JPRS CA Certificate Policy 新旧対照表 JPRS CA Certificate Policy(変更履歴付)	JPRS CA Certificate Policy (整形版)	備考
JPRS CA Certificate Policy Version 3. <u>7</u> 60	JPRS CA Certificate Policy Version 3.70	凡例: <u>赤字(下線付き)</u> :追加 <del>青字(取消線付き)</del> :削除 バージョンの更新
<mark>AprilFebruary 1122</mark> , 2024 Japan Registry Services Co., Ltd.	April 11, 2024 Japan Registry Services Co., Ltd.	改訂日の更新
	1/44	

JPRS CA Certificate Policy(変更履歴付)		
		Version History
Version Number	Date	Description
1.00	2019.06.17	Publication of the first version
1.10	2019.09.25	Revision of "3.2.2.4 Validation of Domain Authorization or Control" (adding the additional information of "general e- mail address indicating an administrator"
1.20	2020.04.01	Revision due to Mozilla Root Store Policy (v2.7)
1.30	2020.07.10	Revision of "7.1.2 Subordinate CA Certificate Profile"
2.00	2020.07.22	Revision of "7. Certificate, CRL, and OCSP Profiles"
2.10	2020.08.20	Revision of the maximum validity period of certificate
2.20	2020.10.06	Revision of "3.2.2.4 Validation of Domain Authorization or Control"
2.21	2021.04.01	Revision of the date and version
2.22	2021.04.28	Revision due to Mozilla Root Store Policy (v2.7.1)
2.23	2021.05.27	<ul> <li>Clarification of "3.2.2.4 Validation of Domain Authorization or Control"</li> <li>Delete the description of invalid Subordinate CAs from "7. Certificate, CRL, and OCSP Profiles".</li> </ul>
2.30	2021.11.18	<ul> <li>Revision of "3.2.2.4.18 Agreed-Upon Change to Website v2"</li> <li>Sunset of "subject:organizationalUnitName"</li> </ul>
3.00	2021.12.08	Revisions due to new service provision
3.10	2022.03.02	Add a reference to the new terms and conditions
3.11	2022.04.01	Revision of the date and version
3.20	2022.09.30	<ul> <li>Revision of "6.3 Other Aspects of Key Pair Management"</li> <li>Add description of Revocation Reason Code to be applied in this CA.</li> </ul>
3.30	2023.04.24	$\cdot$ Revision of the maximum validity period of certificate
3.40	2023.06.08	<ul><li>Revision of "1.1 Overview"</li><li>Revision of "7.3 OCSP Profile"</li></ul>
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"
<u>3.70</u>	2024.04.11	Revision of Table 7.1-2 and Table 7.1-3

JPRS CA Certificate Policy (整形成)		
		Version History
Version	Date	Description
Number		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 Author
		Control" (adding the additional information of
		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 Pro
2.00	2020.07.22	Revision of "7. Certificate, CRL, and OCSP Profil
2.10	2020.08.20	Revision of the maximum validity period of certif
2.20	2020.10.06	Revision of "3.2.2.4 Validation of Domain Authori
		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"
		• Delete the description of invalid Subordinate C
		"7. Certificate, CRL, and OCSP Profiles".
2.30	2021.11.18	• Revision of "3.2.2.4.18 Agreed-Upon Change to
		v2"
		• Sunset of "subject:organizationalUnitName"
3.00	2021.12.08	Revisions due to new service provision
3.10	2022.03.02	Add a reference to the new terms and conditions
3.11	2022.04.01	Revision of the date and version
3.20	2022.09.30	• Revision of "6.3 Other Aspects of Key Pair Man
		• Add description of Revocation Reason Code to b
0.00	0000 04 04	in this CA.
3.30	2023.04.24	Revision of the maximum validity period of cer     Revision of "1.1 Overview"
3.40	2023.06.08	
0.50		Revision of "7.3 OCSP Profile"
3.50	2023.08.28	Revision of description to clarify compliance with
0.00	2024.02.02	Requirements
3.60	2024.02.22	Revision of "7. Certificate, CRL, and OCSP Profi
3.70	2024.04.11	Revision of Table 7.1-2 and Table 7.1-3

TPRS CA Cortificate Policy (敷形版)

# 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.

# 1. Introduction

### 1.1 Overview

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

Various procedures regarding the operation and maintenance of the CA are the JPRS CA Certification Practice Statement (hereinafter referred to as the A certificate for one-way and mutual certification has been issued to the C Communication RootCA2, Security Communication ECC RootCA1 or SEC Root CA 2024, a Certification Authority operated by SECOM Trust Sys (hereinafter referred to as "SECOM Trust Systems"), and the CA is author certificates to Subscribers.

	供此
	備考
orization or	
"general e-	
general e	
ofile"	
iles"	
ificate	
rization or	
1)	
CA a from	
CAs from	
o Website	
o website	
8	
nagement"	
be applied	
ertificate	
h Baseline	
n Daseinie	
ofiles"	
	ᄮᆕᆓᆓᆇᄽᆆᆕ
	改訂履歴の追記
as "this CP"),	
n, etc. of Digital	
referred to as	
the purpose of	
erred to as the	
e stipulated in	
e "CPS").	
CA by Security	
COM TLS RSA	
tems Co., Ltd.	
orized to issue	

#### 1.3.1 CA

#### JPRS CA Certificate Policy (変更履歴付)

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

If any inconsistency is found among the provisions of this CP, 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 <u>the Japanese version</u> and the English version of this CP, the English version shall prevail over <u>the Japanese version</u>. 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

#### JPRS CA Certificate Policy (整形版)

Certificates issued by the CA are used for encrypting information for server and on communication pathways. "The Terms and Conditions of JPRS Dig Issuance Services" and "The Terms and Conditions of JPRS Digital Certi Services for ACME" (hereinafter, both will be referred to as the "Terms and 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

Terms and Conditions, this CP, and the CPS in light of his/her/its own purper 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 Management of Publicly-Trusted TLS Server Certificates" (hereinafter refe "Baseline Requirements") published by CA/Browser Forum at https://www and the Application Software Supplier Standards published."

Table	1.1 List of Standards
Types of certificates issued	Standards to comply with
by the CA	
	<ul> <li>Baseline Requirements for the Issuance and Management of P</li> <li>Trusted TLS Server Certification</li> </ul>
TLS Server Certificate	<ul> <li>Apple Root Certificate Program</li> <li>Chrome Root Program Policy</li> <li>Microsoft Trusted Root Program</li> <li>Mozilla Root Store Policy</li> </ul>

If any inconsistency is found among the provisions of this CP, the Terms a and the CPS, the provisions of the Terms and Conditions shall prevail over to and the CPS, and the provisions of this CP shall prevail over those of the C inconsistency is found among the provisions of <u>the Japanese version</u> are version of this CP, the English version shall prevail over <u>the Japanese</u> event of any inconsistency between the documents established by the CA not limited to, this CP, the CPS, the Terms and Conditions, and the relate and Baseline Requirements, Baseline Requirements take precedent

This CP conforms to the RFC 3647 "Internet X.509 Public Key Infrastruct Policy and Certification Practices Framework" advocated by the IETF as a the operation of Certification Authorities.

With any developments or improvements pertaining to the CA in terms of operation, this CP shall be revised, as needed, in order to reflect such de 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") assign 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
JPRS CA Certification Practice Statement (CPS)	1.3.6.1.4.1.53827.1

## **1.3 PKI Participants**

	備考
authentication gital Certificate ficate Issuance nd Conditions")	
to consider the oses of use, and	
e Issuance and ferred to as the a.cabforum.org/,	
Publicly ates	
n	
and Conditions, those of this CP PS. Also, if any nd the English <u>version</u> . In the (including, but ted documents) ce over these	
ture Certificate framework for	
technologies or evelopments or	
gned by the CA	
7.1.1.4	
7.1.2.4	

JPRS CA Certificate Policy (変更履歴付)	JPRS CA Certificate Policy (整形版)
"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	certificate status using the OCSP (Online Certificate Status Protocol) server, g
protects the CA's own Private Keys, and registers Subscribers.	protects the CA's own Private Keys, and registers Subscribers.
1.3.2 RA	1.3.2 RA
"RA" stands for "Registration Authority," an entity that mainly performs reviews to verify the existence and validate the identities of applicants who apply for the issuance or revocation of certificates, registers information necessary for issuing certificates, and requests the CA to issue certificates, among the operations of the CA. The CA acts as an RA.	the existence and validate the identities of applicants who apply for the revocation of certificates, registers information necessary for issuing cert
1.3.3 Subscribers	1.3.3 Subscribers
"Subscribers" means an individual, corporation, or organization that has been issued a certificate by the CA and uses the certificate. "Subscriber Certificate" means the certificate issued by the CA to the Subscribers.	
1.3.4 Relying Parties	1.3.4 Relying Parties
A "Relying Party" means an individual, corporation, or organization that verifies the validity of certificates issued by the CA.	A "Relying Party" means an individual, corporation, or organization that validity of certificates issued by the CA.
1.3.5 Other Participants	1.3.5 Other Participants
No stipulation.	No stipulation.
1.4 Certificate Usage	1.4 Certificate Usage
1.4.1 Appropriate Certificate Uses	1.4.1 Appropriate Certificate Uses
Certificates issued by the CA are used to encrypt information for server authentication and on communication pathways.	Certificates issued by the CA are used to encrypt information for server auther on communication pathways.
1.4.2 Prohibited Certificate Uses	1.4.2 Prohibited Certificate Uses
Certificates issued by the CA may be used solely as set forth in "1.4.1 Appropriate Certificate Uses," and may not be used for any other purposes.	Certificates issued by the CA may be used solely as set forth in "1.4.1 Certificate Uses," and may not be used for any other purposes.
1.5 Policy Administration	1.5 Policy Administration
1.5.1 Organization Administering the Document	1.5.1 Organization Administering the Document
This CP shall be maintained and administered by the CA.	This CP shall be maintained and administered by the CA.
1.5.2 Contact Information	1.5.2 Contact Information
Inquiries concerning this CP should be directed to: Contact: Inquiries contact office, Japan Registry Services Co., Ltd. Address: Chiyoda First Bldg. East, 3-8-1 Nishi-Kanda, Chiyoda-ku, Tokyo 101-0065 JAPAN E-mail: <u>info@jprs.jp</u>	Inquiries concerning this CP should be directed to: Contact: Inquiries contact office, Japan Registry Services Co., Ltd. Address: Chiyoda First Bldg. East, 3-8-1 Nishi-Kanda, Chiyoda-ku, Tokyo 101- E-mail: <u>info@jprs.jp</u>
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: <u>https://jprs.jp/pubcert/f_mail/</u>	If a compromise or unauthorized use of any Private Key or any other trouble a certificate issued by the CA is revealed, please notify via the following webfor <u>https://jprs.jp/pubcert/f_mail/</u>
1.5.3 Person Determining CP Suitability as Policy	1.5.3 Person Determining CP Suitability as Policy
The details of this CP shall be determined by the CA's Certificate Operation Conference.	The details of this CP shall be determined by the CA's Certificate Operation Co
1.5.4 Approval Procedures	1.5.4 Approval Procedures
This CP shall come into effect upon approval of the CA's Certificate Operation Conference.	This CP shall come into effect upon approval of the CA's Certificate Operation

	備考
es and revokes rmation on the r, generates and	
eviews to verify the issuance or ertificates, and e CA acts as an	
s been issued a s the certificate	
nat verifies the	
hentication and	
4.1 Appropriate	
01-0065 JAPAN	
le pertaining to oform <sup>:</sup>	
Conference.	
on Conference.	

#### **1.6 Definitions and Acronyms**

#### ACME (Automated Certificate Management Environment)

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

#### <u>Archive</u>

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

#### Audit Log

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

#### Authorization Domain Name

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

#### Base Domain Name

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

#### CA (Certification Authority)

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

#### CAA (Certificate Authority Authorization)

"CAA" stands for "Certificate Authority Authorization," a function to prevent unintended erroneous issuance of certificates from unauthorized Certification Authorities in connection with the authority to use a domain by adding information to the DNS record in order to specify the Certification Authority authorized to issue a certificate for the domain. This function is stipulated in RFC 6844.

#### CP (Certificate Policy)

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

#### CPS (Certification Practices Statement)

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

#### JPRS CA Certificate Policy (整形版)

#### **1.6 Definitions and Acronyms**

ACME (Automated Certificate Management Environment)

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

#### Archive

"Archive" means information acquired for the purpose of keeping a histo or other reason.

#### <u>Audit Log</u>

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

#### Authorization Domain Name

The Domain Name used to obtain authorization for certificate issuand FQDN. The CA may use the FQDN returned from a DNS CNAME lookup for the purposes of domain validation. If the FQDN contains a wildcard of the CA MUST remove all wildcard labels from the left most portion of req The CA may prune zero or more labels from left to right until encour Domain Name and may use any one of the intermediate values for the purp validation.

#### Base Domain Name

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

#### CA (Certification Authority)

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

#### CAA (Certificate Authority Authorization)

"CAA" stands for "Certificate Authority Authorization," a function unintended erroneous issuance of certificates from unauthorized Authorities in connection with the authority to use a domain by adding the DNS record in order to specify the Certification Authority authority certificate for the domain. This function is stipulated in RFC 6844.

#### <u>CP (Certificate Policy)</u>

"CP" stands for "Certificate Policy," a document that sets forth poli certificates to be issued by the CA, such as the types of certificates, the set certificates may be issued, the usages of certificates, procedures for ap issuance of certificates, and the criteria for such issuance.

#### CPS (Certification Practices Statement)

"CPS" stands for "Certification Practice Statement," a document the provisions to be followed in operating the CA, such as various operation and security standards.

	備考
, a protocol that and certificate	
ory for any legal	
pertaining to itoring accesses	
nce for a given up as the FQDN character, then equested FQDN. intering a Base rpose of domain	
eft of a registry- lic suffix (e.g. nain name node gTLD itself may	
es, renews, and vides and stores ortificate Status , and registers	
ion to prevent d Certification g information to rized to issue a	
licies regarding ervers for which applying for the	
that sets forth onal procedures	

#### JPRS CA Certificate Policy (変更履歴付) JPRS CA Certificate Policy (整形版) CRL (Certificate Revocation List) CRL (Certificate Revocation List) "CRL" stands for "Certificate Revocation List," a list of information about certificates "CRL" stands for "Certificate Revocation List," a list of information abo revoked during their period of validity for any reason, including changes in the revoked during their period of validity for any reason, including cl particulars described in the certificates or the compromise of any Private Keys. particulars described in the certificates or the compromise of any Private F CT (Certificate Transparency) CT (Certificate Transparency) "CT" stands for "Certificate Transparency," a scheme stipulated in RFC 6962 to register "CT" stands for "Certificate Transparency," a scheme stipulated in RFC 6 and publish information about certificates on a log server (CT log server) for the purpose and publish information about certificates on a log server (CT log server) of monitoring and auditing information about issued certificates. of monitoring and auditing information about issued certificates. **Digital** Certificates **Digital** Certificates A "Digital Certificate" means digital data certifying that a Public Key is possessed by the A "Digital Certificate" means digital data certifying that a Public Key is po party specified in the data. The validity of a Digital Certificate is assured by a digital party specified in the data. The validity of a Digital Certificate is assured signature of the relevant CA affixed to the Digital Certificate. signature of the relevant CA affixed to the Digital Certificate. ECDSA (Elliptic Curve Digital Signature Algorithm) ECDSA (Elliptic Curve Digital Signature Algorithm) "ECDSA" is one of the most standard encryption technologies. ECDSA is widely used as "ECDSA" is one of the most standard encryption technologies. ECDSA is a public key cryptosystem. a public key cryptosystem. Escrow Escrow Escrow" means the placement (entrustment) of an asset in the control of an "Escrow" means the placement (entrustment) of an asset in the independent third party. independent third party. FIPS 140-2 FIPS 140-2 "FIPS 140-2" are a set of security accreditation criteria for cryptographic modules "FIPS 140-2" are a set of security accreditation criteria for cryptogr developed by the United States NIST (National Institute of Standards and Technology). developed by the United States NIST (National Institute of Standards an Four levels, from Level 1 (the lowest) to Level 4 (the highest), have been defined. Four levels, from Level 1 (the lowest) to Level 4 (the highest), have been de FQDN (Fully-Qualified Domain Name) FQDN (Fully-Qualified Domain Name) A Domain Name that includes the Domain Labels of all superior nodes in the Internet A Domain Name that includes the Domain Labels of all superior nodes Domain Name System. Domain Name System. HSM (Hardware Security Module) HSM (Hardware Security Module) "HSM" stands for "Hardware Security Module," a tamper-resistant encryption device to "HSM" stands for "Hardware Security Module," a tamper-resistant encry be used for generating, storing, using, or otherwise handling Private Keys for the be used for generating, storing, using, or otherwise handling Private purpose of maintaining security. purpose of maintaining security. JPRS Partners JPRS Partners "JPRS Partners" mean business enterprises authorized by JPRS in connection with the "JPRS Partners" mean business enterprises authorized by JPRS in conne Digital Certificate Issuance Services to be provided by JPRS. Digital Certificate Issuance Services to be provided by JPRS. Key Pair Key Pair A "Key Pair" means a pair consisting of a Private Key and Public Key A "Key Pair" means a pair consisting of a Private Key and Public Key in a public key cryptosystem. cryptosystem. NTP (Network Time Protocol) NTP (Network Time Protocol) "NTP" stands for "Network Time Protocol," a protocol designed to synchronize the "NTP" stands for "Network Time Protocol," a protocol designed to sy internal clocks of computers over a network. internal clocks of computers over a network. OCSP (Online Certificate Status Protocol) OCSP (Online Certificate Status Protocol) "OCSP" stands for "Online Certificate Status Protocol," a protocol for providing "OCSP" stands for "Online Certificate Status Protocol," a protocol information on the status of a certificate in real time. information on the status of a certificate in real time.

OID (Object Identifier)

#### 6/44

**OID** (Object Identifier)

	備考
oout certificates changes in the Keys.	
6962 to register for the purpose	
oossessed by the red by a digital	
s widely used as	
control of an	
raphic modules nd Technology). lefined.	
in the Internet	
yption device to e Keys for the	
nection with the	
in a public key	
synchronize the	
l for providing	

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

#### PKI (Public Key Infrastructure)

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

#### Private Key

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

#### Public Key

A "Public Key" means a key of a Key Pair used in a public key cryptosystem. A Public Key corresponds to a certain Private Key and is disclosed to the other party to communication.

#### RA (Registration Authority)

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

#### Random Value

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

#### <u>Repository</u>

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

#### RFC 3647 (Request for Comments 3647)

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

#### RFC 5280 (Request for Comments 5280)

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

#### RSA

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

#### SHA-1 (Secure Hash Algorithm 1)

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

#### SHA-256 (Secure Hash Algorithm 256)

#### JPRS CA Certificate Policy (整形版)

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

#### <u>PKI (Public Key Infrastructure)</u>

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

#### Private Key

A "Private Key" means a key of a Key Pair used in a public key cryptosys Key corresponds to a certain Public Key and is possessed only by the pers A Private Key may be referred to as a "secret key."

#### <u>Public Key</u>

A "Public Key" means a key of a Key Pair used in a public key cryptosy Key corresponds to a certain Private Key and is disclosed to the o communication.

#### RA (Registration Authority)

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

#### Random Value

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

#### <u>Repository</u>

The "Repository" means the database in which CA certificates, CRLs, a stored and published.

#### RFC 3647 (Request for Comments 3647)

"RFC 3647" stands for "Request for Comments 3647," a document framework for CP and CPS published by the IETF (Internet Engineering 7 industry group that establishes technical standards for the Internet.

#### RFC 5280 (Request for Comments 5280)

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

#### RSA

"RSA" is one of the most standard encryption technologies. RSA IS with public key cryptosystem.

#### SHA-1 (Secure Hash Algorithm 1)

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

#### SHA-256 (Secure Hash Algorithm 256)

	備老
nal registration for maintaining services or the	Unit
g the encryption nologies such as	
stem. A Private son in question.	
ystem. A Public other party to	
orms reviews to for the issuance certificates, and	
f entropy.	
and others are	
nt defining the Task Force), an	
ining the public rce), an industry	
idely used as a	
hash functions a computation pit length is one s in an original cansmitted and	

"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.

#### <u>Time Stamp</u>

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

#### Wildcard Certificate

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

#### Wildcard Domain Name

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

# 2. Publication and Repository Responsibilities

#### 2.1 Repository

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

#### 2.2 Publication of Information

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

### 2.3 Time or Frequency of Publication

This CP and the CPS shall be 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.

The frequency of CRL issuance is specified in Section 4.9.7.

### 2.4 Access Controls on Repositories

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

# 3. Identification and Authentication

#### 3.1 Naming

#### 3.1.1 Types of Names

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

#### 3.1.2 Need for Names to Be Meaningful

The information included in certificates issued by the CA and their meanings are specified in Section 7.1.1.

#### JPRS CA Certificate Policy (整形版)

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

#### <u>Time Stamp</u>

"Time Stamp" means recorded data indicating dates and times when electronic files have been prepared and a system has performed processing

#### Wildcard Certificate

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

#### Wildcard Domain Name

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

# 2. Publication and Repository Responsibilit

#### 2.1 Repository

The CA shall maintain and manage the Repository to allow access to the san (24) hours a day, three hundred sixty-five (365) days a year. Note, how Repository may be temporarily unavailable at times for system mainten reasons.

#### 2.2 Publication of Information

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

### 2.3 Time or Frequency of Publication

This CP and the CPS shall be revised at least annually and published on the revised. The CA describes to the CP and the CPS in detail how the CA in latest version of Baseline Requirements.

The frequency of CRL issuance is specified in Section 4.9.7.

#### 2.4 Access Controls on Repositories

The CA does not exercise any specific access control over information pu Repository. The CA's CRLs shall be made available to Subscribers and F through the Repository. Access to the Repository shall be granted through interface.

# 3. Identification and Authentication

### 3.1 Naming

#### 3.1.1 Types of Names

The name of each Subscriber to be described in certificates to be issued by t configured according to the Distinguished Name (DN) format for the recommendations (recommendations formulated by the International Teleo Union Telecommunication Standardization Sector (ITU-T)).

#### 3.1.2 Need for Names to Be Meaningful

The information included in certificates issued by the CA and their meaning in Section 7.1.1.

hash functions	備考
undred fifty-six message during	
n, for example, g.	
ject Alternative	
P) immediately	
ties	
me twenty-four wever, that the nance or other	
to allow online	
e Repository as implements the	
ublished on the Relying Parties a general Web	
the CA shall be e X.500 series ecommunication	
gs are specified	

JPRS CA Certificate Policy(変更履歴付)	JPRS CA Certificate Policy (整形版)
3.1.3 Anonymity or Pseudonymity of Subscribers	3.1.3 Anonymity or Pseudonymity of Subscribers
	No name identical to any anonym or pseudonym used in any certificate to be issued by the CA may be registered.
3.1.4 Rules for Interpreting Various Name Forms	3.1.4 Rules for Interpreting Various Name Forms
	The Distinguished Name (DN) format of the X.500 series shall stipulate the rules for interpreting various name forms and shall be complied with accordingly.
.1.5 Uniqueness of Names	3.1.5 Uniqueness of Names
	The attribute of a Distinguished Name (DN) to be described in a certificate to be issued by the CA shall be unique to the server covered by the issuance.
.1.6 Recognition, Authentication, and Roles of Trademarks	3.1.6 Recognition, Authentication, and Roles of Trademarks
ame described in a certificate application. No Subscriber may submit to the CA a retrificate application with any registered trademark or associated name of any third carty. If any dispute arises between a Subscriber and any third party in connection with a gistered trademark or the like, the CA will not undertake to arbitrate or settle the aspute. The CA is entitled to reject a Subscriber's certificate application or to revoke an	The CA does not verify whether an applicant holds any intellectual property right to the name described in a certificate application. No Subscriber may submit to the CA a certificate application with any registered trademark or associated name of any third party. If any dispute arises between a Subscriber and any third party in connection with a registered trademark or the like, the CA will not undertake to arbitrate or settle the dispute. The CA is entitled to reject a Subscriber's certificate application or to revoke an issued certificate on account of such a dispute.
3.2 Initial Identity Validation	3.2 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
levant Certificate Signing Request (hereinafter referred to as "CSR") and confirming that referred to as "CSR") and confirming that referred to as "CSR" and confirming to as "CSR" and confirming to a s "CSR" and confirming to as "CSR" and confirming to as "CSR" and confirming to a s "CSR" and confirming to as "CSR" and confirming to as "CSR" and confirming to a s "CSR" and confirming to a s "CSR" and confirming to as "CSR" and confirming to a s "CSR" and confirming	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.
.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.
<ul> <li>a CA does not verify the existence of organizations.</li> <li>b Organization Validation</li> <li>c CA shall verify the existence of organizations by using public documents issued by, or</li> <li>c D pages or Web page databases of, the relevant country or local public entity, or using public entity, or using public made by any third party that is deemed reliable by the CA, or the databases of it</li> </ul>	<ul> <li>3.2.2.1 Authentication of Organization Identity</li> <li>(1) Domain Validation</li> <li>The CA does not verify the existence of organizations.</li> <li>(2) Organization Validation</li> <li>The CA shall verify the existence of organizations by using public documents issued by, or</li> <li>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.</li> </ul>
	<b>3.2.2.2 DBA/Tradename</b> 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."
	<b>3.2.2.3 Verification of a Country</b> 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	<b>3.2.2.4 Validation of Domain Authorization or Control</b> The CA SHALL confirm that prior to issuance, the CA has validated each FQDN listed in

JPRS CA Certificate Policy(変更履歴付)	JPRS CA Certificate Policy (整形版)
specified by BR.	specified by BR.
The CA doesn't issue certificates if "RFC 7686 - The ".onion" Special-Use Domain Name" is	The CA doesn't issue certificates if "RFC 7686 - The ".onion" Special-Use Do
included in the certificates.	included in the certificates.
The CA SHALL maintain a record of which domain validation method, including relevant	The CA SHALL maintain a record of which domain validation method, inclu
BR version number, they used to validate every domain.	BR version number, they used to validate every domain.
3.2.2.4.1 Validating the Applicant as a Domain Contact	3.2.2.4.1 Validating the Applicant as a Domain Contact
Not applicable	Not applicable
3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact	3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact
Confirming the Applicant's control over the FQDN by sending a Random Value via	Confirming the Applicant's control over the FQDN by sending a Ram
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.	email and then receiving a confirming response utilizing the Rand Random Value MUST be sent to an email address listed in the WHOI
The CA does not use fax, SMS, or postal mail to send a Random Values.	The CA does not use fax, SMS, or postal mail to send a Random Value
The Random Value SHALL be unique in each email. The Random Value SHALL	The Random Value SHALL be unique in each email. The Random
remain valid for use in a confirming response for no more than 25 days from its	remain valid for use in a confirming response for no more than 2
creation.	creation.
3.2.2.4.3 Phone Contact with Domain Contact	3.2.2.4.3 Phone Contact with Domain Contact
Not applicable	Not applicable
3.2.2.4.4 Constructed Email to Domain Contact	3.2.2.4.4 Constructed Email to Domain Contact
Confirm the Applicant's control over the FQDN by	Confirm the Applicant's control over the FQDN by
1. Sending an email to one or more addresses created by using 'admin',	1. Sending an email to one or more addresses created by
'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part,	'administrator', 'webmaster', 'hostmaster', or 'postmaster' as
followed by the at-sign (""@""), followed by the Authorization Domain Name;	followed by the at-sign (""@""), followed by the Authorization
and	and
2. including a Random Value in the email; and	2. including a Random Value in the email; and
3. receiving a confirming response utilizing the Random Value.	3. receiving a confirming response utilizing the Random Value.
The Random Value SHALL be unique in each email. The Random Value SHALL	-
remain valid for use in a confirming response for no more than 25 days from its creation.	remain valid for use in a confirming response for no more than 2 creation.
3.2.2.4.5 Domain Authorization Document	3.2.2.4.5 Domain Authorization Document
Not applicable	Not applicable
3.2.2.4.6 Agreed-Upon Change to Website	3.2.2.4.6 Agreed-Upon Change to Website
Not applicable	Not applicable
3.2.2.4.7 DNS Change	3.2.2.4.7 DNS Change
Confirming the Applicant's control over the FQDN by confirming the presence of a	Confirming the Applicant's control over the FQDN by confirming the
Random Value in a DNS TXT record of the Authorization Domain Name that is	Random Value in a DNS TXT record of the Authorization Domain
prefixed with a Domain Label that begins with "_acme-challenge".	prefixed with a Domain Label that begins with "_acme-challenge".
The CA MUST provide a Random Value unique to the certificate request. The	
Random Value MUST remain valid for use in a confirming response for no more	Random Value MUST remain valid for use in a confirming respon-
than 25 days from its creation.	than 25 days from its creation.
3.2.2.4.8 IP Address	3.2.2.4.8 IP Address
Not applicable 3.2.2.4.9 Test Certificate	Not applicable 3.2.2.4.9 Test Certificate
Not applicable	Not applicable
3.2.2.4.10 TLS Using a Random Value	3.2.2.4.10 TLS Using a Random Value
Not applicable	Not applicable
3.2.2.4.11 Any Other Method	3.2.2.4.11 Any Other Method
Not applicable	Not applicable
3.2.2.4.12 Validating Applicant as a Domain Contact	3.2.2.4.12 Validating Applicant as a Domain Contact
Confirming the Applicant's control over the FQDN by validating the Applicant is the	
registrant of the domain name. This method may only be used if the CA is also the	
Domain Name Registrar, or an Affiliate of the Registrar, of the Base Domain Name.	Domain Name Registrar, or an Affiliate of the Registrar, of the Base I
3.2.2.4.13 Email to DNS CAA Contact	3.2.2.4.13 Email to DNS CAA Contact
Not applicable	Not applicable
3.2.2.4.14 Email to DNS TXT Contact	3.2.2.4.14 Email to DNS TXT Contact
Not applicable	Not applicable
3.2.2.4.15 Phone Contact with Domain Contact	3.2.2.4.15 Phone Contact with Domain Contact

	備考
main Name" is	
ading relevant	
ndom Value via dom Value. The S record. es. 1 Value SHALL 5 days from its	
using 'admin', the local part, Domain Name;	
1 Value SHALL 5 days from its	
ne presence of a n Name that is e request. The ase for no more	
Applicant is the e CA is also the Domain Name.	

Not applicable

- **3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact** Not applicable
- **3.2.2.4.17 Phone Contact with DNS CAA Phone Contact** Not applicable
- 3.2.2.4.18 Agreed-Upon Change to Website v2

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

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

The file containing the Random Value:

- 1. MUST be located on the Authorization Domain Name, and
- 2. MUST be located under the "/.well-known/pki-validation" directory, and
- 3. MUST be retrieved via either the "http" or "https" scheme, and

4. MUST be accessed over port 80 (http) or 443 (https).

If the CA follows redirects, the following apply:

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

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

For Certificates issued on or after 2021-11-18, this method is not applicable for validating Wildcard Domain Names.

#### 3.2.2.4.19 Agreed-Upon Change to Website - ACME

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

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

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

#### JPRS CA Certificate Policy (整形版)

#### Not applicable

- 3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact Not applicable
- 3.2.2.4.17 Phone Contact with DNS CAA Phone Contact Not applicable
- 3.2.2.4.18 Agreed-Upon Change to Website v2

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

- 1. The entire Random Value MUST NOT appear in the request u the file, and
- 2. the CA MUST receive a successful HTTP response from the re a 2xx HTTP status code must be received).
- The file containing the Random Value:
  - 1. MUST be located on the Authorization Domain Name, and
  - 2. MUST be located under the "/.well-known/pki-validation" direct
  - 3. MUST be retrieved via either the "http" or "https" scheme, and
- 4. MUST be accessed over port 80 (http) or 443 (https).
- If the CA follows redirects, the following apply:
- 1. Redirects MUST be initiated at the HTTP protocol layer.
  - Redirects MUST be the result of a 301, 302, or 307 HT response, as defined in RFC 7231, Section 6.4, or a 303 code response, as defined in RFC 7538, Section 3.
  - Redirects MUST be to the final value of the Location 1 header, as defined in RFC 7231, Section 7.1.2.
- 2. Redirects MUST be to resource URLs with either the "h scheme.
- 3. Redirects MUST be to resource URLs accessed via port 80 (https).

The CA MUST provide a Random Value unique to the certificate Random Value MUST remain valid for use in a confirming response than 25 days from its creation.

For Certificates issued on or after 2021-11-18, this method is not validating Wildcard Domain Names.

#### 3.2.2.4.19 Agreed-Upon Change to Website - ACME

Confirming the Applicant's control over a FQDN by validating domain FQDN using the ACME HTTP Challenge method defined in Section 8. The following are additive requirements to RFC 8555.

- 1. The CA MUST receive a successful HTTP response from (meaning a 2xx HTTP status code must be received).
- 2. The CA MUST provide a Random Value unique to the cert The Random Value MUST remain valid for use in a confirmin no more than 25 days from its creation.
- 3. If the CA follows redirects, the following apply:
  - 1. Redirects MUST be initiated at the HTTP protocol layer.
    - Redirects MUST be the result of a 301, 302, or 30 code response, as defined in RFC 7231, Section HTTP status code response, as defined in RFC 753
    - Redirects MUST be to the final value of the I response header, as defined in RFC 7231, Section
  - 2. Redirects MUST be to resource URLs with either the "l scheme.
  - 3. Redirects MUST be to resource URLs accessed via port 8 (https).

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

	備考
	V田 ペラ
at the Random	
used to retrieve	
quest (meaning	
ctory, and d	
TTP status code 08 HTTP status	
HTTP response	
nttp" or "https"	
0 (http) or 443	
e request. The use for no more	
t applicable for	
in control of the 3.3 of RFC 8555.	
om the request	
tificate request. ing response for	
07 HTTP status n 6.4, or a 308 38, Section 3.	
Location HTTP 7.1.2. http" or "https"	
80 (http) or 443	

#### 3.2.2.5 Authentication for an IP Address

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

#### 3.2.2.6 Wildcard Domain Validation

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

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

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

#### 3.2.2.7 Data Source Accuracy

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

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

#### 3.2.2.8 CAA Records

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

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

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

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

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

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

#### 3.2.3 Authentication of Individual Identity

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

#### 3.2.4 Non-Verified Subscriber Information

(1) Domain Validation

The CA stipulates no policies on non-verified information on Subscribers. (2) Organization Validation

#### 3.2.2.5 Authentication for an IP Address

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

JPRS CA Certificate Policy (整形版)

#### 3.2.2.6 Wildcard Domain Validation

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

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

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

#### 3.2.2.7 Data Source Accuracy

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

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

#### 3.2.2.8 CAA Records

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

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

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

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

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

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

#### 3.2.3 Authentication of Individual Identity

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

#### 3.2.4 Non-Verified Subscriber Information

(1) Domain Validation

The CA stipulates no policies on non-verified information on Subscribers. (2) Organization Validation

	備考
s.	
y a documented n Name in the co.uk", see RFC	
" or is a "public al control of the , but MAY issue	
on of a Country nts.	
L evaluate the cation. The CA	
ess CAA records extension that lo so within the	
wild, and iodef e contents of the CA MUST NOT Requirements.	
y encounter an	
CANN root.	

<ul> <li>The CA signification of Authority</li> <li>Domain Validation</li> <li>B.2.5 Validation of Authority</li> <li>Domain Validation</li> <li>Domain Validation</li> <li>Domain Validation</li> <li>Domain Validation</li> <li>Domain Validation</li> <li>Of Promains out the CA shall verify that the Subscriber is a registrant of the domain name by the crigitrant.</li> <li>Domain Validation</li> <li>Domain Validation</li> <li>Domain Validation</li> <li>Domain Validation</li> <li>Charled Validation</li> <li>Charle</li></ul>		
<ul> <li>3.2.5 Validation of Authority</li> <li>Domain Validation</li> <li>In the issuing a cortificate, the CA shall worly that the Subscriber is a registrant of the domain name to be described in the cortificate or has been granted an exclusive right to use the domain name by the registrant. (b) Urganization Validation</li> <li>Organization Validation</li> <li>CA shall evolution to save to be used for 3.2.2. Authentication of the cortificate by making contact with a contact person that may be verified by any for a cortification with a contact person that may be verified by any for a cortification save to bus used for 3.2.2. Authentication of a cortificate by making contact with a contact person that may be verified by any for a cortification of Interoperation</li> <li>S.4.6 Criteria for Interoperation</li> <li>S.4.6 Criteria for Interoperation</li> <li>C.4 Criteria for Interoperation for CR-exeq Requests</li> <li>C.4 Criteria for Interoperation for Reveal the source of the CP.</li> <li>C.4 Criteria for Interoperation for Reveal the source of the CP.</li> <li>C.4 Criteria for Interoperation for Reveal the source of the CP.</li> <li>C.4 Criteria for Interoperation for Reveal the source of the CP.</li> <li>C.4 Criteria for Interoperation for Reveal the so</li></ul>	JPRS CA Certificate Policy(変更履歴付)	JPRS CA Certificate Policy (整形版)
<ul> <li>Domain Validation</li> <li>C Ashall verify that an applicant for a certificate has been grained in exclusive right to use the domain name by the registrant.</li> <li>Deganization Validation</li> <li>C Ashall verify that an applicant for a certificate has been grained in exclusive right to use the domain name by the registrant.</li> <li>Deganization Validation</li> <li>C Ashall verify that an applicant for a certificate has been issued to the CA by Security Communication Recet Security Secure Security Security Secure Security Secure Security Security Secure Security Secure Security Secure Security Secure Security Secure</li></ul>		
<ul> <li>here issuing a certificate, the CA shall verify that the Subscriber is a registrant of the minin name to be described in the certificate or has been granted an exclusive right to the the domain name by the registrant.</li> <li>Organization Validation</li> <li>be CA shall verify that an applicant for a certificate has the legitimate authority to apply for a certificate by making contrast 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 Validation</li> <li>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 Validation</li> <li>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 Validation</li> <li>a certificate for one-way mutual certification has been issued to the CA by Security Communication RodCA2. Security Communication RodCA2 is exertificate for one-way mutual certification and Authentication for Re-key Requests</li> <li>a Cartification and Authentication for Re-key Requests</li> <li>back All validate an identity of orget Subscriber at a rekey in the same fination the application for secure of the CA.</li> <li>a distributed to maintentive the identity of ony Subscriber at a rekey in the same fination in durative of this CP.</li> <li>a distributed to maintentive the identity of ony Subscriber at a rekey in the same fination in the septiencino for issuarce of the certificate isseed under ACME protocol and the Revocation Request is signed by private key of the certificate Application</li> <li>back and undiation in durative index coust granted to the subscriber.</li> <li>certificate Application</li> <li>back and and ander ACME protocol and the Revocation Request is signed by private</li></ul>	-	
<ul> <li>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.</li> <li>a cleartification and Authentication for Re-key Requests</li> <li>b CA shall perform validate and authenticate the identity of any Subserber at a rekey in the same manner as set forth in "3.2 Initial Identity Validation" of this CP.</li> <li>4 Identification and Authentication for Re-key Requests</li> <li>b CA shall perform validate and authenticate the identity of any Subserber at a rekey in the same manner as set forth in "3.2 Initial Identity Validation" of this CP.</li> <li>b CA shall validate an identity in order to accept Revocation Request by check one of the following:</li> <li>The Revocation Request from any Subserber through the Designated Business Enterprise that has acted as an agent in the application for issuance of the certificate issued under ACME protocol and the Revocation Request is signed by private key of the account granted to the subseriber.</li> <li>The certificate Application</li> <li>D main Validation person who is a registrant of the domain name by the registrant may apply for the certificate.</li> <li>Organization Validation person who is a registrant of the domain name by the registrant may apply for the certificate.</li> <li>Organization Validation person who is a registrant of the domain name by the registrant may apply for the certificate.</li> <li>Organization Validation person who is a neglestion faving his/her address within Japan, whether incorporated in eaveliave regime to the contificate.</li> <li>Organization Validation is also perprivate weight to use the domain name by the registrant may apply for the certificate.</li> <li>Organization Validation is also perprivate weight to use the domain name by the registrum may apply for the certificate.</li> <li>Organization Va</li></ul>	<ul> <li>(1) Domain Validation</li> <li>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.</li> <li>(2) Organization Validation</li> <li>(2) 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.</li> </ul>	<ul> <li>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.</li> <li>(2) Organization Validation</li> <li>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</li> </ul>
<ul> <li>annunication RootCA2, Security Communication ECC RootCA1 or SECOM TLS RSA Root CA 2024, a Certification Authority operated by SECOM Trust Systems.</li> <li>aldentification and Authentication for Re-key Requests</li> <li>be CA shall perform validate and authoritiente the identity of any Subscriber at a rekey in the same manner as set forth in "3.2 Initial Identity Validation" of this CP.</li> <li>4 Identification and Authentication for Revocation Requests</li> <li>CA shall validate an identity in order to accept Revocation Request by check one of the Iloving:</li> <li>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 rus of services.</li> <li>The certificate issued under ACME protocol and the Revocation Request is signed by private key of the certificate.</li> <li>Certificate Life-Cycle Operational Requirements</li> <li>Certificate Application</li> <li>Domain Validation</li> <li>Derson who is a registrant of the domain name to be described in a certificate or has been strief an exclusive right to use the domain name by the registrant may apply for the certificate.</li> <li>Organization Validation</li> <li>Derson who is a registrant of the domain name by the registrant may apply for the requirement permanent place to the foregoing within Japan, or an organization is a sole proprietor having his/her address within Japan, whether incorporated in exclusive right to use the domain name by the registrant may apply for the certificate.</li> <li>Organization Validation</li> <li>Person who is a registrant of the domain name by the registrant may apply for the requirement as a colusive right to use the domain name by the registrant may apply for the certificate or principal office, branch office or subdivision, place of business, or ther equivalent permanent place to the foregoing within Japan, whether incorporated, may apply for the certific</li></ul>	3.2.6 Criteria for Interoperation	3.2.6 Criteria for Interoperation
<ul> <li>be 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.</li> <li>4 Identification and Authentication for Revocation Request to check one of the Idowing:</li> <li>1. The Revocation Request from any Subscriber through the Designated Business. Interprise that has acted as an agent in the application for issuance of the certificate issued under ACME protocol and the Revocation Request is signed by private key of the account granted to the subscriber.</li> <li>2. The certificate issued under ACME protocol and the Revocation Request is signed by private key of the account granted to the subscriber.</li> <li>3. The certificate issued under ACME protocol and the Revocation Request is signed by private key of the account granted to the subscriber.</li> <li>4. Certificate Life-Cycle Operational Requirements</li> <li>1. The Revocation Nalidation</li> <li>Person who is a registrant of the domain name to be described in a certificate or has been arrated an exclusive right to use the domain name by the registrant may apply for the certificate.</li> <li>4. Organization Validation</li> <li>Person who is a solo proprietor having his/her address within Japan, or an organization ving its head office or principal office, branch office or subdivision, place of business, or here equivalent permanent place to the foregoing within Japan, whether incorporated of may apply for the certificate.</li> </ul>	certificate for one-way mutual certification has been issued to the CA by Security ommunication RootCA2, Security Communication ECC RootCA1 or SECOM TLS RSA oot CA 2024, a Certification Authority operated by SECOM Trust Systems.	Communication RootCA2, Security Communication ECC RootCA1 or SECOM TLS RSA
<ul> <li>he CA shall validate an identity in order to accept Revocation Request by check one of the llowing:</li> <li>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 issued under ACME protocol and the Revocation Request is signed by private key of the account granted to the subscriber.</li> <li>The certificate issued under ACME protocol and the Revocation Request is signed by private key of the account granted to the subscriber.</li> <li>The certificate issued under ACME protocol and the Revocation Request is signed by private key of the certificate.</li> <li>Certificate Application</li> <li>L1 Who Can Submit a Certificate Application</li> <li>Domain Validation person who is a registrant of the domain name to be described in a certificate or has been anted an exclusive right to use the domain name by the registrant may apply for the retificate.</li> <li>Organization Validation person who is a sole proprietor having his/her address within Japan, or an organization validation aving its head office or principal office, branch office or subdivision, place of business, or there equivalent permanent place to the foregoing within Japan, whether incorporated may apply for the certificate.</li> </ul>	<b>3.3 Identification and Authentication for Re-key Requests</b> 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.	The CA shall perform validate and authenticate the identity of any Subscriber at a rekey
<ul> <li>A.1 Certificate Application</li> <li>A.1.1 Who Can Submit a Certificate Application</li> <li>Domain Validation</li> <li>person who is a registrant of the domain name to be described in a certificate or has been ranted an exclusive right to use the domain name by the registrant may apply for the registrant may apply for the certificate.</li> <li>Organization Validation</li> <li>person who is a sole proprietor having his/her address within Japan, or an organization aving its head office or principal office, branch office or subdivision, place of business, or her equivalent permanent place to the foregoing within Japan, whether incorporated, may apply for the certificate.</li> <li>A person who is a sole proprietor having his/her address within Japan, whether incorporated or unincorporated, may apply for the certificate.</li> </ul>	<ul><li>Enterprise that has acted as an agent in the application for issuance of the certificate or use of services.</li><li>2. The certificate issued under ACME protocol and the Revocation Request is signed by private key of the account granted to the subscriber.</li><li>3. The certificate issued under ACME protocol and the Revocation Request is signed by private key of the certificate.</li></ul>	<ul> <li>The CA shall validate an identity in order to accept Revocation Request by check one of the following;</li> <li>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.</li> <li>2. The certificate issued under ACME protocol and the Revocation Request is signed by private key of the account granted to the subscriber.</li> <li>3. The certificate issued under ACME protocol and the Revocation Request is signed by private key of the certificate.</li> </ul>
<ul> <li>A.1.1 Who Can Submit a Certificate Application</li> <li>Domain Validation</li> <li>person who is a registrant of the domain name to be described in a certificate or has been ranted an exclusive right to use the domain name by the registrant may apply for the refirence.</li> <li>Organization Validation</li> <li>person who is a sole proprietor having his/her address within Japan, or an organization aving its head office or principal office, branch office or subdivision, place of business, or her equivalent permanent place to the foregoing within Japan, whether incorporated, may apply for the certificate.</li> <li>Organization Validation</li> <li>person who is a sole proprietor having his/her address within Japan, or an organization aving its head office or principal office, branch office or subdivision, place of business, or her equivalent permanent place to the foregoing within Japan, whether incorporated or unincorporated, may apply for the certificate.</li> <li>Organization Validation</li> <li>A person who is a sole proprietor having his/her address within Japan, whether incorporated or business, or her equivalent permanent place to the foregoing within Japan, whether incorporated or unincorporated, may apply for the certificate.</li> </ul>	4. Certificate Life-Cycle Operational Requirements	4. Certificate Life-Cycle Operational Requirements
<ul> <li>Domain Validation</li> <li>person who is a registrant of the domain name to be described in a certificate or has been ranted an exclusive right to use the domain name by the registrant may apply for the reficate.</li> <li>Organization Validation</li> <li>person who is a sole proprietor having his/her address within Japan, or an organization aving its head office or principal office, branch office or subdivision, place of business, or her equivalent permanent place to the foregoing within Japan, whether incorporated or nincorporated, may apply for the certificate.</li> <li>(1) Domain Validation</li> <li>(2) Organization Validation</li> <li>A person who is a sole proprietor having his/her address within Japan, or an organization her equivalent permanent place to the foregoing within Japan, whether incorporated or nincorporated, may apply for the certificate.</li> </ul>	4.1 Certificate Application	4.1 Certificate Application
<ul> <li>Person who is a registrant of the domain name to be described in a certificate or has been canted an exclusive right to use the domain name by the registrant may apply for the certificate.</li> <li>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.</li> <li>Organization Validation person who is a sole proprietor having his/her address within Japan, or an organization aving its head office or principal office, branch office or subdivision, place of business, or her equivalent permanent place to the foregoing within Japan, whether incorporated or nincorporated, may apply for the certificate.</li> <li>Calculation (2) Organization Validation</li> <li>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 her equivalent permanent place to the foregoing within Japan, whether incorporated or nincorporated, may apply for the certificate.</li> </ul>	4.1.1 Who Can Submit a Certificate Application	4.1.1 Who Can Submit a Certificate Application
4.1.2 Enrollment Process and Responsibilities 4.1.2 Enrollment Process and Responsibilities	<ol> <li>Domain Validation</li> <li>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.</li> <li>Organization Validation</li> <li>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.</li> </ol>	<ul> <li>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.</li> <li>(2) Organization Validation</li> <li>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</li> </ul>
	4.1.2 Enrollment Process and Responsibilities	4.1.2 Enrollment Process and Responsibilities

#### 4.1.2 Enrollment Process and Responsibilities

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

#### 4.2 Certificate Application Processing

#### **4.2 Certificate Application Processing**

the Certificate Application submitted to the CA is accurate.

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 CA shall review application information by considering the information in the manner set forth in "3.2 Initial Identity Validation" of this CP. 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	The CA shall review application information by considering the information is set forth in "3.2 Initial Identity Validation" of this CP. The certificate request MAY include all factual information about the Ap included in the Certificate, and such additional information as is necessary obtain from the Applicant in order to comply with these Requirements
	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.	Certificate Policy and/or Certification Practice Statement. In cases where request does not contain all the necessary information about the Applicant, to obtain the remaining information from the Applicant or, having obtained it frindependent, third-party data source, confirm it with the Applicant. The stablish and follow a documented procedure for verifying all data requested in the Certificate by the Applicant.
	Applicant information MUST include, but not be limited to, at least one Fully-Qualified Domain Name or IP address to be included in the Certificate's subjectAltName extension.	Applicant information MUST include, but not be limited to, at least one F Domain Name or IP address to be included in the Certificate's subjectAltNam
	Section 6.3.2 of this CP limits the validity period of Subscriber Certificates. The CA MAY use the documents and data provided in Section 3.2 of this CP to verify certificate information, or may reuse previous validations themselves, provided that the CA obtained the data or document from a source specified under Section 3.2 of this CP or completed the validation itself no more than 825 days prior to issuing the Certificate.	Section 6.3.2 of this CP limits the validity period of Subscriber Certificates. The CA MAY use the documents and data provided in Section 3.2 of this certificate information, or may reuse previous validations themselves, provide obtained the data or document from a source specified under Section 3.2 completed the validation itself no more than 825 days prior to issuing the Cert
	For validation of Domain Names according to Section 3.2.2.4 of this CP, any reused data, document, or completed validation MUST be obtained no more than 398 days prior to issuing the Certificate. In no case may a prior validation be reused if any data or document used in the prior validation was obtained more than the maximum time permitted for reuse of the data or document prior to issuing the Certificate.	For validation of Domain Names according to Section 3.2.2.4 of this CP, any document, or completed validation MUST be obtained no more than 398 issuing the Certificate. In no case may a prior validation be reused if any data or document used validation was obtained more than the maximum time permitted for reuse document prior to issuing the Certificate.
	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.	The CA SHALL develop, maintain, and implement documented procedures and require additional verification activity for High Risk Certificate Request Certificate's approval, as reasonably necessary to ensure that such requests verified under these Requirements.
	4.2.2 Approval or Rejection of a Certificate Application	4.2.2 Approval or Rejection of a Certificate Application
	On approving any certificate application as a result of the review, the CA shall proceed to the issuance registration of the certificate.	On approving any certificate application as a result of the review, the CA sh the issuance registration of the certificate.
	If any certificate application is not complete, the CA shall reject the application and request the person who has submitted the application to submit an application again after correction or addition.	If any certificate application is not complete, the CA shall reject the ap request the person who has submitted the application to submit an application correction or addition.
	4.2.3 Time to Process Certificate Applications	4.2.3 Time to Process Certificate Applications
	After approving a certificate application, the CA shall proceed to the issuance registration of the certificate in a timely manner.	After approving a certificate application, the CA shall proceed to the issuance of the certificate in a timely manner.
	4.2.4 Check of CAA Records	4.2.4 Check of CAA Records
	In reviewing the application information, the CA shall check the CAA records in accordance with RFC 6844. The domain of the CA to be described in the CAA records shall be "jprs.jp." The Certificate Subscribers who want to grant the authority to issue certificates to the	accordance with RFC 6844. The domain of the CA to be described in the CAA be "jprs.jp." The Certificate Subscribers who want to grant the authority to issue cert
- 1	FQDN must include the value of "jprs.jp" in the property "issue" of the CAA record for each	FQDN must include the value of "jprs.jp" in the property "issue" of the CAA r

4.2.1 Performing Identification and Authentication Functions

4.3 Certificate Issuance

DNS zone.

### 4.3 Certificate Issuance

JPRS CA Certificate Policy(整形版)	備考
4.2.1 Performing Identification and Authentication Functions	
The CA shall review application information by considering the information in the manner set forth in "3.2 Initial Identity Validation" of this CP. 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.	
Applicant information MUST include, but not be limited to, at least one Fully-Qualified Domain Name or IP address to be included in the Certificate's subjectAltName extension.	
Section 6.3.2 of this CP limits the validity period of Subscriber Certificates. The CA MAY use the documents and data provided in Section 3.2 of this CP to verify certificate information, or may reuse previous validations themselves, provided that the CA obtained the data or document from a source specified under Section 3.2 of this CP or completed the validation itself no more than 825 days prior to issuing the Certificate.	
For validation of Domain Names according to Section 3.2.2.4 of this CP, any reused data, document, or completed validation MUST be obtained no more than 398 days prior to issuing the Certificate. In no case may a prior validation be reused if any data or document used in the prior validation was obtained more than the maximum time permitted for reuse of the data or document prior to issuing the Certificate.	
The CA SHALL develop, maintain, and implement documented procedures that identify and require additional verification activity for High Risk Certificate Requests prior to the Certificate's approval, as reasonably necessary to ensure that such requests are properly verified under these Requirements.	
4.2.2 Approval or Rejection of a Certificate Application	
On approving any certificate application as a result of the review, the CA shall proceed to the issuance registration of the certificate.	
If any certificate application is not complete, the CA shall reject the application and request the person who has submitted the application to submit an application again after correction or addition.	
4.2.3 Time to Process Certificate Applications	
After approving a certificate application, the CA shall proceed to the issuance registration of the certificate in a timely manner.	
4.2.4 Check of CAA Records	
In reviewing the application information, the CA shall check the CAA records in accordance with RFC 6844. The domain of the CA to be described in the CAA records shall be "jprs.jp." 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	

#### 4.3.1 CA Actions during Certificate Issuance

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

#### 4.3.2 Notification to Subscriber of Certificate Issuance

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

#### 4.4 Certificate Acceptance

#### 4.4.1 Conduct Constituting Certificate Acceptance

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

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

#### 4.4.2 Publication of the Certificates by the CA

The CA does not publish certificates of Subscribers.

#### 4.4.3 Notification of Certificate Issuance by the CA to Other Entities

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

#### 4.5 Key Pair and Certificate Usage

#### 4.5.1 Subscriber Private Key and Certificate Usage

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

#### 4.5.2 Relying Party Public Key and Certificate Usage

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

#### 4.6 Certificate Renewal

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

#### 4.6.1 Circumstances for Certificate Renewal

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

#### JPRS CA Certificate Policy (整形版)

### 4.3.1 CA Actions during Certificate Issuance

After completing a review of a certificate application, the CA shall regist that is based on the application information and necessary for the issuance on a CT log server operated by a third party and prescribed by the CA, and certificate. The information to be registered on the CT log server shall be a "7.1 Certificate Profile" of this CP.

#### 4.3.2 Notification to Subscriber of Certificate Issuance

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

#### 4.4 Certificate Acceptance

#### 4.4.1 Conduct Constituting Certificate Acceptance

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

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

### 4.4.2 Publication of the Certificates by the CA

The CA does not publish certificates of Subscribers.

#### 4.4.3 Notification of Certificate Issuance by the CA to Other

The CA does not notify any third party (excluding Designated Business Enterissuance of certificates.

### 4.5 Key Pair and Certificate Usage

#### 4.5.1 Subscriber Private Key and Certificate Usage

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

### 4.5.2 Relying Party Public Key and Certificate Usage

Relying Parties may verify the reliability of certificates issued by the CA certificates. Relying Parties shall understand and consent to the provisions the CPS before verifying the reliability of certificates issued by the CA and same.

### 4.6 Certificate Renewal

A "certificate renewal" means the issuance of a new certificate to a Subscrib change in his/her/its Public Key. When a Subscriber has his/her/its certificate CA recommends that the Subscriber generate a new Key Pair.

### 4.6.1 Circumstances for Certificate Renewal

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

	備考
ter information of a certificate, l then issue the as described in	
an e-mail to the te issued under	
of the following	
criber-only web	
protocol and the d under ACME	
ther than 1 and	
• <b>Entities</b> terprises) of the	
e corresponding cation and on	
by using such of this CP and relying on the	
per without any te renewed, the	
ate is about to	

JPRS CA Certificate Policy(変更履歴付)	JPRS CA Certificate Policy (整形版)	備考
4.6.2 Who May Request Renewal	4.6.2 Who May Request Renewal	
The provisions of "4.1.1 Who Can Submit a Certificate Application" of this CP shall apply correspondingly.	The provisions of "4.1.1 Who Can Submit a Certificate Application" of this CP shall apply correspondingly.	
4.6.3 Processing Certificate Renewal Requests	4.6.3 Processing Certificate Renewal Requests	
The provisions of "4.3.1 CA Actions during Certificate Issuance" of this CP shall apply correspondingly.	The provisions of "4.3.1 CA Actions during Certificate Issuance" of this CP shall apply correspondingly.	
4.6.4 Notification of New Certificate Issuance to Subscriber	4.6.4 Notification of New Certificate Issuance to Subscriber	
The provisions of "4.3.2 Notification to Subscriber of Certificate Issuance" of this CP shall apply correspondingly.	The provisions of "4.3.2 Notification to Subscriber of Certificate Issuance" of this CP shall apply correspondingly.	
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate	4.6.5 Conduct Constituting Acceptance of a Renewal Certificate	
The provisions of "4.4.1 Conduct Constituting Certificate Acceptance" of this CP shall apply correspondingly.	The provisions of "4.4.1 Conduct Constituting Certificate Acceptance" of this CP shall apply correspondingly.	
4.6.6 Publication of the Renewal Certificate by the CA	4.6.6 Publication of the Renewal Certificate by the CA	
The provisions of "4.4.2 Publication of the Certificates by the CA" of this CP shall apply correspondingly.	The provisions of "4.4.2 Publication of the Certificates by the CA" of this CP shall apply correspondingly.	
4.6.7 Notification of Certificate Issuance by the CA to Other Entities	4.6.7 Notification of Certificate Issuance by the CA to Other Entities	
The provisions of "4.4.3 Notification of Certificate Issuance by the CA to Other Entities" of this CP shall apply correspondingly.	The provisions of "4.4.3 Notification of Certificate Issuance by the CA to Other Entities" of this CP shall apply correspondingly.	
<b>4.7 Certificate Re-key</b> A "certificate re-key" means the issuance of a new certificate to a Subscriber after generating a new Key Pair.	<b>4.7 Certificate Re-key</b> A "certificate re-key" means the issuance of a new certificate to a Subscriber after generating a new Key Pair.	
4.7.1 Circumstances for Certificate Re-key	4.7.1 Circumstances for Certificate Re-key	
A certificate may be renewed without involving re-key when the certificate is about to expire.	A certificate may be renewed without involving re-key when the certificate is about to expire.	
4.7.2 Who May Request Certification of a New Public Key	4.7.2 Who May Request Certification of a New Public Key	
The provisions of "4.1.1 Who Can Submit a Certificate Application" of this CP shall apply correspondingly.	The provisions of "4.1.1 Who Can Submit a Certificate Application" of this CP shall apply correspondingly.	
4.7.3 Processing Certificate Re-keying Requests	4.7.3 Processing Certificate Re-keying Requests	
The provisions of "4.3.1 CA Actions during Certificate Issuance" of this CP shall apply correspondingly.	The provisions of "4.3.1 CA Actions during Certificate Issuance" of this CP shall apply correspondingly.	
4.7.4 Notification of New Certificate Issuance to Subscriber	4.7.4 Notification of New Certificate Issuance to Subscriber	
The provisions of "4.3.2 Notification to Subscriber of Certificate Issuance" of this CP shall apply correspondingly.	The provisions of "4.3.2 Notification to Subscriber of Certificate Issuance" of this CP shall apply correspondingly.	
4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate	4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate	
The provisions of "4.4.1 Conduct Constituting Certificate Acceptance" of this CP shall apply correspondingly.	The provisions of "4.4.1 Conduct Constituting Certificate Acceptance" of this CP shall apply correspondingly.	
4.7.6 Publication of the Re-keyed Certificates by the CA	4.7.6 Publication of the Re-keyed Certificates by the CA	
The provisions of "4.4.2 Publication of the Certificates by the CA" of this CP shall apply correspondingly.	The provisions of "4.4.2 Publication of the Certificates by the CA" of this CP shall apply correspondingly.	
4.7.7 Notification of Certificate Issuance by the CA to Other Entities	4.7.7 Notification of Certificate Issuance by the CA to Other Entities	

JPRS CA Certificate Policy(変更履歴付)	JPRS CA Certificate Policy (整形版)
The provisions of "4.4.3 Notification of Certificate Issuance by the CA to Other Entities" of this CP shall apply correspondingly.	The provisions of "4.4.3 Notification of Certificate Issuance by the CA to Othe this CP shall apply correspondingly.
4.8 Certificate Modification	4.8 Certificate Modification
4.8.1 Circumstances for Certificate Modification	4.8.1 Circumstances for Certificate Modification
If a need arises to modify any registered information in a certificate (excluding the common name used in the certificate), the certificate shall be modified.	If a need arises to modify any registered information in a certificate (excluding name used in the certificate), the certificate shall be modified.
4.8.2 Who May Request Certificate Modification	4.8.2 Who May Request Certificate Modification
The provisions of "4.1.1 Who Can Submit a Certificate Application" of this CP shall apply correspondingly.	The provisions of "4.1.1 Who Can Submit a Certificate Application" of this C correspondingly.
4.8.3 Processing Certificate Modification Requests	4.8.3 Processing Certificate Modification Requests
The provisions of "4.3.1 CA Actions during Certificate Issuance" of this CP shall apply correspondingly.	The provisions of "4.3.1 CA Actions during Certificate Issuance" of this C correspondingly.
4.8.4 Notification of New Certificate Issuance to Subscriber	4.8.4 Notification of New Certificate Issuance to Subscriber
The provisions of "4.3.2 Notification to Subscriber of Certificate Issuance" of this CP shall apply correspondingly.	The provisions of "4.3.2 Notification to Subscriber of Certificate Issuance" of apply correspondingly.
4.8.5 Conduct Constituting Acceptance of Modified Certificate	4.8.5 Conduct Constituting Acceptance of Modified Certification
The provisions of "4.4.1 Conduct Constituting Certificate Acceptance" of this CP shall apply correspondingly.	The provisions of "4.4.1 Conduct Constituting Certificate Acceptance" of this C correspondingly.
4.8.6 Publication of the Modified Certificate by the CA	4.8.6 Publication of the Modified Certificate by the CA
The provisions of "4.4.2 Publication of the Certificates by the CA" of this CP shall apply correspondingly.	The provisions of "4.4.2 Publication of the Certificates by the CA" of this C correspondingly.
4.8.7 Notification of Certificate Issuance by the CA to Other Entities	4.8.7 Notification of Certificate Issuance by the CA to Other I
The provisions of "4.4.3 Notification of Certificate Issuance by the CA to Other Entities" of this CP shall apply correspondingly.	The provisions of "4.4.3 Notification of Certificate Issuance by the CA to Othe this CP shall apply correspondingly.
4.9 Certificate Revocation and Suspension	4.9 Certificate Revocation and Suspension
4.9.1 Circumstances for Certificate Revocation	4.9.1 Circumstances for Certificate Revocation
<ul> <li>If any one of the following events occurs, the Subscriber must apply to the CA to have the corresponding certificate revoked: <ul> <li>the information described in the certificate has changed;</li> <li>the Private Key has been or may be compromised for any reason, including theft, loss, leakage, or unauthorized use thereof;</li> <li>any of the particulars described in the certificate or its purposes of use are incorrect;</li> <li>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</li> </ul> </li> </ul>	<ul> <li>If any one of the following events occurs, the Subscriber must apply to the C corresponding certificate revoked: <ul> <li>the information described in the certificate has changed;</li> <li>the Private Key has been or may be compromised for any reason, include loss, leakage, or unauthorized use thereof;</li> <li>any of the particulars described in the certificate or its purposes of use a</li> <li>the Subscriber finds that an improper string has been designated for, or in, a value set in any information in the certificate (as set forth in "3.1.1 Names" of this CP) (for Organization Validation only); or</li> <li>the Subscriber stops using the certificate.</li> </ul> </li> </ul>
The CA SHALL revoke a Certificate within 24 hours and use the corresponding CRLReason if one or more of the following occurs:	The CA SHALL revoke a Certificate within 24 hours and use the CRLReason if one or more of the following occurs:
1. The Subscriber requests in writing, without specifying a CRLreason, that the CA revoke the Certificate (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL);	1. The Subscriber requests in writing, without specifying a CRLreason, t revoke the Certificate (CRLReason "unspecified (0)" which results in n extension being provided in the CRL);
2. The Subscriber notifies the CA that the original certificate request was not	2. The Subscriber notifies the CA that the original certificate request was

	供力
ther Entities" of	備考
ing the common	
CP shall apply	
CP shall apply	
of this CP shall	
ate	
s CP shall apply	
CP shall apply	
Entities	
her Entities" of	
CA to have the	
iding theft,	
e are incorrect;	
or is included .1 Types of	
corresponding	
that the CA	
no reasonCode	
as not	

authorized and does not retroactively grant authorization (CRLReason #9, privilegeWithdrawn);

- 3. The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise (CRLReason #1, keyCompromise);
- 4. The CA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys) (CRLReason #1, keyCompromise);
- 5. The CA obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon (CRLReason #4, superseded).

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

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

#### 4.9.2 Who Can Request Revocation

The following can request the Revocation Request; 1. The Subscriber

#### JPRS CA Certificate Policy (整形版)

authorized and does not retroactively grant authorization (CRLRease privilegeWithdrawn);

- 3. The CA obtains evidence that the Subscriber's Private Key correspond Public Key in the Certificate suffered a Key Compromise (CRLReaso keyCompromise);
- 4. The CA is made aware of a demonstrated or proven method that can the Subscriber's Private Key based on the Public Key in the Certifica Debian weak key, see https://wiki.debian.org/SSLkeys) (CRLReason # keyCompromise);
- 5. The CA obtains evidence that the validation of domain authorization any Fully-Qualified Domain Name or IP address in the Certificate sh relied upon (CRLReason #4, superseded).

The CA SHOULD revoke a certificate within 24 hours and MUST revok within 5 days and use the corresponding CRLReason if one or more of the fol

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

#### 4.9.2 Who Can Request Revocation

The following can request the Revocation Request; The Subscriber

1.

	備考
on #9,	
nding to the n #1,	
easily compute ate (such as a #1,	
or control for nould not be	
xe a Certificate llowing occurs:	
perseded); on #9,	
its material eason #9,	
QDN in the as revoked a t licensing or pplicant has Domain Name)	
authenticate a geWithdrawn); ined in the	
nce with these	
bearing in the	
pires or is tinue " which results	
tion Practice by this section h results in no	
oses the that the specific	

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

#### 4.9.3 Procedures for Revocation Request

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

- 1. Request through Designated Business Enterprise
- $2. \ \ Request \ under \ ACME \ protocol$

#### 4.9.4 Revocation Request Grace Period

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

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

#### 4.9.5 Time within Which the CA Shall Process the Revocation Request

Upon accepting a valid Revocation Request of a certificate, the CA shall promptly process the Revocation Request and reflect the relevant information in the certificate on the CRL. Within 24 hours after receiving a Certificate Problem Report, the CA SHALL investigate the facts and circumstances related to a Certificate Problem Report and provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report.

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

#### 4.9.6 Revocation Checking Requirement for Relying Parties

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

#### 4.9.7 CRL Issuance Frequency

The CA SHALL update and reissue CRLs at least once every seven days, and the value of the nextUpdate field MUST NOT be more than ten days beyond the value of the thisUpdate field.

#### 4.9.8 Maximum Latency for CRLs

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

#### 4.9.9 On-line Revocation/Status Checking Availability

Information on the certificate status shall be provided online via the OCSP server. OCSP responses MUST conform to RFC 6960 and/or RFC 5019. OCSP responses MUST either:

- 1. Be signed by the CA that issued the Certificates whose revocation status is being checked, or
- 2. Be signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked.

#### JPRS CA Certificate Policy (整形版)

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

#### **4.9.3 Procedures for Revocation Request**

The CA SHALL accept the Revocation Request received in one of the follor revoke the certificate after verification the Revocation Request by section 3.4 1. Request through Designated Business Enterprise

2. Request under ACME protocol

#### 4.9.4 Revocation Request Grace Period

If someone who can request revocation determines that the Private Key has be compromised, he/she/it must promptly file the Revocation Request of the of The CA SHALL maintain a continuous 24x7 ability to accept and respond requests and Certificate Problem Reports.

#### 4.9.5 Time within Which the CA Shall Process the Revocation

Upon accepting a valid Revocation Request of a certificate, the CA shall prothe Revocation Request and reflect the relevant information in the certificate Within 24 hours after receiving a Certificate Problem Report, the CA SHA the facts and circumstances related to a Certificate Problem Report a preliminary report on its findings to both the Subscriber and the entity Certificate Problem Report.

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

#### 4.9.6 Revocation Checking Requirement for Relying Parties

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

#### 4.9.7 CRL Issuance Frequency

The CA SHALL update and reissue CRLs at least once every seven days, at the nextUpdate field MUST NOT be more than ten days beyond the thisUpdate field.

#### 4.9.8 Maximum Latency for CRLs

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

#### 4.9.9 On-line Revocation/Status Checking Availability

Information on the certificate status shall be provided online via the OCSP s OCSP responses MUST conform to RFC 6960 and/or RFC 5019. OCSP res either:

- 1. Be signed by the CA that issued the Certificates whose revocation sta checked, or
- 2. Be signed by an OCSP Responder whose Certificate is signed by the the Certificate whose revocation status is being checked.

	備考	
the application	UH ~J	
owing way, and l.		
as been or may certificate. d to revocation		
on Request		
omptly process e on the CRL. LL investigate and provide a who filed the		
Subscriber and elated notice to ich the CA will lem Report or time frame set		
sued by the CA. ng Party must ain information		
nd the value of e value of the		
erver. sponses MUST		
atus is being		
CA that issued		
	1	

JPRS CA Certificate Policy(変更履歴付)	JPRS CA Certificate Policy (整形版)	備考
	In the latter case, the OCSP signing Certificate MUST contain an extension of type id- pkix-ocsp-nocheck, as defined by RFC 6960.	
4.9.10 On-line Revocation/Status Checking Requirements	4.9.10 On-line Revocation/Status Checking Requirements	
he 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 hrough the OCSP server. DCSP responders operated by the CA SHALL support the HTTP GET method, as described n RFC 6960 and/or RFC 5019. The validity interval of an OCSP response is the difference in time between he thisUpdate and nextUpdate field, inclusive. For purposes of computing differences, a	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. OCSP responders operated by the CA SHALL support the HTTP GET method, as described in RFC 6960 and/or RFC 5019. 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. For the status of Subscriber Certificates:	
1. OCSP responses MUST have a validity interval greater than or equal to eight hours;	1. OCSP responses MUST have a validity interval greater than or equal to eight hours;	
<ol> <li>OCSP responses MUST have a validity interval less than or equal to ten days;</li> <li>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.</li> </ol>	<ol> <li>OCSP responses MUST have a validity interval less than or equal to ten days;</li> <li>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.</li> </ol>	
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.	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.	
s "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 <u>Section</u> 7.1.2.3 or <u>Section 7.1.2.5</u> , the responder MUST NOT respond with a "good" status for such	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 <u>Section 7.1.2.3</u> or <u>Section 7.1.2.5</u> , the responder MUST NOT respond with a "good" status for such requests.	
oart of its security response procedures. The OCSP responder MAY provide definitive responses about "reserved" certificate serial	The CA SHOULD monitor the OCSP responder for requests for "unused" serial numbers as part of its security response procedures. The OCSP responder MAY provide definitive responses about "reserved" certificate serial numbers, as if there was a corresponding Certificate that matches the Precertificate [RFC]	
5962]. A certificate serial number within an OCSP request is one of the following three options:	6962]. A certificate serial number within an OCSP request is one of the following three options:	
<ol> <li>"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</li> <li>"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</li> </ol>	<ol> <li>"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</li> <li>"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 <u>Section</u></li> </ol>	
<ul> <li><u>7.1.2.4</u>, associated with the Issuing CA; or</li> <li>3. "unused" if neither of the previous conditions are met.</li> </ul>	<ul> <li><u>7.1.2.4</u>, associated with the Issuing CA; or</li> <li>3. "unused" if neither of the previous conditions are met.</li> </ul>	
4.9.11 Other Forms of Revocation Advertisements Available	4.9.11 Other Forms of Revocation Advertisements Available	
4.9.11 Other Forms of Revocation Advertisements Available Not applicable.	Not applicable.	
4.9.12 Special Requirements Regarding Key Compromise	4.9.12 Special Requirements Regarding Key Compromise	
	If a compromise of any Private Key pertaining to a certificate issued by the CA is revealed, please notify via the following webform:	

JPRS CA Certificate Policy(変更履歴付)	JPRS CA Certificate Policy (整形版)
<ul> <li>Please include either of the following information in your report.</li> <li>The compromised private key itself</li> <li>A CSR signed by the compromised private key (A CSR must contain a string indicating that a private key has been compromised in the "CN" field. e.g. CN="This key is compromised")</li> <li>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.</li> </ul>	<ul> <li>Please include either of the following information in your report.</li> <li>The compromised private key itself</li> <li>A CSR signed by the compromised private key (A CSR must contain a string indicating that a private key has been compre "CN" field. e.g. CN="This key is compromised")</li> <li>The CA shall verify whether any of the certificates issued by the CA use t</li> </ul>
4.9.13 Circumstances for Suspension	4.9.13 Circumstances for Suspension
Not applicable.	Not applicable.
4.9.14 Who Can Request Suspension	4.9.14 Who Can Request Suspension
Not applicable.	Not applicable.
4.9.15 Procedures for Suspension Request	4.9.15 Procedures for Suspension Request
Not applicable.	Not applicable.
4.9.16 Limits on Suspension Period	4.9.16 Limits on Suspension Period
Not applicable.	Not applicable.
4.10 Certificate Status Services	4.10 Certificate Status Services
4.10.1 Operational Characteristics	4.10.1 Operational Characteristics
Subscribers and Relying Parties may check information on the status of a certificate through the OCSP server. Revocation entries on a CRL or OCSP Response MUST NOT be removed until after the Expiry Date of the revoked Certificate.	through the OCSP server.
4.10.2 Service Availability	4.10.2 Service Availability
The CA shall manage the OCSP server to allow Subscribers and Relying Parties to check information on the status of a certificate twenty-four (24) hours a day, three hundred sixty- five (365) days a year. However, the OCSP server may be temporarily unavailable at times for maintenance or other reasons. The CA SHALL operate and maintain its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.	information on the status of a certificate twenty-four (24) hours a day, three h five (365) days a year. However, the OCSP server may be temporarily unavail for maintenance or other reasons. The CA SHALL operate and maintain its CRL and OCSP capability wi
The CA SHALL maintain an online 24x7 Repository that application software can use to automatically check the current status of all unexpired Certificates issued by the CA.	The CA SHALL maintain an online 24x7 Repository that application softwar automatically check the current status of all unexpired Certificates issued by t
The CA SHALL maintain a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint.	
4.10.3 Optional Features	4.10.3 Optional Features
No stipulation.	No stipulation.
<b>4.11 End of Subscription (Registration)</b> 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 procedures for certificate renewal and his/her/its certificate expires, registration shall terminate. However, the CA may treat a Subscriber who has been issued a certificate under ACME protocol differently from the above. Other details regarding the cancellation of the Service

21/44

	備考
promised in the	
e the presented rate key, the CA	
of a certificate	
until after the	
Parties to check hundred sixty- ailable at times	
with resources rmal operating	
ware can use to by the CA.	
a high-priority mplaint to law ch a complaint.	
the Subscriber	
fails to carry the certificate	
e under ACME n of the Service	

JPRS CA Certificate Policy(変更履歴付)	JPRS CA Certificate Policy (整形版) 備考
by the Subscriber are specified in the Terms and Conditions.	by the Subscriber are specified in the Terms and Conditions.
4.12 Key Escrow and Recovery	4.12 Key Escrow and Recovery
4.12.1 Key Escrow and Recovery Policy and Practices	4.12.1 Key Escrow and Recovery Policy and Practices
The CA does not escrow the Private Keys of Subscribers.	The CA does not escrow the Private Keys of Subscribers.
<b>4.12.2 Session Key Encapsulation and Recovery Policy and Practices</b> Not applicable.	<b>4.12.2 Session Key Encapsulation and Recovery Policy and Practices</b> Not applicable.
5. Facility, Management, and Operational Controls	5. Facility, Management, and Operational Controls
<b>5.1 Physical Security Controls</b> Stipulated in the CPS.	5.1 Physical Security Controls Stipulated in the CPS.
<b>5.2 Procedural Controls</b> Stipulated in the CPS.	5.2 Procedural Controls Stipulated in the CPS.
<b>5.3 Personnel Controls</b> Stipulated in the CPS.	5.3 Personnel Controls Stipulated in the CPS.
5.4 Audit Logging Procedures	5.4 Audit Logging Procedures
5.4.1 Types of Events Recorded	5.4.1 Types of Events Recorded
Stipulated in the CPS.	Stipulated in the CPS.
5.4.2 Frequency of Processing Audit Log	5.4.2 Frequency of Processing Audit Log
Stipulated in the CPS.	Stipulated in the CPS.
5.4.3 Retention Period for Audit Log	5.4.3 Retention Period for Audit Log
Stipulated in the CPS. Audit Logs on the RA system shall be archived for at least seven (7) years.	Stipulated in the CPS. Audit Logs on the RA system shall be archived for at least seven (7) years.
5.4.4 Protection of Audit Log	5.4.4 Protection of Audit Log
Stipulated in the CPS.	Stipulated in the CPS.
5.4.5 Audit Logs Backup Procedure	5.4.5 Audit Logs Backup Procedure
Stipulated in the CPS.	Stipulated in the CPS.
5.4.6 Audit Log Collection System	5.4.6 Audit Log Collection System
Stipulated in the CPS.	Stipulated in the CPS.
5.4.7 Notification to Event-Causing Subject	5.4.7 Notification to Event-Causing Subject
Stipulated in the CPS.	Stipulated in the CPS.
5.4.8 Vulnerability Assessments	5.4.8 Vulnerability Assessments
Stipulated in the CPS.	Stipulated in the CPS.
5.5 Records Archival	5.5 Records Archival
5.5.1 Types of Records Archived	5.5.1 Types of Records Archived
The CA shall archive the following information in addition to the information prescribed in '5.5 Records Archival" of the CPS:	The CA shall archive the following information in addition to the information prescribed in "5.5 Records Archival" of the CPS:

JPRS CA Certificate Policy(変更履歴付)	JPRS CA Certificate Policy (整形版) 備考
this CP; documents prepared under this CP stipulating the business operations of the	<ul> <li>this CP;</li> <li>documents prepared under this CP stipulating the business operations of the Custification A the it is</li> </ul>
Certification Authority; records and audit reports on the results of audits; and information on applications from Subscribers and the histories thereof.	<ul> <li>Certification Authority;</li> <li>records and audit reports on the results of audits; and</li> <li>information on applications from Subscribers and the histories thereof.</li> </ul>
5.5.2 Retention Period for Archive	5.5.2 Retention Period for Archive
	Stipulated in the CPS. The CA shall archive the following information for at least seven (7)
ears: this CP;	years: • this CP;
documents prepared under this CP stipulating the business operations of the	· documents prepared under this CP stipulating the business operations of the
Certification Authority; records and audit reports on the results of audits; and	Certification Authority; • records and audit reports on the results of audits; and
information on applications from Subscribers and the histories thereof.	• information on applications from Subscribers and the histories thereof.
5.5.3 Protection of Archive	5.5.3 Protection of Archive
ipulated in the CPS.	Stipulated in the CPS.
5.5.4 Archive Backup Procedures	5.5.4 Archive Backup Procedures
tipulated in the CPS.	Stipulated in the CPS.
5.5.5 Requirements for Time-Stamping of Records	5.5.5 Requirements for Time-Stamping of Records
cipulated in the CPS.	Stipulated in the CPS.
5.5.6 Archive Collection System	5.5.6 Archive Collection System
cipulated in the CPS.	Stipulated in the CPS.
5.5.7 Procedures to Obtain and Verify Archive Information	5.5.7 Procedures to Obtain and Verify Archive Information
cipulated in the CPS.	Stipulated in the CPS.
norter than the maximum validity period of certificates issued to Subscribers, a new	<b>5.6 Key Changeover</b> 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.
<b>.7 Compromise and Disaster Recovery</b>	<b>5.7 Compromise and Disaster Recovery</b> Stipulated in the CPS.
.8 CA or RA Termination	5.8 CA or RA Termination
	If the CA is required to suspend its operations as a Certification Authority or Registration
uthority, the CA shall notify Subscribers to that effect in advance by any of the means set orth in "9.11 Individual Notices and Communications with Participants."	Authority, the CA shall notify Subscribers to that effect in advance by any of the means set forth in "9.11 Individual Notices and Communications with Participants."
6. Technical Security Controls	6. Technical Security Controls
.1 Key Pair Generation and Installation	6.1 Key Pair Generation and Installation
6.1.1 Key Pair Generation	6.1.1 Key Pair Generation
6.1.1 Generation of Key Pairs" of the CPS stipulates a policy on Private Keys of the CA.	"6.1.1 Generation of Key Pairs" of the CPS stipulates a policy on Private Keys of the CA.
	6.1.2 Private Key Delivery to Subscriber

h Subscriber's Private Ke	y shall be generate	licy(変更履歴付) ed by the Subscriber himself/herself/its		ch Subscriber's Private Ke	ey shall be generat	Policy (整形版) ted by the Subscriber himself/herself/itself.	備考
_		Keys of Subscribers to Subscribers.		-		Keys of Subscribers to Subscribers.	
1.3 Public Key Delive	•			.1.3 Public Key Delive	-		
		Xey to the CA online when applying ays for such delivery shall be encrypted	by his			Key to the CA online when applying for vays for such delivery shall be encrypted by	
I.4 CA' Public Key De	livery to Relyir	ng Parties	6.	.1.4 CA' Public Key D	elivery to Relyi	ng Parties	
ving Parties may obtain Pu	blic Keys of the CA	A by accessing the CA's Repository.	Re	lying Parties may obtain P	ublic Keys of the C	A by accessing the CA's Repository.	
I.5 Key Sizes			6.	.1.5 Key Sizes			
en issuing a TLS server cer wing confirmation need to	-	lies with Baseline Requirements, the		nen issuing a TLS server ce lowing confirmation need t		olies with Baseline Requirements, the	
RSA key pairs the CA SH.	ALL:		For	r RSA key pairs the CA SH	ALL:		
<ul><li>Ensure that the modul</li><li>Ensure that the modul</li></ul>	,	ded, is at least 2048 bits, and; evenly divisible by 8.		<ul><li>Ensure that the module</li><li>Ensure that the module</li></ul>		oded, is at least 2048 bits, and; evenly divisible by 8.	
ECDSA key pairs the CAS Ensure that the key r elliptic curve.		point on the NIST P-256 or NIST P-3		<ul><li>r ECDSA key pairs the CA</li><li>Ensure that the key elliptic curve.</li></ul>		point on the NIST P-256 or NIST P-384	
other algorithms or key siz	es are permitted.		No	other algorithms or key si	zes are permitted.		
I.6 Public Key Param	eters Generatio	on and Quality Checking	6.	.1.6 Public Key Paran	neters Generat	ion and Quality Checking	
ulated in the CPS. No pol Public Key parameters of		n the generation and quality inspection		pulated in the CPS. No po e Public Key parameters of		on the generation and quality inspection of	
I.7 Key Usage Purpo	ses		6.	.1.7 Key Usage Purpo	oses		
following table summariz ed by the CA:	es the usages of ke	eys intended by the CA and by certifica		e following table summari ued by the CA :	zes the usages of k	acys intended by the CA and by certificates	
	Table 6.1 Key Us	age Purposes			Table 6.1 Key Us	sage Purposes	
	the CA	Certificates issued by the CA			the CA	Certificates issued by the CA	
digitalSignature		yes		digitalSignature	—	yes	
nonRepudiation	—	—		nonRepudiation	—		
keyEncipherment	_	yes (except for certificates issued by using ECDSA key)		keyEncipherment	_	yes (except for certificates issued by using ECDSA key)	
dataEncipherment	—			dataEncipherment	—	—	
keyAgreement	—	—		keyAgreement	—	—	
keyCertSign	yes			keyCertSign	yes		
cRLSign	yes	—		cRLSign	yes		
encipherOnly decipherOnly	<u> -</u>	—		encipherOnly			
			1	decipherOnly			

### 24/44

JPRS CA Certificate Policy(変更履歴付)			JPRS CA Certificate Policy (整形版)					
6.3 Other A	3 Other Aspects of Key Pair Management				6.3 Other Aspects of Key Pair Management			
6.3.1 Publi	c key archival			6.3.1 Publ	6.3.1 Public key archival			
stipulated in t	-			Stipulated in	the CPS.			
6.3.2 Certif	ficate operation	al periods and key pair usage perio	ods	6.3.2 Certi	ficate operation	al periods and key pair usage peri	ods	
Subscriber Cer period greater	rtificates issued on	ir and CA certificate of the CA is stipulate or after 1 September 2020 MUST NOT h ubscriber Certificates issued prior to 1 Sep or less.	ave a validity	Subscriber Ce period greate	ertificates issued on	ir and CA certificate of the CA is stipulate or after 1 September 2020 MUST NOT h ubscriber Certificates issued prior to 1 Se or less.	nave a validity	
	this, including frac	day is measured as 86,400 seconds. Any an actional seconds and/or leap seconds, shall			this, including frac	day is measured as 86,400 seconds. Any a ctional seconds and/or leap seconds, shall		
<b>6.4 Activat</b> Stipulated in t				6.4 Activat Stipulated in				
<b>5.5 Compu</b> Stipulated in t	iter Security C be CPS.	ontrols		6.5 Compu Stipulated in	uter Security C the CPS.	ontrols		
6.6 Life Cy Stipulated in t	cle Technical ( he CPS.	Controls		6.6 Life Cycle Technical Controls Stipulated in the CPS.				
<b>5.7 Networ</b> tipulated in t	the CPS.	ntrols		6.7 Network Security Controls Stipulated in the CPS.				
<b>5.8 Time S</b> tipulated in t	• •			<b>6.8 Time Stamping</b> Stipulated in the CPS.				
. Certifi	icate, CRL,	and OCSP Profiles		7. Certificate, CRL, and OCSP Profiles				
The CA SHAL Information, S Generation an The CA SHAL and less than S	Section 6.1.5 - Ke d Quality Checking L generate non-sec 2^159 containing at	cal requirements set forth in Section 2.2 - ey Sizes, and Section 6.1.6 - Public Key of this CP. quential Certificate serial numbers greater t least 64 bits of output from a CSPRNG. form to RFC 5280, the profile of which are in	y Parameters than zero (0)	The CA SHA Information, Generation and The CA SHA and less than	Section 6.1.5 - Ke ad Quality Checking LL generate non-sec 2^159 containing at	cal requirements set forth in Section 2.2 - ey Sizes, and Section 6.1.6 - Public Ke of this CP. quential Certificate serial numbers greater c least 64 bits of output from a CSPRNG. form to RFC 5280, the profile of which are in	y Parameters r than zero (0)	
Domain Valid		ate Profile (applicable to certificates issued or JPRS Organization Validation Authority		Domain Vali		ate Profile (applicable to certificates iss 4 or JPRS Organization Validation Authori		
Basic field		Description of setting	critical	Basic field Version		Description of setting	critical	
Version Serial Numb	ber	Version 3An integral serial number to be assigned by the CA to the certificate	-	Serial Num	ber	Version 3An integral serial number to be assigned by the CA to the certificate	-	
Signature A	lgorithm	sha256 with RSA Encryption	-	Signature A	0	sha256 with RSA Encryption	-	
F	Country	C=JP	-	Issuer	Country	C=JP	-	
	Organization Common Name	O=Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS Domain Validation Authority - G4	-		Organization Common Name	O=Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS Domain Validation Authority - G4	-	
		(2) Organization Validation				(2) Organization Validation		

	JPRS CA Cer	tificate Policy(変更履歴付)		JPRS CA	Certificate Policy(整形版)	備考	
		CN=JPRS Organization Validation			CN=JPRS Organization Validation		
		Authority – G4			Authority – G4		
alidity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-	
v	NotAfter	E.g.) 2009/3/1 00:00:00 GMT		NotAfter	E.g.) 2009/3/1 00:00:00 GMT	-	
ubject	Country	(1) Domain Validation	Subject	Country	(1) Domain Validation	-	
angeet	e o unior y	No description			No description		
		(2) Organization Validation			(2) Organization Validation		
		C=JP as the address of the Subscriber			C=JP as the address of the Subscriber		
		(country)			(country)		
	State or Province	(1) Domain Validation		State or Province	(1) Domain Validation		
	State of Province			State or Province			
		No description			No description		
		(2) Organization Validation			(2) Organization Validation		
		Address of the Subscriber (prefecture			Address of the Subscriber (prefecture		
		name) (mandatory)			name) (mandatory)		
	Locality	(1) Domain Validation		Locality	(1) Domain Validation	-	
		No description			No description		
		(2) Organization Validation			(2) Organization Validation		
		Address of the Subscriber (city, town, or			Address of the Subscriber (city, town, or		
		village name) (mandatory)			village name) (mandatory)		
	Organization	(1) Domain Validation		Organization	(1) Domain Validation	-	
		No description			No description		
		(2) Organization Validation			(2) Organization Validation		
		Name of the Subscriber (mandatory)			Name of the Subscriber (mandatory)		
	Organizational	(1) Domain Validation		Organizational	(1) Domain Validation		
	Unit	No description		Unit	No description		
	Omt	(2) Organization Validation		Omt	(2) Organization Validation		
		Business division name of the					
		Subscriber (optional ).			Subscriber (optional ).		
		However, this item will not be included			However, this item will not be included		
		in certificates issued on or after 18			in certificates issued on or after 18		
		November 2021.			November 2021.		
		• A string comprising symbols only			• A string comprising symbols only		
		or spaces only may not be			or spaces only may not be		
		designated, and any of the			designated, and any of the		
		following strings may not be			following strings may not be		
		included:			included:		
		• any name, company name,			• any name, company name,		
		trade name, or trademark that			trade name, or trademark that		
		is likely to cause others to			is likely to cause others to		
		misconstrue that the relevant			misconstrue that the relevant		
		information is the information			information is the information		
		of any organization other than			of any organization other than		
		the applicant organization;			the applicant organization;		
		any string indicating a legal			any string indicating a legal		
		personality, such as "Co., Ltd";			personality, such as "Co., Ltd";		
		<ul> <li>any string referring to a</li> </ul>			• any string referring to a		
		specific natural person;			specific natural person;		
		• any string indicating an			• any string indicating an		
		address;			address;		
		• any phone number;			• any phone number;		
		• any domain name or IP			• any domain name or IP		
		address; or			address; or		
		• any string meaning "blank",			• any string meaning "blank",		
		"not applicable" or the like			"not applicable" or the like		
		("null", "N/A" or the like)			("null", "N/A" or the like)		
	Common Name	A host name used in the DNS of the		Common Name	A host name used in the DNS of the	-	

JPRS CA Cer	tificate Policy(変更履歴付)			JPRS CA C	Certificate Policy(整形版)	
	server in which the certificate is scheduled to be installed (mandatory) - The value must be encoded as a character-for-character copy of the dNSName entry value from the Subject Alternative Name extension.				server in which the certificate is scheduled to be installed (mandatory) - The value must be encoded as a character-for-character copy of the dNSName entry value from the Subject Alternative Name extension.	
Subject Public Key Info	Specifically. The subject's Public Key (RSA 2048 bits)	-		Subject Public Key Info	Specifically. The subject's Public Key (RSA 2048 bits)	-
Extended field	Description of setting	critical		Extended field	Description of setting	critical
KeyUsage	digitalSignature, keyEncipherment	v		KeyUsage	digitalSignature, keyEncipherment	v
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	<ul> <li>[1] Certificate Policy</li> <li>1.3.6.1.4.1.53827.1.1.4</li> <li>CPS</li> <li>http://jprs.jp/pubcert/info/repository/</li> <li>[2] Certificate Policy</li> <li>(1) Domain Validation</li> <li>2.23.140.1.2.1</li> <li>(2) Organization Validation</li> <li>2.23.140.1.2.2</li> </ul>	n		CertificatePolicies	<ul> <li>[1] Certificate Policy <ol> <li>1.3.6.1.4.1.53827.1.1.4</li> <li>CPS</li> <li>http://jprs.jp/pubcert/info/repository/</li> </ol> </li> <li>[2] Certificate Policy <ol> <li>Domain Validation</li> <li>2.23.140.1.2.1</li> <li>Organization Validation</li> <li>2.23.140.1.2.2</li> </ol> </li> </ul>	n
CRL Distribution Points	<ul> <li>(1) Domain Validation</li> <li>http://repo.pubcert.jprs.jp/sppca/jprs/dv</li> <li>ca_g4/fullcrl.crl</li> <li>(2) Organization Validation</li> <li>http://repo.pubcert.jprs.jp/sppca/jprs/ovc</li> <li>a_g4/fullcrl.crl</li> </ul>	n		CRL Distribution Points	<ul> <li>(1) Domain Validation</li> <li>http://repo.pubcert.jprs.jp/sppca/jprs/dv</li> <li>ca_g4/fullcrl.crl</li> <li>(2) Organization Validation</li> <li>http://repo.pubcert.jprs.jp/sppca/jprs/ovc</li> <li>a_g4/fullcrl.crl</li> </ul>	n
Authority Information Access	<ul> <li>[1] ocsp (1.3.6.1.5.5.7.48.1)</li> <li>(1) Domain Validation</li> <li>http://dv.g4.ocsp.pubcert.jprs.jp</li> <li>(2) Organization Validation</li> <li>http://ov.g4.ocsp.pubcert.jprs.jp</li> <li>[2] ca issuers (1.3.6.1.5.5.7.48.2)</li> <li>(1) Domain Validation</li> <li>http://repo.pubcert.jprs.jp/sppca/jprs/dv</li> <li>ca_g4/JPRS_DVCA_G4_DER.cer</li> <li>(2) Organization Validation</li> <li>http://repo.pubcert.jprs.jp/sppca/jprs/ovc</li> <li>a_g4/JPRS_OVCA_G4_DER.cer</li> </ul>	n		Authority Information Access	<ul> <li>[1] ocsp (1.3.6.1.5.5.7.48.1)</li> <li>(1) Domain Validation</li> <li>http://dv.g4.ocsp.pubcert.jprs.jp</li> <li>(2) Organization Validation</li> <li>http://ov.g4.ocsp.pubcert.jprs.jp</li> <li>[2] ca issuers (1.3.6.1.5.5.7.48.2)</li> <li>(1) Domain Validation</li> <li>http://repo.pubcert.jprs.jp/sppca/jprs/dv</li> <li>ca_g4/JPRS_DVCA_G4_DER.cer</li> <li>(2) Organization Validation</li> <li>http://repo.pubcert.jprs.jp/sppca/jprs/ovc</li> <li>a_g4/JPRS_OVCA_G4_DER.cer</li> </ul>	n
Authority Key Identifier Subject Key Identifier	<ul><li>SHA-1 hash for the issuer's Public Key (160 bits)</li><li>SHA-1 hash for the subject's Public Key</li></ul>	n n		Authority Key Identifier Subject Key Identifier	<ul><li>SHA-1 hash for the issuer's Public Key (160 bits)</li><li>SHA-1 hash for the subject's Public Key</li></ul>	n
Judjeet isey identified	(160 bits)	11		Subject isey identifier	(160 bits)	11
Certificate Transparency Fimestamp 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
SA CA 2024 G1 or JPRS OV RSA			DV	RSA CA 2024 G1 or JPRS OV RS		-
Basic field	Description of setting Version 3	critical		Basic field Version	Description of settingVersion 3	critical
Tomaion	version 5	-				
Version Serial Number Signature Algorithm	An integral serial number to be assigned by the CA to the certificate sha256 with RSA Encryption	-		Serial Number Signature Algorithm	An integral serial number to be assigned by the CA to the certificate sha256 with RSA Encryption	

Basic field		Description of setting	critical
Version		Version 3	-
Serial Num	ber	An integral serial number to be assigned by the CA to the certificate	-
Signature A	lgorithm	sha256 with RSA Encryption	-
Issuer	Country	C=JP	-

JPRS CA C	ertificate Policy(整形版)		
	server in which the certificate is		
	scheduled to be installed (mandatory)		
	- The value must be encoded as a		
	character-for-character copy of the		
	dNSName entry value from the		
	Subject Alternative Name extension.		
	Specifically.		
ubject Public Key Info	The subject's Public Key (RSA 2048	-	
ubject i ublic Rey Illio	bits)		
Extended field	Description of setting	critical	
eyUsage	digitalSignature, keyEncipherment	y	
xtendedKeyUsage	TLS Web Server Authentication	n	
ubject Alt Name	dNSName= name(s) of the server(s)	n	
ertificatePolicies	[1] Certificate Policy	n	
entificater officies	1.3.6.1.4.1.53827.1.1.4	11	
	CPS		
	http://jprs.jp/pubcert/info/repository/		
	[2] Certificate Policy		
	(1) Domain Validation		
	2.23.140.1.2.1		
	(2) Organization Validation		
	2.23.140.1.2.2		
RL Distribution Points	(1) Domain Validation	n	
	http://repo.pubcert.jprs.jp/sppca/jprs/dv	11	
	ca_g4/fullcrl.crl		
	(2) Organization Validation		
	http://repo.pubcert.jprs.jp/sppca/jprs/ovc		
	a_g4/fullcrl.crl		
uthority Information Access	[1] ocsp (1.3.6.1.5.5.7.48.1)	n	
futionity information recess	(1) Domain Validation	11	
	http://dv.g4.ocsp.pubcert.jprs.jp		
	(2) Organization Validation		
	http://ov.g4.ocsp.pubcert.jprs.jp		
	[2] ca issuers (1.3.6.1.5.5.7.48.2)		
	(1) Domain Validation		
	http://repo.pubcert.jprs.jp/sppca/jprs/dv		
	ca_g4/JPRS_DVCA_G4_DER.cer		
	(2) Organization Validation		
	http://repo.pubcert.jprs.jp/sppca/jprs/ovc		
	a_g4/JPRS_OVCA_G4_DER.cer		
Authority Key Identifier	SHA-1 hash for the issuer's Public Key	n	
	(160 bits)		
ubject Key Identifier	SHA-1 hash for the subject's Public Key	n	
Jubjeet Rey Tuentiner	(160 bits)	11	
Certificate Transparency	Value of an OCTET STRING containing	n	
Fimestamp List	the encoded	n	
-			
(1.3.6.1.4.1.11129.2.4.2)	SignedCertificateTimestampList		
	Dusfile (applieshle to service the service the service states in t	h. IDDO	DΨ
	e Profile (applicable to certificates issued	by JPRS	D٧
SA CA 2024 G1 or JPRS OV RSA		··· 1	
	Description of setting	critical	
		-	
Version	Version 3		
Version	An integral serial number to be	-	
Version Serial Number	An integral serial number to be assigned by the CA to the certificate	-	
Basic field Version Serial Number Signature Algorithm Issuer Country	An integral serial number to be	-	

	JPRS CA Cer	tificate Policy(変更履歴付)			JPRS CA C	Certificate Policy(整形版)		備考
	Organization	O=Japan Registry Services Co., Ltd.	-		Organization	O=Japan Registry Services Co., Ltd.	-	
	Common Name	(1) Domain Validation CN= JPRS DV RSA CA 2024 G1	-		Common Name	(1) Domain Validation CN= JPRS DV RSA CA 2024 G1	-	
		<ul> <li>(2) Organization Validation</li> <li>CN= JPRS OV RSA CA 2024 G1</li> </ul>				<ul> <li>(2) Organization Validation</li> <li>CN= JPRS OV RSA CA 2024 G1</li> </ul>		
Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-	Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-	
vallulty	NotAfter	E.g.) 2009/3/1 00:00:00 GMT	-	valuely	NotAfter	E.g.) 2009/3/1 00:00:00 GMT	-	
Subject	Country	(1) Domain Validation	-	Subject	Country	(1) Domain Validation	-	
Subject	country	<ul> <li>No description</li> <li>(2) Organization Validation</li> <li>C=JP as the address of the Subscriber</li> <li>(country)</li> </ul>		Subject	country	<ul> <li>No description</li> <li>(2) Organization Validation</li> <li>C=JP as the address of the Subscriber</li> <li>(country)</li> </ul>		
	State or Province	<ul> <li>(1) Domain Validation</li> <li>No description</li> <li>(2) Organization Validation</li> <li>Address of the Subscriber (prefecture name) (mandatory)</li> </ul>	-		State or Province	<ul> <li>(1) Domain Validation</li> <li>No description</li> <li>(2) Organization Validation</li> <li>Address of the Subscriber (prefecture name) (mandatory)</li> </ul>	-	
	Locality	<ul> <li>(1) Domain Validation</li> <li>(1) No description</li> <li>(2) Organization Validation</li> <li>Address of the Subscriber (city, town, or village name) (mandatory)</li> </ul>	-		Locality	<ul> <li>(1) Domain Validation</li> <li>(1) Domain Validation</li> <li>(2) Organization Validation</li> <li>(2) Address of the Subscriber (city, town, or village name) (mandatory)</li> </ul>	-	
	Organization	<ul> <li>(1) Domain Validation</li> <li>No description</li> <li>(2) Organization Validation</li> <li>Name of the Subscriber (mandatory)</li> </ul>	-		Organization	<ul> <li>(1) Domain Validation</li> <li>No description</li> <li>(2) Organization Validation</li> <li>Name of the Subscriber (mandatory)</li> </ul>	-	
	Common Name	A host name used in the DNS of the server in which the certificate is scheduled to be installed (mandatory) - The value must be encoded as a character-for-character copy of the dNSName entry value from the Subject Alternative Name extension. Specifically.			Common Name	A host name used in the DNS of the server in which the certificate is scheduled to be installed (mandatory) - The value must be encoded as a character-for-character copy of the dNSName entry value from the Subject Alternative Name extension. Specifically.	-	
-	blic Key Info	The subject's Public Key (RSA 4096 bits, RSA3072 bits or RSA 2048 bits)			ublic Key Info	The subject's Public Key (RSA 4096 bits, RSA3072 bits or RSA 2048 bits)	-	
Extended f		Description of setting	critical	Extended		Description of setting	critical	
KeyUsage		digitalSignature, keyEncipherment	У	KeyUsage		digitalSignature, keyEncipherment	У	
ExtendedK		TLS Web Server Authentication TLS Web Client Authentication	n	Extended		TLS Web Server Authentication TLS Web Client Authentication	n	
Subject Alt		dNSName= name(s) of the server(s)	n	Subject Al		dNSName= name(s) of the server(s)	n	
Certificate	Policies	<ul> <li>[1]-Certificate Policy</li> <li>(1) Domain Validation</li> <li>2.23.140.1.2.1</li> <li>(2) Organization Validation</li> <li>2.23.140.1.2.2</li> </ul>	n	Certificate	Policies	Certificate Policy (1) Domain Validation 2.23.140.1.2.1 (2) Organization Validation 2.23.140.1.2.2	n	
		[2] Certificate Policy 1.3.6.1.4.1.53827.1.1.4						プロファイルの変更に伴い削除
CRL Distri	ibution Points	<ul> <li>(1) Domain Validation</li> <li>http://repo.pubcert.jprs.jp/sppca/jprs/dv</li> <li>ca_rsa2024g1/fullcrl.crl</li> <li>(2) Organization Validation</li> <li>http://repo.pubcert.jprs.jp/sppca/jprs/ovc</li> </ul>	n	CRL Distr	ibution Points	<ul> <li>(1) Domain Validation</li> <li>http://repo.pubcert.jprs.jp/sppca/jprs/dv</li> <li>ca_rsa2024g1/fullcrl.crl</li> <li>(2) Organization Validation</li> <li>http://repo.pubcert.jprs.jp/sppca/jprs/ovc</li> </ul>	n	
		a_rsa2024g1/fullcrl.crl				a_rsa2024g1/fullcrl.crl		

JPRS CA Cer	tificate Policy(変更履歴付)	
Authority Information Access	<ul> <li>[1] ocsp (1.3.6.1.5.5.7.48.1)</li> <li>(1) Domain Validation http://dv.rsa2024g1.ocsp.pubcert.jprs.jp</li> <li>(2) Organization Validation http://ov.rsa2024g1.ocsp.pubcert.jprs.jp</li> <li>[2] ca issuers (1.3.6.1.5.5.7.48.2)</li> <li>(1) Domain Validation http://repo.pubcert.jprs.jp/sppca/jprs/dv</li> <li>ca_rsa2024g1/JPRS_DVCA_RSA2024G</li> <li>1_DER.cer</li> <li>(2) Organization Validation http://repo.pubcert.jprs.jp/sppca/jprs/ovc</li> <li>a_rsa2024g1/JPRS_OVCA_RSA2024G1 _DER.cer</li> <li>[2] Ca issuers</li> </ul>	n
Authority Key Identifier	SHA-1 hash for the issuer's Public Key (160 bits)	n
Subject Key Identifier	SHA-1 hash for the subject's Public Key (160 bits)	n
Certificate Transparency Timestamp List (1.3.6.1.4.1.11129.2.4.2)	Value of an OCTET STRING containing the encoded SignedCertificateTimestampList(option al).	n

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

Basic field		Description of setting	critical
Version		Version 3	-
Serial Number		An integral serial number to be assigned by the CA to the certificate	-
Signature Algorithm		ecdsa-with-SHA384	-
Issuer	Country	C=JP	-
	Organization	O=Japan Registry Services Co., Ltd.	-
	Common Name	(1) Domain Validation	-
		CN= JPRS DV ECC CA 2024 G1	
		(2) Organization Validation	
		CN= JPRS OV ECC CA 2024 G1	
Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-
·	NotAfter	E.g.) 2009/3/1 00:00:00 GMT	-
Subject	Country	(1) Domain Validation	-
·	· ·	No description	
		(2) Organization Validation	
		C=JP as the address of the Subscriber	
		(country)	
	State or Province	(1) Domain Validation	-
		No description	
		(2) Organization Validation	
		Address of the Subscriber (prefecture	
		name) (mandatory)	
	Locality	(1) Domain Validation	-
		No description	
		(2) Organization Validation	
		Address of the Subscriber (city, town, or	
		village name) (mandatory)	
	Organization	(1) Domain Validation	-
		No description	
		(2) Organization Validation	

		Certificate Policy(整形版)			備考
Authority I	Information Access	$[1] \operatorname{ocsp} (1.3.6.1.5.5.7.48.1)$	n		
		(1) Domain Validation			
		http://dv.rsa2024g1.ocsp.pubcert.jprs.jp			
		(2) Organization Validation			
		http://ov.rsa2024g1.ocsp.pubcert.jprs.jp			
		[2] ca issuers (1.3.6.1.5.5.7.48.2)			
		(1) Domain Validation			
		http://repo.pubcert.jprs.jp/sppca/jprs/dv			
		ca_rsa2024g1/JPRS_DVCA_RSA2024G 1_DER.cer			
		(2) Organization Validation			
		http://repo.pubcert.jprs.jp/sppca/jprs/ovc			
		a_rsa2024g1/JPRS_OVCA_RSA2024G1			
		DER.cer			
Authority	Key Identifier	SHA-1 hash for the issuer's Public Key	n	-	
1401101109 1		(160 bits)			
Subject Ke	y Identifier	SHA-1 hash for the subject's Public Key	n	1	
	v	(160 bits)			
Certificate	Transparency	Value of an OCTET STRING containing	n	1	
Fimestamp		the encoded			
	.1.11129.2.4.2)	SignedCertificateTimestampList(option			
		al).			
			critical		
CC CA 202 <mark>Basic field</mark> Version		Description of setting           Version 3	critical -		
Basic field		Description of settingVersion 3An integral serial number to be	critical - -		
Basic field Version Serial Num	nber	Description of settingVersion 3An integral serial number to be assigned by the CA to the certificate	critical - -		
Basic field Version Serial Num Signature A	nber Algorithm	Description of settingVersion 3An integral serial number to be assigned by the CA to the certificateecdsa-with-SHA384	critical - -		
Basic field Version Serial Num	nber Algorithm Country	Description of settingVersion 3An integral serial number to be assigned by the CA to the certificateecdsa-with-SHA384C=JP	- - - -		
Basic field Version Serial Num Signature A	nber Algorithm Country Organization	Description of settingVersion 3An integral serial number to be assigned by the CA to the certificateecdsa-with-SHA384C=JPO=Japan Registry Services Co., Ltd.	critical		
Basic field Version Serial Num Signature A	nber Algorithm Country	Description of settingVersion 3An integral serial number to be assigned by the CA to the certificateecdsa-with-SHA384C=JPO=Japan Registry Services Co., Ltd.(1) Domain Validation	- - - -		
Basic field Version Serial Num Signature A	nber Algorithm Country Organization	Description of settingVersion 3An integral serial number to be assigned by the CA to the certificateecdsa-with-SHA384C=JPO=Japan Registry Services Co., Ltd.(1) Domain Validation CN= JPRS DV ECC CA 2024 G1	- - - -		
Basic field Version Serial Num Signature A	nber Algorithm Country Organization	Description of settingVersion 3An integral serial number to be assigned by the CA to the certificateecdsa-with-SHA384C=JPO=Japan Registry Services Co., Ltd.(1) Domain ValidationCN= JPRS DV ECC CA 2024 G1(2) Organization Validation	- - - -		
Basic field Version Serial Num Signature A	nber Algorithm Country Organization Common Name	Description of settingVersion 3An integral serial number to be assigned by the CA to the certificateecdsa-with-SHA384C=JPO=Japan Registry Services Co., Ltd.(1) Domain Validation CN= JPRS DV ECC CA 2024 G1(2) Organization Validation CN= JPRS OV ECC CA 2024 G1	- - - -		
Basic field Version Serial Num Signature A	nber Algorithm Country Organization Common Name NotBefore	Description of settingVersion 3An integral serial number to be assigned by the CA to the certificateecdsa-with-SHA384C=JPO=Japan Registry Services Co., Ltd.(1) Domain Validation CN= JPRS DV ECC CA 2024 G1(2) Organization Validation CN= JPRS OV ECC CA 2024 G1(2) Organization Validation CN= JPRS OV ECC CA 2024 G1E.g.) 2008/3/1 00:00:00 GMT	- - - - -		
Basic field Version Serial Num Signature A Issuer Validity	nber Algorithm Country Organization Common Name NotBefore NotAfter	Description of settingVersion 3An integral serial number to be assigned by the CA to the certificateecdsa-with-SHA384C=JPO=Japan Registry Services Co., Ltd.(1) Domain Validation CN= JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1E.g.) 2008/3/1 00:00:00 GMTE.g.) 2009/3/1 00:00:00 GMT	- - - - -		
Basic field Version Serial Num Signature A	nber Algorithm Country Organization Common Name NotBefore	Description of settingVersion 3An integral serial number to be assigned by the CA to the certificateecdsa-with-SHA384C=JPO=Japan Registry Services Co., Ltd.(1) Domain ValidationCN= JPRS DV ECC CA 2024 G1(2) Organization ValidationCN= JPRS OV ECC CA 2024 G1E.g.) 2008/3/1 00:00:00 GMTE.g.) 2009/3/1 00:00:00 GMT(1) Domain Validation	- - - - -		
Basic field Version Serial Num Signature A Issuer Validity	nber Algorithm Country Organization Common Name NotBefore NotAfter	Description of settingVersion 3An integral serial number to be assigned by the CA to the certificateecdsa-with-SHA384C=JPO=Japan Registry Services Co., Ltd.(1) Domain Validation CN= JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1E.g.) 2008/3/1 00:00:00 GMTE.g.) 2009/3/1 00:00:00 GMT	- - - - -		
Basic field Version Serial Num Signature A Issuer Validity	nber Algorithm Country Organization Common Name NotBefore NotAfter	Description of settingVersion 3An integral serial number to be assigned by the CA to the certificateecdsa-with-SHA384C=JPO=Japan Registry Services Co., Ltd.(1) Domain Validation CN= JPRS DV ECC CA 2024 G1(2) Organization Validation CN= JPRS OV ECC CA 2024 G1E.g.) 2008/3/1 00:00:00 GMTE.g.) 2009/3/1 00:00:00 GMT(1) Domain Validation No description	- - - - -		
Basic field Version Serial Num Signature A Issuer Validity	nber Algorithm Country Organization Common Name NotBefore NotAfter	Description of settingVersion 3An integral serial number to be assigned by the CA to the certificateecdsa-with-SHA384C=JPO=Japan Registry Services Co., Ltd.(1) Domain ValidationCN= JPRS DV ECC CA 2024 G1(2) Organization ValidationCN= JPRS OV ECC CA 2024 G1E.g.) 2008/3/1 00:00:00 GMTE.g.) 2009/3/1 00:00:00 GMT(1) Domain ValidationNo description(2) Organization ValidationC=JP as the address of the Subscriber(country)	- - - - -		
Basic field Version Serial Num Signature A Issuer Validity	nber Algorithm Country Organization Common Name NotBefore NotAfter	Description of settingVersion 3An integral serial number to be assigned by the CA to the certificateecdsa-with-SHA384C=JPO=Japan Registry Services Co., Ltd.(1) Domain Validation CN= JPRS DV ECC CA 2024 G1(2) Organization Validation CN= JPRS OV ECC CA 2024 G1E.g.) 2008/3/1 00:00:00 GMTE.g.) 2009/3/1 00:00:00 GMT(1) Domain Validation No description (2) Organization Validation C=JP as the address of the Subscriber (country)(1) Domain Validation	- - - - -		
Basic field Version Serial Num Signature A Issuer Validity	nber Algorithm Country Organization Common Name NotBefore NotAfter Country	Description of settingVersion 3An integral serial number to be assigned by the CA to the certificateecdsa-with-SHA384C=JPO=Japan Registry Services Co., Ltd.(1) Domain Validation CN= JPRS DV ECC CA 2024 G1(2) Organization Validation CN= JPRS OV ECC CA 2024 G1E.g.) 2008/3/1 00:00:00 GMTE.g.) 2009/3/1 00:00:00 GMT(1) Domain Validation No description (2) Organization ValidationC=JP as the address of the Subscriber (country)(1) Domain Validation No descriptionC=JP as the address of the Subscriber (country)	- - - - -		
Basic field Version Serial Num Signature A Issuer Validity	nber Algorithm Country Organization Common Name NotBefore NotAfter Country	Description of settingVersion 3An integral serial number to be assigned by the CA to the certificateecdsa-with-SHA384C=JPO=Japan Registry Services Co., Ltd.(1) Domain Validation CN= JPRS DV ECC CA 2024 G1(2) Organization Validation CN= JPRS OV ECC CA 2024 G1E.g.) 2008/3/1 00:00:00 GMTE.g.) 2009/3/1 00:00:00 GMT(1) Domain Validation No description (2) Organization ValidationC=JP as the address of the Subscriber (country)(1) Domain Validation No description (2) Organization Validation	- - - - -		
Basic field Version Serial Num Signature A Issuer Validity	nber Algorithm Country Organization Common Name NotBefore NotAfter Country	Description of settingVersion 3An integral serial number to be assigned by the CA to the certificateecdsa-with-SHA384C=JPO=Japan Registry Services Co., Ltd.(1) Domain ValidationCN= JPRS DV ECC CA 2024 G1(2) Organization ValidationCN= JPRS OV ECC CA 2024 G1E.g.) 2008/3/1 00:00:00 GMTE.g.) 2009/3/1 00:00:00 GMT(1) Domain ValidationNo description(2) Organization ValidationC=JP as the address of the Subscriber(country)(1) Domain ValidationNo description(2) Organization ValidationAddress of the Subscriber (prefecture	- - - - -		
Basic field Version Serial Num Signature A Issuer Validity	Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province	Description of settingVersion 3An integral serial number to be assigned by the CA to the certificateecdsa-with-SHA384C=JPO=Japan Registry Services Co., Ltd.(1) Domain ValidationCN= JPRS DV ECC CA 2024 G1(2) Organization ValidationCN= JPRS OV ECC CA 2024 G1E.g.) 2008/3/1 00:00:00 GMTE.g.) 2009/3/1 00:00:00 GMT(1) Domain ValidationNo description(2) Organization ValidationC=JP as the address of the Subscriber (country)(1) Domain ValidationNo description(2) Organization ValidationMathematical Context of the Subscriber (prefecturename) (mandatory)	- - - - -		
Basic field Version Serial Num Signature A Issuer Validity	nber Algorithm Country Organization Common Name NotBefore NotAfter Country	Description of settingVersion 3An integral serial number to be assigned by the CA to the certificateecdsa-with-SHA384C=JPO=Japan Registry Services Co., Ltd.(1) Domain Validation CN= JPRS DV ECC CA 2024 G1(2) Organization Validation CN= JPRS OV ECC CA 2024 G1E.g.) 2008/3/1 00:00:00 GMTE.g.) 2009/3/1 00:00:00 GMT(1) Domain Validation No description (2) Organization Validation C=JP as the address of the Subscriber (country)(1) Domain Validation No description (2) Organization Validation No description (2) Organization Validation No description (1) Domain Validation (2) Organization Validation (1) Domain Validation (2) Organization Validation (1) Domain Validation (2) Organization Validation (2) Organization Validation (1) Domain Validation (2) Organization Validation (1) Domain Validation (2) Organization Validation (3) Organization Validation (4) Domain Validation	- - - - -		
Basic field Version Serial Num Signature A Issuer Validity	Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province	Description of settingVersion 3An integral serial number to be assigned by the CA to the certificateecdsa-with-SHA384C=JPO=Japan Registry Services Co., Ltd.(1) Domain Validation CN= JPRS DV ECC CA 2024 G1(2) Organization Validation CN= JPRS OV ECC CA 2024 G1E.g.) 2008/3/1 00:00:00 GMTE.g.) 2009/3/1 00:00:00 GMT(1) Domain Validation No description (2) Organization ValidationC=JP as the address of the Subscriber (country)(1) Domain Validation No description (2) Organization Validation No description (2) Organization Validation No description (1) Domain Validation No description (2) Organization Validation No description (1) Domain Validation No description (2) Organization Validation No description (1) Domain Validation No description (2) Organization Validation No description (2) Organization Validation No description (1) Domain Validation No description (2) Organization Validation No description (2) Organization Validation No description No description	- - - - -		
Basic field Version Serial Num Signature A Issuer Validity	Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province	Description of settingVersion 3An integral serial number to be assigned by the CA to the certificateecdsa-with-SHA384C=JPO=Japan Registry Services Co., Ltd.(1) Domain ValidationCN= JPRS DV ECC CA 2024 G1(2) Organization ValidationCN= JPRS OV ECC CA 2024 G1E.g.) 2008/3/1 00:00:00 GMTE.g.) 2009/3/1 00:00:00 GMT(1) Domain ValidationNo description(2) Organization ValidationC=JP as the address of the Subscriber (country)(1) Domain ValidationNo description(2) Organization ValidationNo description(2) Organization ValidationNo description(1) Domain ValidationNo description(2) Organization Validation	- - - - -		
Basic field Version Serial Num Signature A Issuer Validity	Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province	Description of settingVersion 3An integral serial number to be assigned by the CA to the certificateecdsa-with-SHA384C=JPO=Japan Registry Services Co., Ltd.(1) Domain ValidationCN= JPRS DV ECC CA 2024 G1(2) Organization ValidationCN= JPRS OV ECC CA 2024 G1E.g.) 2008/3/1 00:00:00 GMTE.g.) 2009/3/1 00:00:00 GMT(1) Domain ValidationNo description(2) Organization ValidationC=JP as the address of the Subscriber (country)(1) Domain ValidationNo description(2) Organization ValidationAddress of the Subscriber (prefecture name) (mandatory)(1) Domain ValidationNo description(2) Organization ValidationAddress of the Subscriber (city, town, or	- - - - -		
Basic field Version Serial Num Signature A Issuer Validity	Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality	Description of settingVersion 3An integral serial number to be assigned by the CA to the certificateecdsa-with-SHA384C=JPO=Japan Registry Services Co., Ltd.(1) Domain ValidationCN= JPRS DV ECC CA 2024 G1(2) Organization ValidationCN= JPRS OV ECC CA 2024 G1E.g.) 2008/3/1 00:00:00 GMTE.g.) 2009/3/1 00:00:00 GMT(1) Domain ValidationNo description(2) Organization ValidationC=JP as the address of the Subscriber (country)(1) Domain ValidationNo description(2) Organization ValidationAddress of the Subscriber (prefecture name) (mandatory)(1) Domain ValidationNo description(2) Organization ValidationAddress of the Subscriber (city, town, or village name) (mandatory)	- - - - -		
Basic field Version Serial Num Signature A Issuer Validity	Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province	Description of settingVersion 3An integral serial number to be assigned by the CA to the certificateecdsa-with-SHA384C=JPO=Japan Registry Services Co., Ltd.(1) Domain ValidationCN= JPRS DV ECC CA 2024 G1(2) Organization ValidationCN= JPRS OV ECC CA 2024 G1E.g.) 2008/3/1 00:00:00 GMTE.g.) 2009/3/1 00:00:00 GMT(1) Domain ValidationNo description(2) Organization ValidationC=JP as the address of the Subscriber (country)(1) Domain ValidationNo description(2) Organization ValidationAddress of the Subscriber (prefecture name) (mandatory)(1) Domain ValidationNo description(2) Organization ValidationAddress of the Subscriber (city, town, or	- - - - -		

	TDPS CA C	artificato Poliar (軟形版)			
A . 1		Certificate Policy (整形版)			備考
Authority	Information Access	$[1] \operatorname{ocsp} (1.3.6.1.5.5.7.48.1)$	n		
		(1) Domain Validation			
		http://dv.rsa2024g1.ocsp.pubcert.jprs.jp			
		(2) Organization Validation			
		http://ov.rsa2024g1.ocsp.pubcert.jprs.jp			
		[2] ca issuers (1.3.6.1.5.5.7.48.2)			
		(1) Domain Validation			
		http://repo.pubcert.jprs.jp/sppca/jprs/dv			
		ca_rsa2024g1/JPRS_DVCA_RSA2024G			
		1_DER.cer			
		$(\overline{2})$ Organization Validation			
		http://repo.pubcert.jprs.jp/sppca/jprs/ovc			
		a_rsa2024g1/JPRS_OVCA_RSA2024G1			
		DER.cer			
Authority	Key Identifier	SHA-1 hash for the issuer's Public Key	n		
autionity	Rey Identifier	(160 bits)	n		
Subject Ke	y Identifier	SHA-1 hash for the subject's Public Key	n		
	J	(160 bits)			
Certificate	Transparency	Value of an OCTET STRING containing	n	1	
Fimestam		the encoded			
1	(.1.11129.2.4.2)	SignedCertificateTimestampList(option			
(	,	al).			
			1		
able 7.1-3	Subscriber Certificat	e Profile (applicable to certificates issued	by JPRS	DV	
	24 G1 or JPRS OV EC		U		
			critical	1	
		Description of setting	Unitat		
Basic field		Description of setting Version 3	-		
Basic field Version	nhor	Version 3	-		
<mark>Basic field</mark> Version	nber	Version 3 An integral serial number to be	- -		
Basic field Version Serial Nun		Version 3 An integral serial number to be assigned by the CA to the certificate			
Basic field Version Serial Nun Signature J	Algorithm	Version 3 An integral serial number to be assigned by the CA to the certificate ecdsa-with-SHA384	- - -		
Basic field Version Serial Nun Signature J	Algorithm Country	Version 3 An integral serial number to be assigned by the CA to the certificate ecdsa-with-SHA384 C=JP			
Basic field Version Serial Nun Signature J	Algorithm Country Organization	Version 3 An integral serial number to be assigned by the CA to the certificate ecdsa-with-SHA384 C=JP O=Japan Registry Services Co., Ltd.			
<mark>Basic field</mark> Version Serial Nun	Algorithm Country	Version 3 An integral serial number to be assigned by the CA to the certificate ecdsa-with-SHA384 C=JP O=Japan Registry Services Co., Ltd. (1) Domain Validation			
Basic field Version Serial Nun Signature J	Algorithm Country Organization	Version 3 An integral serial number to be assigned by the CA to the certificate ecdsa-with-SHA384 C=JP O=Japan Registry Services Co., Ltd. (1) Domain Validation CN= JPRS DV ECC CA 2024 G1	- - - - -		
Basic field Version Serial Nun Signature A	Algorithm Country Organization	Version 3 An integral serial number to be assigned by the CA to the certificate ecdsa-with-SHA384 C=JP O=Japan Registry Services Co., Ltd. (1) Domain Validation CN= JPRS DV ECC CA 2024 G1 (2) Organization Validation	- - - - -		
Basic field Version Serial Nun Signature A ssuer	Algorithm Country Organization Common Name	Version 3 An integral serial number to be assigned by the CA to the certificate ecdsa-with-SHA384 C=JP O=Japan Registry Services Co., Ltd. (1) Domain Validation CN= JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1	- - - - -		
Basic field Version Serial Nun Signature A ssuer	Algorithm Country Organization	Version 3 An integral serial number to be assigned by the CA to the certificate ecdsa-with-SHA384 C=JP O=Japan Registry Services Co., Ltd. (1) Domain Validation CN= JPRS DV ECC CA 2024 G1 (2) Organization Validation			
Basic field Version Serial Nun Signature A ssuer	Algorithm Country Organization Common Name	Version 3 An integral serial number to be assigned by the CA to the certificate ecdsa-with-SHA384 C=JP O=Japan Registry Services Co., Ltd. (1) Domain Validation CN= JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1			
Basic field Version Serial Nun Signature 2 Signature 2 Signature 2 Validity	Algorithm Country Organization Common Name NotBefore	Version 3 An integral serial number to be assigned by the CA to the certificate ecdsa-with-SHA384 C=JP O=Japan Registry Services Co., Ltd. (1) Domain Validation CN= JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT	- - - - - - - - - - - - - -		
Basic field Version Serial Nun Signature 2 Signature 2 Sisuer	Algorithm Country Organization Common Name NotBefore NotAfter	Version 3 An integral serial number to be assigned by the CA to the certificate ecdsa-with-SHA384 C=JP O=Japan Registry Services Co., Ltd. (1) Domain Validation CN= JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2009/3/1 00:00:00 GMT (1) Domain Validation			
Basic field Version Serial Nun Signature J	Algorithm Country Organization Common Name NotBefore NotAfter	Version 3 An integral serial number to be assigned by the CA to the certificate ecdsa-with-SHA384 C=JP O=Japan Registry Services Co., Ltd. (1) Domain Validation CN= JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2009/3/1 00:00:00 GMT (1) Domain Validation No description	- - - - - - - - - - -		
Basic field Version Serial Nun Signature 2 Signature 2 Signature 2 Validity	Algorithm Country Organization Common Name NotBefore NotAfter	Version 3 An integral serial number to be assigned by the CA to the certificate ecdsa-with-SHA384 C=JP O=Japan Registry Services Co., Ltd. (1) Domain Validation CN= JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2009/3/1 00:00:00 GMT (1) Domain Validation No description (2) Organization Validation	- - - - - - - -		
Basic field Version Serial Nun Signature A ssuer Validity	Algorithm Country Organization Common Name NotBefore NotAfter	Version 3 An integral serial number to be assigned by the CA to the certificate ecdsa-with-SHA384 C=JP O=Japan Registry Services Co., Ltd. (1) Domain Validation CN= JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2009/3/1 00:00:00 GMT (1) Domain Validation No description (2) Organization Validation C=JP as the address of the Subscriber	- - - - - - -		
Basic field Version Serial Nun Signature 2 Signature 2 Signature 2 Validity	Algorithm Country Organization Common Name NotBefore NotAfter Country	Version 3 An integral serial number to be assigned by the CA to the certificate ecdsa-with-SHA384 C=JP O=Japan Registry Services Co., Ltd. (1) Domain Validation CN= JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2009/3/1 00:00:00 GMT (1) Domain Validation No description (2) Organization Validation C=JP as the address of the Subscriber (country)			
Basic field Version Serial Nun Signature 2 Signature 2 Signature 2 Validity	Algorithm Country Organization Common Name NotBefore NotAfter	Version 3 An integral serial number to be assigned by the CA to the certificate ecdsa-with-SHA384 C=JP O=Japan Registry Services Co., Ltd. (1) Domain Validation CN= JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2009/3/1 00:00:00 GMT (1) Domain Validation No description (2) Organization Validation C=JP as the address of the Subscriber (country) (1) Domain Validation			
Basic field Version Serial Nun Signature 2 Signature 2 Signature 2 Validity	Algorithm Country Organization Common Name NotBefore NotAfter Country	Version 3 An integral serial number to be assigned by the CA to the certificate ecdsa-with-SHA384 C=JP O=Japan Registry Services Co., Ltd. (1) Domain Validation CN= JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2009/3/1 00:00:00 GMT (1) Domain Validation No description (2) Organization Validation C=JP as the address of the Subscriber (country) (1) Domain Validation No description			
Basic field Version Serial Nun Signature A ssuer Validity	Algorithm Country Organization Common Name NotBefore NotAfter Country	Version 3An integral serial number to be assigned by the CA to the certificateecdsa-with-SHA384C=JPO=Japan Registry Services Co., Ltd.(1) Domain Validation CN= JPRS DV ECC CA 2024 G1(2) Organization Validation CN= JPRS OV ECC CA 2024 G1E.g.) 2008/3/1 00:00:00 GMTE.g.) 2009/3/1 00:00:00 GMT(1) Domain Validation No description (2) Organization Validation C=JP as the address of the Subscriber (country)(1) Domain Validation No description(2) Organization Validation (2) Organization Validation No description(2) Organization Validation (2) Organization Validation (2) Organization Validation	- - - - - - - - - - -		
Basic field Version Serial Nun Signature A ssuer Validity	Algorithm Country Organization Common Name NotBefore NotAfter Country	Version 3An integral serial number to be assigned by the CA to the certificateecdsa-with-SHA384C=JPO=Japan Registry Services Co., Ltd.(1) Domain Validation CN= JPRS DV ECC CA 2024 G1(2) Organization Validation CN= JPRS OV ECC CA 2024 G1E.g.) 2008/3/1 00:00:00 GMTE.g.) 2009/3/1 00:00:00 GMT(1) Domain Validation No description (2) Organization Validation C=JP as the address of the Subscriber (country)(1) Domain Validation No description (2) Organization Validation No description (2) Organization Validation Address of the Subscriber (prefecture	- - - - - - - - - -		
Basic field Version Serial Nun Signature A ssuer Validity	Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province	Version 3 An integral serial number to be assigned by the CA to the certificate ecdsa-with-SHA384 C=JP O=Japan Registry Services Co., Ltd. (1) Domain Validation CN= JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2009/3/1 00:00:00 GMT (1) Domain Validation No description (2) Organization Validation C=JP as the address of the Subscriber (country) (1) Domain Validation No description (2) Organization Validation No description (2) Organization Validation Address of the Subscriber (prefecture name) (mandatory)	- - - - - - - - -		
Basic field Version Serial Nun Signature A ssuer Validity	Algorithm Country Organization Common Name NotBefore NotAfter Country	Version 3 An integral serial number to be assigned by the CA to the certificate ecdsa-with-SHA384 C=JP O=Japan Registry Services Co., Ltd. (1) Domain Validation CN= JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2009/3/1 00:00:00 GMT (1) Domain Validation No description (2) Organization Validation C=JP as the address of the Subscriber (country) (1) Domain Validation No description (2) Organization Validation No description (2) Organization Validation Address of the Subscriber (prefecture name) (mandatory) (1) Domain Validation			
Basic field Version Serial Nun Signature A ssuer Validity	Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province	Version 3 An integral serial number to be assigned by the CA to the certificate ecdsa-with-SHA384 C=JP O=Japan Registry Services Co., Ltd. (1) Domain Validation CN= JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2009/3/1 00:00:00 GMT (1) Domain Validation No description (2) Organization Validation C=JP as the address of the Subscriber (country) (1) Domain Validation No description (2) Organization Validation Address of the Subscriber (prefecture name) (mandatory) (1) Domain Validation No description			
Basic field Version Serial Nun Signature 2 Signature 2 Sisuer	Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province	Version 3An integral serial number to be assigned by the CA to the certificateecdsa-with-SHA384C=JPO=Japan Registry Services Co., Ltd.(1) Domain Validation CN= JPRS DV ECC CA 2024 G1(2) Organization Validation CN= JPRS OV ECC CA 2024 G1E.g.) 2008/3/1 00:00:00 GMTE.g.) 2009/3/1 00:00:00 GMT(1) Domain Validation No description (2) Organization Validation C=JP as the address of the Subscriber (country)(1) Domain Validation No description (2) Organization Validation Address of the Subscriber (prefecture name) (mandatory)(1) Domain Validation No description (2) Organization Validation Address of the Subscriber (prefecture name) (mandatory)(1) Domain Validation No description (2) Organization Validation No description (2) Organization Validation			
Basic field Version Serial Nun Signature 2 Signature 2 Sisuer	Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province	Version 3An integral serial number to be assigned by the CA to the certificateecdsa-with-SHA384C=JPO=Japan Registry Services Co., Ltd.(1) Domain Validation CN= JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1E.g.) 2008/3/1 00:00:00 GMTE.g.) 2009/3/1 00:00:00 GMT(1) Domain Validation No description (2) Organization Validation C=JP as the address of the Subscriber (country)(1) Domain Validation No description (2) Organization Validation No description (2) Organization Validation No description (2) Organization Validation Address of the Subscriber (prefecture name) (mandatory)(1) Domain Validation No description (2) Organization Validation Address of the Subscriber (prefecture name) (mandatory)(1) Domain Validation Address of the Subscriber (city, town, or			
Basic field Version Serial Nun Signature 2 Signature 2 Sisuer	Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province	Version 3 An integral serial number to be assigned by the CA to the certificate ecdsa-with-SHA384 C=JP O=Japan Registry Services Co., Ltd. (1) Domain Validation CN= JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2009/3/1 00:00:00 GMT (1) Domain Validation No description (2) Organization Validation C=JP as the address of the Subscriber (country) (1) Domain Validation No description (2) Organization Validation Address of the Subscriber (prefecture name) (mandatory) (1) Domain Validation No description (2) Organization Validation Address of the Subscriber (prefecture name) (mandatory) (1) Domain Validation No description (2) Organization Validation No description (2) Organization Validation	- - - - - - - - - -		
Basic field Version Serial Nun Signature 2 Signature 2 Sisuer	Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province	Version 3An integral serial number to be assigned by the CA to the certificateecdsa-with-SHA384C=JPO=Japan Registry Services Co., Ltd.(1) Domain Validation CN= JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1E.g.) 2008/3/1 00:00:00 GMTE.g.) 2009/3/1 00:00:00 GMT(1) Domain Validation No description (2) Organization Validation C=JP as the address of the Subscriber (country)(1) Domain Validation No description (2) Organization Validation No description (2) Organization Validation No description (2) Organization Validation Address of the Subscriber (prefecture name) (mandatory)(1) Domain Validation No description (2) Organization Validation Address of the Subscriber (prefecture name) (mandatory)(1) Domain Validation Address of the Subscriber (city, town, or	- - - - - - - - - - - -		
Basic field Version Serial Nun Signature 2 Signature 2 Signature 2 Validity	Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality	Version 3 An integral serial number to be assigned by the CA to the certificate ecdsa-with-SHA384 C=JP O=Japan Registry Services Co., Ltd. (1) Domain Validation CN= JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2009/3/1 00:00:00 GMT (1) Domain Validation No description (2) Organization Validation C=JP as the address of the Subscriber (country) (1) Domain Validation No description (2) Organization Validation Address of the Subscriber (prefecture name) (mandatory) (1) Domain Validation No description (2) Organization Validation Address of the Subscriber (prefecture name) (mandatory) (1) Domain Validation No description (2) Organization Validation No description (2) Organization Validation	- - - - - - - - - - - - -		

JPRS CA Ce	rtificate Policy(変更履歴付)		JPRS CA	Certificate Policy(整形版)		備考
	Name of the Subscriber (mandatory)			Name of the Subscriber (mandatory)		
Common Name	A host name used in the DNS of the	- 1	Common Name	A host name used in the DNS of the	-	
	server in which the certificate is			server in which the certificate is		
	scheduled to be installed (mandatory)			scheduled to be installed (mandatory)		
	- The value must be encoded as a			- The value must be encoded as a		
	character-for-character copy of the			character-for-character copy of the		
	dNSName entry value from the			dNSName entry value from the		
	Subject Alternative Name extension.			Subject Alternative Name extension.		
	Specifically.			Specifically.		
ubject Public Key Info	The subject's Public Key (RSA 4096	-	Subject Public Key Info	The subject's Public Key (RSA 4096	-	
	bits, RSA 3072 bits, RSA 2048 bits, P-			bits, RSA 3072 bits, RSA 2048 bits, P-		
	256 or P-384)			256 or P-384)		
xtended field	Description of setting	critical	Extended field	Description of setting	critical	
eyUsage	digitalSignature,	у	KeyUsage	digitalSignature,	у	
	keyEncipherment (except for			keyEncipherment (except for	-	
	certificates issued by using ECDSA key)			certificates issued by using ECDSA key)		
rtendedKeyUsage	TLS Web Server Authentication	n	ExtendedKeyUsage	TLS Web Server Authentication	n	
	TLS Web Client Authentication			TLS Web Client Authentication		
bject Alt Name	dNSName= name(s) of the server(s)	n	Subject Alt Name	dNSName= name(s) of the server(s)	n	
ertificatePolicies	[1] Certificate Policy	n	CertificatePolicies	Certificate Policy	n	
	(1) Domain Validation			(1) Domain Validation		
	2.23.140.1.2.1			2.23.140.1.2.1		
	(2) Organization Validation			(2) Organization Validation		
	2.23.140.1.2.2			2.23.140.1.2.2		
	[2] Certificate Policy					
	$\frac{1.3.6.1.4.1.53827.1.1.4}{1.3.6.1.4}$					プロファイルの変更に伴い肖
RL Distribution Points	(1) Domain Validation	n	CRL Distribution Points	(1) Domain Validation	n	
	http://repo.pubcert.jprs.jp/sppca/jprs/dv			http://repo.pubcert.jprs.jp/sppca/jprs/dv		
	ca_ecc2024g1/fullcrl.crl			ca_ecc2024g1/fullcrl.crl		
	(2) Organization Validation			(2) Organization Validation		
	http://repo.pubcert.jprs.jp/sppca/jprs/ovc			http://repo.pubcert.jprs.jp/sppca/jprs/ovc		
	a_ecc2024g1/fullcrl.crl			a_ecc2024g1/fullcrl.crl		
uthority Information Access	$[1] \operatorname{ocsp} (1.3.6.1.5.5.7.48.1)$	n	Authority Information Access	$[1] \operatorname{ocsp} (1.3.6.1.5.5.7.48.1)$	n	
	(1) Domain Validation			(1) Domain Validation		
	http://dv.ecc2024g1.ocsp.pubcert.jprs.jp			http://dv.ecc2024g1.ocsp.pubcert.jprs.jp		
	(2) Organization Validation			(2) Organization Validation		
	http://ov.ecc2024g1.ocsp.pubcert.jprs.jp			http://ov.ecc2024g1.ocsp.pubcert.jprs.jp		
	[2] ca issuers (1.3.6.1.5.5.7.48.2)			[2] ca issuers (1.3.6.1.5.5.7.48.2)		
	(1) Domain Validation			(1) Domain Validation		
	http://repo.pubcert.jprs.jp/sppca/jprs/dv			http://repo.pubcert.jprs.jp/sppca/jprs/dv		
	ca_ecc2024g1/JPRSDVCA_ECC2024G1			ca_ecc2024g1/JPRSDVCA_ECC2024G1		
	_DER.cer			_DER.cer		
	(2) Organization Validation			(2) Organization Validation		
	http://repo.pubcert.jprs.jp/sppca/jprs/ovc			http://repo.pubcert.jprs.jp/sppca/jprs/ovc		
	a_ecc2024g1/JPRS_OVCA_ECC2024G1			a_ecc2024g1/JPRS_OVCA_ECC2024G1		
	_DER.cer			_DER.cer		
uthority Key Identifier	SHA-1 hash for the issuer's Public Key	n	Authority Key Identifier	SHA-1 hash for the issuer's Public Key	n	
	(160 bits)			(160 bits)		
ubject Key Identifier	SHA-1 hash for the subject's Public Key	n	Subject Key Identifier	SHA-1 hash for the subject's Public Key	n	
	(160 bits)			(160 bits)		
ertificate Transparency	Value of an OCTET STRING containing	n	Certificate Transparency	Value of an OCTET STRING containing	n	
imestamp List	the encoded		Timestamp List	the encoded		
(1.3.6.1.4.1.11129.2.4.2)	SignedCertificateTimestampLi st (optional)		(1.3.6.1.4.1.11129.2.4.2)	SignedCertificateTimestampLi		
				st (optional)		

Basic field		Description of setting	critical
Version		Version 3	-
Serial Number Signature Algorithm		An integral serial number to be assigned by the CA to the certificate	-
		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	<ul> <li>(1) Organization Validation</li> <li>CN=JPRS Organization Validation</li> <li>Authority - G4</li> <li>(2) Domain Validation</li> <li>CN=JPRS Domain Validation Authority</li> <li>- G4</li> </ul>	-
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 Ke	ey Identifier	SHA-1 hash for the subject's Public Key (160 bits)	n
KeyUsage		Certificate Signing Off-line CRL Signing CRL Signing (06)	У
Certificate	Policies	Certificate Policy 1.2.392.200091.100.901.4 CPS http://repository.secomtrust.net /SC-Root2/	N
Basic Con	straints	Subject Type=CA Path Length Constraint=0	У
Extended	KeyUsage	TLS Web Server Authentication	n
CRL Distr	ibution Points	http://repository.secomtrust.net/SC- Root2/SCRoot2CRL.crl	n
Authority	Information Access	<ul> <li>[1] ocsp (1.3.6.1.5.5.7.48.1)</li> <li>http://scrootca2.ocsp.secomtrust.net</li> <li>[2] ca issuers (1.3.6.1.5.5.7.48.2)</li> <li>http://repository.secomtrust.net/SC-Root2/SCRoot2ca.cer</li> </ul>	n

$\mathbf{T} \mathbf{I} \mathbf{G} \mathbf{D} \mathbf{G} \mathbf{A} \mathbf{D} + (\mathbf{G} \mathbf{A} \circ \mathbf{O} \circ \mathbf{A})$	Table 7.1-5 Subordinate CA Certificate Profile (app	licable to certificates issu	ed by SECOM
TLS RSA Root CA 2024)	TLS RSA Root CA 2024)		

Basic field		Description of setting	critical
Version		Version 3	-
Serial Num	ber	An integral serial number to be assigned by the CA to the certificate	-
Signature A	lgorithm	Sha384 With RSA Encryption	-
Issuer Country		C=JP	-
	Organization	O=SECOM Trust Systems Co., Ltd.	-
	Common Name	CN= SECOM TLS RSA Root CA 2024	-

ecurity Co	mmunication RootCA	Certificate Policy(整形版)	
Basic field		Description of setting	critical
Version		Version 3	-
Serial Nur	nber	An integral serial number to be	-
ooriar riar		assigned by the CA to the certificate	
Signature	Algorithm	sha256 With RSA Encryption	-
Issuer	Country	C=JP	-
100 001	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	-
a usjeet	Organization	O=Japan Registry Services Co., Ltd.	-
	Common Name	(1) Organization Validation	-
	e o minori i tume	CN=JPRS Organization Validation	
		Authority - G4	
		(2) Domain Validation	
		CN=JPRS Domain Validation Authority	
		- G4	
Subject Pu	ıblic Key Info	The subject's Public Key (RSA 2048 bits)	-
Extended t	field	Description of setting	critical
Authority	Key Identifier	SHA-1 hash for the issuer's Public Key (160 bits)	n
Subject Ke	ey Identifier	SHA-1 hash for the subject's Public Key (160 bits)	n
KeyUsage		Certificate Signing	у
		Off-line CRL Signing	5
		CRL Signing (06)	
Certificate	Policies	Certificate Policy	N
		1.2.392.200091.100.901.4 CPS	
		http://repository.secomtrust.net /SC-Root2/	
Basic Cons	straints	Subject Type=CA	У
		Path Length Constraint=0	
Extended	KeyUsage	TLS Web Server Authentication	n
CRL Distr	ibution Points	http://repository.secomtrust.net/SC- Root2/SCRoot2CRL.crl	n
Authority	Information Access	<ul> <li>[1] ocsp (1.3.6.1.5.5.7.48.1)</li> <li>http://scrootca2.ocsp.secomtrust.net</li> <li>[2] ca issuers (1.3.6.1.5.5.7.48.2)</li> <li>http://repository.secomtrust.net/SC-</li> </ul>	n
able 7 1-5	Subordinate CA Cert	Root2/SCRoot2ca.cer ificate Profile (applicable to certificates issu	ed by SE(
LS RSA R	oot CA 2024)		-
Basic field		Description of setting	critical
Version	1	Version 3	-
Serial Nur	nber	An integral serial number to be	-
<u>a.</u>	A.1	assigned by the CA to the certificate	
Signature		Sha384 With RSA Encryption	-
Issuer	Country	C=JP	-
	Organization	O=SECOM Trust Systems Co., Ltd.	-
	Common Name	CN= SECOM TLS RSA Root CA 2024	-

	TPRS CA (	Certificate Policy(整形版)		備考
ogurity Cor	imunication RootCA			
Basic field	Infuncation RootOA	Description of setting	critical	
Version		Version 3	-	
Serial Num	hor	An integral serial number to be	-	
	DEI	assigned by the CA to the certificate		
Signature A	lgorithm	sha256 With RSA Encryption	-	
Issuer	Country	C=JP	-	
155001	Organization	O=SECOM Trust Systems CO.,LTD.	-	
	Common Name	OU=Security Communication RootCA2	-	
Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-	
valuely	NotAfter	E.g.) 2009/3/1 00:00:00 GMT	-	
Subject	Country	C=JP	-	
Jubject	Organization	O=Japan Registry Services Co., Ltd.	-	
	Common Name	(1) Organization Validation		
	Common Mame	CN=JPRS Organization Validation		
		Authority - G4		
		(2) Domain Validation		
		CN=JPRS Domain Validation Authority		
		- G4		
Subject Pub	lic Key Info	The subject's Public Key (RSA 2048	-	
		bits)		
Extended fi	eld	Description of setting	critical	
	ley Identifier	SHA-1 hash for the issuer's Public Key	n	
v	0	(160 bits)		
Subject Key	Identifier	SHA-1 hash for the subject's Public Key	n	
0 0		(160 bits)		
KeyUsage		Certificate Signing	у	
		Off-line CRL Signing	-	
		CRL Signing (06)		
CertificateF	Policies	Certificate Policy	N	
		1.2.392.200091.100.901.4		
		CPS		
		http://repository.secomtrust.net		
		/SC-Root2/		
Basic Const	raints	Subject Type=CA	У	
		Path Length Constraint=0		
ExtendedKe		TLS Web Server Authentication	n	
CRL Distrib	oution Points	http://repository.secomtrust.net/SC-	n	
		Root2/SCRoot2CRL.crl		
Authority In	nformation Access	$[1] \operatorname{ocsp} (1.3.6.1.5.5.7.48.1)$	n	
		http://scrootca2.ocsp.secomtrust.net		
		[2] ca issuers (1.3.6.1.5.5.7.48.2)		
		http://repository.secomtrust.net/SC-		
		Root2/SCRoot2ca.cer		
		ficate Profile (applicable to certificates issu	ed by SECO	M
	ot CA 2024)			
Basic field		Description of setting	critical	
<i>Version</i>	-	Version 3	-	
Serial Num	ber	An integral serial number to be	-	
~.		assigned by the CA to the certificate	<b> </b>	
Signature A		Sha384 With RSA Encryption	-	
lssuer	Country	C=JP	-	
	Organization	O=SECOM Trust Systems Co., Ltd.	-	
	Common Name	CN= SECOM TLS RSA Root CA 2024		

	TDDS CA Con	rtificate Policy(変更履歴付)	
<b>V</b> 7-1:1:4			
Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-
C 1	NotAfter	E.g.) 2009/3/1 00:00:00 GMT	-
Subject	Country	C=JP	-
	Organization	O=Japan Registry Services Co., Ltd.	-
	Common Name	(1) Organization Validation	-
		CN= JPRS OV RSA CA 2024 G1	
		(2) Domain Validation CN= JPRS DV RSA CA 2024 G1	
Calina to Da	hl: . V L. f.	The subject's Public Key (RSA 4096	-
Subject Pu	blic Key Info	bits)	-
Extended	G . ] .]		critical
		Description of settingSHA-1 hash for the issuer's Public Key	
Authority	Key Identifier	(160 bits)	n
Cubicat Va		SHA-1 hash for the subject's Public Key	
Subject Ke	ey Identifier	(160 bits)	n
KeyUsage		Certificate Signing	
ReyUsage		Off-line CRL Signing	У
		CRL Signing (06)	
Certificate	Policios	[1] Certificate Policy	N
Certificate		(1) Domain Validation	11
		2.23.140.1.2.1	
		(2) Organization Validation	
		2.23.140.1.2.2	
		[2] Certificate Policy	
		1.2.392.200091.100.901.11	
Basic Cons	straints	Subject Type=CA	у
Duble com	of annos	Path Length Constraint=0	3
Extended	KevUsage	TLS Web Server Authentication	n
Litteriacai	ioj e sage	TLS Web Client Authentication	
CRL Distr	ibution Points	http://repo1.secomtrust.net/root/tlsrsa/tl	n
		srsarootca2024.crl	
Authority	Information Access	[1] ocsp (1.3.6.1.5.5.7.48.1)	n
5		http://tlsrsarootca2024.ocsp.secom-	
		cert.jp	
		[2] ca issuers $(1.3.6.1.5.5.7.48.2)$	
l		http://repo2.secomtrust.net/root/tlsrsa/tl	
		srsarootca2024.cer	
<u>I</u>			1

	JPRS CA (	Certificate Policy(整形版)		
Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-	
Ū	NotAfter	E.g.) 2009/3/1 00:00:00 GMT	-	
Subject	Country	C=JP	-	
	Organization	O=Japan Registry Services Co., Ltd.	-	
	Common Name	(1) Organization Validation	-	
		CN= JPRS OV RSA CA 2024 G1		
		(2) Domain Validation		
<u> </u>		CN= JPRS DV RSA CA 2024 G1		-
Subject Pul	blic Key Info	The subject's Public Key (RSA 4096	-	
Extended f	: al d	bits)	critical	
	Key Identifier	Description of settingSHA-1 hash for the issuer's Public Key		
Authority I	Xey Identifier	(160 bits)	n	
Subject Key	y Identifier	SHA-1 hash for the subject's Public Key	n	
		(160 bits)		
KeyUsage		Certificate Signing	у	
		Off-line CRL Signing	-	
		CRL Signing (06)		
Certificatel	Policies	[1] Certificate Policy	Ν	
		(1) Domain Validation		
		2.23.140.1.2.1		
		(2) Organization Validation		
		[2] Certificate Policy		
Basic Cons	trainta	1.2.392.200091.100.901.11 Subject Type=CA		-
Dasic Colls	traints	Path Length Constraint=0	У	
ExtendedK	evUsage	TLS Web Server Authentication	n	-
	oj e suge	TLS Web Client Authentication		
CRL Distri	bution Points	http://repo1.secomtrust.net/root/tlsrsa/tl	n	
		srsarootca2024.crl		
Authority I	nformation Access	[1]  ocsp  (1.3.6.1.5.5.7.48.1)	n	
		http://tlsrsarootca2024.ocsp.secom-		
		cert.jp		
		[2] ca issuers (1.3.6.1.5.5.7.48.2)		
		http://repo2.secomtrust.net/root/tlsrsa/tl		
		srsarootca2024.cer		
blo 71-6	Subordinato CA C	ertificate Profile (applicable to certificat		l hu
	nmunication ECC Re		les issuet	L Dy
Basic field		Description of setting	critical	1
Version		Version 3	-	
Serial Num	nber	An integral serial number to be	-	
		assigned by the CA to the certificate		
Signature A	Algorithm	ecdsa-with-SHA384	-	
Issuer	Country	C=JP	-	
	Organization	O=SECOM Trust Systems CO.,LTD.	-	
	Common Name	CN=Security Communication ECC		
TT 1		RootCA1		_
Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-	-
<u>a 1. ,</u>	NotAfter	E.g.) 2009/3/1 00:00:00 GMT	-	_
Subject	Country	C=JP	-	-
	Organization	O=Japan Registry Services Co., Ltd.	-	-
	Common Name	(1) Organization Validation CN= JPRS OV ECC CA 2024 G1		
		01N-01 NO UV EUU UA 2024 GI		<u> </u>

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

Basic field		Description of setting	critical
Version		Version 3	-
Serial Num	ber	An integral serial number to be assigned by the CA to the certificate	-
Signature A	Algorithm	ecdsa-with-SHA384	-
Issuer	Country	C=JP	-
	Organization	O=SECOM Trust Systems CO.,LTD.	-
	Common Name	CN=Security Communication ECC	-
		RootCA1	
Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-
	NotAfter	E.g.) 2009/3/1 00:00:00 GMT	-
Subject	Country	C=JP	-
	Organization	O=Japan Registry Services Co., Ltd.	-
	Common Name	(1) Organization Validation	-
		CN= JPRS OV ECC CA 2024 G1	

	JPRS CA (	Certificate Policy(整形版)		
/alidity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-	
	NotAfter	E.g.) 2009/3/1 00:00:00 GMT	-	1
Subject	Country	C=JP	-	
	Organization	O=Japan Registry Services Co., Ltd.	-	
	Common Name	(1) Organization Validation	-	
		CN= JPRS OV RSA CA 2024 G1		
		(2) Domain Validation		
<u></u>		CN= JPRS DV RSA CA 2024 G1		-
Subject Put	olic Key Info	The subject's Public Key (RSA 4096 bits)	-	
Extended fi	ield	Description of setting	critical	
	Key Identifier	SHA-1 hash for the issuer's Public Key	n	
5		(160 bits)		
Subject Key	y Identifier	SHA-1 hash for the subject's Public Key	n	1
		(160 bits)		
KeyUsage		Certificate Signing	У	
		Off-line CRL Signing		
~	- 1	CRL Signing (06)		4
CertificateI	Policies	[1] Certificate Policy	Ν	
		(1) Domain Validation		
		2.23.140.1.2.1		
		(2) Organization Validation 2.23.140.1.2.2		
		[2] Certificate Policy		
		1.2.392.200091.100.901.11		
Basic Const	traints	Subject Type=CA	у	
Dasie Collise		Path Length Constraint=0	У	
ExtendedK	evUsage	TLS Web Server Authentication	n	
		TLS Web Client Authentication		
CRL Distril	bution Points	http://repo1.secomtrust.net/root/tlsrsa/tl	n	
		srsarootca2024.crl		
Authority I	nformation Access	$[1] \operatorname{ocsp} (1.3.6.1.5.5.7.48.1)$	n	
		http://tlsrsarootca2024.ocsp.secom-		
		cert.jp		
		[2] ca issuers (1.3.6.1.5.5.7.48.2)		
		http://repo2.secomtrust.net/root/tlsrsa/tl		
		srsarootca2024.cer		
	nmunication ECC Re	Certificate Profile (applicable to certificate $C(A_1)$ )	tes issued	l by
Basic field	infuncation ECC N	Description of setting	critical	1
Version		Version 3	-	-
Serial Num	her	An integral serial number to be	-	-
	1001	assigned by the CA to the certificate		
Signature A	Algorithm	ecdsa-with-SHA384	-	1
Issuer	Country	C=JP	-	1
	Organization	O=SECOM Trust Systems CO.,LTD.	-	1
	Common Name	CN=Security Communication ECC	-	1
		RootCA1		
Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-	]
·	NotAfter	E.g.) 2009/3/1 00:00:00 GMT	-	
	Country	C=JP	-	]
Subject	Country	0 01		
Subject	Organization	O=Japan Registry Services Co., Ltd.	-	
Subject			-	_

	TPRS CA	Certificate Policy(整形版)		備考	
Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT			
valially	NotAfter	E.g.) 2009/3/1 00:00:00 GMT	_		
Subject		C=JP	-		
Subject	Country	O=Japan Registry Services Co., Ltd.	_		
	Organization Common Name	(1) Organization Validation	_		
	Common Name	CN= JPRS OV RSA CA 2024 G1			
		(2) Domain Validation			
		CN= JPRS DV RSA CA 2024 G1			
Subject Pu	blic Key Info	The subject's Public Key (RSA 4096	-		
Subject I u		bits)			
Extended f	field	Description of setting	critical		
	Key Identifier	SHA-1 hash for the issuer's Public Key	n		
		(160 bits)			
Subiect Ke	y Identifier	SHA-1 hash for the subject's Public Key	n		
J = = = = = = = = = = = = = = = = = = =	v -	(160 bits)			
KeyUsage		Certificate Signing	у		
• 0-		Off-line CRL Signing			
		CRL Signing (06)			
Certificate	Policies	[1] Certificate Policy	N		
		(1) Domain Validation			
		2.23.140.1.2.1			
		(2) Organization Validation			
		2.23.140.1.2.2			
		[2] Certificate Policy			
		1.2.392.200091.100.901.11			
Basic Cons	straints	Subject Type=CA	у		
		Path Length Constraint=0	Ŭ		
Extended	KeyUsage	TLS Web Server Authentication	n		
	• •	TLS Web Client Authentication			
CRL Distri	ibution Points	http://repo1.secomtrust.net/root/tlsrsa/tl	n		
		srsarootca2024.crl			
Authority I	Information Access	$[1] \operatorname{ocsp} (1.3.6.1.5.5.7.48.1)$	n		
		http://tlsrsarootca2024.ocsp.secom-			
		cert.jp			
		[2] ca issuers (1.3.6.1.5.5.7.48.2)			
		http://repo2.secomtrust.net/root/tlsrsa/tl			
		srsarootca2024.cer			
		Certificate Profile (applicable to certificate	tes issued	by	
	mmunication ECC R				
Basic field		Description of setting	critical		
Version	_	Version 3	-		
Serial Nun	nber	An integral serial number to be	-		
		assigned by the CA to the certificate			
Signature .		ecdsa-with-SHA384	-		
Issuer	Country	C=JP	-		
	Organization	O=SECOM Trust Systems CO.,LTD.	-		
	Common Name	CN=Security Communication ECC	-		
		RootCA1			
Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-		
	NotAfter	E.g.) 2009/3/1 00:00:00 GMT	-		
	Country	C=JP	-		
Subject	· · · · · · · · · · · · · · · · · · ·				
Subject	Organization	O=Japan Registry Services Co., Ltd.	-		
Subject	· · · · · · · · · · · · · · · · · · ·		-		

<u> </u>	rtificate Policy(変更履歴付) (2)Domain Validation	
	CN= JPRS DV ECC CA 2024 G1	
Subject Public Key Info	The subject's Public Key (384 bits)	-
Extended field	Description of setting	critica
Authority Key Identifier	SHA-1 hash for the issuer's Public Key	
	(160 bits)	n
Subject Key Identifier	SHA-1 hash for the subject's Public Key	n
	(160 bits)	
KeyUsage	Certificate Signing	у
	Off-line CRL Signing	-
	CRL Signing (06)	
CertificatePolicies	[1] Certificate Policy	N
	(1) Domain Validation	
	2.23.140.1.2.1	
	(2) Organization Validation	
	2.23.140.1.2.2	
	[2] Certificate Policy	
	1.2.392.200091.100.902.1	
Basic Constraints	Subject Type=CA	У
	Path Length Constraint=0	
ExtendedKeyUsage	TLS Web Server Authentication	n
	TLS Web Client Authentication	
CRL Distribution Points	http://repository.secomtrust.net/SC-	n
	ECC-Root1/SCECCRoot1CRL.crl	
Authority Information Access	[1]  ocsp  (1.3.6.1.5.5.7.48.1)	n
	http://sceccrootca1.ocsp.secomtrust.net	
	[2] ca issuers (1.3.6.1.5.5.7.48.2)	
	http://repository.secomtrust.net/SC-	
	ECC-Root1/SCECCRoot1ca.cer	

	JPRS CA C	ertificate Policy(整形版)	
		(2) Domain Validation	
		CN= JPRS DV ECC CA 2024 G1	
Subject Pu	blic Key Info	The subject's Public Key (384 bits)	-
Extended f		Description of setting	critical
Authority	Key Identifier	SHA-1 hash for the issuer's Public Key	n
		(160 bits)	
Subject Ke	y Identifier	SHA-1 hash for the subject's Public Key	n
		(160 bits)	
KeyUsage		Certificate Signing	У
		Off-line CRL Signing	
<b>AA</b>	D 1: -	CRL Signing (06)	2.7
Certificate	Policies	[1] Certificate Policy	N
		(1) Domain Validation	
		2.23.140.1.2.1	
		(2) Organization Validation	
		2.23.140.1.2.2	
		[2] Certificate Policy 1.2.392.200091.100.902.1	
Basic Cons	trainta	Subject Type=CA	
Dasic Cons	stramts	Path Length Constraint=0	У
Extended	Covlleago	TLS Web Server Authentication	n
Extenueur	Ley Usage	TLS Web Client Authentication	11
CRL Distr	ibution Points	http://repository.secomtrust.net/SC-	n
		ECC-Root1/SCECCRoot1CRL.crl	
Authority	Information Access	[1] ocsp (1.3.6.1.5.5.7.48.1)	n
		http://sceccrootca1.ocsp.secomtrust.net	
		[2] ca issuers (1.3.6.1.5.5.7.48.2)	
		http://repository.secomtrust.net/SC-	
		ECC-Root1/SCECCRoot1ca.cer	
		·	
111			
	Precertificate Profile	e (applicable to certificates issued on or	after July
020)			
020) <mark>Basic field</mark>		Description of setting	after July critical
020) <mark>Basic field</mark>		Description of settingEncoded value MUST be byte-for-byte	
020) <mark>Basic field</mark>		Description of setting Encoded value MUST be byte-for-byte identical to the same field of the	
020) <mark>Basic field</mark> Version		Description of setting Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate.	critical
020) <mark>Basic field</mark> Version Serial Nur	nber	Description of settingEncoded value MUST be byte-for-byteidentical to the same field of theSubuscriber Certificate.Same as above	
020) <mark>Basic field</mark> Version Serial Nun Signature	nber Algorithm	Description of setting Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate. Same as above Same as above	critical
020) <mark>Basic field</mark> Version Serial Nun Signature	nber Algorithm Country	Description of setting Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate. Same as above Same as above Same as above	critical
020) <mark>Basic field</mark> Version Serial Nun Signature	nber Algorithm Country Organization	Description of settingEncoded value MUST be byte-for-byteidentical to the same field of theSubuscriber Certificate.Same as aboveSame as aboveSame as aboveSame as aboveSame as aboveSame as above	critical
020) <mark>Basic field</mark> Version Serial Nur Signature Issuer	nber Algorithm Country Organization Common Name	Description of settingEncoded value MUST be byte-for-byteidentical to the same field of theSubuscriber Certificate.Same as aboveSame as above	critical
020) <mark>Basic field</mark> Version Serial Nur Signature Issuer	nber Algorithm Country Organization Common Name NotBefore	Description of settingEncoded value MUST be byte-for-byteidentical to the same field of theSubuscriber Certificate.Same as aboveSame as above	critical
020) <mark>Basic field</mark> Version Serial Nun Signature Issuer Validity	nber Algorithm Country Organization Common Name NotBefore NotAfter	Description of settingEncoded value MUST be byte-for-byteidentical to the same field of theSubuscriber Certificate.Same as aboveSame as above	critical
020) <mark>Basic field</mark> Version Serial Nun Signature Issuer Validity	nber Algorithm Country Organization Common Name NotBefore NotAfter Country	Description of settingEncoded value MUST be byte-for-byteidentical to the same field of theSubuscriber Certificate.Same as aboveSame as above	critical
020) <mark>Basic field</mark> Version Serial Nun Signature Issuer Validity	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province	Description of settingEncoded value MUST be byte-for-byteidentical to the same field of theSubuscriber Certificate.Same as aboveSame as above	critical
020) <mark>Basic field</mark> Version Serial Nun Signature Issuer Validity	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality	Description of settingEncoded value MUST be byte-for-byteidentical to the same field of theSubuscriber Certificate.Same as aboveSame as above	critical
020) <mark>Basic field</mark> Version Serial Nun Signature Issuer Validity	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization	Description of settingEncoded value MUST be byte-for-byteidentical to the same field of theSubuscriber Certificate.Same as aboveSame as above	critical
020) Basic field Version Serial Nun Signature Issuer Validity	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization Organizational	Description of settingEncoded value MUST be byte-for-byteidentical to the same field of theSubuscriber Certificate.Same as aboveSame as above	critical
020) <mark>Basic field</mark> Version Serial Nun Signature Issuer Validity	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization Organizational Unit	Description of settingEncoded value MUST be byte-for-byteidentical to the same field of theSubuscriber Certificate.Same as aboveSame as above	critical
020) Basic field Version Serial Nun Signature Issuer Validity Subject	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization Organizational Unit Common Name	Description of settingEncoded value MUST be byte-for-byteidentical to the same field of theSubuscriber Certificate.Same as aboveSame as above	critical
020) Basic field Version Serial Nur Signature Signature Issuer Validity Subject Subject Pu	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization Organizational Unit Common Name blic Key Info	Description of settingEncoded value MUST be byte-for-byteidentical to the same field of theSubuscriber Certificate.Same as aboveSame as above	critical
020) Basic field Version Serial Num Signature Issuer Validity Subject Subject Pu Extended f	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization Organizational Unit Common Name blic Key Info	Description of settingEncoded value MUST be byte-for-byteidentical to the same field of theSubuscriber Certificate.Same as aboveSame as above	critical         -
020) Basic field Version Serial Nur Signature Issuer Validity Subject Subject Pu	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization Organizational Unit Common Name blic Key Info	Description of settingEncoded value MUST be byte-for-byteidentical to the same field of theSubuscriber Certificate.Same as aboveSame as above<	critical
020) Basic field Version Serial Num Signature Issuer Validity Subject Subject Pu Extended f	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization Organizational Unit Common Name blic Key Info	Description of settingEncoded value MUST be byte-for-byteidentical to the same field of theSubuscriber Certificate.Same as aboveSame as above	critical         -

 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 Nur	nber	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	Same as above	-
	Unit		
	Common Name	Same as above	-
Subject Public Key Info Extended field		Same as above	-
		Description of setting	critical
Precertific	ate Poison	extnValue OCTET STRING which is	у
		exactly the hex-encoded bytes 0500, the	
		encoded representation of the ASN.1	

	JPRS CA C	ertificate Policy(整形版)		
		(2) Domain Validation		
		CN= JPRS DV ECC CA 2024 G1		
Subject Pu	ıblic Key Info	The subject's Public Key (384 bits)	-	
Extended t	field	Description of setting	critical	
Authority	Key Identifier	SHA-1 hash for the issuer's Public Key	n	
		(160 bits)		
Subject Ke	ey Identifier	SHA-1 hash for the subject's Public Key	n	
		(160 bits)		
KeyUsage		Certificate Signing	У	
		Off-line CRL Signing		
		CRL Signing (06)		
CertificatePolicies		[1] Certificate Policy	N	
		(1) Domain Validation		
		2.23.140.1.2.1		
		(2) Organization Validation		
		2.23.140.1.2.2		
		[2] Certificate Policy		
Basic Cons	etrointe	1.2.392.200091.100.902.1 Subject Type=CA	τ7	
Dasic Cons	511 411118	Path Length Constraint=0	У	
Extended	CevIIsage	TLS Web Server Authentication	n	
BATEIIdeur	sty Usage	TLS Web Server Authentication TLS Web Client Authentication	11	
CRL Distr	ibution Points	http://repository.secomtrust.net/SC-	n	
		ECC-Root1/SCECCRoot1CRL.crl		
Authority	Information Access	[1] ocsp (1.3.6.1.5.5.7.48.1)	n	
11401101103		http://sceccrootca1.ocsp.secomtrust.net		
		http://seccerooteal.ocsp.secontriast.net		
		[2] ca issuers (1 3 6 1 5 5 7 48 2)		
		[2] ca issuers (1.3.6.1.5.5.7.48.2) http://repository.secomtrust.net/SC-		
		[2] ca issuers (1.3.6.1.5.5.7.48.2) http://repository.secomtrust.net/SC- ECC-Root1/SCECCRoot1ca.cer		
		http://repository.secomtrust.net/SC-		
Table 7.1-7	Precertificate Profile	http://repository.secomtrust.net/SC-	after July	29,
	Precertificate Profile	http://repository.secomtrust.net/SC- ECC-Root1/SCECCRoot1ca.cer	after July	29,
2020)		http://repository.secomtrust.net/SC- ECC-Root1/SCECCRoot1ca.cer e (applicable to certificates issued on or Description of setting	after July critical	29,
		http://repository.secomtrust.net/SC- ECC-Root1/SCECCRoot1ca.cer e (applicable to certificates issued on or Description of setting Encoded value MUST be byte-for-byte	-	29,
2020) <mark>Basic field</mark>		http://repository.secomtrust.net/SC- ECC-Root1/SCECCRoot1ca.cer e (applicable to certificates issued on or Description of setting Encoded value MUST be byte-for-byte identical to the same field of the	-	29,
2020) <mark>Basic field</mark> Version		http://repository.secomtrust.net/SC- ECC-Root1/SCECCRoot1ca.cer e (applicable to certificates issued on or Description of setting Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate.	-	29,
2020) <mark>Basic field</mark> Version Serial Nur	nber	http://repository.secomtrust.net/SC- ECC-Root1/SCECCRoot1ca.cer e (applicable to certificates issued on or Description of setting Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate. Same as above	-	29,
2020) Basic field Version Serial Nur Signature	nber Algorithm	http://repository.secomtrust.net/SC- ECC-Root1/SCECCRoot1ca.cere(applicable to certificates issued on orDescription of setting Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate.Same as above Same as above	-	29,
2020) Basic field Version Serial Nur Signature	nber Algorithm Country	http://repository.secomtrust.net/SC- ECC-Root1/SCECCRoot1ca.cere(applicable to certificates issued on orDescription of settingEncoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate.Same as aboveSame as aboveSame as aboveSame as above	-	29,
2020) Basic field Version Serial Nur Signature	nber Algorithm Country Organization	http://repository.secomtrust.net/SC- ECC-Root1/SCECCRoot1ca.cer e (applicable to certificates issued on or Description of setting Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate. Same as above Same as above Same as above Same as above	-	29,
2020) Basic field Version Serial Nur Signature Issuer	nber Algorithm Country Organization Common Name	http://repository.secomtrust.net/SC- ECC-Root1/SCECCRoot1ca.cere(applicable to certificates issued on orDescription of setting Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate.Same as above Same as above Same as above Same as aboveSame as above Same as aboveSame as above Same as aboveSame as above	-	29,
2020) Basic field Version Serial Nur Signature Issuer	nber Algorithm Country Organization Common Name NotBefore	http://repository.secomtrust.net/SC- ECC-Root1/SCECCRoot1ca.cere(applicable to certificates issued on orDescription of setting Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate.Same as above Same as above	-	29,
020) Basic field Version Serial Nur Signature Issuer Validity	nber Algorithm Country Organization Common Name NotBefore NotAfter	http://repository.secomtrust.net/SC- ECC-Root1/SCECCRoot1ca.cere(applicable to certificates issued on orDescription of setting Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate.Same as above Same as above	-	29,
2020) Basic field Version Serial Nur Signature Issuer Validity	nber Algorithm Country Organization Common Name NotBefore NotAfter Country	http://repository.secomtrust.net/SC- ECC-Root1/SCECCRoot1ca.cere(applicable to certificates issued on orDescription of setting Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate.Same as above Same as aboveSame as above	-	29,
2020) <mark>Basic field</mark> Version	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province	http://repository.secomtrust.net/SC- ECC-Root1/SCECCRoot1ca.cere(applicable to certificates issued on orDescription of settingEncoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate.Same as aboveSame as above	-	29,
020) Basic field Version Serial Nur Signature Issuer Validity	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality	http://repository.secomtrust.net/SC- ECC-Root1/SCECCRoot1ca.cere(applicable to certificates issued on orDescription of setting Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate.Same as above Same as aboveSame as above	-	29,
2020) Basic field Version Serial Nur Signature Issuer Validity	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization	http://repository.secomtrust.net/SC- ECC-Root1/SCECCRoot1ca.cere(applicable to certificates issued on orDescription of setting Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate.Same as above Same as aboveSame a	-	29,
2020) Basic field Version Serial Nur Signature Issuer Validity	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization Organizational	http://repository.secomtrust.net/SC- ECC-Root1/SCECCRoot1ca.cere(applicable to certificates issued on orDescription of setting Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate.Same as above Same as aboveSame as above	-	29,
2020) Basic field Version Serial Nur Signature Issuer Validity	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization Organizational Unit	http://repository.secomtrust.net/SC- ECC-Root1/SCECCRoot1ca.cere(applicable to certificates issued on orDescription of setting Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate.Same as above Same as aboveSame as above	critical - - - - - - - - - - - - - - - - - - -	29,
2020) Basic field Version Serial Nur Signature Issuer Validity Subject	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization Organizational Unit Common Name	http://repository.secomtrust.net/SC- ECC-Root1/SCECCRoot1ca.cere(applicable to certificates issued on orDescription of setting Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate.Same as above Same as aboveSame as above	-	29,
2020) Basic field Version Serial Nur Signature Issuer Validity Subject Subject Pu	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization Organizational Unit Common Name iblic Key Info	http://repository.secomtrust.net/SC- ECC-Root1/SCECCRoot1ca.cere(applicable to certificates issued on orDescription of setting Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate.Same as aboveSame as above	critical	29,
2020) Basic field Version Serial Nur Signature Issuer Validity Subject Subject Pu Extended	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization Organizational Unit Common Name ablic Key Info field	http://repository.secomtrust.net/SC- ECC-Root1/SCECCRoot1ca.cere(applicable to certificates issued on orDescription of setting Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate.Same as above Same as aboveSame a	critical	29,
2020) Basic field Version Serial Nur Signature Issuer Validity Subject Subject Pu Extended	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization Organizational Unit Common Name iblic Key Info	http://repository.secomtrust.net/SC- ECC-Root1/SCECCRoot1ca.cere(applicable to certificates issued on orDescription of settingEncoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate.Same as aboveSame as abo	critical	29,
2020) Basic field Version Serial Nur Signature Issuer Validity Subject Subject Pu Extended	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization Organizational Unit Common Name ablic Key Info field	http://repository.secomtrust.net/SC- ECC-Root1/SCECCRoot1ca.cere(applicable to certificates issued on orDescription of setting Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate.Same as above Same as aboveSame a	critical         -	29,

JPRS CA Cert	tificate Policy(変更履歴付)	
	NULL value, as specified in RFC 6962,	
	Section 3.1.	
KeyUsage	Encoded value MUST be byte-for-byte	у
	identical to the same field of the	
	Subuscriber Certificate.	
ExtendedKeyUsage	Same as above	n
Subject Alt Name	Same as above	n
CertificatePolicies	Same as above	n
CRL Distribution Points	Same as above	n
Authority Information Access	Same as above	n
Authority Key Identifier	Same as above	n
Subject Key Identifier	Same as above	n

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

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

JPRS Domain	n Validation Authorit	y – G4 or JPRS Organization Validation Au	thority – (
Basic field		Description of setting	critical
Version		Version 3	-
Serial Nun	nber	Non-sequential values greater than	-
		zero (0) and less than $2^{159}$ containing	
		64 bits of output from a CSPRNG	
Signature	Algorithm	sha256 With RSA Encryption	-
Issuer	Country	C=JP	-
	Organization	O= Japan Registry Services Co., Ltd.	-
	Common Name	(1) Domain Validation	-
		CN=JPRS Domain Validation Authority	
		- G4	
		(2) Organization Validation	
		CN=JPRS Organization Validation	
		Authority – G4	
Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-
	NotAfter	E.g.) 2008/3/5 00:00:00 GMT	-
Subject	Country	C=JP (fixed value)	-
	Organization	Japan Registry Services Co., Ltd. (fixed	-
		value)	
	Common Name	Name of the OCSP server (mandatory)	-
Subject Pu	blic Key Info	The subject's Public Key (RSA 2048	-
		bits)	
Extended f		Description of setting	critical
Authority I	Key Identifier	SHA-1 hash for the issuer's Public Key	n
		(160 bits)	
Subject Ke	y Identifier	SHA-1 hash for the subject's Public Key	n
		(160 bits)	
KeyUsage		digitalSignature	у
ExtendedK		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			
Version Version 3		-		
Serial Number	Non-sequential values greater than	-		
	zero (0) and less than 2 <sup>159</sup> containing			

	TPRS_CA	Certificate Policy(整形版)		
		NULL value, as specified in RFC 6962,		
IZ II.		Section 3.1.		-
KeyUsage		Encoded value MUST be byte-for-byte	У	
		identical to the same field of the		
KeyUsage         ExtendedKeyUsage         Subject Alt Name         CertificatePolicies         CRL Distribution Points         Authority Information Access         Authority Key Identifier         Subject Key Identifier         Subject Key Identifier         Swift the Precertificate Poison ext         Certificate Timestamp List is re         extensions field MUST be byte-for         Table 7.1-8 OCSP Responder O         JPRS Domain Validation Author         Basic field         Version         Serial Number         Signature Algorithm         Issuer       Country         Organization         Common Name         Validity       NotBefore		Subuscriber Certificate. Same as above	n	-
	• •	Same as above	n	-
*		Same as above	n	-
		Same as above		-
		Same as above	n	-
		Same as above	n	-
-		Same as above	n n	-
	0			mod
				une
Atensions n	eiu MOSI be byte io	i byte identical to the Subscriber Certificate	•	
Table 7 1-8	8 OCSP Responder C	ertificate Profile (Applicable to certificates is	ssued by	
		ty - G4 or JPRS Organization Validation Au		<del>7</del> 4)
		Description of setting	critical	1
		Version 3	-	1
	nber	Non-sequential values greater than	-	
2 of fair 1 of fair		zero (0) and less than 2^159 containing		
		64 bits of output from a CSPRNG		
Signature	Algorithm	sha256 With RSA Encryption	-	
-		C=JP	-	
		O= Japan Registry Services Co., Ltd.	-	
	-	(1) Domain Validation	-	
		<b>CN=JPRS</b> Domain Validation Authority		
		- G4		
		(2) Organization Validation		
		CN=JPRS Organization Validation		
		Authority – G4		
Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-	
	NotAfter	E.g.) 2008/3/5 00:00:00 GMT	-	
Subject	Country	C=JP (fixed value)	-	
	Organization	Japan Registry Services Co., Ltd. (fixed	-	
		value)		
	Common Name	Name of the OCSP server (mandatory)	-	
Subject Pu	blic Key Info	The subject's Public Key (RSA 2048	-	
-	-	bits)		
Extended f	field	Description of setting	critical	
Authority	Key Identifier	SHA-1 hash for the issuer's Public Key	n	
		(160 bits)		
Subject Ke	y Identifier	SHA-1 hash for the subject's Public Key	n	
	-	(160 bits)		
KeyUsage		digitalSignature	У	
Extended	KeyUsage	OCSPSigning	Ν	
OCSP No 0	Check	null	Ν	
				_
		ertificate Profile (Applicable to certificates is	ssued by	
		RS OV RSA CA 2024 G1)		-
Basic field		Description of setting	critical	
Version		Version 3	-	]
Serial Nun	nber	Non-sequential values greater than	-	]
		zero (0) and less than 2^159 containing		

	TPRS CA	Certificate Policy(整形版)		
	JI NO ON			
		NULL value, as specified in RFC 6962,		
IZ II.		Section 3.1.		-
KeyUsage		Encoded value MUST be byte-for-byte	У	
		identical to the same field of the		
ExtondodK	or Use me	Subuscriber Certificate. Same as above		-
ExtendedKe Subject Alt		Same as above	n	
Certificate		Same as above	n	
			n	-
	bution Points	Same as above	n	-
Authority Information Access Authority Key Identifier		Same as above	n	-
· · · · · · · · · · · · · · · · · · ·		Same as above	n	-
Subject Key		Same as above	n	1
		ension is removed from the Precertificate, a		
		noved from the Subscriber certificate, the c		the
extensions fie	eld MUST be byte-fo	r-byte identical to the Subscriber Certificate	•	
			11	
		ertificate Profile (Applicable to certificates is		14)
Basic field		ty – G4 or JPRS Organization Validation Au		741 
		Description of setting           Version 3	critical	-
Version Seriel Num	hor		-	-
Serial Num	iber	Non-sequential values greater than $20150$ containing	-	
		zero (0) and less than 2^159 containing		
Ciana a tarana A	<u> </u>	64 bits of output from a CSPRNG	-	-
Signature A		sha256 With RSA Encryption	-	-
Issuer	Country	C=JP	-	
	Organization	O= Japan Registry Services Co., Ltd.	-	
	Common Name	(1) Domain Validation	-	
		CN=JPRS Domain Validation Authority		
		-G4		
		(2) Organization Validation CN=JPRS Organization Validation		
		CN=JPRS Organization Validation Authority – G4		
Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-	-
validity	NotAfter	E.g.) 2008/3/1 00:00:00 GMT		
Subject	Country	C=JP (fixed value)		
Subject				-
	Organization	Japan Registry Services Co., Ltd. (fixed value)	-	
	Common Name	Name of the OCSP server (mandatory)	-	-
Qubicat D. 1				
Subject Put	blic Key Info	The subject's Public Key (RSA 2048 bits)	-	
Extended fi	iald		critical	
	ield Key Identifier	Description of setting		-
Authority K	xey identifier	SHA-1 hash for the issuer's Public Key	n	
Subject V	Idontifican	(160 bits)		-
Subject Key	y identifier	SHA-1 hash for the subject's Public Key	n	
		(160 bits)		-
KeyUsage	· TT	digitalSignature	y N	
ExtendedK		OCSPSigning	N	-
OCSP No C	heck	null	Ν	J
<b>m</b> 11 = 1	0.000 5			
		ertificate Profile (Applicable to certificates is	ssued by	
	A CA 2024 G1 or JP	RS OV RSA CA 2024 G1)		1
Basic field		Description of setting	critical	
Version		Version 3	-	
Serial Num	ıber	Non-sequential values greater than	-	
		zero (0) and less than 2^159 containing		

JPRS CA Certificate NULL va		
NULL va		
	ue, as specified in RFC 6962,	
Section 3.		
	value MUST be byte-for-byte	У
	to the same field of the	
	er Certificate.	
ExtendedKeyUsage Same as a		n
Subject Alt Name Same as a	bove	n
CertificatePolicies Same as a	bove	n
CRL Distribution Points Same as a	bove	n
Authority Information Access Same as a	bove	n
Authority Key Identifier Same as a	bove	n
Subject Key Identifier Same as a		n
*If the Precertificate Poison extension is rem		
Certificate Timestamp List is removed from t		U
extensions field MUST be byte-for-byte identic		
Table 7.1-8 OCSP Responder Certificate Pro	file (Applicable to certificates iss	sued by
JPRS Domain Validation Authority – G4 or JP		
•		critical
Version Version 3		-
	ential values greater than	
1	nd less than 2^159 containing	
	8	
	output from a CSPRNG	
	ith RSA Encryption	-
Issuer Country C=JP		-
	Registry Services Co., Ltd.	-
	n Validation	-
	Domain Validation Authority	
- G4		
Ű	zation Validation	
CN=JPRS	8	
Authority		
	/3/1 00:00:00 GMT	-
U	/3/5 00:00:00 GMT	-
Subject Country C=JP (fin	xed value)	
Organization Japan Reg	gistry Services Co., Ltd. (fixed	-
value)		
Common Name Name of t	he OCSP server (mandatory)	-
	ect's Public Key (RSA 2048	-
bits)		
	n of setting	critical
	sh for the issuer's Public Key	n
Authority Key Identifier SHA-1 ha	the house of a dollo hoy	
(160 bits)	sh for the subject's Public Key	
(160 bits)Subject Key IdentifierSHA-1 ha	sh for the subject's Public Key	n
(160 bits) Subject Key Identifier SHA-1 ha (160 bits)		
(160 bits)Subject Key IdentifierSHA-1 ha (160 bits)KeyUsagedigitalSig	nature	У
(160 bits)Subject Key IdentifierSHA-1 ha(160 bits)KeyUsagedigitalSigExtendedKeyUsageOCSPSign	nature	y N
(160 bits)Subject Key IdentifierSHA-1 ha (160 bits)KeyUsagedigitalSig	nature	У
(160 bits)Subject Key IdentifierSHA-1 ha(160 bits)KeyUsagedigitalSigExtendedKeyUsageOCSP No Checknull	nature ning	y N N
(160 bits)Subject Key IdentifierSHA-1 ha(160 bits)KeyUsagedigitalSigExtendedKeyUsageOCSP No ChecknullTable 7.1-9 OCSP Responder Certificate Pro-	file (Applicable to certificates iss	y N N
(160 bits)Subject Key IdentifierSHA-1 ha(160 bits)KeyUsagedigitalSigExtendedKeyUsageOCSP No ChecknullTable 7.1-9 OCSP Responder Certificate ProJPRS DV RSA CA 2024 G1 or JPRS OV RSA CA	file (Applicable to certificates iss A 2024 G1)	y N N sued by
(160 bits)Subject Key IdentifierSHA-1 ha(160 bits)KeyUsagedigitalSigExtendedKeyUsageOCSP No ChecknullTable 7.1-9 OCSP Responder Certificate ProJPRS DV RSA CA 2024 G1 or JPRS OV RSA COBasic fieldDescription	file (Applicable to certificates iss A 2024 G1)	y N N
(160 bits)Subject Key IdentifierSHA-1 ha(160 bits)KeyUsagedigitalSigExtendedKeyUsageOCSP No ChecknullTable 7.1-9 OCSP Responder Certificate ProJPRS DV RSA CA 2024 G1 or JPRS OV RSA CABasic fieldVersionVersion 3	file (Applicable to certificates iss A 2024 G1) n of setting	y N N sued by
(160 bits)Subject Key IdentifierSHA-1 ha(160 bits)KeyUsagedigitalSigExtendedKeyUsageOCSP No ChecknullTable 7.1-9 OCSP Responder Certificate ProJPRS DV RSA CA 2024 G1 or JPRS OV RSA CABasic fieldDescriptionVersionVersion 3Serial NumberNon-seque	file (Applicable to certificates iss A 2024 G1)	y N N sued by

		Contificato D <del>olion (故心归)</del>		—————————————————————————————————————
	JPRS CA	Certificate Policy(整形版)		備考
		NULL value, as specified in RFC 6962,		
		Section 3.1.		
KeyUsage		Encoded value MUST be byte-for-byte	У	
		identical to the same field of the		
		Subuscriber Certificate.		
ExtendedK	• •	Same as above	n	
Subject Alt		Same as above	n	
Certificate		Same as above	n	
CRL Distri	ibution Points	Same as above	n	
Authority	Information Access	Same as above	n	
Authority 1	Key Identifier	Same as above	n	
Subject Ke	ey Identifier	Same as above	n	
XIf the Prec	ertificate Poison exte	ension is removed from the Precertificate, a	nd the Sig	ned
		noved from the Subscriber certificate, the c		
		r-byte identical to the Subscriber Certificate		
	·			
Table 7.1-8	3 OCSP Responder C	ertificate Profile (Applicable to certificates is	ssued by	
		ty – G4 or JPRS Organization Validation Au		4)
Basic field		Description of setting	critical	
Version		Version 3	-	
Serial Nun	nber	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	-	
100 001	Organization	O= Japan Registry Services Co., Ltd.	-	
	Common Name	(1) Domain Validation	-	
		CN=JPRS Domain Validation Authority		
		- G4		
		(2) Organization Validation		
		CN=JPRS Organization Validation		
		Authority – G4		
Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-	
	NotAfter	E.g.) 2008/3/5 00:00:00 GMT	-	
Subject	Country	C=JP (fixed value)	-	
ie insjere	Organization	Japan Registry Services Co., Ltd. (fixed	-	
	Jigamzanon	value)		
	Common Name	Name of the OCSP server (mandatory)	-	
Subject Pu	iblic Key Info	The subject's Public Key (RSA 2048	-	
	ione ney mit	bits)		
Extended f	field	Description of setting	critical	
	Key Identifier	SHA-1 hash for the issuer's Public Key	n	
Authority	ixey incliniter	(160 bits)	11	
Subject Ke	ey Identifier	SHA-1 hash for the subject's Public Key	n	
Bubject Re	y inclution	(160 bits)	11	
KeyUsage		digitalSignature	**	
			y N	
ExtendedKeyUsage		OCSPSigning	N N	
	опеск	null	IN	
OCSP No (				
OCSP No 0		· · · · · · · · · · · · · · · · · · ·	11	
OCSP No C		ertificate Profile (Applicable to certificates is	ssued by	
OCSP No C Table 7.1-9 JPRS DV RS	SA CA 2024 G1 or JPH	RS OV RSA CA 2024 G1)	-	
OCSP No C Table 7.1-9 JPRS DV RS Basic field	SA CA 2024 G1 or JPH	RS OV RSA CA 2024 G1) Description of setting	ssued by critical	
OCSP No O Table 7.1-9 JPRS DV RS Basic field Version	SA CA 2024 G1 or JPI	RS OV RSA CA 2024 G1)           Description of setting           Version 3	-	
OCSP No C Table 7.1-9 JPRS DV RS Basic field	SA CA 2024 G1 or JPI	RS OV RSA CA 2024 G1) Description of setting	-	

	TPRS_CA	Certificate Policy(整形版)		
	<u></u>	NULL value, as specified in RFC 6962,		
		Section 3.1.		
KeyUsage		Encoded value MUST be byte-for-byte	У	
ReyUsage		identical to the same field of the	У	
		Subuscriber Certificate.		
ExtendedK	evUsage	Same as above	n	
Subject Alt		Same as above	n	
Certificate		Same as above	n	
	bution Points	Same as above	n	
	nformation Access	Same as above	n	
Authority F	Key Identifier	Same as above	n	
Subject Key		Same as above	n	
	ertificate Poison ext	ension is removed from the Precertificate, a	nd the Sig	ned
		moved from the Subscriber certificate, the c	-	
		r-byte identical to the Subscriber Certificate		
		Certificate Profile (Applicable to certificates is		
	n Validation Authori	ity – G4 or JPRS Organization Validation Au	,	<del>3</del> 4)
Basic field		Description of setting	critical	
Version		Version 3	-	
Serial Num	ıber	Non-sequential values greater than	-	
		zero (0) and less than 2 <sup>159</sup> containing		
		64 bits of output from a CSPRNG		
Signature A	-	sha256 With RSA Encryption	-	
Issuer	Country	C=JP	-	
	Organization	O= Japan Registry Services Co., Ltd.	-	
	Common Name	(1) Domain Validation	-	
		CN=JPRS Domain Validation Authority		
		-G4		
		(2) Organization Validation		
		CN=JPRS Organization Validation		
Validity	NotBefore	Authority – G4 E.g.) 2008/3/1 00:00:00 GMT	_	
valuity	NotAfter	E.g.) 2008/3/1 00:00:00 GMT	_	
Subject	Country	C=JP (fixed value)		
Subject		· · · · · · · · · · · · · · · · · · ·		
	Organization	Japan Registry Services Co., Ltd. (fixed	-	
	Common Name	value) Name of the OCSP server (mandatory)	-	
Cubicat Dul	blic Key Info	The subject's Public Key (RSA 2048		
Subject Put	one key mio	bits)	-	
Extended fi		Description of setting	critical	
	Key Identifier	SHA-1 hash for the issuer's Public Key		
Authority P	Xey Identifier	(160 bits)	n	
Subject Key	v Idoptifior	SHA-1 hash for the subject's Public Key	n	
Subject Rey	y Identifier	(160 bits)	11	
KeyUsage		digitalSignature	17	
ExtendedK	oullaga	OCSPSigning	<u> </u>	
		null	N N	
OCSP No C	JIIEUK		IN	l
Tablo 7 1-0	OCSP Rognandor (	Certificate Profile (Applicable to certificates is	sund by	
		RS OV RSA CA 2024 G1)	isueu Dy	
Basic field		Description of setting	critical	
Version		Version 3	-	
Serial Num	bor	Non-sequential values greater than	-	
Serial Num	iber	zero (0) and less than $2^{159}$ containing	-	
L		Zero (0) and less than 2~109 containing		

	JPRS CA Ce	rtificate Policy(変更履歴付)	
		64 bits of output from a CSPRNG	
Signature Algorithm		sha256 With RSA Encryption	-
Issuer	Country	C=JP	-
	Organization	O= Japan Registry Services Co., Ltd.	-
	Common Name	(1) Domain Validation	-
		CN=JPRS DV RSA CA 2024 G1	
		(2) Organization Validation	
		CN= JPRS OV RSA CA 2024 G1	
Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-
	NotAfter	E.g.) 2008/3/5 00:00:00 GMT	-
Subject	Country	C=JP (fixed value)	-
	Organization	Japan Registry Services Co., Ltd. (fixed	-
		value)	
	Common Name	Name of the OCSP server (mandatory)	-
Subject Pu	ablic Key Info	The subject's Public Key (RSA 4096	
-	-	bits , RSA 3072 bits or RSA 2048 bits)	
Extended	field	Description of setting	critical
Authority	Key Identifier	SHA-1 hash for the issuer's Public Key	n
		(160 bits)	
Subject K	ey Identifier	SHA-1 hash for the subject's Public Key	n
		(160 bits)	
KeyUsage		digitalSignature	у
Extended	KeyUsage	OCSPSigning	n
OCSP No	Check	null	n

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

JPRS DV ECC CA 2024 G1 of JPRS OV ECC CA 2024 G1)						
Basic field		Description of setting	critical			
Version		Version 3	-			
Serial Nun	nber	Non-sequential values greater than zero (0) and less than 2^159 containing	-			
		64 bits of output from a CSPRNG				
Signature	Algorithm	ecdsa-with-SHA384	-			
Issuer	Country	C=JP	-			
	Organization	O= Japan Registry Services Co., Ltd.	-			
	Common Name	(1) Domain Validation	-			
		CN=JPRS DV ECC CA 2024 G1	-			
		(2) Organization Validation				
		CN= JPRS OV ECC CA 2024 G1				
Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-			
	NotAfter	E.g.) 2008/3/5 00:00:00 GMT	-			
Subject	Country	C=JP (fixed value)	-			
	Organization	Japan Registry Services Co., Ltd. (fixed	-			
		value)				
	Common Name	Name of the OCSP server (mandatory)	-			
Subject Pu	blic Key Info	The subject's Public Key (256 bits or	-			
		384 bits)				
Extended f	ïeld	Description of setting	critical			
Authority ]	Key Identifier	SHA-1 hash for the issuer's Public Key	n			
		(160 bits)				
Subject Ke	y Identifier	SHA-1 hash for the subject's Public Key	n			
		(160 bits)				
KeyUsage		digitalSignature	У			
ExtendedK	· · · · · · · · · · · · · · · · · · ·	OCSPSigning	n			
OCSP No 0	Check	null	n			

	JI-NOON	Certificate Policy(整形版) 64 bits of output from a CSPRNG	
ignature A	Algorithm	sha256 With RSA Encryption	-
ssuer	Country	C=JP	-
55401	Organization	O= Japan Registry Services Co., Ltd.	-
	Common Name	(1) Domain Validation	-
		CN=JPRS DV RSA CA 2024 G1	
		(2) Organization Validation	
		CN= JPRS OV RSA CA 2024 G1	
alidity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-
v	NotAfter	E.g.) 2008/3/5 00:00:00 GMT	-
ubject	Country	C=JP (fixed value)	-
0	Organization	Japan Registry Services Co., Ltd. (fixed	-
	organization	value)	
	Common Name	Name of the OCSP server (mandatory)	-
ubiect Pu	blic Key Info	The subject's Public Key (RSA 4096	-
		bits , RSA 3072 bits or RSA 2048 bits)	
xtended f	ïeld	Description of setting	critical
uthority l	Key Identifier	SHA-1 hash for the issuer's Public Key	n
U	U C	(160 bits)	
ubject Ke	y Identifier	SHA-1 hash for the subject's Public Key	n
-		(160 bits)	
KeyUsage		digitalSignature	у
xtendedK	leyUsage	OCSPSigning	n
CSP No (	Check	null	n
RS DV EC		Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1)	
RS DV EC <mark>Basic field</mark>		Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1) Description of setting	issued by critical
RS DV EC	C CA 2024 G1 or JP	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1) Description of setting Version 3	
RS DV EC Basic field Version	C CA 2024 G1 or JP	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1) Description of setting	
RS DV EC Basic field Version	C CA 2024 G1 or JP	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than	
RS DV EC Basic field Version Berial Num	C CA 2024 G1 or JP	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing	
RS DV EC Basic field Version Berial Num Bignature A	C CA 2024 G1 or JP	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG	critical
RS DV EC Basic field Version Berial Num	C CA 2024 G1 or JP nber Algorithm Country Organization	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP O= Japan Registry Services Co., Ltd.	critical
RS DV EC Basic field Version Berial Num Bignature A	C CA 2024 G1 or JP ber Algorithm Country	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation	critical
RS DV EC Basic field Version Berial Num Bignature A	C CA 2024 G1 or JP nber Algorithm Country Organization	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS DV ECC CA 2024 G1	critical
RS DV EC Basic field Version Berial Num Bignature A	C CA 2024 G1 or JP nber Algorithm Country Organization	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation	critical
RS DV EC Basic field Version Berial Num Bignature A ssuer	C CA 2024 G1 or JP aber Algorithm Country Organization Common Name	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1	critical - - - - - -
RS DV EC Basic field Version Berial Num Bignature A	C CA 2024 G1 or JP aber Algorithm Country Organization Common Name NotBefore	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT	critical
RS DV EC Basic field Version Berial Num Bignature A ssuer	C CA 2024 G1 or JP ber Algorithm Country Organization Common Name NotBefore NotAfter	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2008/3/5 00:00:00 GMT	critical - - - - - -
RS DV EC Basic field Version Berial Num Bignature A ssuer	C CA 2024 G1 or JP aber Algorithm Country Organization Common Name NotBefore NotAfter Country	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2008/3/5 00:00:00 GMT C=JP (fixed value)	critical - - - - - -
RS DV EC Basic field Version Berial Num Bignature A ssuer	C CA 2024 G1 or JP ber Algorithm Country Organization Common Name NotBefore NotAfter	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2008/3/5 00:00:00 GMT	critical - - - - - -
RS DV EC Basic field Version Berial Num Bignature A ssuer	C CA 2024 G1 or JP aber Algorithm Country Organization Common Name NotBefore NotAfter Country Organization Common Name	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2008/3/5 00:00:00 GMT C=JP (fixed value) Japan Registry Services Co., Ltd. (fixed value) Name of the OCSP server (mandatory)	critical - - - - - -
RS DV EC Basic field Version Berial Num Bignature A ssuer	C CA 2024 G1 or JP aber Algorithm Country Organization Common Name NotBefore NotAfter Country Organization	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2008/3/5 00:00:00 GMT C=JP (fixed value) Japan Registry Services Co., Ltd. (fixed value) Name of the OCSP server (mandatory) The subject's Public Key (256 bits or	critical
RS DV EC Basic field Version Perial Num Prignature A ssuer Validity Pubject Pubject Pu	C CA 2024 G1 or JP aber Algorithm Country Organization Common Name NotBefore NotAfter Country Organization Common Name blic Key Info	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2008/3/5 00:00:00 GMT C=JP (fixed value) Japan Registry Services Co., Ltd. (fixed value) Name of the OCSP server (mandatory) The subject's Public Key (256 bits or 384 bits)	critical         -
RS DV EC Basic field Version Berial Num Bignature A ssuer Validity Subject Bubject Pu Extended f	C CA 2024 G1 or JP aber Algorithm Country Organization Common Name NotBefore NotAfter Country Organization Common Name blic Key Info ield	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2008/3/5 00:00:00 GMT C=JP (fixed value) Japan Registry Services Co., Ltd. (fixed value) Name of the OCSP server (mandatory) The subject's Public Key (256 bits or 384 bits) Description of setting	critical
RS DV EC Basic field Version Berial Num Bignature A ssuer Validity Subject Bubject Pu Extended f	C CA 2024 G1 or JP aber Algorithm Country Organization Common Name NotBefore NotAfter Country Organization Common Name blic Key Info	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2008/3/5 00:00:00 GMT C=JP (fixed value) Japan Registry Services Co., Ltd. (fixed value) Name of the OCSP server (mandatory) The subject's Public Key (256 bits or 384 bits)	critical         -
RS DV EC Basic field Version Ferial Num Fignature A ssuer Validity Subject Subject Pu Eubject Pu Eubject Pu	C CA 2024 G1 or JP aber Algorithm Country Organization Common Name NotBefore NotAfter Country Organization Common Name blic Key Info ield	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2008/3/5 00:00:00 GMT C=JP (fixed value) Japan Registry Services Co., Ltd. (fixed value) Name of the OCSP server (mandatory) The subject's Public Key (256 bits or 384 bits) Description of setting SHA-1 hash for the issuer's Public Key (160 bits) SHA-1 hash for the subject's Public Key	critical 
RS DV EC Basic field Version Berial Num Bignature A ssuer Validity Bubject Bubject Pu Subject Pu Subject Ke	C CA 2024 G1 or JP Algorithm Country Organization Common Name NotBefore NotAfter Country Organization Common Name blic Key Info ield Key Identifier	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN=JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2008/3/5 00:00:00 GMT C=JP (fixed value) Japan Registry Services Co., Ltd. (fixed value) Name of the OCSP server (mandatory) The subject's Public Key (256 bits or 384 bits) Description of setting SHA-1 hash for the issuer's Public Key (160 bits)	critical         -
RS DV EC Basic field Version Ferial Num Fignature A ssuer Validity Subject Subject Pu Eubject Pu Eubject Pu	C CA 2024 G1 or JP aber Algorithm Country Organization Common Name NotBefore NotAfter Country Organization Common Name blic Key Info field Key Identifier y Identifier	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2008/3/5 00:00:00 GMT C=JP (fixed value) Japan Registry Services Co., Ltd. (fixed value) Name of the OCSP server (mandatory) The subject's Public Key (256 bits or 384 bits) Description of setting SHA-1 hash for the issuer's Public Key (160 bits) SHA-1 hash for the subject's Public Key	critical         -

	JPRS CA		
		64 bits of output from a CSPRNG	
Signature		sha256 With RSA Encryption	-
Issuer	Country	C=JP	-
	Organization	O= Japan Registry Services Co., Ltd.	-
	Common Name	(1) Domain Validation	-
		CN=JPRS DV RSA CA 2024 G1	
		(2) Organization Validation	
<b>X7 1.1.</b>		CN= JPRS OV RSA CA 2024 G1	-
Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-
<u>a 1. (</u>	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 Pu	blic Key Info	The subject's Public Key (RSA 4096 bits, RSA 3072 bits or RSA 2048 bits)	-
Extended f	field	Description of setting	critical
	Key Identifier	SHA-1 hash for the issuer's Public Key	n
i i autior i toj i	ney raentiner	(160 bits)	11
Subject Ke	y Identifier	SHA-1 hash for the subject's Public Key	n
17 11		(160 bits)	
KeyUsage	7 TT	digitalSignature	У
Extended OCSP No (	· · ·	OCSPSigning null	n n
PRS DV EC		Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1)	
PRS DV EC <mark>Basic field</mark>		RS OV ECC CA 2024 G1) Description of setting	issued by critical
PRS DV EC <mark>Basic field</mark> Version	C CA 2024 G1 or JP	RS OV ECC CA 2024 G1)           Description of setting           Version 3	
	C CA 2024 G1 or JP	RS OV ECC CA 2024 G1)           Description of setting           Version 3           Non-sequential values greater than	
PRS DV EC <mark>Basic field</mark> Version	C CA 2024 G1 or JP	RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing	
PRS DV EC <mark>Basic field</mark> Version Serial Nun	CCCA 2024 G1 or JP	RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG	
PRS DV EC Basic field Version Serial Nun Signature	C CA 2024 G1 or JP	RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384	
PRS DV EC Basic field Version Serial Nun Signature	C CA 2024 G1 or JP nber Algorithm Country	RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP	
PRS DV EC Basic field Version Serial Nun Signature	C CA 2024 G1 or JP	RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384	
PRS DV EC Basic field Version Serial Nun Signature	C CA 2024 G1 or JP nber Algorithm Country Organization	RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP O= Japan Registry Services Co., Ltd.	
PRS DV EC Basic field Version Serial Nun Signature	C CA 2024 G1 or JP nber Algorithm Country Organization	RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation	
PRS DV EC Basic field Version Serial Nun Signature	C CA 2024 G1 or JP nber Algorithm Country Organization	RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS DV ECC CA 2024 G1	
RS DV EC Basic field Version Serial Nun Signature	C CA 2024 G1 or JP nber Algorithm Country Organization	RS OV ECC CA 2024 G1)           Description of setting           Version 3           Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG           ecdsa-with-SHA384           C=JP           O= Japan Registry Services Co., Ltd.           (1) Domain Validation           CN=JPRS DV ECC CA 2024 G1           (2) Organization Validation	
RS DV EC Basic field Version Serial Nun Signature . Issuer	Algorithm Country Organization Common Name	RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1	critical - - - - - -
PRS DV EC Basic field Version Serial Nun Signature Issuer	Algorithm Country Organization Common Name NotBefore	RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT	critical - - - - - -
PRS DV EC Basic field Version Serial Nun Signature Issuer	C CA 2024 G1 or JP nber Algorithm Country Organization Common Name NotBefore NotAfter	RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2008/3/5 00:00:00 GMT C=JP (fixed value) Japan Registry Services Co., Ltd. (fixed	critical - - - - - -
PRS DV EC Basic field Version Serial Nun Signature Issuer	Algorithm Country Organization Common Name NotBefore NotAfter Country Organization	RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2008/3/5 00:00:00 GMT C=JP (fixed value) Japan Registry Services Co., Ltd. (fixed value)	critical - - - - - - - - - - - - - -
PRS DV EC Basic field Version Serial Num Signature Issuer Validity Subject	Algorithm Country Organization Common Name NotBefore NotAfter Country Organization Common Name	RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2008/3/5 00:00:00 GMT C=JP (fixed value) Japan Registry Services Co., Ltd. (fixed value) Name of the OCSP server (mandatory)	critical - - - - - -
PRS DV EC Basic field Version Serial Nun Signature Issuer Validity Subject	Algorithm Country Organization Common Name NotBefore NotAfter Country Organization	RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2008/3/5 00:00:00 GMT C=JP (fixed value) Japan Registry Services Co., Ltd. (fixed value)	critical - - - - - - - - - - - - - -
PRS DV EC Basic field Version Serial Num Signature Issuer Validity Subject Subject Pu Extended f	Algorithm Algorithm Country Organization Common Name NotBefore NotAfter Country Organization Common Name blic Key Info field	RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2008/3/5 00:00:00 GMT C=JP (fixed value) Japan Registry Services Co., Ltd. (fixed value) Name of the OCSP server (mandatory) The subject's Public Key (256 bits or	critical - - - - - - - - - - - - - -
PRS DV EC Basic field Version Serial Num Signature Issuer Validity Subject Subject Pu Extended f	Algorithm Country Organization Common Name NotBefore NotAfter Country Organization Common Name blic Key Info	RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2008/3/5 00:00:00 GMT C=JP (fixed value) Japan Registry Services Co., Ltd. (fixed value) Name of the OCSP server (mandatory) The subject's Public Key (256 bits or 384 bits) Description of setting SHA-1 hash for the issuer's Public Key	critical
PRS DV EC Basic field Version Serial Num Signature Issuer Validity Subject Subject Pu Extended f Authority	Algorithm Algorithm Country Organization Common Name NotBefore NotAfter Country Organization Common Name blic Key Info field	RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2008/3/5 00:00:00 GMT C=JP (fixed value) Japan Registry Services Co., Ltd. (fixed value) Name of the OCSP server (mandatory) The subject's Public Key (256 bits or 384 bits) Description of setting SHA-1 hash for the issuer's Public Key (160 bits) SHA-1 hash for the subject's Public Key	critical 
PRS DV EC Basic field Version Serial Num Signature Issuer Validity Subject Subject Pu Extended f Authority	Algorithm Algorithm Country Organization Common Name NotBefore NotAfter Country Organization Common Name blic Key Info Field Key Identifier	RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN=JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2008/3/5 00:00:00 GMT C=JP (fixed value) Japan Registry Services Co., Ltd. (fixed value) Name of the OCSP server (mandatory) The subject's Public Key (256 bits or 384 bits) Description of setting SHA-1 hash for the issuer's Public Key (160 bits)	critical
PRS DV EC Basic field Version Serial Num Signature Issuer Validity Subject Subject Pu Extended f Authority Subject Ke KeyUsage	C CA 2024 G1 or JP anber Algorithm Country Organization Common Name NotBefore NotAfter Country Organization Common Name blic Key Info Common Name blic Key Info	RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN=JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2008/3/5 00:00:00 GMT C=JP (fixed value) Japan Registry Services Co., Ltd. (fixed value) Name of the OCSP server (mandatory) The subject's Public Key (256 bits or 384 bits) Description of setting SHA-1 hash for the issuer's Public Key (160 bits) SHA-1 hash for the subject's Public Key (160 bits) digitalSignature	critical
PRS DV EC Basic field Version Serial Num Signature Issuer Validity Subject Subject Pu Extended f Authority	C CA 2024 G1 or JP Algorithm Country Organization Common Name NotBefore NotAfter Country Organization Common Name blic Key Info Field Key Identifier Ender SeyUsage	RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN=JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2008/3/5 00:00:00 GMT C=JP (fixed value) Japan Registry Services Co., Ltd. (fixed value) Name of the OCSP server (mandatory) The subject's Public Key (256 bits or 384 bits) Description of setting SHA-1 hash for the issuer's Public Key (160 bits)	critical         -

#### 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 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.

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

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

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

#### 7.1.5 Name Constraints

Not set in the CA.

#### 7.1.6 Certificate Policy Object Identifier

The OID of the certificate issued by the CA is as described in this CP "1.2 Document Name and Identification".

The following Certificate Policy identifiers are reserved for use by the CA as an optional means of assertaing that a Certificate complies with Baseline Requirements.

[For DV certificate ] {joint-iso-itu-t(2) international-organizations(23) ca-browserforum(140) certificatepolicies(1) baseline-requirements(2) domain-validated(1)} (2.23.140.1.2.1)

[For OV certificate ] {joint-iso-itu-t(2) international-organizations(23) ca-browserforum(140) certificatepolicies(1) baseline-requirements(2) organization-validated(2)} for (2.23.140.1.2.2) (2)

#### JPRS CA Certificate Policy (整形版)

#### 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

#### 7.1.3 Algorithm Object Identifier

The algorithm OID used in this service is as follows:

The algorithm of B about months bervice is as	10110110
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 e in the Certification Path, the encoded content of the Issuer Distinguished I Certificate SHALL be byte-for-byte identical with the encoded form Distinguished Name field of the Issuing CA certificate.

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

Distinguished Names MUST NOT contain only metadata such as '.', '-', and characters, and/or any other indication that the value is absent, incomapplicable.

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

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

#### 7.1.5 Name Constraints

Not set in the CA.

#### 7.1.6 Certificate Policy Object Identifier

The OID of the certificate issued by the CA is as described in this CP "1.2 Do and Identification".

The following Certificate Policy identifiers are reserved for use by the CA means of assertaing that a Certificate complies with Baseline Requirements.

[For DV certificate ] {joint-iso-itu-t(2) international-organizations(2) forum(140) certificatepolicies(1) baseline-requirements(2) domai (2.23.140.1.2.1)

[For OV certificate] {joint-iso-itu-t(2) international-organizations(2) forum(140) certificatepolicies(1) baseline-requirements(2) organizatio (2.23.140.1.2.2)

	備考
CP.	
each Certificate Name field of a of the Subject	
e set forth in its of the Subject ne in a Subject	
d ' ' (i.e. space) mplete, or not	
ion or "common l domain name, ' the dNSName main Labels in are encoded as	
ocument Name	
as an optional	
3) ca-browser- in-validated(1)}	
3) ca-browser- on-validated(2)}	

#### 7.1.7 Use of Policy Constraint Extensions

Not set.

#### 7.1.8 Policy Qualifier Syntax and Semantics

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

#### 7.1.9 How to interpret Critical Certificate Policy Extensions

Not set.

#### 7.2 CRL Profile

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

#### Table 7.2.1 (Deleted)

Table 7.2.2 CRL Profile (applicable to certificates issued by JPRS DV RSA CA 2024 G1 or JPRS OV RSA CA 2024 G1)

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

\*: 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 A	lgorithm	SHA384 with RSAEncryption	-
Issuer	Country	C=JP	-
	Organization	O= Japan Registry Services Co., Ltd.	-
	Common Name	(1) Domain Validation	-
		CN= JPRS DV RSA CA 2024 G1	
		(2) Organization Validation	
		CN=JPRS OV RSA CA 2024 G1	
This Update	e	E.g.) 2008/3/1 00:00:00 GMT	-
Next Update Revoked Serial Number		E.g.) 2008/3/5 00:00:00 GMT	-
		E.g.) 0123456789	-
Certificate	Revocation Date	E.g.) 2008/3/1 00:00:00 GMT	-

	JPRS CA C	Certificate Policy(整形版)		備考
717100	of Policy Constr			
Not set.				
7.1.8 Polic	y Qualifier Synt	ax and Semantics		
For the policy	qualifier, the URI of	f the Web page that publishes this CP and C	CPS is store	d.
719How	to interpret Criti	ical Certificate Policy Extensions		
	to interpret criti			
Not set.				
<b>7.2 CRL P</b> I		y the CA shall be as described in the followi	ng table:	
-	-	,	8	
		le to certificates issued by JPRS DV RSA C	A 2024 G1 o	or
Basic field		Description of setting	critical	
Version		Version 2	-	
Signature A	0	SHA256 with RSAEncryption	-	
Issuer	Country	C=JP	-	
	Organization	O= Japan Registry Services Co., Ltd.	-	
	Common Name	(1) Domain Validation	-	
		CN=JPRS Domain Validation Authority - G4		
		(2) Organization Validation		
		CN=JPRS Organization Validation		
		Authority – G4		
This Update	e	E.g.) 2008/3/1 00:00:00 GMT	-	
Next Updat		E.g.) 2008/3/5 00:00:00 GMT	-	
Revoked	Serial Number	E.g.) 0123456789	-	
Certificate	Revocation Date	E.g.) 2008/3/1 00:00:00 GMT	-	
S	Reason Code	Revocation Reason Code (*)	-	
Extended fi CRL Numb		Description of setting           CRL number	critical	
	Key Identifier	SHA-1 hash for the issuer's Public Key	n n	
		(160 bits)		
		et one of the Revocation Reason code specific		
		on Code is "#0 unspecified", the "Reason Co	ode" field do	Des
not appear	in the CRL profile.			
Table 7.2.3 C	RL Profile (applicab	le to certificates issued by JPRS DV RSA C	A 2024 G1 d	or
	A CA 2024 G1)			
Basic field		Description of setting	critical	
Version		Version 2	-	
Signature A		SHA384 with RSAEncryption	-	
Issuer	Country	C=JP	-	
	Organization Common Name	O= Japan Registry Services Co., Ltd. (1) Domain Validation	-	
	Common Name	CN= JPRS DV RSA CA 2024 G1		
		(2) Organization Validation		
		CN=JPRS OV RSA CA 2024 G1		
This Updat	e	E.g.) 2008/3/1 00:00:00 GMT	-	
Next Updat		E.g.) 2008/3/5 00:00:00 GMT	-	
Revoked	Serial Number	E.g.) 0123456789	-	
Certificate	Revocation Date	E.g.) 2008/3/1 00:00:00 GMT		

	Certificate Policy(整形版)		備考
	aint Extangiana		
of Policy Constra	aint Extensions		
v Qualifier Svnt	ax and Semantics		
		CPS is stored.	
to interpret Criti	cal Certificate Policy Extensions		
ofile			
	y the CA shall be as described in the followi	ng table:	
-		0	
	le to certificates issued by JPRS DV RSA C.	A 2024 G1 or	
. GA 2024 G1)	Description of setting	critical	
	Version 2	-	
lgorithm	SHA256 with RSAEncryption	<u> </u>	
Country	C=JP	-	
Organization		-	
Common Name		-	
	-		
	Authority – G4		
9	E.g.) 2008/3/1 00:00:00 GMT	-	
e		-	
		-	
		-	
		critical	
er		n	
ley Identifier	SHA-1 hash for the issuer's Public Key	n	
	(160 bits)		
	on Code is "#0 unspecified", the "Reason Co	ode" field does	
In the CIVE prome.			
RL Profile (applicab	le to certificates issued by JPRS DV RSA C	A 2024 G1 or	
CA 2024 G1)			
		critical	
1		-	
	* =	-	
-		-	
Common Name	(1) Domain Validation	-	
	CN= JPRS DV RSA CA 2024 G1		
	(2) Organization Validation		
•	I ON-IDDO OV DOA OA 9094 O1		
	CN=JPRS OV RSA CA 2024 G1		
2	E.g.) 2008/3/1 00:00:00 GMT	-	
e e Serial Number		-	
	qualifier, the URI of to interpret Criti Ofile CRLs to be issued by Deleted) RL Profile (applicab CA 2024 G1) lgorithm Country Organization Common Name Serial Number Revocation Date Reason Code eld er ey Identifier son Code" field is se he Revocation Reass in the CRL profile. RL Profile (applicab CA 2024 G1) lgorithm Country Organization	to interpret Critical Certificate Policy Extensions  ofile CRLs to be issued by the CA shall be as described in the followi Deleted) RL Profile (applicable to certificates issued by JPRS DV RSA C CA 2024 G1)  Description of setting Version 2  lgorithm SHA256 with RSAEncryption Country C=JP Organization O= Japan Registry Services Co., Ltd. Common Name (1) Domain Validation CN=JPRS Organization Validation Serial Number E.g.) 2008/3/1 00:00:00 GMT Reason Code Revocation Reason Code (*) ed Description of setting r CRL number ey Identifier SHA-1 hash for the issuer's Public Key (160 bits) son Code" field is set one of the Revocation Reason code specifi he Revocation Reason Code is "#0 unspecified", the "Reason Co in the CRL profile. RL Profile (applicable to certificates issued by JPRS DV RSA C CA 2024 G1)  Description of setting Version 2 lgorithm SHA384 with RSAEncryption Country C=JP Organization O= Japan Registry Services Co., Ltd. Common Name (1) Domain Validation	qualifier, the URI of the Web page that publishes this CP and CPS is stored.         to interpret Critical Certificate Policy Extensions         ofile         CRLs to be issued by the CA shall be as described in the following table:         Deleted)         RL Profile (applicable to certificates issued by JPRS DV RSA CA 2024 G1 or CA 2024 G1)         Image: the transformation of setting issued by JPRS DV RSA CA 2024 G1 or CA 2024 G1         Image: transformation of setting issued by JPRS DV RSA CA 2024 G1 or CA 2024 G1         Image: transformation of setting issued by JPRS DV RSA CA 2024 G1 or CA 2024 G1         Image: transformation of setting issued by JPRS DV RSA CA 2024 G1 or CA 2024 G1         Organization 0       = Japan Registry Services Co., Ltd.         Common Name       (1) Domain Validation issued Validation Authority - G4         (2) Organization Validation CN=JPRS Organization Validation Authority - G4       -         (2) Organization Validation CN=JPRS Organization Validation Authority - G4       -         (2) Organization Reason Code (*)       -         Serial Number       E.g.) 2008/3/1 00:00:00 GMT       -         serial Number       E.g.) 2008/3/1 00:00:00 GMT

	JPRS CA C	Certificate Policy(整形版)	
717100	-	· · · · ·	
Not set.			
7.1.8 Polic	y Qualifier Synt	ax and Semantics	
			PS is store
1 0	-		
7.1.9 How	to interpret Criti	cal Certificate Policy Extensions	
Not set.			
	ofilo		
		the CA shall be as described in the followi	ng tahlo:
The prome of	Citils to be issued by	the OA shall be as described in the following	iig table.
Table 7.2.1 (I	Deleted)		
		le to certificates issued by JPRS DV RSA C	A 2024 G1
	A CA 2024 G1)		·,· 1
Basic field Version			critical
	lgorithm		-
Issuer	Country	C=JP	-
	Organization	O= Japan Registry Services Co., Ltd.	-
	Common Name	(1) Domain Validation	-
		-	
		÷	
		8	
This Update	9	E.g.) 2008/3/1 00:00:00 GMT	-
Next Updat		E.g.) 2008/3/5 00:00:00 GMT	-
Revoked			-
Certificate			-
s Extended fi			oritical
CRL Numbe			
			n
5	0	(160 bits)	
		-	
		on Code is "#0 unspecified", the "Reason Co	ode" field d
not appear	in the CRL profile.		
Table 7.2.3 C	RL Profile (applicab	le to certificates issued by JPRS DV RSA C	A 2024 G1
	2 CRL Profile (applicable to certificates issued by JPRS DV RSA CA 2024         RSA CA 2024 G1)         Id       Description of setting         Version 2       -         re Algorithm       SHA256 with RSAEncryption         Country       C=JP         Organization       O= Japan Registry Services Co., Ltd.         Common Name       (1) Domain Validation         CN=JPRS       Organization         CN=JPRS       Organization         CN=JPRS       Organization         CN=JPRS       Organization         CN=JPRS       Organization         Version 2       -         Common Name       (1) Domain Validation         CN=JPRS       Organization         Authority – G4       -         (2) Organization Validation       -         Authority – G4       -         date       E.g.) 2008/3/1 00:00:00 GMT         edate       E.g.) 0123456789         Revocation Date       E.g.) 2008/3/1 00:00:00 GMT         Reason Code       Revocation Reason Code (*)         Ghield       Description of setting         mber       CRL number         y Key Identifier       CRL number         y Key Identifier       SHA-1 hash for the issuer's		
Basic field		Description of setting	critical
Version			-
			-
Issuer	, , , , , , , , , , , , , , , , , , ,		-
			-
	Common Name		-
		CN=JPRS OV RSA CA 2024 G1	
This Update	9	E.g.) 2008/3/1 00:00:00 GMT	-
Next Updat		E.g.) 2008/3/5 00:00:00 GMT	-
Revoked	Serial Number	E.g.) 0123456789	-
Certificate	Revocation Date	E.g.) 2008/3/1 00:00:00 GMT	-

		JPRS CA Cer	tificate Policy(変更履歴付)	
	s Reason Code		Revocation Reason Code (*)	-
l	Extended fi	eld	Description of setting	critical
	CRL Number		CRL number	n
l	Authority Key Identifier		SHA-1 hash for the issuer's Public Key	n
			(160 bits)	

\*: The "Reason Code" field is set one of the Revocation Reason code specified in the table 7.2.2.1. If the Revocation Reason Code is "#0 unspecified", the "Reason Code" field does not appear in the CRL profile.

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

Basic field		Description of setting	critical
Version		Version 2	-
Signature Algorithm		ecdsa-with-SHA384	-
Issuer	Country	C=JP	-
	Organization	O= Japan Registry Services Co., Ltd.	-
	Common Name	(1) Domain Validation	-
		CN= JPRS DV ECC CA 2024 G1	
		(2) Organization Validation	
		CN=JPRS OV ECC CA 2024 G1	
This Update		E.g.) 2008/3/1 00:00:00 GMT	-
Next Update		E.g.) 2008/3/5 00:00:00 GMT	-
Revoked	Serial Number	E.g.) 0123456789	-
Certificate	Revocation Date	E.g.) 2008/3/1 00:00:00 GMT	-
s	Reason Code	Revocation Reason Code (*)	-
Extended field		Description of setting	critical
CRL Numb	er	CRL number	n
Authority Key Identifier		SHA-1 hash for the issuer's Public Key (160 bits)	n

\*: The "Reason Code" field is set one of the Revocation Reason code specified in the table 7.2.2.1. If the Revocation Reason Code is "#0 unspecified", the "Reason Code" field does not appear in the CRL profile.

#### 7.2.1 Version Number(s)

The CA applies CRL version 2.

#### 7.2.2 CRL 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)".

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,	

JPRS CA Ce		JPRS CA Ce	ertificate Policy(整形版)
	s	Reason Code	Revocation Reason Code (*)
	Extended field CRL Number Authority Key Identifier		Description of setting
			CRL number
			SHA-1 hash for the issuer's Public Key
			(160 bits)

\*: 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 I	ECC (
JPRS OV ECC CA 2024 G1)	

	, ellect ((1)	
Basic field Version		Description of setting
		Version 2
Signature A	lgorithm	ecdsa-with-SHA384
Issuer	Country	C=JP
	Organization	O= Japan Registry Services Co., Ltd.
	Common Name	(1) Domain Validation
		CN= JPRS DV ECC CA 2024 G1
		(2) Organization Validation
		CN=JPRS OV ECC CA 2024 G1
This Update	e	E.g.) 2008/3/1 00:00:00 GMT
Next Update		E.g.) 2008/3/5 00:00:00 GMT
Revoked	Serial Number	E.g.) 0123456789
Certificate	<b>Revocation</b> Date	E.g.) 2008/3/1 00:00:00 GMT
s	Reason Code	Revocation Reason Code (*)
Extended fi	eld	Description of setting
CRL Numbe	er	CRL number
Authority K	ley Identifier	SHA-1 hash for the issuer's Public Key
		(160 bits)

\*: The "Reason Code" field is set one of the Revocation Reason code specified in the table 7.2.2.1. If the Revocation Reason Code is "#0 unspecified", the "Reason Code" field does not appear in the CRL profile.

#### 7.2.1 Version Number(s)

The CA applies CRL version 2.

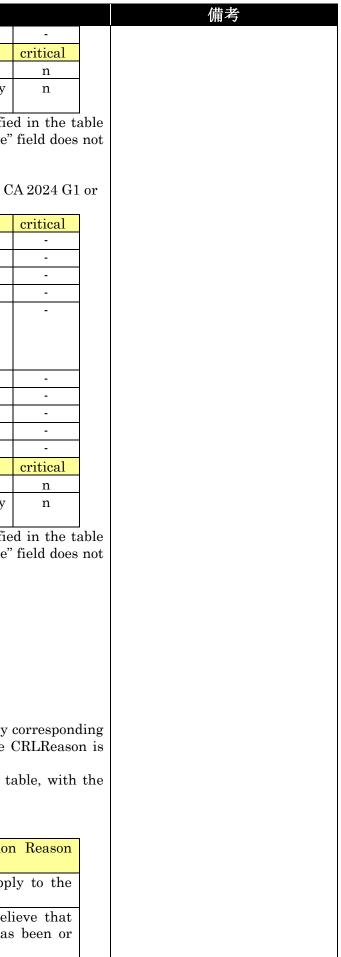
#### 7.2.2 CRL Entry Extensions

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)".

	Revocation Reason Code	Circumstances for setting this Revocation	
		Code	
F	#0 unspecified	When the reason codes below do not app	
		revocation request.	
F	#1 keyCompromise	When the Subscriber have reasons to bel	
		the private key of their certificate has	
		may be compromised,	



JPRS CA Certificate Policy(変更履歴付)		
#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.

# 8. Compliance Audit and Other Assessments

#### 8.1 Frequency and Circumstances of Assessment

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

### 8.2 Identity/Qualifications of Assessor

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

Audits required for obtaining the WebTrust certification shall be performed by audit corporations with the following qualifications and skills:

- Independence from the subject of the audit;
- The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme
- 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;
- licensed by WebTrust; -
- Bound by law, government regulation, or professional code of ethics; and
- Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage

### 8.3 Assessor's Relationship to Assessed Entity

Auditors shall be operationally independent of the auditee divisions, except in matters related to the audits.

#### 8.4 Topics Covered by Assessment

Audits shall be performed mainly to verify whether or not the CA is operated in compliance with this CP and the CPS. The CA shall undergo WebTrust in accordance with one of the

JPRS CA	Certificate Policy(整形版)	備考
#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	
<i>no</i> privilege withdrawn	obligations under the Terms and Conditions.	
7.3 OCSP Profile		
7.3.1 Version Number(s)		
The CA shall apply OCSP Versio	on 1.	
7.3.2 OCSP Extensions		
Refer to Section 7.1 of this CP.		ID
The singleExtensions of an OC 2.5.29.21) CRL entry extension.	CSP response MUST NOT contain the reasonCode (O	
2.5.29.21) CRL entry extension.		
8 Compliance Aug	dit and Other Assessments	
0: Compliance Aut	and other Assessments	
8.1 Frequency and Circ	umstances of Assessment	
	ast once a year to verify whether or not the CA is operat	ted
in compliance with this CP and		
	<i></i>	
8.2 Identity/Qualification		
Compliance audits shall be performed by auditors who are adequately experienced in		
auditing. Audits required for obtaining	the WebTrust contification shall be newformed by	dit
	the WebTrust certification shall be performed by au qualifications and skills:	
corporations with the following of	quanneations and skills.	
- Independence from the s	ubject of the audit;	
- The ability to conduct an	audit that addresses the criteria specified in an Eligible	
Audit Scheme	r · · · · · · · · · · · · · · · · · · ·	
- Employs individuals who	have proficiency in examining Public Key Infrastructur	e
1 0	security tools and techniques, information technology and	
security auditing, and the third-party attestation function;		
- licensed by WebTrust;		
- Bound by law, governme	nt regulation, or professional code of ethics; and	
• • •	Internal Government Auditing Agency, maintains	
Professional Liability/Errors & Omissions insurance with policy limits of at least		
one million US dollars in		
8.3 Assessor's Relationship to Assessed Entity		
Auditors shall be operationally independent of the auditee divisions, except in matters		
related to the audits.		
8.4 Topics Covered by A	Assessment	
•	ly to verify whether or not the CA is operated in complian	
-	CA shall undergo WebTrust in accordance with one of t	
mui uno or anu une or o. The	or onall undergo web i use in accordance with one of	

following schemes: - WebTrust for CAs - WebTrust for CAs SSL Baseline with Network Security	following schemes: - WebTrust for CAs - WebTrust for CAs SSL Baseline with Network Security
<b>8.5 Actions Taken as a Result of Deficiency</b> The CA shall promptly take necessary corrective actions with respect to any deficiencies pointed out in an audit report.	<b>8.5 Actions Taken as a Result of Deficiency</b> The CA shall promptly take necessary corrective actions with respect to a pointed out in an audit report.
<ul> <li>8.6 Communication of Results</li> <li>Auditors shall report the audit results to the CA.</li> <li>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.</li> <li>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.</li> </ul>	<ul> <li>8.6 Communication of Results</li> <li>Auditors shall report the audit results to the CA.</li> <li>The CA will not externally disclose the audit results unless the CA is required the same under any law, or by an associated organization based on an a JPRS, or unless such disclosure has been approved by the CA's Certific Conference.</li> <li>Reports on validation under the WebTrust shall be made referable in according to the provisions of the respective guidelines of the WebTrust.</li> </ul>
<b>8.7 Self-Audits</b> 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.	<b>8.7 Self-Audits</b> The CA shall monitor adherence this CP, the CPS, and strictly control its se performing self audits on at least a quarterly basis against a randomly sel at least three percent of the Certificates issued by it during the period immediately after the previous self-audit sample was taken.
9. Other Business and Legal Matters	9. Other Business and Legal Matters
<b>9.1 Fees</b> To be separately stipulated.	<b>9.1 Fees</b> To be separately stipulated.
<b>9.2 Financial Responsibility</b> The CA shall maintain a sufficient financial foundation required for operating and maintaining the CA.	<b>9.2 Financial Responsibility</b> The CA shall maintain a sufficient financial foundation required for maintaining the CA.
9.3 Confidentiality of Business Information	9.3 Confidentiality of Business Information
9.3.1 Scope of Confidential Information	9.3.1 Scope of Confidential Information
Stipulated in the CPS.	Stipulated in the CPS.
9.3.2 Information not within the Scope of Confidential Information	9.3.2 Information not within the Scope of Confidential Information
Stipulated in the CPS.	Stipulated in the CPS.
<b>9.3.3 Responsibility to Protect Confidential Information</b> Stipulated in the CPS.	<b>9.3.3 Responsibility to Protect Confidential Information</b> Stipulated in the CPS.
<b>9.4 Privacy of Personal Information</b> Stipulated in the CPS.	<b>9.4 Privacy of Personal Information</b> Stipulated in the CPS.
9.5 Intellectual Property Rights	9.5 Intellectual Property Rights
Unless separately agreed, all intellectual property rights pertaining to the following information shall belong to JPRS:	Unless separately agreed, all intellectual property rights pertaining to information shall belong to JPRS:
$\cdot$ certificates and site seals issued by the CA, as well as information on certificate	$\cdot$ certificates and site seals issued by the CA, as well as information on $c$
<ul><li>revocation;</li><li>this CP, the CPS, and related documents;</li></ul>	<ul><li>revocation;</li><li>this CP, the CPS, and related documents;</li></ul>
<ul> <li>Public Keys and Private Keys of the CA; and</li> </ul>	<ul> <li>Public Keys and Private Keys of the CA; and</li> </ul>
<ul> <li>software provided by JPRS.</li> </ul>	<ul> <li>software provided by JPRS.</li> </ul>
This CP is published under the Creative Commons license Attribution- NoDerivatives (CC-	This CP is published under the Creative Commons license Attribution- NoD
	40/44

JPRS CA Certificate Policy(整形版)

JPRS CA Certificate Policy(変更履歴付)

	(供 共
	佩考
any deficiencies	
uired to disclose	
agreement with icate Operation	
a specific site	
a specific site	
ervice quality by ected sample of	
od commencing	
operating and	
operating and	
mation	
o the following	
certificate	
Derivatives (CC-	

# BY-ND) 4.0 International.

#### 9.6 Representations and Warranties

#### 9.6.1 CA Representations and Warranties

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

- securely generate and manage the CA's Private Keys;
- accurately manage certificate issuance and revocation based on applications from the RA;
- monitor and operate the CA's system at work; and
- issue and publish the CRLs.

#### 9.6.2 RA Representations and Warranties

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

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

#### 9.6.3 Subscriber Representations and Warranties

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

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

- 1. Accuracy of Information: An obligation and warranty to provide accurate and complete information at all times to the CA, both in the certificate request and as otherwise requested by the CA in connection with the issuance of the Certificate(s) to be supplied by the CA;
- 2. **Protection of Private Key**: An obligation and warranty by the Applicant to take all reasonable measures to assure control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token);
- 3. Acceptance of Certificate: An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy;
- 4. **Use of Certificate**: An obligation and warranty to install the Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate, and to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use;
- 5. **Reporting and Revocation**: An obligation and warranty to: a. promptly request revocation of the Certificate, and cease using it and its associated Private Key, if

#### JPRS CA Certificate Policy (整形版)

BY-ND) 4.0 International.



#### 9.6 Representations and Warranties

#### 9.6.1 CA Representations and Warranties

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

- securely generate and manage the CA's Private Keys;
- accurately manage certificate issuance and revocation based on applica RA;
- monitor and operate the CA's system at work; and
- issue and publish the CRLs.

#### 9.6.2 RA Representations and Warranties

The CA shall bear the following obligations in performing its business operat

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

#### 9.6.3 Subscriber Representations and Warranties

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

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

- 9. Accuracy of Information: An obligation and warranty to provide accur complete information at all times to the CA, both in the certificate reotherwise requested by the CA in connection with the issuance of the to be supplied by the CA;
- 10. **Protection of Private Key**: An obligation and warranty by the Applica reasonable measures to assure control of, keep confidential, and propall times the Private Key that corresponds to the Public Key to be inc requested Certificate(s) (and any associated activation data or device, or token);
- 11. Acceptance of Certificate: An obligation and warranty that the Subscreview and verify the Certificate contents for accuracy;
- 12. Use of Certificate: An obligation and warranty to install the Certificat servers that are accessible at the subjectAltName(s) listed in the Cert use the Certificate solely in compliance with all applicable laws and s accordance with the Subscriber Agreement or Terms of Use;
- 13. **Reporting and Revocation**: An obligation and warranty to: a. promptly revocation of the Certificate, and cease using it and its associated Pri

	備考
	して UHI UHI して して して して して して して して して して
erations as the	
ations from the	
tions as an RA: m;	
ons for	
in processing	
se, that the efit of the CA	
ing on the	
under a warranties:	
rate and quest and as	
e Certificate(s)	
ant to take all	
perly protect at cluded in the	
e, e.g. password	
.1 .11	
eriber will	
ate only on	
tificate, and to solely in	
-	
ly request	
ivate Key, if	

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

- 6. **Termination of Use of Certificate**: An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise.
- 7. **Responsiveness**: An obligation to respond to the CA's instructions concerning Key Compromise or Certificate misuse within a specified time period.
- 8. Acknowledgment and Acceptance: An acknowledgment and acceptance that the CA is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber Agreement or Terms of Use or if revocation is required by the CA's CP, CPS, or these Baseline Requirements.

#### 9.6.4 Relying Party Representations and Warranties

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

#### 9.6.5 Representations and Warranties of Other Participants

No stipulation.

#### 9.7 Disclaimer of Warranties

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

#### 9.8 Limitations of Liability

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

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

#### JPRS CA Certificate Policy (整形版)

there is any actual or suspected misuse or compromise of the Subscrib Key associated with the Public Key included in the Certificate, and be request revocation of the Certificate, and cease using it, if any inform Certificate is or becomes incorrect or inaccurate;

- 14. **Termination of Use of Certificate**: An obligation and warranty to produse of the Private Key corresponding to the Public Key included in the upon revocation of that Certificate for reasons of Key Compromise.
- 15. **Responsiveness**: An obligation to respond to the CA's instructions con Compromise or Certificate misuse within a specified time period.
- 16. Acknowledgment and Acceptance: An acknowledgment and acceptance is entitled to revoke the certificate immediately if the Applicant were terms of the Subscriber Agreement or Terms of Use or if revocation is the CA's CP, CPS, or these Baseline Requirements.

#### 9.6.4 Relying Party Representations and Warranties

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

#### 9.6.5 Representations and Warranties of Other Participants

No stipulation.

#### 9.7 Disclaimer of Warranties

The CA is not liable for any indirect, special, incidental, or consequential dar connection with any of the warranties stipulated in "9.6.1 CA Repres Warranties" of this CP, or for lost profits, loss of data, or any oth consequential damage whatsoever.

#### 9.8 Limitations of Liability

The CA is not liable for the provisions of "9.6.1 CA Representations and War CP if damage falling under any of the following occurs:

- any or all damage arising from any unlawful conduct, unauthorized use or any other cause not attributable to the CA;
- any damage resulting from a failure of a Subscriber to perform any of l obligations;
- any or all damage arising from any cause attributable to a Subscriber's
- any damage arising from any defect or malfunction, or operation, of the software of the CA or a Subscriber;
- any damage caused by any information published in a certificate or the reason not attributable to the CA;
- any or all damage incurred by a failure in normal communication cause reason not attributable to the CA;
- any or all damage arising in connection with the use of a certificate, su debts;
- any damage caused by an improvement, beyond expectations at this po the cryptographic algorithm decoding capabilities of hardware or softw
- any or all damage caused by the suspension of the CA's business opera force majeure event, including, but not limited to, any act of God, earth volcanic eruption, fire, tsunami, flood disaster, lightning strike, war, ci or terrorism; or
- any or all damage arising concomitantly with, or in connection with, republication on the CT log server of information necessary for certificate

	備考
iber's Private b. promptly nation in the	
omptly cease all he Certificate	
ncerning Key	
nce that the CA e to violate the is required by	
of this CP. If Party shall	
5	
mage arising in esentations and her indirect or	
rranties" of this	
se, negligence,	
his/her/its	
's system; ne hardware or	
e CRL, for any	
sed by any	
uch as business	
oint in time, in vare; ations due to a hquake, tivil commotion	
egistration and te issuance.	

#### 9.9 Indemnities

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

#### 9.10 Term and Termination

#### 9.10.1 Term

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

#### 9.10.2 Termination

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

#### 9.10.3 Effect of Termination and Survival

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

#### 9.11 Individual Notices and Communications with Participants

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

#### 9.12 Amendments

#### 9.12.1 Procedure for Amendment

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

#### 9.12.2 Notification Mechanism and Period

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

#### 9.12.3 Circumstances under Which OID Must Be Changed

No stipulation.

#### 9.13 Dispute Resolution Provisions

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

#### 9.14 Governing Law

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

#### JPRS CA Certificate Policy (整形版)

#### 9.9 Indemnities

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

#### 9.10 Term and Termination

#### 9.10.1 Term

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

#### 9.10.2 Termination

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

#### 9.10.3 Effect of Termination and Survival

Even in the event of termination of an agreement on use or the like betwee and the CA, or termination of the CA itself, any provisions of this CP that such termination, by the nature thereof, shall continue to apply to Subscr Parties, and the CA, regardless of the reason of such termination.

#### 9.11 Individual Notices and Communications with Partic

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

#### 9.12 Amendments

#### 9.12.1 Procedure for Amendment

This CP may be revised at the discretion of the CA, as appropriate, and the shereof shall come into effect upon approval of the CA's Certificate Operation

#### 9.12.2 Notification Mechanism and Period

If the CA amends this CP, the CA shall promptly publish the amended vers which shall be deemed to be a notification thereof to Subscribers.

#### 9.12.3 Circumstances under Which OID Must Be Changed

No stipulation.

#### 9.13 Dispute Resolution Provisions

If any party, for the purpose of resolving a dispute over the use of a certificat a lawsuit, refer the dispute to arbitration, or take any other legal action a such party shall notify the CA to that effect in advance. The Tokyo Distr have the agreed exclusive jurisdiction over all disputes involving the Servi instance.

#### 9.14 Governing Law

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

the CA or any ng, and trusting abilities include performance, or and Conditions	備考
tion Conference. ation stipulated	
in "9.10.3 Effect	
en a Subscriber should survive cribers, Relying	
<b>cipants</b> its Web site, by	
revised version Conference.	
rsion of this CP,	
ate, seeks to file against the CA, rict Court shall ices in the first	
s of Japan shall r the use of a	

#### 9.15 Compliance with Applicable Laws

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

#### 9.16 Miscellaneous Provisions

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.

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.

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.

9.17 Other Provisions

Not applicable.

#### JPRS CA Certificate Policy (整形版)

#### 9.15 Compliance with Applicable Laws

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

#### 9.16 Miscellaneous Provisions

In the event of a conflict between these Requirements and a law, regulation order (hereinafter 'Law') of any jurisdiction in which the CA operates or issue the CA MAY modify any conflicting requirement to the minimum extent nece the requirement valid and legal in the jurisdiction. This applies only to certificate issuances that are subject to that Law. In such event, th immediately (and prior to issuing a certificate under the modified requirem Section 9.16.3 of the CA's CPS a detailed reference to the Law requiring a these Requirements under this section, and the specific modificat Requirements implemented by the CA.

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

Any modification to the CA practice enabled under this section MUST be and when the Law no longer applies, or these Requirements are modifipossible to comply with both them and the Law simultaneously. An appropripractice, modification to the CA's CPS and a notice to the CA/Browser Foruabove, MUST be made within 90 days.

### 9.17 Other Provisions

Not applicable.

	備考
l law applicable operates.	
or government ues certificates, essary to make o operations or he CA SHALL hent) include in modification of tion to these	
irement) notify S by sending a been posted to s available at d links as the ble revisions to	
discontinued if ied to make it riate change in um, as outlined	