondingly.<br>**4.8.7 Notification of Certificate Issuance by the CA to Other Entities**<br>The provisions of “4.4.3 Notification of Certificate Issuance by the CA to Other Entities” of this CP shall apply correspondingly.<br>**4.9 Certificate Revocation and Suspension**<br>**4.9.1 Circumstances for Certificate Revocation**<br>If any one of the following events occurs, the Subscriber must apply to the CA to have the corresponding certificate revoked:<br>・ the information described in the certificate has changed;<br>・ the Private Key has been or may be compromised for any reason, including theft, loss, leakage, or unauthorized use thereof;<br>・ any of the particulars described in the certificate or its purposes of use are incorrect;<br>・ the Subscriber finds that an improper string has been designated for, or is included in, a value set in any information in the certificate (as set forth in “3.1.1 Types of Names” of this CP) (for Organization Validation only); or<br>・ the Subscriber stops using the certificate.<br><br>The CA SHALL revoke a Certificate within 24 hours and use the corresponding CRLReason if one or more of the following occurs:<br><br>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);<br>2. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization (CRLReason #9, privilegeWithdrawn);<br>3. The CA obtains evidence that the Subscriber's Private Key corresponding to the | |

| 変更履歴あり | 整形版 | 備考 |
| --- | --- | --- |
| Public Key in the Certificate suffered a Key Compromise (CRLReason #1, keyCompromise);<br>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), CPS “6.1.1 Key Pair Generation”~~(such as a Debian weak key, see https://wiki.debian.org/SSLkeys)~~ (CRLReason #1, keyCompromise);<br>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).<br><br>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:<br><br>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);<br>7. The CA obtains evidence that the Certificate was misused (CRLReason #9, privilegeWithdrawn);<br>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);<br>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);<br>10. The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate FQDN (CRLReason #9, privilegeWithdrawn);<br>11. The CA is made aware of a material change in the information contained in the Certificate (CRLReason #9, privilegeWithdrawn);<br>12. The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's CP or CPS(CRLReason #4, superseded);<br>13. The CA determines or is made aware that any of the information appearing in the Certificate is inaccurate (CRLReason #9, privilegeWithdrawn);<br>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 | Public Key in the Certificate suffered a Key Compromise (CRLReason #1, keyCompromise);<br>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), CPS “6.1.1 Key Pair Generation” (CRLReason #1, keyCompromise);<br>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).<br><br>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:<br><br>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);<br>7. The CA obtains evidence that the Certificate was misused (CRLReason #9, privilegeWithdrawn);<br>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);<br>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);<br>10. The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate FQDN (CRLReason #9, privilegeWithdrawn);<br>11. The CA is made aware of a material change in the information contained in the Certificate (CRLReason #9, privilegeWithdrawn);<br>12. The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's CP or CPS(CRLReason #4, superseded);<br>13. The CA determines or is made aware that any of the information appearing in the Certificate is inaccurate (CRLReason #9, privilegeWithdrawn);<br>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 | Baseline Requirementsへの準拠を明確にするための追記 |

| 変更履歴あり | 整形版 | 備考 |
| --- | --- | --- |
| in no reasonCode extension being provided in the CRL);<br>15. Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement 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<br>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).<br>**4.9.2 Who Can Request Revocation**<br>The following can request the Revocation Request;<br>1. The Subscriber<br>2. Designated Business Enterprise that has acted as an agent in the application for issuance of the certificate or use of services.<br>3. Owner of the private key for the Certificate.<br>**4.9.3 Procedures for Revocation Request**<br>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.<br>1. Request through Designated Business Enterprise<br>2. Request under ACME protocol<br>**4.9.4 Revocation Request Grace Period**<br>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.<br>The CA SHALL maintain a continuous 24x7 ability to accept and respond to revocation requests and Certificate Problem Reports.<br>**4.9.5 Time within Which the CA Shall Process the Revocation Request**<br>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.<br>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.<br>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 | in no reasonCode extension being provided in the CRL);<br>15. Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement 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<br>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).<br>**4.9.2 Who Can Request Revocation**<br>The following can request the Revocation Request;<br>1. The Subscriber<br>2. Designated Business Enterprise that has acted as an agent in the application for issuance of the certificate or use of services.<br>3. Owner of the private key for the Certificate.<br>**4.9.3 Procedures for Revocation Request**<br>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.<br>1. Request through Designated Business Enterprise<br>2. Request under ACME protocol<br>**4.9.4 Revocation Request Grace Period**<br>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.<br>The CA SHALL maintain a continuous 24x7 ability to accept and respond to revocation requests and Certificate Problem Reports.<br>**4.9.5 Time within Which the CA Shall Process the Revocation Request**<br>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.<br>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.<br>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 | |

| 変更履歴あり | 整形版 | 備考 |
| --- | --- | --- |
| forth in Section 4.9.1.1 of this CP.<br>**4.9.6 Revocation Checking Requirement for Relying Parties**<br>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.<br>**4.9.7 CRL Issuance Frequency**<br>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.<br>**4.9.8 Maximum Latency for CRLs**<br>The CA shall forthwith reflect an issued CRL in the Repository.<br>**4.9.9 On-line Revocation/Status Checking Availability**<br>Information on the certificate status shall be provided online via the OCSP server.<br>OCSP responses MUST conform to RFC 6960 and/or RFC 5019. OCSP responses MUST either:<br>1. Be signed by the CA that issued the Certificates whose revocation status is being checked, or<br>2. Be signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked.<br>In the latter case, the OCSP signing Certificate MUST contain an extension of type id-pkix-ocsp-nocheck, as defined by RFC 6960.<br>**4.9.10 On-line Revocation/Status Checking Requirements**<br>Before placing trust and using a certificate issued by the CA, the Relying Party must verify the validity of the certificate. If any Relying Party does not confirm whether or not the revocation of the certificate has been registered by checking the CRL included in the Repository, the Relying Party shall check the information on the certificate status provided through the OCSP server.<br>OCSP responders operated by the CA SHALL support the HTTP GET method, as described in RFC 6960 and/or RFC 5019.<br>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.<br>For the status of Subscriber Certificates: | forth in Section 4.9.1.1 of this CP.<br>**4.9.6 Revocation Checking Requirement for Relying Parties**<br>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.<br>**4.9.7 CRL Issuance Frequency**<br>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.<br>**4.9.8 Maximum Latency for CRLs**<br>The CA shall forthwith reflect an issued CRL in the Repository.<br>**4.9.9 On-line Revocation/Status Checking Availability**<br>Information on the certificate status shall be provided online via the OCSP server.<br>OCSP responses MUST conform to RFC 6960 and/or RFC 5019. OCSP responses MUST either:<br>1. Be signed by the CA that issued the Certificates whose revocation status is being checked, or<br>2. Be signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked.<br>In the latter case, the OCSP signing Certificate MUST contain an extension of type id-pkix-ocsp-nocheck, as defined by RFC 6960.<br>**4.9.10 On-line Revocation/Status Checking Requirements**<br>Before placing trust and using a certificate issued by the CA, the Relying Party must verify the validity of the certificate. If any Relying Party does not confirm whether or not the revocation of the certificate has been registered by checking the CRL included in the Repository, the Relying Party shall check the information on the certificate status provided through the OCSP server.<br>OCSP responders operated by the CA SHALL support the HTTP GET method, as described in RFC 6960 and/or RFC 5019.<br>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.<br>For the status of Subscriber Certificates: | |

| 変更履歴あり | 整形版 | 備考 |
| --- | --- | --- |
| 1. OCSP responses MUST have a validity interval greater than or equal to eight hours;<br>2. OCSP responses MUST have a validity interval less than or equal to ten days;<br>3. For OCSP responses with validity intervals less than sixteen hours, then the CA SHALL update the information provided via an Online Certificate Status Protocol prior to one-half of the validity period before the nextUpdate.<br>4. For OCSP responses with validity intervals greater than or equal to sixteen hours, then the CA SHALL update the information provided via an Online Certificate Status Protocol at least eight hours prior to the nextUpdate, and no later than four days after the thisUpdate.<br><br>If the OCSP responder receives a request for the status of a certificate serial number that is "unused", 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, the responder MUST NOT respond with a "good" status for such requests.<br>The CA SHOULD monitor the OCSP responder for requests for "unused" serial numbers as part of its security response procedures.<br>The OCSP responder MAY provide definitive responses about "reserved" certificate serial numbers, as if there was a corresponding Certificate that matches the Precertificate [RFC 6962].<br>A certificate serial number within an OCSP request is one of the following three options:<br><br>1. "assigned" if a Certificate with that serial number has been issued by the Issuing CA, using any current or previous key associated with that CA subject; or<br>2. "reserved" if a Precertificate [RFC 6962] with that serial number has been issued by a. the Issuing CA; or b. a Precertificate Signing Certificate, as defined in Section 7.1.2.4, associated with the Issuing CA; or<br>3. "unused" if neither of the previous conditions are met.<br><br>**4.9.11 Other Forms of Revocation Advertisements Available**<br><br>Not applicable.<br><br>**4.9.12 Special Requirements Regarding Key Compromise**<br><br>If a compromise of any Private Key pertaining to a certificate issued by the CA is revealed, please notify via the following webform:<br>https://jprs.jp/pubcert/f_mail/<br>Please include either of the following information in your report.<br>・The compromised private key itself<br>・A CSR signed by the compromised private key | 1. OCSP responses MUST have a validity interval greater than or equal to eight hours;<br>2. OCSP responses MUST have a validity interval less than or equal to ten days;<br>3. For OCSP responses with validity intervals less than sixteen hours, then the CA SHALL update the information provided via an Online Certificate Status Protocol prior to one-half of the validity period before the nextUpdate.<br>4. For OCSP responses with validity intervals greater than or equal to sixteen hours, then the CA SHALL update the information provided via an Online Certificate Status Protocol at least eight hours prior to the nextUpdate, and no later than four days after the thisUpdate.<br><br>If the OCSP responder receives a request for the status of a certificate serial number that is "unused", 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, the responder MUST NOT respond with a "good" status for such requests.<br>The CA SHOULD monitor the OCSP responder for requests for "unused" serial numbers as part of its security response procedures.<br>The OCSP responder MAY provide definitive responses about "reserved" certificate serial numbers, as if there was a corresponding Certificate that matches the Precertificate [RFC 6962].<br>A certificate serial number within an OCSP request is one of the following three options:<br><br>1. "assigned" if a Certificate with that serial number has been issued by the Issuing CA, using any current or previous key associated with that CA subject; or<br>2. "reserved" if a Precertificate [RFC 6962] with that serial number has been issued by a. the Issuing CA; or b. a Precertificate Signing Certificate, as defined in Section 7.1.2.4, associated with the Issuing CA; or<br>3. "unused" if neither of the previous conditions are met.<br><br>**4.9.11 Other Forms of Revocation Advertisements Available**<br><br>Not applicable.<br><br>**4.9.12 Special Requirements Regarding Key Compromise**<br><br>If a compromise of any Private Key pertaining to a certificate issued by the CA is revealed, please notify via the following webform:<br>https://jprs.jp/pubcert/f_mail/<br>Please include either of the following information in your report.<br>・The compromised private key itself<br>・A CSR signed by the compromised private key | |

| 変更履歴あり | 整形版 | 備考 |
| --- | --- | --- |
| (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")<br>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.<br>**4.9.13 Circumstances for Suspension**<br>Not applicable.<br>**4.9.14 Who Can Request Suspension**<br>Not applicable.<br>**4.9.15 Procedures for Suspension Request**<br>Not applicable.<br>**4.9.16 Limits on Suspension Period**<br>Not applicable.<br>**4.10 Certificate Status Services**<br>**4.10.1 Operational Characteristics**<br>Subscribers and Relying Parties may check information on the status of a certificate through the OCSP server.<br>Revocation entries on a CRL or OCSP Response MUST NOT be removed until after the Expiry Date of the revoked Certificate.<br>**4.10.2 Service Availability**<br>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.<br>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.<br><br>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.<br><br>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.<br>**4.10.3 Optional Features** | (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")<br>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.<br>**4.9.13 Circumstances for Suspension**<br>Not applicable.<br>**4.9.14 Who Can Request Suspension**<br>Not applicable.<br>**4.9.15 Procedures for Suspension Request**<br>Not applicable.<br>**4.9.16 Limits on Suspension Period**<br>Not applicable.<br>**4.10 Certificate Status Services**<br>**4.10.1 Operational Characteristics**<br>Subscribers and Relying Parties may check information on the status of a certificate through the OCSP server.<br>Revocation entries on a CRL or OCSP Response MUST NOT be removed until after the Expiry Date of the revoked Certificate.<br>**4.10.2 Service Availability**<br>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.<br>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.<br><br>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.<br><br>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.<br>**4.10.3 Optional Features** | |

| 変更履歴あり | 整形版 | 備考 |
| --- | --- | --- |
| No stipulation.<br>**4.11 End of Subscription (Registration)**<br>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.<br>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.<br>**4.12 Key Escrow and Recovery**<br>**4.12.1 Key Escrow and Recovery Policy and Practices**<br>The CA does not escrow the Private Keys of Subscribers.<br>**4.12.2 Session Key Encapsulation and Recovery Policy and Practices**<br>Not applicable.<br>**5. Facility, Management, and Operational Controls**<br>**5.1 Physical Security Controls**<br>Stipulated in the CPS.<br>**5.2 Procedural Controls**<br>Stipulated in the CPS.<br>**5.3 Personnel Controls**<br>Stipulated in the CPS.<br>**5.4 Audit Logging Procedures**<br>**5.4.1 Types of Events Recorded**<br>Stipulated in the CPS.<br>**5.4.2 Frequency of Processing Audit Log**<br>Stipulated in the CPS.<br>**5.4.3 Retention Period for Audit Log**<br>Stipulated in the CPS. Audit Logs on the RA system shall be archived for at least seven (7) years.<br>**5.4.4 Protection of Audit Log** | No stipulation.<br>**4.11 End of Subscription (Registration)**<br>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.<br>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.<br>**4.12 Key Escrow and Recovery**<br>**4.12.1 Key Escrow and Recovery Policy and Practices**<br>The CA does not escrow the Private Keys of Subscribers.<br>**4.12.2 Session Key Encapsulation and Recovery Policy and Practices**<br>Not applicable.<br>**5. Facility, Management, and Operational Controls**<br>**5.1 Physical Security Controls**<br>Stipulated in the CPS.<br>**5.2 Procedural Controls**<br>Stipulated in the CPS.<br>**5.3 Personnel Controls**<br>Stipulated in the CPS.<br>**5.4 Audit Logging Procedures**<br>**5.4.1 Types of Events Recorded**<br>Stipulated in the CPS.<br>**5.4.2 Frequency of Processing Audit Log**<br>Stipulated in the CPS.<br>**5.4.3 Retention Period for Audit Log**<br>Stipulated in the CPS. Audit Logs on the RA system shall be archived for at least seven (7) years.<br>**5.4.4 Protection of Audit Log** | |

| 変更履歴あり | 整形版 | 備考 |
| --- | --- | --- |
| Stipulated in the CPS.<br>**5.4.5 Audit Logs Backup Procedure**<br>Stipulated in the CPS.<br>**5.4.6 Audit Log Collection System**<br>Stipulated in the CPS.<br>**5.4.7 Notification to Event-Causing Subject**<br>Stipulated in the CPS.<br>**5.4.8 Vulnerability Assessments**<br>Stipulated in the CPS.<br>**5.5 Records Archival**<br>**5.5.1 Types of Records Archived**<br>The CA shall archive the following information in addition to the information prescribed in "5.5 Records Archival" of the CPS:<br>・ this CP;<br>・ documents prepared under this CP stipulating the business operations of the Certification Authority;<br>・ records and audit reports on the results of audits; and<br>・ information on applications from Subscribers and the histories thereof.<br>**5.5.2 Retention Period for Archive**<br>Stipulated in the CPS. The CA shall archive the following information for at least seven (7) years:<br>・ this CP;<br>・ documents prepared under this CP stipulating the business operations of the Certification Authority;<br>・ records and audit reports on the results of audits; and<br>・ information on applications from Subscribers and the histories thereof.<br>**5.5.3 Protection of Archive**<br>Stipulated in the CPS.<br>**5.5.4 Archive Backup Procedures**<br>Stipulated in the CPS.<br>**5.5.5 Requirements for Time-Stamping of Records**<br>Stipulated in the CPS.<br>**5.5.6 Archive Collection System** | Stipulated in the CPS.<br>**5.4.5 Audit Logs Backup Procedure**<br>Stipulated in the CPS.<br>**5.4.6 Audit Log Collection System**<br>Stipulated in the CPS.<br>**5.4.7 Notification to Event-Causing Subject**<br>Stipulated in the CPS.<br>**5.4.8 Vulnerability Assessments**<br>Stipulated in the CPS.<br>**5.5 Records Archival**<br>**5.5.1 Types of Records Archived**<br>The CA shall archive the following information in addition to the information prescribed in "5.5 Records Archival" of the CPS:<br>・ this CP;<br>・ documents prepared under this CP stipulating the business operations of the Certification Authority;<br>・ records and audit reports on the results of audits; and<br>・ information on applications from Subscribers and the histories thereof.<br>**5.5.2 Retention Period for Archive**<br>Stipulated in the CPS. The CA shall archive the following information for at least seven (7) years:<br>・ this CP;<br>・ documents prepared under this CP stipulating the business operations of the Certification Authority;<br>・ records and audit reports on the results of audits; and<br>・ information on applications from Subscribers and the histories thereof.<br>**5.5.3 Protection of Archive**<br>Stipulated in the CPS.<br>**5.5.4 Archive Backup Procedures**<br>Stipulated in the CPS.<br>**5.5.5 Requirements for Time-Stamping of Records**<br>Stipulated in the CPS.<br>**5.5.6 Archive Collection System** | |

| 変更履歴あり | 整形版 | 備考 |
| --- | --- | --- |
| Stipulated in the CPS.<br>#### 5.5.7 Procedures to Obtain and Verify Archive Information<br>Stipulated in the CPS.<br>### 5.6 Key Changeover<br>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.<br>### 5.7 Compromise and Disaster Recovery<br>Stipulated in the CPS.<br>### 5.8 CA or RA Termination<br>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."<br>## 6. Technical Security Controls<br>### 6.1 Key Pair Generation and Installation<br>#### 6.1.1 Key Pair Generation<br>"6.1.1 Generation of Key Pairs" of the CPS stipulates a policy on Private Keys of the CA.<br>#### 6.1.2 Private Key Delivery to Subscriber<br>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.<br>#### 6.1.3 Public Key Delivery to the Certificate Issuer<br>A Subscriber shall deliver his/her/its Public Key to the CA online when applying for his/her/its certificate. The communication pathways for such delivery shall be encrypted by the TLS.<br>#### 6.1.4 CA' Public Key Delivery to Relying Parties<br>Relying Parties may obtain Public Keys of the CA by accessing the CA's Repository.<br>#### 6.1.5 Key Sizes<br>When issuing a TLS server certificate that complies with Baseline Requirements, the following confirmation need to be done: | Stipulated in the CPS.<br>#### 5.5.7 Procedures to Obtain and Verify Archive Information<br>Stipulated in the CPS.<br>### 5.6 Key Changeover<br>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.<br>### 5.7 Compromise and Disaster Recovery<br>Stipulated in the CPS.<br>### 5.8 CA or RA Termination<br>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."<br>## 6. Technical Security Controls<br>### 6.1 Key Pair Generation and Installation<br>#### 6.1.1 Key Pair Generation<br>"6.1.1 Generation of Key Pairs" of the CPS stipulates a policy on Private Keys of the CA.<br>#### 6.1.2 Private Key Delivery to Subscriber<br>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.<br>#### 6.1.3 Public Key Delivery to the Certificate Issuer<br>A Subscriber shall deliver his/her/its Public Key to the CA online when applying for his/her/its certificate. The communication pathways for such delivery shall be encrypted by the TLS.<br>#### 6.1.4 CA' Public Key Delivery to Relying Parties<br>Relying Parties may obtain Public Keys of the CA by accessing the CA's Repository.<br>#### 6.1.5 Key Sizes<br>When issuing a TLS server certificate that complies with Baseline Requirements, the following confirmation need to be done: | |

| 変更履歴あり | 整形版 | 備考 |
| --- | --- | --- |

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

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

### 6.1.7 Key Usage Purposes

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

Table 6.1 Key Usage Purposes

| | the CA | Certificates issued by the CA |
| --- | --- | --- |
| digitalSignature | — | yes |
| nonRepudiation | — | — |
| keyEncipherment | — | yes<br>(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

Stipulated in the CPS.

## 6.3 Other Aspects of Key Pair Management

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

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

### 6.1.7 Key Usage Purposes

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

Table 6.1 Key Usage Purposes

| | the CA | Certificates issued by the CA |
| --- | --- | --- |
| digitalSignature | — | yes |
| nonRepudiation | — | — |
| keyEncipherment | — | yes<br>(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

Stipulated in the CPS.

## 6.3 Other Aspects of Key Pair Management

| 変更履歴あり | 整形版 | 備考 |
| --- | --- | --- |
| ### 6.3.1 Public key archival<br>Stipulated in the CPS.<br>### 6.3.2 Certificate operational periods and key pair usage periods<br>The Validity period of the key pair and CA certificate of the CA is stipulated in the CPS. Subscriber Certificates issued on or after 1 September 2020 MUST NOT have a validity period greater than 398 days. Subscriber Certificates issued prior to 1 September 2020 have a validity period of 825 days or less.<br><br>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.<br>## 6.4 Activation Data<br>Stipulated in the CPS.<br>## 6.5 Computer Security Controls<br>Stipulated in the CPS.<br>## 6.6 Life Cycle Technical Controls<br>Stipulated in the CPS.<br>## 6.7 Network Security Controls<br>Stipulated in the CPS.<br>## 6.8 Time Stamping<br>Stipulated in the CPS.<br><br># 7. Certificate, CRL, and OCSP Profiles<br><br>## 7.1 Certificate Profile<br>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.<br>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.<br>Certificates issued by the CA conform to RFC 5280, the profile of which are indicated in the tables below.<br><br>Table 7.1-1 Subscriber Certificate Profile (applicable to certificates issued by JPRS Domain Validation Authority – G4 or JPRS Organization Validation Authority – G4) | ### 6.3.1 Public key archival<br>Stipulated in the CPS.<br>### 6.3.2 Certificate operational periods and key pair usage periods<br>The Validity period of the key pair and CA certificate of the CA is stipulated in the CPS. Subscriber Certificates issued on or after 1 September 2020 MUST NOT have a validity period greater than 398 days. Subscriber Certificates issued prior to 1 September 2020 have a validity period of 825 days or less.<br><br>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.<br>## 6.4 Activation Data<br>Stipulated in the CPS.<br>## 6.5 Computer Security Controls<br>Stipulated in the CPS.<br>## 6.6 Life Cycle Technical Controls<br>Stipulated in the CPS.<br>## 6.7 Network Security Controls<br>Stipulated in the CPS.<br>## 6.8 Time Stamping<br>Stipulated in the CPS.<br><br># 7. Certificate, CRL, and OCSP Profiles<br><br>## 7.1 Certificate Profile<br>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.<br>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.<br>Certificates issued by the CA conform to RFC 5280, the profile of which are indicated in the tables below.<br><br>Table 7.1-1 Subscriber Certificate Profile (applicable to certificates issued by JPRS Domain Validation Authority – G4 or JPRS Organization Validation Authority – G4) | |

| 変更履歴あり | | | | 整形版 | | | | 備考 |
|---|---|---|---|---|---|---|---|---|
| Basic field | | Description of setting | critical | Basic field | | Description of setting | critical | |
| Version | | Version 3 | - | Version | | Version 3 | - | |
| Serial Number | | An integral serial number to be assigned by the CA to the certificate | - | Serial Number | | An integral serial number to be assigned by the CA to the certificate | - | |
| Signature Algorithm | | sha256 with RSA Encryption | - | Signature Algorithm | | sha256 with RSA Encryption | - | |
| Issuer | Country | C=JP | - | Issuer | Country | C=JP | - | |
| | Organization | O=Japan Registry Services Co., Ltd. | - | | Organization | O=Japan Registry Services Co., Ltd. | - | |
| | Common Name | (1) Domain Validation<br>CN=JPRS Domain Validation Authority - G4<br>(2) Organization Validation<br>CN=JPRS Organization Validation Authority – G4 | - | | Common Name | (1) Domain Validation<br>CN=JPRS Domain Validation Authority - G4<br>(2) Organization Validation<br>CN=JPRS Organization Validation Authority – G4 | - | |
| Validity | NotBefore | E.g.) 2008/3/1 00:00:00 GMT | - | Validity | NotBefore | E.g.) 2008/3/1 00:00:00 GMT | - | |
| | NotAfter | E.g.) 2009/3/1 00:00:00 GMT | - | | NotAfter | E.g.) 2009/3/1 00:00:00 GMT | - | |
| Subject | Country | (1) Domain Validation<br>No description<br>(2) Organization Validation<br>C=JP as the address of the Subscriber (country) | - | Subject | Country | (1) Domain Validation<br>No description<br>(2) Organization Validation<br>C=JP as the address of the Subscriber (country) | - | |
| | State or Province | (1) Domain Validation<br>No description<br>(2) Organization Validation<br>Address of the Subscriber (prefecture name) (mandatory) | - | | State or Province | (1) Domain Validation<br>No description<br>(2) Organization Validation<br>Address of the Subscriber (prefecture name) (mandatory) | - | |
| | Locality | (1) Domain Validation<br>No description<br>(2) Organization Validation<br>Address of the Subscriber (city, town, or village name) (mandatory) | - | | Locality | (1) Domain Validation<br>No description<br>(2) Organization Validation<br>Address of the Subscriber (city, town, or village name) (mandatory) | - | |
| | Organization | (1) Domain Validation<br>No description<br>(2) Organization Validation<br>Name of the Subscriber (mandatory) | - | | Organization | (1) Domain Validation<br>No description<br>(2) Organization Validation<br>Name of the Subscriber (mandatory) | - | |
| | Organizational Unit | (1) Domain Validation<br>No description<br>(2) Organization Validation<br>Business division name of the Subscriber (optional ). | - | | Organizational Unit | (1) Domain Validation<br>No description<br>(2) Organization Validation<br>Business division name of the Subscriber (optional ). | - | |

| 変更履歴あり | | | | 整形版 | | | | 備考 |
|---|---|---|---|---|---|---|---|---|
| | | However, this item will not be included in certificates issued on or after 18 November 2021.<br>● A string comprising symbols only or spaces only may not be designated, and any of the following strings may not be included:<br>・ 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;<br>・ any string indicating a legal personality, such as “Co., Ltd”;<br>・ any string referring to a specific natural person;<br>・ any string indicating an address;<br>・ any phone number;<br>・ any domain name or IP address; or<br>・ any string meaning “blank”, “not applicable” or the like (“null”, “N/A” or the like) | | | | However, this item will not be included in certificates issued on or after 18 November 2021.<br>● A string comprising symbols only or spaces only may not be designated, and any of the following strings may not be included:<br>・ 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;<br>・ any string indicating a legal personality, such as “Co., Ltd”;<br>・ any string referring to a specific natural person;<br>・ any string indicating an address;<br>・ any phone number;<br>・ any domain name or IP address; or<br>・ 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)<br>- The value must be encoded as a character-for-character copy of the dNSName entry value from the Subject Alternative Name extension. Specifically. | - | | Common Name | A host name used in the DNS of the server in which the certificate is scheduled to be installed (mandatory)<br>- 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) | - | Subject Public Key Info | | The subject’s Public Key (RSA 2048 bits) | - | |
| Extended field | | Description of setting | critical | Extended field | | Description of setting | critical | |
| KeyUsage | | digitalSignature, keyEncipherment | y | KeyUsage | | digitalSignature, keyEncipherment | y | |
| ExtendedKeyUsage | | TLS Web Server Authentication | n | ExtendedKeyUsage | | TLS Web Server Authentication | n | |
| Subject Alt Name | | dNSName= name(s) of the server(s) | n | Subject Alt Name | | dNSName= name(s) of the server(s) | n | |
| CertificatePolicies | | [1] Certificate Policy<br>1.3.6.1.4.1.53827.1.1.4<br>CPS<br>http://jprs.jp/pubcert/info/repository/ | n | CertificatePolicies | | [1] Certificate Policy<br>1.3.6.1.4.1.53827.1.1.4<br>CPS<br>http://jprs.jp/pubcert/info/repository/ | n | |

| 変更履歴あり | | | 整形版 | | | 備考 |
|---|---|---|---|---|---|---|
| | [2] Certificate Policy<br>(1) Domain Validation<br>2.23.140.1.2.1<br>(2) Organization Validation<br>2.23.140.1.2.2 | | | [2] Certificate Policy<br>(1) Domain Validation<br>2.23.140.1.2.1<br>(2) Organization Validation<br>2.23.140.1.2.2 | | |
| CRL Distribution Points | (1) Domain Validation<br>http://repo.pubcert.jprs.jp/sppca/jprs/dvca_g4/fullcrl.crl<br>(2) Organization Validation<br>http://repo.pubcert.jprs.jp/sppca/jprs/ovca_g4/fullcrl.crl | n | CRL Distribution Points | (1) Domain Validation<br>http://repo.pubcert.jprs.jp/sppca/jprs/dvca_g4/fullcrl.crl<br>(2) Organization Validation<br>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)<br>(1) Domain Validation<br>http://dv.g4.ocsp.pubcert.jprs.jp<br>(2) Organization Validation<br>http://ov.g4.ocsp.pubcert.jprs.jp<br>[2] ca issuers (1.3.6.1.5.5.7.48.2)<br>(1) Domain Validation<br>http://repo.pubcert.jprs.jp/sppca/jprs/dvca_g4/JPRS_DVCA_G4_DER.cer<br>(2) Organization Validation<br>http://repo.pubcert.jprs.jp/sppca/jprs/ovca_g4/JPRS_OVCA_G4_DER.cer | n | Authority Information Access | [1] ocsp (1.3.6.1.5.5.7.48.1)<br>(1) Domain Validation<br>http://dv.g4.ocsp.pubcert.jprs.jp<br>(2) Organization Validation<br>http://ov.g4.ocsp.pubcert.jprs.jp<br>[2] ca issuers (1.3.6.1.5.5.7.48.2)<br>(1) Domain Validation<br>http://repo.pubcert.jprs.jp/sppca/jprs/dvca_g4/JPRS_DVCA_G4_DER.cer<br>(2) Organization Validation<br>http://repo.pubcert.jprs.jp/sppca/jprs/ovca_g4/JPRS_OVCA_G4_DER.cer | n | |
| Authority Key Identifier | SHA-1 hash for the issuer's Public Key (160 bits) | 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 | 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 | 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 | - |

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 | - |

| 変更履歴あり | | | | 整形版 | | | | 備考 |
|---|---|---|---|---|---|---|---|---|
| | Organization | O=Japan Registry Services Co., Ltd. | - | | Organization | O=Japan Registry Services Co., Ltd. | - | |
| | Common Name | (1) Domain Validation<br>CN= JPRS DV RSA CA 2024 G1<br>(2) Organization Validation<br>CN= JPRS OV RSA CA 2024 G1 | - | | Common Name | (1) Domain Validation<br>CN= JPRS DV RSA CA 2024 G1<br>(2) Organization Validation<br>CN= JPRS OV RSA CA 2024 G1 | - | |
| Validity | NotBefore | E.g.) 2008/3/1 00:00:00 GMT | - | Validity | NotBefore | E.g.) 2008/3/1 00:00:00 GMT | - | |
| | NotAfter | E.g.) 2009/3/1 00:00:00 GMT | - | | NotAfter | E.g.) 2009/3/1 00:00:00 GMT | - | |
| Subject | Country | (1) Domain Validation<br>No description<br>(2) Organization Validation<br>C=JP as the address of the<br>Subscriber (country) | - | Subject | Country | (1) Domain Validation<br>No description<br>(2) Organization Validation<br>C=JP as the address of the<br>Subscriber (country) | - | |
| | State or Province | (1) Domain Validation<br>No description<br>(2) Organization Validation<br>Address of the Subscriber<br>(prefecture name) (mandatory) | - | | State or Province | (1) Domain Validation<br>No description<br>(2) Organization Validation<br>Address of the Subscriber<br>(prefecture name) (mandatory) | - | |
| | Locality | (1) Domain Validation<br>No description<br>(2) Organization Validation<br>Address of the Subscriber (city,<br>town, or village name)<br>(mandatory) | - | | Locality | (1) Domain Validation<br>No description<br>(2) Organization Validation<br>Address of the Subscriber (city,<br>town, or village name)<br>(mandatory) | - | |
| | Organization | (1) Domain Validation<br>No description<br>(2) Organization Validation<br>Name of the Subscriber<br>(mandatory) | - | | Organization | (1) Domain Validation<br>No description<br>(2) Organization Validation<br>Name of the Subscriber<br>(mandatory) | - | |
| | Common Name | A host name used in the DNS of<br>the server in which the certificate<br>is scheduled to be installed<br>(mandatory)<br>- The value must be encoded as<br>a character-for-character copy<br>of the dNSName entry value<br>from the Subject Alternative<br>Name extension. Specifically. | - | | Common Name | A host name used in the DNS of<br>the server in which the certificate<br>is scheduled to be installed<br>(mandatory)<br>- The value must be encoded as<br>a character-for-character copy<br>of the dNSName entry value<br>from the Subject Alternative<br>Name extension. Specifically. | - | |
| Subject Public Key Info | | The subject's Public Key (RSA<br>4096 bits, RSA3072 bits or | - | Subject Public Key Info | | The subject's Public Key (RSA<br>4096 bits, RSA3072 bits or | - | |

| 変更履歴あり | | | 整形版 | | | 備考 |
|---|---|---|---|---|---|---|
| | RSA 2048 bits) | | | RSA 2048 bits) | | |
| Extended field | Description of setting | critical | Extended field | Description of setting | critical | |
| KeyUsage | digitalSignature,<br>keyEncipherment | y | KeyUsage | digitalSignature,<br>keyEncipherment | y | |
| ExtendedKeyUsage | TLS Web Server Authentication<br>TLS Web Client Authentication | n | ExtendedKeyUsage | TLS Web Server Authentication<br>TLS Web Client Authentication | n | |
| Subject Alt Name | dNSName= name(s) of the server(s) | n | Subject Alt Name | dNSName= name(s) of the server(s) | n | |
| CertificatePolicies | Certificate Policy<br>(1) Domain Validation<br>2.23.140.1.2.1<br>(2) Organization Validation<br>2.23.140.1.2.2 | n | CertificatePolicies | Certificate Policy<br>(1) Domain Validation<br>2.23.140.1.2.1<br>(2) Organization Validation<br>2.23.140.1.2.2 | n | |
| CRL Distribution Points | (1) Domain Validation<br>http://repo.pubcert.jprs.jp/sppca/<br>jprs/dvca_rsa2024g1/fullcrl.crl<br>(2) Organization Validation<br>http://repo.pubcert.jprs.jp/sppca/<br>jprs/ovca_rsa2024g1/fullcrl.crl | n | CRL Distribution Points | (1) Domain Validation<br>http://repo.pubcert.jprs.jp/sppca/<br>jprs/dvca_rsa2024g1/fullcrl.crl<br>(2) Organization Validation<br>http://repo.pubcert.jprs.jp/sppca/<br>jprs/ovca_rsa2024g1/fullcrl.crl | n | |
| Authority Information Access | [1] ocsp (1.3.6.1.5.5.7.48.1)<br>(1) Domain Validation<br>http://dv.rsa2024g1.ocsp.pubcert<br>.jprs.jp<br>(2) Organization Validation<br>http://ov.rsa2024g1.ocsp.pubcert<br>.jprs.jp<br>[2] ca issuers (1.3.6.1.5.5.7.48.2)<br>(1) Domain Validation<br>http://repo.pubcert.jprs.jp/sppca/<br>jprs/dvca_rsa2024g1/JPRS_DV<br>CA_RSA2024G1_DER.cer<br>(2) Organization Validation<br>http://repo.pubcert.jprs.jp/sppca/<br>jprs/ovca_rsa2024g1/JPRS_OV<br>CA_RSA2024G1_DER.cer | n | Authority Information Access | [1] ocsp (1.3.6.1.5.5.7.48.1)<br>(1) Domain Validation<br>http://dv.rsa2024g1.ocsp.pubcert<br>.jprs.jp<br>(2) Organization Validation<br>http://ov.rsa2024g1.ocsp.pubcert<br>.jprs.jp<br>[2] ca issuers (1.3.6.1.5.5.7.48.2)<br>(1) Domain Validation<br>http://repo.pubcert.jprs.jp/sppca/<br>jprs/dvca_rsa2024g1/JPRS_DV<br>CA_RSA2024G1_DER.cer<br>(2) Organization Validation<br>http://repo.pubcert.jprs.jp/sppca/<br>jprs/ovca_rsa2024g1/JPRS_OV<br>CA_RSA2024G1_DER.cer | n | |
| Authority Key Identifier | SHA-1 hash for the issuer's<br>Public Key (160 bits) | n | Authority Key Identifier | SHA-1 hash for the issuer's<br>Public Key (160 bits) | n | |
| Subject Key Identifier | SHA-1 hash for the subject's<br>Public Key (160 bits) | n | Subject Key Identifier | SHA-1 hash for the subject's<br>Public Key (160 bits) | n | |
| Certificate Transparency | Value of an OCTET STRING containing | n | Certificate Transparency | Value of an OCTET STRING containing | n | |

| 変更履歴あり | | | 整形版 | | | 備考 |
|---|---|---|---|---|---|---|
| Timestamp List （1.3.6.1.4.1.11129.2.4.2） | the encoded SignedCertificateTimestampList(optional). | | Timestamp List （1.3.6.1.4.1.11129.2.4.2） | the encoded SignedCertificateTimestampList(optional). | | |

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<br>CN= JPRS DV ECC CA 2024 G1<br>(2) Organization Validation<br>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<br>No description<br>(2) Organization Validation<br>C=JP as the address of the Subscriber (country) | - |
| | State or Province | (1) Domain Validation<br>No description<br>(2) Organization Validation<br>Address of the Subscriber (prefecture name) (mandatory) | - |
| | Locality | (1) Domain Validation<br>No description<br>(2) Organization Validation<br>Address of the Subscriber (city, town, or village name) (mandatory) | - |
| | Organization | (1) Domain Validation<br>No description<br>(2) Organization Validation<br>Name of the Subscriber (mandatory) | - |
| | Common Name | A host name used in the DNS | - |

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<br>CN= JPRS DV ECC CA 2024 G1<br>(2) Organization Validation<br>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<br>No description<br>(2) Organization Validation<br>C=JP as the address of the Subscriber (country) | - |
| | State or Province | (1) Domain Validation<br>No description<br>(2) Organization Validation<br>Address of the Subscriber (prefecture name) (mandatory) | - |
| | Locality | (1) Domain Validation<br>No description<br>(2) Organization Validation<br>Address of the Subscriber (city, town, or village name) (mandatory) | - |
| | Organization | (1) Domain Validation<br>No description<br>(2) Organization Validation<br>Name of the Subscriber (mandatory) | - |
| | Common Name | A host name used in the DNS | - |

| 変更履歴あり | | | | 整形版 | | | | 備考 |
|---|---|---|---|---|---|---|---|---|
| | | of the server in which the certificate is scheduled to be installed (mandatory)<br>- The value must be encoded as a character-for-character copy of the dNSName entry value from the Subject Alternative Name extension. Specifically. | | | | of the server in which the certificate is scheduled to be installed (mandatory)<br>- 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) | - | 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 | Extended field | | Description of setting | critical | |
| KeyUsage | | digitalSignature,<br>keyEncipherment (except for certificates issued by using ECDSA key) | y | KeyUsage | | digitalSignature,<br>keyEncipherment (except for certificates issued by using ECDSA key) | y | |
| ExtendedKeyUsage | | TLS Web Server Authentication<br>TLS Web Client Authentication | n | ExtendedKeyUsage | | TLS Web Server Authentication<br>TLS Web Client Authentication | n | |
| Subject Alt Name | | dNSName= name(s) of the server(s) | n | Subject Alt Name | | dNSName= name(s) of the server(s) | n | |
| CertificatePolicies | | Certificate Policy<br>(1) Domain Validation<br>2.23.140.1.2.1<br>(2) Organization Validation<br>2.23.140.1.2.2 | n | CertificatePolicies | | Certificate Policy<br>(1) Domain Validation<br>2.23.140.1.2.1<br>(2) Organization Validation<br>2.23.140.1.2.2 | n | |
| CRL Distribution Points | | (1) Domain Validation<br>http://repo.pubcert.jprs.jp/sppca/jprs/dvca_ecc2024g1/fullcrl.crl<br>(2) Organization Validation<br>http://repo.pubcert.jprs.jp/sppca/jprs/ovca_ecc2024g1/fullcrl.crl | n | CRL Distribution Points | | (1) Domain Validation<br>http://repo.pubcert.jprs.jp/sppca/jprs/dvca_ecc2024g1/fullcrl.crl<br>(2) Organization Validation<br>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)<br>(1) Domain Validation<br>http://dv.ecc2024g1.ocsp.pubcert.jprs.jp<br>(2) Organization Validation<br>http://ov.ecc2024g1.ocsp.pubcert.jprs.jp<br>[2] ca issuers (1.3.6.1.5.5.7.48.2)<br>(1) Domain Validation | n | Authority Information Access | | [1] ocsp (1.3.6.1.5.5.7.48.1)<br>(1) Domain Validation<br>http://dv.ecc2024g1.ocsp.pubcert.jprs.jp<br>(2) Organization Validation<br>http://ov.ecc2024g1.ocsp.pubcert.jprs.jp<br>[2] ca issuers (1.3.6.1.5.5.7.48.2)<br>(1) Domain Validation | n | |

| 変更履歴あり | | | 整形版 | | | 備考 |
|---|---|---|---|---|---|---|
| | http://repo.pubcert.jprs.jp/sppca/jprs/dvca_ecc2024g1/JPRSDVCA_ECC2024G1_DER.cer<br>(2) Organization Validation<br>http://repo.pubcert.jprs.jp/sppca/jprs/ovca_ecc2024g1/JPRS_OVCA_ECC2024G1_DER.cer | | | http://repo.pubcert.jprs.jp/sppca/jprs/dvca_ecc2024g1/JPRSDVCA_ECC2024G1_DER.cer<br>(2) Organization Validation<br>http://repo.pubcert.jprs.jp/sppca/jprs/ovca_ecc2024g1/JPRS_OVCA_ECC2024G1_DER.cer | | |
| Authority Key Identifier | SHA-1 hash for the issuer's Public Key (160 bits) | 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 | 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 | 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<br>CN=JPRS Organization Validation Authority - G4<br>(2) Domain Validation<br>CN=JPRS Domain Validation Authority - G4 | - |
| Subject Public Key Info | | The subject's Public Key (RSA 2048 bits) | - |
| Extended field | | Description of setting | critical |

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<br>CN=JPRS Organization Validation Authority - G4<br>(2) Domain Validation<br>CN=JPRS Domain Validation Authority - G4 | - |
| Subject Public Key Info | | The subject's Public Key (RSA 2048 bits) | - |
| Extended field | | Description of setting | critical |

| 変更履歴あり | | | 整形版 | | | 備考 |
|---|---|---|---|---|---|---|
| Authority Key Identifier | SHA-1 hash for the issuer's Public Key (160 bits) | 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 | Subject Key Identifier | SHA-1 hash for the subject's Public Key (160 bits) | n | |
| KeyUsage | Certificate Signing<br>Off-line CRL Signing<br>CRL Signing (06) | y | KeyUsage | Certificate Signing<br>Off-line CRL Signing<br>CRL Signing (06) | y | |
| CertificatePolicies | Certificate Policy<br>1.2.392.200091.100.901.4<br>CPS<br>http://repository.secomtrust.net/SC-Root2/ | N | CertificatePolicies | Certificate Policy<br>1.2.392.200091.100.901.4<br>CPS<br>http://repository.secomtrust.net/SC-Root2/ | N | |
| Basic Constraints | Subject Type=CA<br>Path Length Constraint=0 | y | Basic Constraints | Subject Type=CA<br>Path Length Constraint=0 | y | |
| ExtendedKeyUsage | TLS Web Server Authentication | n | ExtendedKeyUsage | TLS Web Server Authentication | n | |
| CRL Distribution Points | http://repository.secomtrust.net/SC-Root2/SCRoot2CRL.crl | 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)<br>http://scrootca2.ocsp.secomtrust.net<br>[2] ca issuers (1.3.6.1.5.5.7.48.2)<br>http://repository.secomtrust.net/SC-Root2/SCRoot2ca.cer | n | Authority Information Access | [1] ocsp (1.3.6.1.5.5.7.48.1)<br>http://scrootca2.ocsp.secomtrust.net<br>[2] ca issuers (1.3.6.1.5.5.7.48.2)<br>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<br>CN= JPRS OV RSA CA 2024 G1 | - |

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<br>CN= JPRS OV RSA CA 2024 G1 | - |

| 変更履歴あり | | | | 整形版 | | | | 備考 |
|---|---|---|---|---|---|---|---|---|
| | | (2) Domain Validation<br>CN= JPRS DV RSA CA 2024 G1 | | | | (2) Domain Validation<br>CN= JPRS DV RSA CA 2024 G1 | | |
| Subject Public Key Info | | The subject's Public Key (RSA 4096 bits) | - | Subject Public Key Info | | The subject's Public Key (RSA 4096 bits) | - | |
| Extended field | | Description of setting | critical | Extended field | | Description of setting | critical | |
| Authority Key Identifier | | SHA-1 hash for the issuer's Public Key (160 bits) | 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 | Subject Key Identifier | | SHA-1 hash for the subject's Public Key (160 bits) | n | |
| KeyUsage | | Certificate Signing<br>Off-line CRL Signing<br>CRL Signing (06) | y | KeyUsage | | Certificate Signing<br>Off-line CRL Signing<br>CRL Signing (06) | y | |
| CertificatePolicies | | [1] Certificate Policy<br>（1）Domain Validation<br>2.23.140.1.2.1<br>（2）Organization Validation<br>2.23.140.1.2.2<br>[2] Certificate Policy<br>1.2.392.200091.100.901.11 | N | CertificatePolicies | | [1] Certificate Policy<br>（1）Domain Validation<br>2.23.140.1.2.1<br>（2）Organization Validation<br>2.23.140.1.2.2<br>[2] Certificate Policy<br>1.2.392.200091.100.901.11 | N | |
| Basic Constraints | | Subject Type=CA<br>Path Length Constraint=0 | y | Basic Constraints | | Subject Type=CA<br>Path Length Constraint=0 | y | |
| ExtendedKeyUsage | | TLS Web Server Authentication<br>TLS Web Client Authentication | n | ExtendedKeyUsage | | TLS Web Server Authentication<br>TLS Web Client Authentication | n | |
| CRL Distribution Points | | http://repo1.secomtrust.net/root/tlsrsa/tlsrsarootca2024.crl | 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）<br>http://tlsrsarootca2024.ocsp.secom-cert.jp<br>[2] ca issuers（1.3.6.1.5.5.7.48.2）<br>http://repo2.secomtrust.net/root/tlsrsa/tlsrsarootca2024.cer | n | Authority Information Access | | [1] ocsp（1.3.6.1.5.5.7.48.1）<br>http://tlsrsarootca2024.ocsp.secom-cert.jp<br>[2] ca issuers（1.3.6.1.5.5.7.48.2）<br>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 | - |

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 | - |

| 変更履歴あり | | | | 整形版 | | | | 備考 |
|---|---|---|---|---|---|---|---|---|
| Issuer | Country | C=JP | - | Issuer | Country | C=JP | - | |
| | Organization | O=SECOM Trust Systems CO.,LTD. | - | | Organization | O=SECOM Trust Systems CO.,LTD. | - | |
| | Common Name | CN=Security Communication ECC RootCA1 | - | | Common Name | CN=Security Communication ECC RootCA1 | - | |
| Validity | NotBefore | E.g.) 2008/3/1 00:00:00 GMT | - | Validity | NotBefore | E.g.) 2008/3/1 00:00:00 GMT | - | |
| | NotAfter | E.g.) 2009/3/1 00:00:00 GMT | - | | NotAfter | E.g.) 2009/3/1 00:00:00 GMT | - | |
| Subject | Country | C=JP | - | Subject | Country | C=JP | - | |
| | Organization | O=Japan Registry Services Co., Ltd. | - | | Organization | O=Japan Registry Services Co., Ltd. | - | |
| | Common Name | (1) Organization Validation<br>CN= JPRS OV ECC CA 2024 G1<br>(2) Domain Validation<br>CN= JPRS DV ECC CA 2024 G1 | - | | Common Name | (1) Organization Validation<br>CN= JPRS OV ECC CA 2024 G1<br>(2) Domain Validation<br>CN= JPRS DV ECC CA 2024 G1 | - | |
| Subject Public Key Info | | The subject's Public Key (384 bits) | - | Subject Public Key Info | | The subject's Public Key (384 bits) | - | |
| Extended field | | Description of setting | critical | Extended field | | Description of setting | critical | |
| Authority Key Identifier | | SHA-1 hash for the issuer's Public Key (160 bits) | 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 | Subject Key Identifier | | SHA-1 hash for the subject's Public Key (160 bits) | n | |
| KeyUsage | | Certificate Signing<br>Off-line CRL Signing<br>CRL Signing (06) | y | KeyUsage | | Certificate Signing<br>Off-line CRL Signing<br>CRL Signing (06) | y | |
| CertificatePolicies | | [1] Certificate Policy<br>（1） Domain Validation<br>2.23.140.1.2.1<br>（2） Organization Validation<br>2.23.140.1.2.2<br>[2] Certificate Policy<br>1.2.392.200091.100.902.1 | N | CertificatePolicies | | [1] Certificate Policy<br>（1） Domain Validation<br>2.23.140.1.2.1<br>（2） Organization Validation<br>2.23.140.1.2.2<br>[2] Certificate Policy<br>1.2.392.200091.100.902.1 | N | |
| Basic Constraints | | Subject Type=CA<br>Path Length Constraint=0 | y | Basic Constraints | | Subject Type=CA<br>Path Length Constraint=0 | y | |
| ExtendedKeyUsage | | TLS Web Server Authentication<br>TLS Web Client Authentication | n | ExtendedKeyUsage | | TLS Web Server Authentication<br>TLS Web Client Authentication | n | |
| CRL Distribution Points | | http://repository.secomtrust.net/SC-ECC-Root1/SCECCRoot1CRL.crl | 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）<br>http://sceccrootca1.ocsp.secomtrust.net<br>[2] ca issuers（1.3.6.1.5.5.7.48.2）<br>http://repository.secomtrust.net/SC-ECC-Root1/SCECCRoot1ca.cer | n | Authority Information Access | | [1] ocsp（1.3.6.1.5.5.7.48.1）<br>http://sceccrootca1.ocsp.secomtrust.net<br>[2] ca issuers（1.3.6.1.5.5.7.48.2）<br>http://repository.secomtrust.net/SC-ECC-Root1/SCECCRoot1ca.cer | n | |

| 変更履歴あり | 整形版 | 備考 |
|---|---|---|

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

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

| 変更履歴あり | 整形版 | 備考 |
|---|---|---|

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<br>CN=JPRS Domain Validation Authority - G4<br>(2) Organization Validation<br>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 | - |

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<br>CN=JPRS Domain Validation Authority - G4<br>(2) Organization Validation<br>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 | - |

| 変更履歴あり | | | | 整形版 | | | | 備考 |
|---|---|---|---|---|---|---|---|---|
| | | (0) and less than 2^159 containing 64 bits of output from a CSPRNG | | | | (0) and less than 2^159 containing 64 bits of output from a CSPRNG | | |
| Signature Algorithm | | sha256 With RSA Encryption | - | Signature Algorithm | | sha256 With RSA Encryption | - | |
| Issuer | Country | C=JP | - | Issuer | Country | C=JP | - | |
| | Organization | O= Japan Registry Services Co., Ltd. | - | | Organization | O= Japan Registry Services Co., Ltd. | - | |
| | Common Name | (1) Domain Validation<br>CN=JPRS DV RSA CA 2024 G1<br>(2) Organization Validation<br>CN= JPRS OV RSA CA 2024 G1 | - | | Common Name | (1) Domain Validation<br>CN=JPRS DV RSA CA 2024 G1<br>(2) Organization Validation<br>CN= JPRS OV RSA CA 2024 G1 | - | |
| Validity | NotBefore | E.g.) 2008/3/1 00:00:00 GMT | - | Validity | NotBefore | E.g.) 2008/3/1 00:00:00 GMT | - | |
| | NotAfter | E.g.) 2008/3/5 00:00:00 GMT | - | | NotAfter | E.g.) 2008/3/5 00:00:00 GMT | - | |
| Subject | Country | C=JP （fixed value） | - | Subject | Country | C=JP （fixed value） | - | |
| | Organization | Japan Registry Services Co., Ltd. (fixed value) | - | | Organization | Japan Registry Services Co., Ltd. (fixed value) | - | |
| | Common Name | Name of the OCSP server (mandatory) | - | | 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) | - | 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 | Extended field | | Description of setting | critical | |
| Authority Key Identifier | | SHA-1 hash for the issuer's Public Key (160 bits) | 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 | Subject Key Identifier | | SHA-1 hash for the subject's Public Key (160 bits) | n | |
| KeyUsage | | digitalSignature | y | KeyUsage | | digitalSignature | y | |
| ExtendedKeyUsage | | OCSPSigning | n | ExtendedKeyUsage | | OCSPSigning | n | |
| OCSP No Check | | null | 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<br>CN=JPRS DV ECC CA 2024 G1<br>(2) Organization Validation | - |

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<br>CN=JPRS DV ECC CA 2024 G1<br>(2) Organization Validation | - |

| 変更履歴あり | | | | 整形版 | | | | 備考 |
|---|---|---|---|---|---|---|---|---|
| | | CN= JPRS OV ECC CA 2024 G1 | | | | CN= JPRS OV ECC CA 2024 G1 | | |
| Validity | NotBefore | E.g.) 2008/3/1 00:00:00 GMT | - | Validity | NotBefore | E.g.) 2008/3/1 00:00:00 GMT | - | |
| | NotAfter | E.g.) 2008/3/5 00:00:00 GMT | - | | NotAfter | E.g.) 2008/3/5 00:00:00 GMT | - | |
| Subject | Country | C=JP （fixed value） | - | Subject | Country | C=JP （fixed value） | - | |
| | Organization | Japan Registry Services Co., Ltd. (fixed value) | - | | Organization | Japan Registry Services Co., Ltd. (fixed value) | - | |
| | Common Name | Name of the OCSP server (mandatory) | - | | Common Name | Name of the OCSP server (mandatory) | - | |
| Subject Public Key Info | | The subject's Public Key (256 bits or 384 bits) | - | Subject Public Key Info | | The subject's Public Key (256 bits or 384 bits) | - | |
| Extended field | | Description of setting | critical | Extended field | | Description of setting | critical | |
| Authority Key Identifier | | SHA-1 hash for the issuer's Public Key (160 bits) | 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 | Subject Key Identifier | | SHA-1 hash for the subject's Public Key (160 bits) | n | |
| KeyUsage | | digitalSignature | y | KeyUsage | | digitalSignature | y | |
| ExtendedKeyUsage | | OCSPSigning | n | ExtendedKeyUsage | | OCSPSigning | n | |
| OCSP No Check | | null | n | OCSP No Check | | null | n | |

### 7.1.1 Version Number(s)

The CA applies version 3.

### 7.1.2 Certificate Extension

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

### 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 Format

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

| 変更履歴あり | 整形版 | 備考 |
| --- | --- | --- |
| CP and/or 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.<br>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.<br>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.<br>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.<br>**7.1.5 Name Constraints**<br>Not set in the CA.<br>**7.1.6 Certificate Policy Object Identifier**<br>The OID of the certificate issued by the CA is as described in this CP "1.2 Document Name and Identification".<br>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.<br><br>【 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)<br><br>【 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)<br>**7.1.7 Use of Policy Constraint Extensions**<br>Not set.<br>**7.1.8 Policy Qualifier Syntax and Semantics**<br>For the policy qualifier, the URI of the Web page that publishes this CP and CPS is stored.<br>**7.1.9 How to interpret Critical Certificate Policy Extensions**<br>Not set.<br>**7.2 CRL Profile**<br>The profile of CRLs to be issued by the CA shall be as described in the following table: | CP and/or 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.<br>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.<br>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.<br>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.<br>**7.1.5 Name Constraints**<br>Not set in the CA.<br>**7.1.6 Certificate Policy Object Identifier**<br>The OID of the certificate issued by the CA is as described in this CP "1.2 Document Name and Identification".<br>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.<br><br>【 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)<br><br>【 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)<br>**7.1.7 Use of Policy Constraint Extensions**<br>Not set.<br>**7.1.8 Policy Qualifier Syntax and Semantics**<br>For the policy qualifier, the URI of the Web page that publishes this CP and CPS is stored.<br>**7.1.9 How to interpret Critical Certificate Policy Extensions**<br>Not set.<br>**7.2 CRL Profile**<br>The profile of CRLs to be issued by the CA shall be as described in the following table: | |

| 変更履歴あり | 整形版 | 備考 |
|---|---|---|

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<br>CN=JPRS Domain Validation Authority - G4<br>(2) Organization Validation<br>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<br>CN= JPRS DV RSA CA 2024 G1<br>(2) Organization Validation<br>CN=JPRS OV RSA CA 2024 G1 | - |

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<br>CN=JPRS Domain Validation Authority - G4<br>(2) Organization Validation<br>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<br>CN= JPRS DV RSA CA 2024 G1<br>(2) Organization Validation<br>CN=JPRS OV RSA CA 2024 G1 | - |

| 変更履歴あり | | | | 整形版 | | | | 備考 |
|---|---|---|---|---|---|---|---|---|
| This Update | | E.g.) 2008/3/1 00:00:00 GMT | - | This Update | | E.g.) 2008/3/1 00:00:00 GMT | - | |
| Next Update | | E.g.) 2008/3/5 00:00:00 GMT | - | Next Update | | E.g.) 2008/3/5 00:00:00 GMT | - | |
| Revoked Certificates | Serial Number | E.g.) 0123456789 | - | Revoked Certificates | Serial Number | E.g.) 0123456789 | - | |
| | Revocation Date | E.g.) 2008/3/1 00:00:00 GMT | - | | Revocation Date | E.g.) 2008/3/1 00:00:00 GMT | - | |
| | Reason Code | Revocation Reason Code (*) | - | | Reason Code | Revocation Reason Code (*) | - | |
| Extended field | | Description of setting | critical | Extended field | | Description of setting | critical | |
| CRL Number | | CRL number | n | CRL Number | | CRL number | n | |
| Authority Key Identifier | | SHA-1 hash for the issuer's Public Key (160 bits) | 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.

*: 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<br>CN= JPRS DV ECC CA 2024 G1<br>(2) Organization Validation<br>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.

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<br>CN= JPRS DV ECC CA 2024 G1<br>(2) Organization Validation<br>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)

### 7.2.1 Version Number(s)

| 変更履歴あり | 整形版 | 備考 |
|---|---|---|

The CA applies CRL version 2.

### 7.2.2 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.

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


The CA applies CRL version 2.

### 7.2.2 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.

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

| 変更履歴あり | 整形版 | 備考 |
| --- | --- | --- |
| **8. Compliance Audit and Other Assessments**<br><br>**8.1 Frequency and Circumstances of Assessment**<br>JPRS shall perform audits at least once a year to verify whether or not the CA is operated in compliance with this CP and the CPS.<br><br>**8.2 Identity/Qualifications of Assessor**<br>Compliance audits shall be performed by auditors who are adequately experienced in auditing.<br>Audits required for obtaining the WebTrust certification shall be performed by audit corporations with the following qualifications and skills:<br><br>- Independence from the subject of the audit;<br>- The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme<br>- 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;<br>- licensed by WebTrust;<br>- Bound by law, government regulation, or professional code of ethics; and<br>- 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<br><br>**8.3 Assessor's Relationship to Assessed Entity**<br>Auditors shall be operationally independent of the auditee divisions, except in matters related to the audits.<br><br>**8.4 Topics Covered by Assessment**<br>Audits shall be performed mainly to verify whether or not the CA is operated in compliance with this CP and the CPS. The CA shall undergo WebTrust in accordance with one of the following schemes:<br>- ・ WebTrust for CAs<br>・ WebTrust for CAs - SSL Baseline ~~with Network Security~~<br>・ WebTrust for CAs - Network Security<br><br>**8.5 Actions Taken as a Result of Deficiency**<br>The CA shall promptly take necessary corrective actions with respect to any deficiencies pointed out in an audit report. | **8. Compliance Audit and Other Assessments**<br><br>**8.1 Frequency and Circumstances of Assessment**<br>JPRS shall perform audits at least once a year to verify whether or not the CA is operated in compliance with this CP and the CPS.<br><br>**8.2 Identity/Qualifications of Assessor**<br>Compliance audits shall be performed by auditors who are adequately experienced in auditing.<br>Audits required for obtaining the WebTrust certification shall be performed by audit corporations with the following qualifications and skills:<br><br>- Independence from the subject of the audit;<br>- The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme<br>- 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;<br>- licensed by WebTrust;<br>- Bound by law, government regulation, or professional code of ethics; and<br>- 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<br><br>**8.3 Assessor's Relationship to Assessed Entity**<br>Auditors shall be operationally independent of the auditee divisions, except in matters related to the audits.<br><br>**8.4 Topics Covered by Assessment**<br>Audits shall be performed mainly to verify whether or not the CA is operated in compliance with this CP and the CPS. The CA shall undergo WebTrust in accordance with one of the following schemes:<br>・ WebTrust for CAs<br>・ WebTrust for CAs - SSL Baseline<br>・ WebTrust for CAs - Network Security<br><br>**8.5 Actions Taken as a Result of Deficiency**<br>The CA shall promptly take necessary corrective actions with respect to any deficiencies pointed out in an audit report. | Baseline Requirementsへの準拠を明確にするための修正 |

| 変更履歴あり | 整形版 | 備考 |
| --- | --- | --- |
| **8.6 Communication of Results**<br>Auditors shall report the audit results to the CA.<br>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.<br>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.<br>**8.7 Self-Audits**<br>The CA shall monitor adherence this CP, the CPS, and strictly control its service quality by performing self audits on at least a quarterly basis against a randomly selected sample of at least three percent of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.<br>**9. Other Business and Legal Matters**<br>**9.1 Fees**<br>To be separately stipulated.<br>**9.2 Financial Responsibility**<br>The CA shall maintain a sufficient financial foundation required for operating and maintaining the CA.<br>**9.3 Confidentiality of Business Information**<br>**9.3.1 Scope of Confidential Information**<br>Stipulated in the CPS.<br>**9.3.2 Information not within the Scope of Confidential Information**<br>Stipulated in the CPS.<br>**9.3.3 Responsibility to Protect Confidential Information**<br>Stipulated in the CPS.<br>**9.4 Privacy of Personal Information**<br>Stipulated in the CPS.<br>**9.5 Intellectual Property Rights**<br>Unless separately agreed, all intellectual property rights pertaining to the following information shall belong to JPRS:<br>・ certificates and site seals issued by the CA, as well as information on certificate | **8.6 Communication of Results**<br>Auditors shall report the audit results to the CA.<br>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.<br>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.<br>**8.7 Self-Audits**<br>The CA shall monitor adherence this CP, the CPS, and strictly control its service quality by performing self audits on at least a quarterly basis against a randomly selected sample of at least three percent of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.<br>**9. Other Business and Legal Matters**<br>**9.1 Fees**<br>To be separately stipulated.<br>**9.2 Financial Responsibility**<br>The CA shall maintain a sufficient financial foundation required for operating and maintaining the CA.<br>**9.3 Confidentiality of Business Information**<br>**9.3.1 Scope of Confidential Information**<br>Stipulated in the CPS.<br>**9.3.2 Information not within the Scope of Confidential Information**<br>Stipulated in the CPS.<br>**9.3.3 Responsibility to Protect Confidential Information**<br>Stipulated in the CPS.<br>**9.4 Privacy of Personal Information**<br>Stipulated in the CPS.<br>**9.5 Intellectual Property Rights**<br>Unless separately agreed, all intellectual property rights pertaining to the following information shall belong to JPRS:<br>・ certificates and site seals issued by the CA, as well as information on certificate | |

| 変更履歴あり | 整形版 | 備考 |
| --- | --- | --- |
| revocation;<br>・ this CP, the CPS, and related documents;<br>・ Public Keys and Private Keys of the CA; and<br>・ software provided by JPRS.<br>This CP is published under the Creative Commons license Attribution- NoDerivatives (CC-BY-ND) 4.0 International.<br>  <br>(https://creativecommons.org/licenses/by-nd/4.0/) | revocation;<br>・ this CP, the CPS, and related documents;<br>・ Public Keys and Private Keys of the CA; and<br>・ software provided by JPRS.<br>This CP is published under the Creative Commons license Attribution- NoDerivatives (CC-BY-ND) 4.0 International.<br>  <br>(https://creativecommons.org/licenses/by-nd/4.0/) | |
| **9.6 Representations and Warranties**<br>**9.6.1 CA Representations and Warranties**<br>The CA shall bear the following obligations in performing its business operations as the CA:<br>・ securely generate and manage the CA's Private Keys;<br>・ accurately manage certificate issuance and revocation based on applications from the RA;<br>・ monitor and operate the CA's system at work; and<br>・ issue and publish the CRLs.<br>**9.6.2 RA Representations and Warranties**<br>The CA shall bear the following obligations in performing its business operations as an RA:<br>・ install registration terminals in a secure environment and operate them;<br>・ accurately communicate information to the CA in processing applications for certificate issuance and revocation;<br>・ promptly communicate information to the CA during operating hours in processing applications for certificate revocation; and<br>・ maintain and administer the Repository.<br>**9.6.3 Subscriber Representations and Warranties**<br>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.<br><br>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:<br><br>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 | **9.6 Representations and Warranties**<br>**9.6.1 CA Representations and Warranties**<br>The CA shall bear the following obligations in performing its business operations as the CA:<br>・ securely generate and manage the CA's Private Keys;<br>・ accurately manage certificate issuance and revocation based on applications from the RA;<br>・ monitor and operate the CA's system at work; and<br>・ issue and publish the CRLs.<br>**9.6.2 RA Representations and Warranties**<br>The CA shall bear the following obligations in performing its business operations as an RA:<br>・ install registration terminals in a secure environment and operate them;<br>・ accurately communicate information to the CA in processing applications for certificate issuance and revocation;<br>・ promptly communicate information to the CA during operating hours in processing applications for certificate revocation; and<br>・ maintain and administer the Repository.<br>**9.6.3 Subscriber Representations and Warranties**<br>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.<br><br>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:<br><br>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 | |

| 変更履歴あり | 整形版 | 備考 |
| --- | --- | --- |
| by the CA;<br><br>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);<br><br>3. **Acceptance of Certificate**: An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy;<br><br>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;<br><br>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;<br><br>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.<br><br>7. **Responsiveness**: An obligation to respond to the CA's instructions concerning Key Compromise or Certificate misuse within a specified time period.<br><br>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. | by the CA;<br><br>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);<br><br>3. **Acceptance of Certificate**: An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy;<br><br>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;<br><br>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;<br><br>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.<br><br>7. **Responsiveness**: An obligation to respond to the CA's instructions concerning Key Compromise or Certificate misuse within a specified time period.<br><br>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<br><br>Each Relying Party warrants that he/she/it will comply with the provisions of this CP. If any Relying Party fails to comply with any provision of this CP, the Relying Party shall assume all responsibilities therefor.<br><br>### 9.6.5 Representations and Warranties of Other Participants<br><br>No stipulation.<br><br>## 9.7 Disclaimer of Warranties | ### 9.6.4 Relying Party Representations and Warranties<br><br>Each Relying Party warrants that he/she/it will comply with the provisions of this CP. If any Relying Party fails to comply with any provision of this CP, the Relying Party shall assume all responsibilities therefor.<br><br>### 9.6.5 Representations and Warranties of Other Participants<br><br>No stipulation.<br><br>## 9.7 Disclaimer of Warranties | |

| 変更履歴あり | 整形版 | 備考 |
| --- | --- | --- |
| The CA is not liable for any indirect, special, incidental, or consequential damage arising in connection with any of the warranties stipulated in “9.6.1 CA Representations and Warranties” of this CP, or for lost profits, loss of data, or any other indirect or consequential damage whatsoever.<br><br>**9.8 Limitations of Liability**<br>The CA is not liable for the provisions of “9.6.1 CA Representations and Warranties” of this CP if damage falling under any of the following occurs:<br>・ any or all damage arising from any unlawful conduct, unauthorized use, negligence, or any other cause not attributable to the CA;<br>・ any damage resulting from a failure of a Subscriber to perform any of his/her/its obligations;<br>・ any or all damage arising from any cause attributable to a Subscriber’s system;<br>・ any damage arising from any defect or malfunction, or operation, of the hardware or software of the CA or a Subscriber;<br>・ any damage caused by any information published in a certificate or the CRL, for any reason not attributable to the CA;<br>・ any or all damage incurred by a failure in normal communication caused by any reason not attributable to the CA;<br>・ any or all damage arising in connection with the use of a certificate, such as business debts;<br>・ any damage caused by an improvement, beyond expectations at this point in time, in the cryptographic algorithm decoding capabilities of hardware or software;<br>・ 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<br>・ 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.<br><br>**9.9 Indemnities**<br>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.<br><br>**9.10 Term and Termination**<br>**9.10.1 Term** | The CA is not liable for any indirect, special, incidental, or consequential damage arising in connection with any of the warranties stipulated in “9.6.1 CA Representations and Warranties” of this CP, or for lost profits, loss of data, or any other indirect or consequential damage whatsoever.<br><br>**9.8 Limitations of Liability**<br>The CA is not liable for the provisions of “9.6.1 CA Representations and Warranties” of this CP if damage falling under any of the following occurs:<br>・ any or all damage arising from any unlawful conduct, unauthorized use, negligence, or any other cause not attributable to the CA;<br>・ any damage resulting from a failure of a Subscriber to perform any of his/her/its obligations;<br>・ any or all damage arising from any cause attributable to a Subscriber’s system;<br>・ any damage arising from any defect or malfunction, or operation, of the hardware or software of the CA or a Subscriber;<br>・ any damage caused by any information published in a certificate or the CRL, for any reason not attributable to the CA;<br>・ any or all damage incurred by a failure in normal communication caused by any reason not attributable to the CA;<br>・ any or all damage arising in connection with the use of a certificate, such as business debts;<br>・ any damage caused by an improvement, beyond expectations at this point in time, in the cryptographic algorithm decoding capabilities of hardware or software;<br>・ 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<br>・ 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.<br><br>**9.9 Indemnities**<br>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.<br><br>**9.10 Term and Termination**<br>**9.10.1 Term** | |

| 変更履歴あり | 整形版 | 備考 |
| --- | --- | --- |
| This CP shall come into effect upon approval by the CA's Certificate Operation Conference. This CP shall not lose its effect under any circumstances before its termination stipulated in "9.10.2 Termination" herein.<br>**9.10.2 Termination**<br>This CP shall lose its effect upon termination of the CA, except as provided in "9.10.3 Effect of Termination and Survival" herein.<br>**9.10.3 Effect of Termination and Survival**<br>Even in the event of termination of an agreement on use or the like between a Subscriber and the CA, or termination of the CA itself, any provisions of this CP that should survive such termination, by the nature thereof, shall continue to apply to Subscribers, Relying Parties, and the CA, regardless of the reason of such termination.<br>**9.11 Individual Notices and Communications with Participants**<br>JPRS shall provide necessary notices to Subscribers and Relying Parties on its Web site, by e-mail, in writing, or by other means.<br>**9.12 Amendments**<br>**9.12.1 Procedure for Amendment**<br>This CP may be revised at the discretion of the CA, as appropriate, and the revised version hereof shall come into effect upon approval of the CA's Certificate Operation Conference.<br>**9.12.2 Notification Mechanism and Period**<br>If the CA amends this CP, the CA shall promptly publish the amended version of this CP, which shall be deemed to be a notification thereof to Subscribers.<br>**9.12.3 Circumstances under Which OID Must Be Changed**<br>No stipulation.<br>**9.13 Dispute Resolution Provisions**<br>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.<br>**9.14 Governing Law**<br>Regardless of the respective addresses of the CA and Subscribers, the laws of Japan shall apply to any dispute over the interpretation or validity of this CP, or the use of a certificate.<br>**9.15 Compliance with Applicable Laws**<br>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. | This CP shall come into effect upon approval by the CA's Certificate Operation Conference. This CP shall not lose its effect under any circumstances before its termination stipulated in "9.10.2 Termination" herein.<br>**9.10.2 Termination**<br>This CP shall lose its effect upon termination of the CA, except as provided in "9.10.3 Effect of Termination and Survival" herein.<br>**9.10.3 Effect of Termination and Survival**<br>Even in the event of termination of an agreement on use or the like between a Subscriber and the CA, or termination of the CA itself, any provisions of this CP that should survive such termination, by the nature thereof, shall continue to apply to Subscribers, Relying Parties, and the CA, regardless of the reason of such termination.<br>**9.11 Individual Notices and Communications with Participants**<br>JPRS shall provide necessary notices to Subscribers and Relying Parties on its Web site, by e-mail, in writing, or by other means.<br>**9.12 Amendments**<br>**9.12.1 Procedure for Amendment**<br>This CP may be revised at the discretion of the CA, as appropriate, and the revised version hereof shall come into effect upon approval of the CA's Certificate Operation Conference.<br>**9.12.2 Notification Mechanism and Period**<br>If the CA amends this CP, the CA shall promptly publish the amended version of this CP, which shall be deemed to be a notification thereof to Subscribers.<br>**9.12.3 Circumstances under Which OID Must Be Changed**<br>No stipulation.<br>**9.13 Dispute Resolution Provisions**<br>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.<br>**9.14 Governing Law**<br>Regardless of the respective addresses of the CA and Subscribers, the laws of Japan shall apply to any dispute over the interpretation or validity of this CP, or the use of a certificate.<br>**9.15 Compliance with Applicable Laws**<br>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. | |

| 変更履歴あり | 整形版 | 備考 |
| --- | --- | --- |
| **9.16 Miscellaneous Provisions**<br>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 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.<br><br>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 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.<br><br>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 CPS and a notice to the CA/Browser Forum, as outlined above, MUST be made within 90 days.<br>**9.17 Other Provisions**<br>Not applicable. | **9.16 Miscellaneous Provisions**<br>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 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.<br><br>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 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.<br><br>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 CPS and a notice to the CA/Browser Forum, as outlined above, MUST be made within 90 days.<br>**9.17 Other Provisions**<br>Not applicable. | |