Appendix 1

JPNIC 資源管理認証局 認証業務規定

第１版 英語訳

<Appendix１について >

- この資料は、JPNIC 資源管理認証局の認証業務規程を英訳したものである。
  - 諸外国の技術者による内容の理解を図るために翻訳されたものである。
    正確な内容確認には原文を参照する必要がある。

JPNIC Resource Service Certification Authority Certification Practice Statement

Version 1.0

Japan Network Information Center

CONTENTS

1. Introduction 1
1.1. Overview 1
1.2. Documentation Name and Identification 1
1.3. Individuals and Entities related to the PKI 3
1.4. Certificate Usage Methods 6
1.5. Policy Management 7
1.6. Definitions and Abbreviations 8
2. Disclosure and Repository Liability 10
2.1. Repository 10
2.2. Certification Information Disclosure 10
2.3. Disclosure Timing and Frequency 10
2.4. Repository Access Management 11
3. Identification and Authentication 12
3.1. Name Determination 12
3.2. Initial Authentication of Individual or Entity 13
3.3. Identification and Authentication of Individual or Entity when Applying for Key Update 15
3.4. Identification and Authentication of Individual or Entity during Certificate Revocation Application 15
4. Operational Requirements concerning Certificate Lifecycle 16
4.1. Certificate Application 16
4.2. Certificate Application Procedures 17
4.3. Certificate Issue 19
4.4. Certificate Receipt Confirmation 20
4.5. Utilization of Key Pairs and Certificates 21
4.6. Certificate Updating 22
4.7. Certificate Key Updating 23
4.8. Certificate Revision 24
4.9. Certificate Revocation and Temporary Suspension 25
4.10. Certificate Status Confirmation Service 29
4.11. Registration Completion 29
4.12. Key Escrow and Key Recovery 29
5. Facility, Management, and Operational Controls 30
5.1. Physical Controls 30
5.2. Procedural Controls 32
5.3. Personnel Controls 33
5.4. Audit Log Procedures 35
5.5. Record Storage 37
5.6. Key Switching 39
5.7. Recovery from Key Compromise and Disasters 40

5.8. Termination of Certification Authority or Registration Authority Practices 41
6. Technical Security Management 42
6.1. Key Pair Generation and Installation 42
6.2. Private Key Protection and Cryptographic Module Technical Administration 44
6.3. Other Key Pair Administration 46
6.4. Activated Data 47
6.6. Administration of Life Cycle Technology 48
6.7. Network Security Management 48
6.8. Time-stamps 48
7. Profiles of Certificates, Certificate Revocation Lists, and OCSP Profiles 49
7.1. Certificate Profile 49
7.2. Profile of Certificate Revocation List 52
7.3. OCSP Profile 54
8. Compliance Audit and Other Assessments 55
8.1. Assessment Frequency and Circumstances requiring Assessment 55
8.2. Identity and Qualifications of Assessor 55
8.3. Relationship between the Assessor and the Entity Assessed 55
8.4. Items covered by the Assessment 55
8.5. Measures taken in Event of Unsatisfactory Results 55
8.6. Assessment Result Information Exchange 56
9. Problems relating to Other Practices and Legal Problems 57
9.1. Fees 57
9.2. Financial Liability 57
9.3. Information Confidentiality 57
9.4. Protection of Personal Data Privacy 59
9.5. Intellectual Property Rights 61
9.6. Representation Warranties 62
9.7. Limitations of Warranty 63
9.8. Limitations of Liability 64
9.9. Indemnity 65
9.10. Periods of Validity and Termination 65
9.11. Individual Notification and Contact between Related Persons 66
9.12. Amendments 66
9.13. Dispute Resolution Procedures 66
9.14. Governing Law 67
9.15. Compliance with Applicable Laws 67
9.16. Miscellaneous Regulations 67
9.17. Other Provisions 67

1. Introduction

1.1. Overview

This JPNIC Resource Service Certification Authority Certification Practice Statement (CPS) defines operational practices of JPNIC Resource Service Certification Authority (the Certification Authority) which issues digital certificates that are used in various authentications relating to IP addresses and AS numbers between Japan Network Information Center (JPNIC) and IP Address Management Agents.

Based on this CPS, the Certification Authority provides various certification services, such as issuing certificates, to persons belonging to the IP Address Management Agents who conduct various application processing practices (Resource Holders). The Certification Authority is operated on an experimental basis.

The structure of this CPS conforms to the RFC3647 Certificate Policy and Certification Practices Statement Framework standardized by the IETF PKIX WG.

The Certification Authority does not determine each of CP (Certificate Policy) and CPS (Certification Practices Statement) as independent items; rather it stipulates certificate policy and operations statement as this CPS.

Concerning a provision of certification practices, JPNIC comprehensively determines its own policies and obligations of certificate subjects and relying parties in this CPS and the certificate subject agreement. Note that if there is variance between the content of this CPS and the certificate subject agreement, the certificate subject agreement shall be given priority in application.

This CPS is disclosed on JPNIC CA's Website at http://jpnic-ca.nic.ad.jp/ in order that it may be viewed at any time by certificate subjects and relying parties.

(1) CPS
The CPS is a document that describes certificate purposes, applicable ranges certificate profiles, identification methods and certificate subject key administrations, together with the general regulations relating to certification practices. This CPS refers whenever necessary to the certificate subject agreement.

(2) Certificate Subject Agreement
The certificate subject agreement is a document that describes various practices for use of the certification service between subscribers and JPNIC, including details of certification services and obligations of subscribers.

1.2. Documentation Name and Identification

The official name of this CPS is the "JPNIC Resource Service Certification Authority

Certification Practice Statement".

The object identifiers relating to JPNIC and the Certification Authority are shown in Table 1.1.

Table 1-1. Object Identifiers(OID) for JPNIC and JPNIC Resource Service Certification Authority

Object	Object Identifier
Japan Network Information Center	1.2.392.200175
JPNIC Resource Service Certification Authority Certification Practice Statement (CPS)	1.2.392.200175.1.2.1
End-entity Certification Policy	1.2.392.200175.1.2.1

1.3. Individuals and Entities related to the PKI

1.3.1. Certification Authority, Registration Authority, Certificate Subjects, and Relying Parties

The community of individuals or entities related to the PKI to whom the Certification Authority distributes certificates includes the participants shown in Table 1-2.

Table 1-2 Participants and Roles relating to the Community

Participant	Abbreviated Name	Role and Explanation
Resource Subscriber		Individuals or entities conducting IP address and AS number assignment and return practices.
Server		JPNIC server utilized in the certification practices
Resource Subscriber Certificate		Certificate issued to resource subscribers.
Contract/Resource Administrator		Individuals or entities conducting resource subscriber appointment, removal, and custody.
Contract/Resource Administrator Certificate		One of the operations certificates required for the Certification Authority certification practices. It is the certificate required for certification of contract/resource administrators when issuing certificates to resource subscribers. Concerning the handling of this certificate, management and operations are carried out while strictly following the operation regulations.
JPNIC Staff Certificate		One of the operations certificates required for the Certification Authority certification practices. It is the certificate issued for JPNIC staffs conducting practices such as management of contract/resource administrator identifiers in the IP registry system.
End-entity	EE	General name for subjects of certificate issuing, such as resource subscribers, contract/resource administrators, and JPNIC staffs.
End-entity Certificate	EE Certificate	General name for certificates issued to end-entities.

Participant	Abbreviated Name	Role and Explanation
Certificate Subscriber	Subscriber	Individuals or entities that are subscribing to certificates.
Certificate Subject	Subject	Signifies individuals or entities that have carried out certificate issue application, generated their own key, and have had certificates issued by the Certification Authority. In this CPS, this means individuals or entities that are EE certificate subjects, or server administrators.
Relying Party	RP	Individuals or entities that receive certificates, and who use these certificates for verification, carrying out their actions based on the certificate and/or a digital signature.
JPNIC Issuing Authority	JPNIC IA	General name for the Issuing Authority inside JPNIC Primary Root Certification Authority and the Issuing Authority inside JPNIC Resource Service Certification Authority. It is a conducting role that administers the certificate issuing practices in JPNIC Primary Root Certification Authority and JPNIC Resource Service Certification Authority. It issues certificates that have been requested from RA. It is used inside the Certification Authority (CA) in the situation where the certification administration functions, including certificate issuing and revocation, are to be shown.
JPNIC Registration Authority	JPNIC RA	A conducting role that confirms that the subscriber for the certificate issue is the correct individual or entity, and mainly administers registration and revocation practices. Takes responsibility for confirming and authenticating the certificate subject.
Trustee in Charge		This is the trustee in charge of JPNIC security operations, who determines JPNIC Certification Authority operations policy.
CA (Certification Authority) Operator	CAO	Individual or entity that operates and administers the Certification Authority system, including the CA Server and Directory Server.
RA (Registration Authority) Operator	RAO	Individual or entity that manages and operates Registration Authority (RA). Carries out registration work for certificate issuing and revocation.

Participant	Abbreviated Name	Role and Explanation
Repository		Database where certificates signed by the Certification Authority and CRLs are stored and published.
JPNIC Primary Root Certification Authority		This is the Root Certification Authority of all the Certification Authorities operated by JPNIC. It is positioned at the top of the certification hierarchy route in JPNIC, and carries out self-signing as well as the electronic signing of certificates for subordinate downstream Certification Authorities (Resource Service Certification Authority etc).
JPNIC Resource Service Certification Authority		This is the Certification Authority that carries out issuing of certificates relating to IP address administration practices operated by JPNIC. JPNIC Resource Service Certification Authority certificates are electronically signed by JPNIC Primary Root Certification Authority.
JPNIC Certification Authorities		General name for the Certification Authorities operated by JPNIC.
Local RA		This is an conducting role or group different from a role that issues certificates. In RA practices, this role carries out identification and judging of the correct individual or entity, certificate issue application processing, and certificate revocation processing. In the case of JPNIC Certification Authority, the IP Address Management Agents are Local RAs.
Local RA Manager		Manager of Local RA practices in the IP Address Management Agent, who conducts the appointment and removal of contract/resource administrators.
Contract/resource Administrator	Agreement/ Resource Administrator	Carries out resource subscriber member administration and certification, and resource subscriber certificate issue application operations inside the IP Address Management Agent.

1.3.2. Other Related Individuals or Entities

Not prescribed.

1.4. Certificate Usage Methods

1.4.1. Appropriate Usage of Certificates

Certificates issued according to this CPS are used by JPNIC's registry system for authentication of users and messages for the purpose of various applications and communications in IP address administration practices carried out by JPNIC.

1.4.2. Prohibited Usage of Certificates

Certificates issued according to this CPS are intended for use in various application processing operations in JPNIC. Although JPNIC does not restrict mutual use of certificates between resource subscribers of IP Address Management Agents, it does not accept any liability for use in this way.

1.4.3. Inter-operability

JPNIC Certification Authority may carry out reciprocal certification with another Certification Authority.

1.5. Policy Management

1.5.1. Organization Administrating the Documentation, and Contact Details

The organization administrating this CPS, and its contact details, are described as follows:

Japan Network Information Center

Inquiries accepted: Monday to Friday 10:00-18:00 (Excepting year-end, new year and public holidays)

E-mail address: ca-query@nic.ad.jp

1.5.2. Person determining CPS Policy Compatibility

JPNIC trustee in charge will conduct judgment of whether or not the CPS is compatible with the Certification Authority's operational polices.

1.5.3. CPS Approval Procedures

Revisions to this CPS will be disclosed after approval has been received from the trustee in charge.

1.6. Definitions and Abbreviations

The terms used in this CPS are as shown in Table 1-3.

Table 1-3 Terms Used

Term	Abbreviation	Explanation
Digital Certificate	Certificate	This is a digital document which certifies that the content described using a certain public key is held by the sender. The digital signing of the document by the Certification Authority ensures its correctness. In this CPS, provided there are no special restrictions, the resource subscriber certificate, server's certificate, and operations certificate are all known under the general name of "certificate".
Certification Authority	CA	This is a conducting role that carries out certificate issuing, update, and revocation, private key generation and protection, and certificate subscriber registration. In this CPS, in cases where only Certification Authority is mentioned, it includes the certificate issuing practices and the registration practices.
RFC 3647 (Request For Comments 3647)		Support framework for writers of CPS for Certification Authorities and PKI.
Object Identifier	OID	This is a name of identifier registered in a registration organization (such as ISO or ITU) that will become globally unique. Registered items such as the algorithm used by the PKI, the name stored in certificates (subject), and types (attributes such as the country name) and other items are used as object identifiers.
X.509		Format of certificates and certificate revocation lists standardized in ITU-T. In X.509 v3, extension fields are added for further optional information.
Public Key		This is the key that is made public which corresponds to the private key. The public key is utilized in encryption method and in verification method for signatures.

Term	Abbreviation	Explanation
Private Key		This is the key corresponding to the public key which is held only by the individual or entity concerned.
Certificate Signing Request	CSR	This is the data format makes the basis when issuing a certificate. The CSR includes the public key of the individual or entity requesting the certificate issuerance and the certificate is issued with the signature of the issuer to certify this public key.
Certificate Revocation List	CRL	This is the revocation list of EE certificates and operational certificates that have been revoked during the certificate validity period for reasons such as compromise of EE's private key.
PIN (Personal Identification Number)		Information used for identification of individuals.

2. Disclosure and Repository Liability

2.1. Repository

The Certification Authority strives for maintenance and administration that will allow repository use 24 hours per day, seven days a week. The repository includes a certificate repository and an information disclosure repository. In the situation where it is necessary to suspend the system for system maintenance, notification will be sent to certificate subjects, relying parties and related individuals or entities beforehand, or an announcement will be made on the Webpage. However, this may not always be possible, such as on the occurrence of unavoidable situations, including natural disasters, incidents, and problems.

2.2. Certification Information Disclosure

The following information is disclosed on the information disclosure repository:

- CPS

Further, the following information is disclosed on the certificate repository.

- EE certificates
- CRL

However, the EE certificates and CRL will only be disclosed to relying parties.

Note that important information relating to the CPS and the Certification Authority is disclosed on the Webpage with the URL shown below.

http://jpnic-ca.nic.ad.jp/

2.3. Disclosure Timing and Frequency

Regarding the information disclosed by the Certification Authority, the disclosure timing and frequency will be as follows:

- For the CPS, disclosure will be made whenever revisions are made.
- For self-signed certificates, linked certificates, and downstream Certification Authority certificates, disclosure will be made whenever issued or updates are made.
- For the CRL, disclosure will be made whenever issued. The frequency of issue will be as stipulated in “4.9.7 Certification Revocation List Issuing Frequency” in this CPS.
- Important information and other information concerning the Certification Authority will be updated as appropriate whenever necessary.
- For EE certificates, disclosure will be made whenever issued or updated.

2.4. Repository Access Management

Concerning the information disclosed by the Certification Authority, with the exception of read-only control, special degrees of access control are not implemented. The relying party for the EE certificates used for verification will be JPNIC. Accordingly, the certificate repository is basically provided to JPNIC.

3. Identification and Authentication

3.1. Name Determination

3.1.1. Types of Names

The certificate issuer name and issue subject name will be configured according to the regulations for the identifying name in the X.500 Series definitions.

3.1.2. Necessity for Names to Incorporate Meanings

It is necessary that names described in the certificate should show the subject individual's name, organization, role name, and equipment name.

3.1.3. Subject Anonymity

In the certificate, as long as the name allows specification of the individual, organization, role, and equipment, it is not necessary to use real names.

3.1.4. Rules for Interpreting Various Name Formats

The rules for interpreting the various name formats follow the rules for the identifying name in the X.500 Series definitions.

3.1.5. Uniqueness of Names

The names described in the certificates issued based on the same policy by the Certification Authority will be unique for all EEs. In the situation where an update has been carried out on a certificate for the same EE, there may be duplication of the certificate and name prior to updating.

3.1.6. Trademark Recognition, Authentication and Roles

Not specified.

3.2. Initial Authentication of Individual or Entity

3.2.1. Method used to Prove Possession of Private Key

The Certification Authority confirms that the applicant for the resource subscriber certificate possesses the private key utilizing a certificate signing request (CSR) that has been digitally signed following PKCS#10 (Public-Key Cryptography Standards #10) or another method determined by the Certification Authority.

Concerning the server's certificate, the Certification Authority uses a method stipulated beforehand to confirm that the certificate subscriber possesses it's private key.

3.2.2. Authentication of Organization Identity

The Certification Authority conducts authentication of organizations and groups as Local Registration Authorities. Organizations and groups intending to receive authentication as Local RAs must be IP Agents.

Regarding server's certificates, the Certification Authority confirms that the organization or group conducting the operation and maintenance of the server for which the certificate is to be issued is JPNIC, or an organization or group approved by JPNIC.

3.2.3. Authentication of Individuals

When conducting issue registration of applicants for contract/resource administrator certificates, JPNIC authenticates the applicants following the prescribed procedures.
When conducting issue registration of applicants for resource subscriber certificates, contract/resource administrators take responsibility for carrying out authentication of the applicants following the prescribed procedures.
When conducting issue registration of applicants for JPNIC staff certificates, JPNIC will authenticate the applicants following the prescribed procedures.

Concerning server's certificates, the Certification Authority will confirm that persons requesting the issue of certificates are persons who have received permission for certificate issue from JPNIC or an organization or group approved by JPNIC.

3.2.4. Unconfirmed Subject Information

Not specified.

3.2.5. Confirmation of Authority Appropriateness

Regarding the receipt of application registration for resource subscriber certificates from contract/resource administrators, the Certification Authority will confirm the appropriateness of the contract/resource administrator concerned.

3.2.6. Interoperability requirements

Not stipulated.

3.3. Identification and Authentication of Individual or Entity when Applying for Key Update

3.3.1. Identification and Authentication of Individual or Entity for Normal Key Updating

Same as procedures defined in “3.2 Initial Authentication of Individual or Entity” in this CPS.

3.3.2. Identification and Authentication of Individual or Entity for Key Updating after Certificate Revocation

Same as procedures defined in “3.2 Initial Authentication of Individual or Entity” in this CPS.

3.4. Identification and Authentication of Individual or Entity during Certificate Revocation Application

After conducting identification of an individual or entity as the revocation applicant for contract/resource administrator certificates, JPNIC will have the Certification Authority carry out revocation registration according to the methods determined by the Certification Authority.

The contract/resource administrator will in principle conduct identification of an individual or entity as the revocation applicant for resource subscriber certificates, and will have the Certification Authority carry out revocation registration according to the methods determined by the Certification Authority.

After conducting identification of an individual or entity as the revocation applicant for JPNIC staff certificates, JPNIC will have the Certification Authority carry out revocation registration according to the methods determined by the Certification Authority.

Regarding server’s certificates, the Certification Authority will confirm using a method prescribed beforehand that the individual or entity applying for the certificate revocation has received permission to issue certificates from JPNIC or an organization or group approved by JPNIC.

4. Operational Requirements concerning Certificate Lifecycle

4.1. Certificate Application

4.1.1. Individuals or Entities that can Submit Certificate Applications

Individuals or entities that can apply for contract/resource administrator certificates will be persons employed by IP Agents.

Individuals or entities that may apply for resource subscriber certificates will be verified contract/resource administrators.

Individuals who may apply for JPNIC staff certificates will be persons employed by JPNIC.

Individuals who may submit applications for server certification will be JPNIC staffs or persons specified by JPNIC.

4.1.2. Registration Procedures and Responsibilities

Applicants for contract/resource administrator certificates should apply to JPNIC for issue of the certificate according to the method notified beforehand by JPNIC. According to the content of the application, the contract/resource administrator will confirm the role.

Applicants for resource subscriber certificates should submit the certificate issue application to the contract/resource administrator using the method notified beforehand by the contract/resource administrator. Further, providing that the certificate applicant has been notified by the Certification Authority of the 2 types of information necessary for key pair generation and certificate issue, the key pairs should be generated and the digitally signed certificate signing request should be sent via secure online communications to the Certification Authority following the certificate signing request data format such as PKCS#10. The digital signature of the certificate signing request will be verified.

Applicants for server's certificates should conduct certificate issue application using the method prescribed beforehand by the Certification Authority.

Applicants for JPNIC staff certificates should carry out certificate issue application using the method prescribed beforehand by the Certification Authority.

Concerning the application for certificates, the certificate applicant will bear the following responsibilities:

- Acceptance of the contents of this CPS and other documentation disclosed by the Certification Authority.
- Correct production of certificate application content.

4.2. Certificate Application Procedures

4.2.1. Individual or Entity Identification and Authentication Function Implementation

Authentication of individual or entity as an applicant for contract/resource administrator certificates is carried out by JPNIC Registration Authority administrator.
Authentication of an individual or entity as an applicant for resource subscriber certificates is carried out by the contract/resource administrator. The contract/resource administrator implements authentication of correct individual or entity as applicants for resource subscriber certificates based on “3.2.3 Authentication of Individuals” in this CPS. The contract/resource administrator takes responsibility relating to the authentication of an individual or entity as an applicant for resource subscriber certificates.
Authentication of an individual or entity as an applicant for JPNIC staff certificates is carried out according to the method prescribed in advance by the Certification Authority.

Authentication of an individual or entity as an applicant for server’s certificates is carried out according to the method prescribed in advance by the Certification Authority.

4.2.2. Certificate Application Approval and Rejection

Regarding the applications from applicants for resource subscriber certificates, the contract/resource administrator determines whether the certificate application will be accepted or rejected based on judging standards prescribed beforehand. In the case where the application is accepted, certificate application registration will be carried out for the Certification Authority. The contract/resource administrator will take responsibility for the application judging.

Regarding the applications from applicants for contract/resource administrator certificates, JPNIC Registration Authority administrator determines whether the certificate application will be accepted or rejected based on judging standards prescribed beforehand. In the case where the application is accepted, certificate application registration will be carried out for the Certification Authority. JPNIC Registration Authority administrator will take responsibility for the application judging.

Note that after conducting confirmation of correct individual or entity as the contract/resource administrator carrying out application registration of the resource subscriber certificate, the Certification Authority will begin the certificate issuing procedures.

Regarding JPNIC staff certificates, the Certification Authority will determine whether the application will be accepted or rejected.
Regarding server's certificates, the Certification Authority will determine whether the application will be accepted or rejected.

4.2.3. Certificate Application Processing Time

In the case where the issue application from applicants for resource subscriber certificates is accepted, the contract/resource administrator will swiftly carry out the certificate issue application registration.

In the case where the issue application from applicants for contract/resource administrator certificates is accepted, JPNIC Registration Authority administrator will swiftly carry out the certificate issue application registration.

In the case where the issue application registration is accepted from the contract/resource administrator or JPNIC Registration Authority administrator, the certificate will be swiftly issued.

Regarding JPNIC staff certificates, in the case where the Certification Authority accepts an issue application from an individual or entity prescribed in "4.1.1 Individuals or Entities that can Submit Certification Applications", it will swiftly carry out issue of the certificate.

Regarding server's certificates, in the case where the Certification Authority accepts an issue application from an individual or entity prescribed in "4.1.1 Individuals or Entities that can Submit Certification Applications", it will swiftly carry out issue of the certificate.

4.3. Certificate Issuing

4.3.1. Certification Authority Actions in the Certificate Issuing Process

Concerning the receipt of the issue application registration for resource subscriber certificates from the contract/resource administrator, the Certification Authority will conduct authority confirmation of the contract/resource administrator using the method prescribed beforehand. Further, concerning the receipt of issue application registration for contract/resource administrator certificates, authority confirmation of the contract/resource administrator will be carried out according to previously prescribed methods. After confirming the authenticity of the application registration, the Certification Authority will give out notification of the permission for issue of the certificate to the applicant for the resource subscriber certificate using the methods prescribed in “4.3.2 Certificate Issue Notification for Certification Authority Subjects” in this CPS.

The Certification Authority verifies the digital signature of the certificate signing request sent by the applicant for the resource subscriber certificate. Then, after confirming the authenticity of the certificate signing request, the certificate is issued to the applicant for the resource subscriber certificate via secure online communications.

The Certification Authority verifies the digital signature of the certificate signing request sent by the applicant for the contract/resource administrator certificate. Then, after confirming the authenticity of the certificate signing request, the certificate is issued to the applicant for the contract/resource administrator certificate via offline means.

Concerning JPNIC staff certificates, after conducting confirmation of correct individual or entity for the applicant, the Certification Authority will issue the certificate using the method prescribed beforehand.

Concerning server’s certificates, after conducting confirmation of correct individual or entity for the applicant, the Certification Authority will issue the certificate using the method prescribed beforehand.

4.3.2. Certification Issue Notification for Certification Authority Subjects

Issue notification regarding contract/resource administrator certificates will be sent to applicants using offline means.

The Certification Authority will generate the 2 types of information required for the certificate issuing, and will notify the applicant for the resource subscriber certificate via the contract/resource administrator using two different methods.

Regarding JPNIC staff certificates, the Certification Authority conducts issue notification to applicants using methods prescribed beforehand.

Regarding server's certificates, the Certification Authority conducts issue notification to applicants using methods prescribed beforehand.

4.4. Certificate Receipt Confirmation

4.4.1. Certificate Receipt Confirmation Actions

Receipt of contract/resource administrator certificates will be conducted using offline means. In the case where there is a problem with the certificate, contact should be made with JPNIC. If no contact is received by JPNIC within 1 week of sending the certificate, it will be considered to have been received.

The Certification Authority will deliver contract/resource administrator certificates by a method that will allow confirmation of the certificate's arrival. Downloading of the certificate will be carried out by the applicant for the resource subscriber certificate, and the certificate should be received after confirming the content. In the case where there is a problem with the certificate, contact should be made with JPNIC via the contract/resource administrator. If no contact is received by JPNIC within 1 week of sending the certificate, it will be considered to have been received.

Regarding JPNIC staff certificates, the Certification Authority will confirm the receipt of the certificate using a method involving offline means prescribed beforehand.

Regarding server's certificates, the Certification Authority will confirm the receipt of the certificate using a method involving offline means prescribed beforehand.

Note that the applicant for the certificate must confirm that the certificate file is possible to be used on their computing environment, and that the details described in the certificate are correct.

4.4.2. Disclosure of the Certificate by the Certification Authority

The Certification Authority will disclose the certification using the repository according to "2.2. Certification Information Disclosure" in this CPS.

4.4.3. Certification Issue Notification by Certification Authority to Other Entities

The Certification Authority will not carry out certification issue notification to other entities.

4.5. Utilization of Key Pairs and Certificates

4.5.1. Subject Private Key and Certificate Use

Certificates issued based on this CPS are intended to be used for practices such as applications between JPNIC and IP Address Management Agents.

Certificate subjects will bear the following responsibilities regarding the use of the private key and the certificate:

- Confirmation and reporting of any errors in the content of the certificate on receipt of the certificate.
- Taking of adequate care and administration of the private key to prevent theft, leakage, loss, or inappropriate use by another entity.
- Swift revocation application in situations where there is a danger or possibility of the key becoming compromised.
- Confirmation of the usage purpose and use within this purpose.
- Maintaining the confidentiality of the private key and administering the correspondence of the private key and public key.

4.5.2. Relying Party Public Key and Certificate Use

The certificate relying party bears the following responsibilities concerning the reliability of the certificate:

- Understanding and agreement with this CPS at the point of time that the certificate is trusted.
- Agreement that the certificate usage purpose and the relying party's usage purpose are in accord.
- Verification of the digital signature used in the certificate and confirmation of the issuing authority.
- Confirmation of the certificate period of validity and the described items.
- Confirmation using the Certificate Revocation List (CRL) that the certificate has not been revoked.
- Confirmation of all certificates on the certificate path regarding falsification, periods of validity, revocation, and usage purpose.

4.6. Certificate Updating

In the Certification Authority, certification updating will not be conducted without revising the key pair. In the case where the certificate is updated, a new key pair will be generated using the procedure defined in “4.7 Certificate Key Updating” in this CPS.

4.6.1. Case where Certificate Updating is to be Conducted

Not stipulated.

4.6.2. Individuals or Entities that can Apply to Update Certificates

Not stipulated.

4.6.3. Certificate Updating Application Processing

Not stipulated.

4.6.4. Notification to Subjects of New Certificates

Not stipulated.

4.6.5. Updated Certificate Receipt Confirmation Actions

Not stipulated.

4.6.6. Disclosure of Certificates Updated by the Certification Authority

Not stipulated.

4.6.7. Notification to Other Entities

Not stipulated.

4.7. Certificate Key Updating

4.7.1. Situations where Certificate Key is Updated

Certificate key updating will be carried out in the following situations:

- Case where the certificate period of validity has expired.
- Case where certificate has been revoked due to the reason of key compromise.

4.7.2. Individuals or Entities that can Apply for New Public Key Certification

Same as “4.4.1. Certificate Receipt Confirmation Actions” in this CPS.

4.7.3. Certificate Key Updating Application Processing

Same as procedures defined in “4.2. Certificate Application Procedures” and “4.3. Certificate Issue” in this CPS.

4.7.4. New Certificate Notification for Subjects

Same as “4.3.2. Certificate Issue Notification for Certification Authority Subjects” in this CPS.

4.7.5. Key Updated Certificate Receipt Confirmation Actions

Same as “4.4.1. Certificate Receipt Confirmation Actions” in this CPS.

4.7.6. Disclosure of Certificate that has had Key Updated by the Certification Authority

Same as “4.4.2. Disclosure of the Certificate by the Certification Authority” in this CPS.

4.7.7. Notification to Other Entities

Same as “4.4.3. Certificate Issue Notification by Certification Authority to Other Entities“ in this CPS.

4.8. Certificate Revision

4.8.1. Case where Certificates will be Revised

Certificate revision will be carried out in the following situation:

- Case where information in the certificate other than the public key has been revised.

4.8.2. Individuals and Entities that can Apply for Revisions to Certificates

Same as “4.7.2 Individuals or Entities that can Apply for New Public Key Certification” in this CPS.

4.8.3. Revision Application Processing

Same as “4.7.3. Certificate Key Updating Application Processing” in this CPS.

4.8.4. New Certificate Notification for Subjects

Same as “4.7.4. New Certificate Notification for Subjects” in this CPS.

4.8.5. Receipt Confirmation Actions for Revised Certificates

Same as “4.7.5. Key Updated Certificate Receipt Confirmation Actions” in this CPS.

4.8.6. Disclosure of Revised Certificates by Certification Authority

Same as “4.7.6. Disclosure of Certificate that has had Key Updated by the Certification Authority” in this CPS.

4.8.7. Certificate Issue Notification by Certification Authority to Other Entities

Same as “4.7.7. Notification to Other Entities” in this CPS.

4.9. Certificate Revocation and Temporary Suspension

4.9.1. Circumstances of Certification Revocation

The subject of the resource subscriber certificate must carry out certificate revocation application to the contract/resource administrator.

The subject of the contract/resource administrator certificate must carry out certificate revocation application to JPNIC.

In situations where it is determined that the following items apply, the Certification Authority will be able to revoke the various certificates:

- Situation where the Certification Authority is abolished.
- Situation where the Certification Authority private key has been compromised, or there is a danger of compromise.
- Situation where the certificate content items differ from the actual situation.
- Situation where the private key of the certificate subject has been compromised, or there is a danger of compromise.
- Situation of inappropriate use of certification, or the danger of inappropriate use.
- Situation where the certificate subject or the local RA does not implement work according to this CPS or other agreements, regulations and laws.
- Situation where the agreement between JPNIC Certification Authority and the IP Address Management Agent has been cancelled.
- Other situations in which the Certification Authority has determined that revocation is necessary.

In the situation where the following items apply to the subject of the server's certificate, revocation application must be carried out through the Certification Authority.

- Situation where the server use is suspended.
- Situation where the server private key has been compromised (or if there is a danger of compromise).

Further, in the situation where the following items apply, it will be possible to carry out server's certificate revocation in addition to cases where the Certification Authority receives a revocation request from the certificate subject.

- Situation where the Certification Authority is abolished.
- Situation where the Certification Authority private key has been compromised, or there is a danger of compromise.
- Situation where the certificate content items differ from the actual situation.
- Situation where the server private key has been compromised, or there is a danger of compromise.
- Certificate inappropriate use, or the danger of inappropriate use.

- Situation where the certificate subject does not implement work according to this CPS or other agreements, regulations and laws.
- Other situations in which the Certification Authority judges that revocation is necessary.

4.9.2. Individuals or Entities that can Apply for Certificate Revocation

Individuals or entities that can request revocation of resource subscriber certificates are as follows:

- Certificate subject
- Legal representative of the certificate subject
- Local RA manager and contract/resource administrator of the organization to which the certificate subject belongs
- The Certification Authority

Individuals or entities that can request revocation of server's certificates are as follows:

- Certificate subject
- The Certification Authority

4.9.3. Revocation Application Procedures

After confirming the appropriateness of the revocation request according to the specified procedures, the contract/resource administrator carries out certificate revocation registration in the Certification Authority.

After confirming the appropriateness of the revocation request according to the specified procedures, JPNIC carries out certificate revocation registration in the Certification Authority.

The server's certificate subject carries out the revocation application for the Certification Authority using methods that have been previously prescribed.

Note that in the situation where the Certification Authority has determined that the items specified in "4.9.1. Circumstances of Certificate Revocation" are applicable; this Certificate Authority may carry out the certificate revocation registration following its own judgment

4.9.4. Revocation Application Delay Period

In the situation where conditions have occurred that require certification revocation, the revocation will be conducted as swiftly as possible.

4.9.5. Period during which the Certification Authority should carry out Processing of the Revocation Application

The certificate revocation processing will be carried out in the Certification Authority within five working days of receiving the revocation application.

4.9.6. Relying Party Revocation Checking Request

Concerning the reliance and use of the certificate issued by the Certification Authority, the certificate relying party must refer to the latest Certificate Revocation List (CRL) to confirm that the certificate in question has not had revocation processing carried out.

4.9.7. Certificate Revocation List Issuing Frequency

Regardless of whether or not there are certificate revocations, the CRL will be updated within 24 hours. In the situation where certificate revocation has been applied for, the CRL will be updated as soon as the revocation procedures have been completed.

4.9.8. Maximum Grace Period for Issue of Certificate Revocation List

After generating the CRL, the Certification Authority will swiftly disclose it on the repository.

4.9.9. Applicability of Revocation/Status Confirmation Online

Online revocation or status check functions such as OCSP are not supported.

4.9.10. Requirements for Conducting Online Revocation/Status Confirmation

Not stipulated.

4.9.11. Other Formats of Revocation Notification that may be Used

Not stipulated.

4.9.12. Special Conditions regarding Compromise of the Key Update

In the situation where there has been a compromise or danger of compromise of the private key of the Certification Authority, revocation processing of all of the certificates will be immediately conducted. Certificates will be registered in the CRL, and the facts of the compromise of the Certification Authority's private key and the notification of certificate revocation will be sent to certificate subjects using means such as E-mail.

4.9.13. Situation of Certificate Temporary Suspension

The Certification Authority will not temporarily suspend a certificate that has been issued.

4.9.14. Individuals or Entities that can Apply for Temporary Suspension of Certificates

Not stipulated.

4.9.15. Certificate Temporary Suspension Application Procedures

Not stipulated.

4.9.16. Period over which the Temporary Suspension can be Continued

Not stipulated.

4.10. Certificate Status Confirmation Service

4.10.1. Characteristics of Operation

The Certification Authority will provide CRLs as a means for relying parties to confirm certificate status. The conditions for accessing the CRL are specified in “2.4. Repository Access Management” in this CPS. Further, the CRL issue frequency and maximum issue grace period are specified in “4.9.7. Certificate Revocation List Issuing Frequency” and “4.9.8. Maximum Grace Period for Issue of Certificate Revocation List” in this CPS.

4.10.2. Service Usage Possibility

Specified in “2.1 Repository” in this CPS.

4.10.3. Optional Specifications

Not stipulated.

4.11. Registration Completion

In the situation where the certificate subject has completed the Certification Authority service usage registration, the Certification Authority will revoke all of the certification issued to the certificate subject.

4.12. Key Escrow and Key Recovery

The Certification Authority will not deposit its private key with any third party.

4.12.1. Key Escrow and Key Recovery Policy and Implementation

Not stipulated.

4.12.2. Session Key Encapsulation and Key Recovery Policy and Implementation

Not stipulated.

5. Facility, Management, and Operational Controls

5.1. Physical Controls

5.1.1. Site Location and Construction

The important facilities related to the Certification Authority are installed in locations where they will not be easily affected by damage from fire, water exposure, earthquakes, lightning or other natural disasters. The building structure incorporates measures for resistance to earthquakes and fire, and prevents against illegal entry. There is no indication of the location of the certification facilities room inside and outside the building.

Further, the equipment used will be located in a secure place, protected from disasters and improper access.

5.1.2. Physical Access

Concerning the certification facilities room, the Certification Authority conducts room entry-exit management that allows identification of persons who have been cleared for entry beforehand and confirmation of entry clearance. The Certification Authority in principle does not permit entry to the room of persons who do not have entry clearance. In situations where it is necessary for entry to be permitted, clearance will be obtained from the Certification Authority Operation Administrator beforehand, and the person granted entry will be accompanied at all times by a person who has clearance to enter the room.

5.1.3. Electric Power and Air Conditioning

In addition to securing an adequate capacity of electric power supply for operating the equipment, the Certification Authority will also implement measures to prepare against momentary power lapses, power failures, and fluctuations in voltage and frequency. Further, regarding air conditioning equipment, the room temperature will be maintained and administered at levels that will not adversely affect the various equipment being used.

5.1.4. Measures against Water Exposure and Earthquakes

Measures against water exposure will be implemented in the room where the Certification Authority is located in order to keep the level of damage due to water exposure to a minimum. Further, JPNIC Certification Authority will implement measures to prevent equipment and furniture from toppling over or falling down in the occurrence of an earthquake.

5.1.5. Fire Prevention and Fire Protection Measures

The Certification Authority has located the facilities inside fire prevention blocks that divide the area using firewalls. Further, inside the fire prevention blocks, fire prevention measures are implemented in the power source and air conditioning equipment, and fire detectors and fire-fighting equipment is also installed.

5.1.6. Media Storage Location

The media including archived data and backup data are stored in a storage warehouse inside a room where appropriate entry-exit management is carried out. Further, duplicates of important media will be stored in a storage warehouse that is separate from the Certification Authority's equipment location inside a room where appropriate entry-exit management is carried out.

5.1.7. Disposal Processing

For documentation and recording media including information that requires handling as confidential data, the Certification Authority will conduct appropriate disposal processing following methods prescribed beforehand including information initializing and deletion.

5.1.8. Backup Outside the Facilities

Not stipulated.

5.2. Procedural Controls

5.2.1. Trusted Roles

Persons carrying out key practices such as certificate issue, updating, and revocation undertake trusted roles in this CPS.

5.2.2. Employees Required for Each Operation

In the situation where it is necessary for persons who do not have entry authority to enter the Certification facilities room, such as for the maintenance of the Certification Authority facilities and responses during failures of JPNIC Certification Authority equipment, the people will at all times be accompanied by a person who is authorized to be in the room.

5.2.3. Identification and Authentication of Individual or Entity for Particular Roles

The Certification Authority equipment includes a function for discriminating between operators and necessary authorization. Further, the authorization for operation of the Certification Authority equipment can be configured for each operator.

5.2.4. Roles Requiring Task Division

By dividing authority among several persons rather than concentrating authority in a particular person, it is intended to prevent the occurrence of improper actions caused by individual operation. The authority will be divided for system operation, approval actions, and auditing.

5.3. Personnel Controls

5.3.1. Qualifications, Experience, and Identification Requirements

When appointing employees to roles in the Certification Authority, and periodically afterwards, JPNIC will implement appropriate character investigations before making appointments. When making appointments, non-disclosure agreements will be signed, and appropriate information management will be carried out. Further, during daily practices, continuous personnel management will be carried out including mental health and health management and appropriate treatment.

5.3.2. Regulatory Items relating to Personnel Assignments

Concerning the appointment of key persons for the Certification Authority practices, appropriate personnel will be allocated to avoid problems occurring during operation execution. Allocated employees will be required to submit pledges to strictly maintain confidentiality and observe internal regulations.

5.3.3. Training Requirements

For the education of key operational personnel, the following will be carried out:

- Before the key operational personnel take up their roles, necessary education will be implemented regarding the Certification Authority operations.
- Education and training plans will be developed supporting each role, and regular education and training will be implemented following the plans.
- In the situation where changes are made to the practice procedures, the changes to the work handling points will be made without delay, and education and training relating to these changes will be implemented.

5.3.4. Retraining Frequency and Requirements

JPNIC will regularly conduct appropriate education for Certification Authority key employees, and will carry out re-education afterwards if necessary.

5.3.5. Work Rotation Frequency and Order

Not stipulated.

5.3.6. Penalties for Carrying out Unapproved Actions

Concerning unapproved actions carried out by Certification Authority key operational personnel, penalties will be imposed according to the regulations specified beforehand.

5.3.7. Independent Contractor Requirements

JPNIC will clearly explain the details of the commissioned work in the commissioning agreement, clarifying for the contractor the strict observance of JPNIC directions, liability sharing, warranty, and penalties for infringements, and will also enter into a non-disclosure agreement. Further, after commissioning the work, auditing and administration will be carried out to confirm that the practices are being implemented appropriately.

5.3.8. Materials Supplied to Key Employees

Documentation necessary for the operations will be disclosed and notified to the operations key employees.

5.4. Audit Log Procedures

5.4.1. Types of Events Recorded

For events occurring in the Certification Authority system, regardless of whether they occur manually or automatically, the date, time, subject of the event, and the event details will be recorded.

The following records will be recorded as the necessary audit log for detecting Certification Authority mistaken operation and improper operation, and certifying the appropriateness of operations:

- Records relating to the operation of the Certification Authority private key
- Records relating to certificate issue and revocation work
- Records relating to the revocation information production practices
- Records relating to the confirmation of the audit log

Further, the records of accesses to the Certification Authority equipment will be recorded.

5.4.2. Frequency of Processing the Audit Log

The Certification Authority regularly reviews the audit log and the related records.

5.4.3. Period during which the Audit Log is Retained

The audit log will be retained on the server inside the Certification Authority for a minimum of 2 months. After this time, it will be stored for a fixed period on an external recording medium. Records relating to the entry and exit from the certification facilities room, and records concerning improper access will be retained until completion of the next audit.

5.4.4. Audit Log Protection

In order that only authorized JPNIC staffs can access the audit log file, the Certification Authority appoints an authorizer to protect the log file from being viewed, edited, or deleted by unauthorized persons. Further, the audit log will be regularly backed-up to external recording media which will be stored in a lockable storage warehouse in a room with appropriate entry and exit administration.

5.4.5. Audit Log Backup Procedure

Following procedures determined beforehand, the audit log together with the Certification Authority system database will be regularly backed-up on external recording media, and the media stored in a safe facility.

5.4.6. Audit Log Collection System

An audit log collection function is incorporated as one of the functions in the Certification Authority system, and important events relating to security are collected as the audit log.

5.4.7. Notification to Subject causing the Event

In the Certification Authority, the audit log collection is carried out without giving notification to the person, system or application that caused the event.

5.4.8. Vulnerability Assessment

The hardware and software used in the certification practices is assessed for security vulnerabilities from the system and operations points of view using audit log inspections, and the latest applicable security technology is introduced to improve security measures.

5.5. Record Storage

5.5.1. Archive Record Types

In addition to the audit log specified in “5.4.1. Types of Recorded Events” in this CPS, the Certification Authority stores the following records:

[Events Recorded in the Certification Authority System]

- Generation of the Certification Authority signature key pair
- Additions and deletions of certificate subjects from the system
- Changes in keys, including certificate issues and revocations
- Additions, changes and deletions of Registration Authority administrator authority

[Events Recorded as Paper Media and External Recording Media]

The Certification Authority maintains and administers an archive relating to the following operations-related records.

- Records relating to this CPS and the certificate subject agreement, and changes made to them.
- Records relating to the responsibilities and authority of persons conducting the certification practices, and changes made to them.
- In the case where part of the certification practices are commissioned to another entity, the original documentation relating to the commissioning agreement.
- Records relating to the audit implementation result, and the audit report.

5.5.2. Archive Storage Period

The Certification Authority will store the Certification Authority system database records and the audit log file records for a fixed period. The storage period for paper media and external recording media are defined in “5.5.1. Archive Record Types” in this CPS.

5.5.3. Archive Protection

Access control is implemented for the archived data, together with measures that allow detection of alterations. The Certification Authority regularly backs up the archived data to external recording media, restricting access only to persons who have received clearance from JPNIC Administration Division, and storing the media in facilities that are protected from environmental dangers such as temperature and humidity.

5.5.4. Archive Backup Procedures

The Certification Authority implements automatic and regular backups of the Certification Authority system database on the server. Further, the audit log is also regularly stored on external recording media.

5.5.5. Requirements for Attaching Time-stamps to Records

The Certification Authority attaches time-stamps to each record of important information recorded in the Certification Authority. The time-stamps indicated here do not utilize cryptographic technology.

5.5.6. Archive Collection System

A Certification Authority server database record collection system is incorporated in the Certification Authority server system. The audit log file record collection system is defined in “5.4.6. Audit Log Collection System” in this CPS.

5.5.7. Procedures for Obtaining and Verifying Archived Information

For the archived data, a person permitted to access the strictly administered storage section will obtain the data and regularly confirm the readability of the external recording media. Further, when necessary, the data will be copied onto new media and the old media that has exceeded its storage period will be destroyed in consideration of maintaining the completeness and confidentiality of the archived data.

5.6. Key Switching

Before the remaining validity period of the Certification Authority private key becomes less than the maximum validity period of the EE certificates, JPNIC will prevent the issue of new EE certificates using the key. JPNIC will then generate a new Certification Authority key pair using the method specified in “6.1. Key Pair Generation and Installation” in this CPS. The new public key will receive issue of a certificate from JPNIC Primary Root Certification Authority, and will be distributed in the same way as the method specified in “6.1.4. Delivery of Certification Authority Public Key to Relying Parties” in this CPS.

5.7. Recovery from Key Compromise and Disasters

5.7.1. Handling Procedures for Incidents and Key Compromise

In situations where the Certification Authority private key has been compromised or there is a danger of compromise, or when a disaster has occurred that has led to the interruption or suspension of certification practices, the Certification Authority will strive to restart the certification practices following plans and procedures defined beforehand.

5.7.2. Case where Computer Resources, Software and/or Data has been Corrupted

In a situation where hardware, software or data has been corrupted, JPNIC Certification Authority will strive to quickly implement recovery work using backup hardware, software and data following recovery plans determined beforehand.

5.7.3. Procedures when Entity Private Key has been Compromised

In a situation where the Certification Authority private key has been compromised, plans defined beforehand will be followed to halt the certification practices and then carry out the following procedures:

- Revocation procedures for contract/resource administrator certificates, resource subscriber certificates, and JPNIC staff certificates
- Procedures to destroy the Certification Authority private key and generate new keys
- Procedures to re-issue the contract/resource administrator certificates, resource subscriber certificates, and JPNIC staff certificates

Further, in the situation where a certificate subject's private key has been compromised, certificate revocation procedures will be carried out based on procedures determined beforehand in "4.9. Certificate Revocation and Temporary Suspension" in this CPS.

5.7.4. Business Continuation Capability after Disaster Occurrence

In the situation where JPNIC Certification Authority facilities receive damage due to a disaster or incident, JPNIC will strive to re-start operations by securing reserve equipment and using backup data.

5.8. Termination of Certification Authority or Registration Authority Practices

In the case where JPNIC has decided to terminate its Certification Authority certification practices, the specified practices termination procedures will be implemented, in which notification will be given to certificate subjects and relying parties 14 days before the termination of practices, explaining that the certification practices of JPNIC Certification Authority will be terminated. The explanation will also describe the storage organization and disclosure method for the Certification Authority backup data and archive data after the termination of business

6. Technical Security Management

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

Generation of Certification Authority key pairs should be carried out by several CAOs in the presence of the key administrator inside the certification facilities room. The generation of Certification Authority key pairs is carried out using FIPS140-1 Level 3 cryptographic modules.

Generation of key pairs for contract/resource administrator certificates and JPNIC staff certificates should be carried out using FIPS140-2 Level 3 cryptographic modules.

6.1.2. Delivery of Private Keys to Subjects

Generation of key pairs for contract/resource administrator certificates and JPNIC staff certificates is conducted by the Certification Authority inside the cryptographic module. The generated key pair will be delivered to applicants using a hardware token that includes a cryptographic module.

Because the Certification Authority does not carry out generation of key pairs for resource subscriber certificates, this item is not regulated.

6.1.3. Delivery of Public Keys to Certificate Issuers

The delivery of resource subscriber certificate public keys to the Certification Authority should be carried out by using encrypted communications to send the PKCS#10 format file to the Certification Authority.

6.1.4. Delivery of Certification Authority Public Keys to Relying Parties

Distribution of certificates by the Certification Authority is carried out using the most appropriate of the following two methods according to the EE.

- The Certification Authority certificates are disclosed on JPNIC Certification Authority Webpage. In the disclosure of the Certification Authority certificates, a secure protocol with an encryption function is used, and alteration prevention measures are applied. Certificate relying parties download the Certification Authority certificates from the same page for use. The relying parties compare the fingerprint of the downloaded Certification Authority certificates with the fingerprint that has been disclosed using a non-Internet method and confirm that they match.

- For resource subscribers, Certification Authority certificates will be handed over by the contract/resource administrator.

6.1.5. Key Size

The Certification Authority uses 2048-bit RSA key pairs. EEs are obliged to use RSA key pairs with 1024 bits or more.

6.1.6. Public Key Parameter Generation and Quality Inspection

The public key parameters for generating the Certification Authority key pairs use Random Number Generation (known henceforth as RNG) incorporated in software that includes highly secure cryptographic modules for use in the key pair generation.

For the quality inspection of the public key parameters, there is no particular specification.

6.1.7. Key Application Purpose

The Certification Authority certificate keyUsage uses the keyCertSign and cRLSign bits. The Certification Authority private key is only used for issuing EE certificates and the CRL.

The contract/resource administrator certificate, resource subscriber certificate, and JPNIC staff certificate keyUsage uses the digitalSignature, keyEncipherment, and dataencipherment bits. They are only used for S/MIME and SSL/TLS client certificates.

6.2. Private Key Protection and Cryptographic Module Technical Administration

6.2.1. Cryptographic Module Standards and Administration

Not stipulated.

6.2.2. Multi-person Control of Private Key

The Certification Authority private key administration is carried out by investing authority in a number of CAOs. It will not be possible to operate the Certification Authority private key unless there are two or more CAOs present.

6.2.3. Private Key Escrow

Specified in “4.12. Key Escrow and Key Recovery” in this CPS.

6.2.4. Private Key Backup

The Certification Authority private key will be backed-up on external recording media determined beforehand. During production of the backup, it will also be necessary for the key administrator and several CAOs to be in attendance.

The Certification Authority will store the backup in a storage location determined beforehand.

Note that the Certification Authority will not carry out backing-up of EE private keys.

6.2.5. Private Key Archiving

Archiving of the Certification Authority private key will not be conducted.

Similarly, archiving of EE private keys will not be carried out.

6.2.6. Transferring Into or From the Private Key Cryptographic Module

The Certification Authority private key is generated using software that includes a highly secure cryptographic module, with no intervention from other hardware or software.

6.2.7. Storage of Private Key in the Cryptographic Module

The Certification Authority private key is generated and stored in a highly secure cryptographic module.

For the resource subscriber private key, the resource subscriber will carry out generation and storage of the private key themselves. The confidential keys of contract/resource administrators and JPNIC staffs will be generated and stored inside highly secure cryptographic modules by JPNIC. However, for the server, the server's certificate administrator will carry out the storage.

6.2.8. Private Key Activation Method

Activation of the Certification Authority private key is carried out inside the certification facilities room.

The EE private key activation is not stipulated.

6.2.9. Private Key Deactivation Method

Deactivation of the Certification Authority private key is carried out inside the certification facilities room, with the work divided between the person conducting the operation and a person supervising.

The EE private key deactivation is not stipulated.

6.2.10. Private Key Destruction Method

In the situation where the Certification Authority private key must be destroyed, the key administrator will completely initialize or physically destroy the hard disk on which the private key was stored. At the same time, the backup private key will also be destroyed using the same procedures.

EE private keys should be completely destroyed by the EE itself. The confidential key of the contract/resource administrator will basically be destroyed by JPNIC. However, in situations such as when it has been lost, this may not be carried out.

6.2.11. Cryptographic Module Assessment

Not stipulated

6.3. Other Key Pair Administration

6.3.1. Public Key Archiving

The Certification Authority will back-up the Certification Authority certificates and all the certificates issued by the Certification Authority.

6.3.2. Period of Certificate Operation and Key Pair Usage Period

The period of validity of Certification Authority certificates is 10 years and the validity period of the private key is 8 years. The Certification Authority will update the key pair before the private key validity period ends.

The period of validity of EE certificates is 2 years. Use will be permitted for more than 2 years only in situations where private key decoding is carried out.

6.4. Activated Data

6.4.1. Activated Data Generation and Configuration

Including the Certification Authority private key, the PINs and passwords used in the Certification Authority have lengths of 8 or more capital or small alphanumeric characters.

6.4.2. Activated Data Protection

Regarding the PINs and passwords used in the Certification Authority, after sealing, they are stored under the administration of the operations administrator.

6.4.3. Other Considerations for Activated Data

Not stipulated.

6.5. Computer Security Management

6.5.1. Technical Requirements relating to the Security of Particular Computers

Practices relating to the Certification Authority server system will in principle be conducted by several CAOs. However, work that is necessary to be carried out such as during hardware failures by persons with specialized knowledge will be conducted by maintenance persons in the presence of the CAO. Important operations concerning the system are all configured to be stored in the log. All passwords used for accessing the system will have appropriate administration conducted. Regarding the Certification Authority server system, constant resource monitoring will be carried out, and appropriate measures will be implemented swiftly in the situation where a system abnormality or improper operation is detected.

6.5.2. Computer Security Assessment

All of the software and hardware used by the Certification Authority will have operation testing conducted before use to confirm the reliability.

6.6. Technical Administration of Life Cycle

6.6.1. System Development Administration

In order to maintain the system quality and security, administration of each process during development and assessment before introduction will be implemented.

6.6.2. Security Operations Administration

For the system security management, usage administration including room entry-exit administration, key employee administration including education, and authority administration will be carried out. Security measures such as improper entry measures and virus countermeasures, and the timely updating of security countermeasures software will be implemented.

6.6.3. Life Cycle Security Management

Using the specified administration method, assessment will be carried out regarding whether the system is being managed.

Regarding the Certification Authority system, information collection will be conducted relating to security, and appropriate assessment and improvements will be implemented while referring to the latest trends.

6.7. Network Security Management

A firewall is used for the network in the Certification Authority, and access from outside the firewall is restricted using the necessary minimum protocol. Further, the hosts that can be accessed are also limited.

6.8. Time-stamps

Requirements relating to the use of time-stamps are stipulated in “5.5.5. Requirements for Attaching Time-stamps to Records” in this CPS.

7. Profiles of Certificates, Certificate Revocation Lists, and OCSP Profiles

7.1. Certificate Profile

Certificates issued by the Certification Authority conform to X.509 certificate format v3. The certificate profile is as shown in Table 7-1.

7.1.1. Version No.

All certificates issued by the Certification Authority conform to X.509 v3 certificate format.

7.1.2. Certificate Extensions

The extension fields used in certificates issued by the Certification Authority are shown below:

7.1.2.1. authorityKeyIdentifier

The Certification Authority public key 160-bit SHA-1 hash value is used as the keyIdentifier value. This extension is non-critical.

7.1.2.2. subjectKeyIdentifier

The public key 160-bit SHA-1 hash value of the certificate subject concerned is used. This extension is non-critical.

7.1.2.3. keyUsage

Contract/resource administrator certificates, resource subscriber certificates, and JPNIC staff certificates use digitalSignature, keyEncipherment, and dataEncipherment. The server's certificates use digitalSignature and keyEncipherment only. This extension is non-critical.

7.1.2.4. certificatePolicies

Contract/resource administrator certificates, resource subscriber certificates, and JPNIC staff certificates use the certificatePolicies extension. The policyIdentifier value is shown in "7.1.6. Certificate Policy OID" in this CPS, and the policyQualifiers value is shown in "7.1.8. Policy Qualifier Description and Meaning" in this CPS. This extension is non-critical.

7.1.2.5. subjectAltName

The E-mail address of the certificate subject is written as the rfc822Name. This extension is non-critical.

7.1.2.6. cRLDistributionPoints

The URI of the CRLs issued by the Certification Authority is written. This extension is non-critical.

7.1.3. Algorithm OID

The algorithm OIDs used in certificates issued by the Certification Authority are the two shown below:

- sha1withRSAEncryption（1.2.840.113549.1.1.5）
- rsaEncryption（1.2.840.113549.1.1.1）

7.1.4. Name Format

Conforms to “3.1.1. Types of Names” in this CPS.

7.1.5. Naming Constraints

The nameConstraints extension is not used in any of the certificates issued by the Certification Authority.

7.1.6. Certificate Policy OID

Resource subscriber certificates, contract/resource administrator certificates, and JPNIC staff certificates each use the EE certificate policy OID defined in “1.2. Documentation Name and Identification” in this CPS.

7.1.7. Policy Constraints Extensions

The policyConstraints extension is not used in any of the certificates issued by the Certification Authority.

7.1.8. Policy Qualifier Description and Meaning

The URI disclosed in this CPS is used both in resource subscriber certificates and server's certificates as the policy qualifier value.

7.1.9. Processing of certificatePolicies Extensions for Critical Certificates

The certificatePolicies extensions included in certificates issued by the Certification Authority are all non-critical, and regulations are not carried out for this item.

Table 7.1 Profile of Certificates issued by JPNIC Resource Service Certification Authority

Field	Critical Flag	Contract/resource Administrator Certificate, Resource Subscriber Certificate, JPNIC staff Certificate
version	NA	2
serialNumber	NA	Non-negative integer
signature	NA	
algorithm		sha1withRSAEncryption
parameters		null
issuer	NA	
		PrintableString*1
validity	NA	
notBefore		UTCTime
notAfter		UTCTime 2 years after notBefore time
subject	NA	
		PrintableString*2
subjectPublicKeyInfo	NA	
algorithm		rsaEncryption
parameters		null
subjectPublicKey		Public key BIT STRING
authorityKeyIdentifier	n	
keyIdentifier		160-bit SHA-1 hash value of JPNIC IP Address Certification Authority public key
authorityCertIssuer		Not used
authorityCertSerialNumber		Not used
subjectKeyIdentifier	n	160-bit SHA-1 hash value of public key
keyUsage	n	
digitalSignature		1
nonRepudiation		0
keyEncipherment		1
dataEncipherment		1
certificatePolicies	n	
policyIdentifier		OID of this CP
policyQualifiers		
policyQualifierId		CPSUri
qualifier		URI disclosed by this CP/CPS
subjectAltName	n	
rfc822Name		E-mail address
cRLDistributionPoints	n	
DistributionPoint		
distributionPoint		URL where CRL is disclosed by the Certification Authority
reasons		Not used
cRLIssuer		Not used

※1 C=JP, O=Japan Network Information Center, OU=Internet Resource Service, OU=JPNIC Resource Service Certification Authority

※2 C=JP, O=(Organization Name), O=Resource Holder, O=LIR Corporate Administrator, OU=(One out of LIR Corporate Administrator, LIR Administrator, or LIR Hostmaster), OU=(Maintainer code allocated by JPNIC in resource administration units) CN=(One out of LIR-CO, LIR-AD, LIR-HM, ASN-HLD, JPNIC-AD, or JPNIC-CO)＋(Certification ID allocated by JPNIC to each user)＋(Alphabetical notation giving the name of the certificate issue subject)

7.2. Profile of Certificate Revocation List

CRLs issued by the Certification Authority comply with X.509 CRL format v2. The CRL profile is as shown in Table 7-2.

7.2.1. Version No.

All CRLs issued by the Certification Authority comply with X.509 v2 CRL format.

7.2.2. CRL and CRL Entry Extensions

The Certification Authority uses the following two CRL extensions, and CRL entry extensions are not used.

7.2.2.1. cRLNumber

CRLs issued by the Certification Authority use a non-negative integer that will become unique.

7.2.2.2. authorityKeyIdentifier

The Certification Authority public key 160-bit SHA-1 hash value is used as the keyIdentifier value. This extension is non-critical.

Table 7.2 Profile of CRLs Issued by JPNIC Resource Service Certification Authority

Field	Critical Flag	Certificate Revocation List
version	NA	1
signature	NA	
algorithm		sha1withRSAEncryption
parameters		null
issuer	NA	
		PrintableString*1
thisUpdate	NA	UTCTime
nextUpdate	NA	UTCTime　24 hours after thisUpdate
revokedCertificates	NA	
revokedCertificate		
userCertificate		Serial number of revoked certificate
revocationDate		UTCTime　Time that certificate was revoked
crlEntryExtensions		
		Not used
crlExtensions	NA	
cRLNumber	n	Non-negative integer
authorityKeyIdentifier	n	160-bit SHA-1 hash value of Certification Authority public key

※1 C=JP, O=Japan Network Information Center, OU=Internet Resource Service, OU=JPNIC Resource Service Certification Authority

7.3. OCSP Profile

7.3.1. Version Information

Not stipulated

7.3.2. OCSP Extensions

Not stipulated

8. Compliance Audit and Other Assessments

8.1. Assessment Frequency and Circumstances requiring Assessment

The Certification Authority will implement audits whenever required.

8.2. Identity and Qualifications of Assessor

JPNIC will have the Certification Authority compliance audit implemented by an assessor who is knowledgeable of the certification practices selected by the trustee in charge.

8.3. Relationship between the Assessor and the Entity Assessed

JPNIC will select the assessor from among personnel excluding key persons relating to the Certification Authority certification practices.

8.4. Items covered by the Assessment

The Certification Authority compliance audit will assess whether the management of the Certification Authority strictly complies with this CPS and other related stipulations.

Further, in situations where the trustee in charge determines it necessary, audits will be implemented according to audit purposes specified by the trustee in charge.

Note that JPNIC has the authority to conduct audits of local RAs.

8.5. Measures taken in Event of Unsatisfactory Results

For items indicated in the audit report, the Certification Authority trustee in charge will decide the measures. For the specified items, the trustee in charge will give direction including measures for solving the problems to JPNIC Certification Authority manager responsible, based on the latest trends in security technology. The response measures implemented will be reported to the trustee in charge, and will be assessed and confirmed in the next audit. In the situation where a response is not made to the unsatisfactory items discovered by the assessment, penalties determined beforehand by the trustee in charge will be applied.

8.6. Assessment Result Information Exchange

Reporting of the assessment result will be carried out by the assessor to the trustee in charge. Except in situations where the Certification Authority is legally required to make a disclosure, the assessment results will not be disclosed outside the organization.

Note that JPNIC Certification Authority manager in charge has a responsibility to store and administer the audit reports for a period of at least 5 years.

9. Problems relating to Other Practices and Legal Problems

9.1. Fees

The issuing fees, updating fees, and usage fees relating to the certificates issued by the Certification Authority will be determined separately and notified beforehand to individuals and entities concerned.

9.2. Financial Liability

Not stipulated

9.3. Information Confidentiality

9.3.1. Scope of Confidential Information

Information retained by the Certification Authority will be treated as confidential information, with the exception of the information determined for disclosure in “2.2. Certification Information Disclosure” in this CPS, information explicitly disclosed as part of the CPS, information disclosed on the Website, reasons for certificate revocation and other detailed information relating to certificate revocation.

The private keys of certificate subjects are information that should be treated as confidential information by the certificate subject.

9.3.2. Information Outside the Scope of Confidential Information

Information determined for disclosure in this CPS, information explicitly disclosed as part of the CPS, information disclosed on the Website, and CRLs including information about the Certification Authority as the certificate issuer and the revocation date are not treated as confidential information. In addition, information satisfying the following conditions will not be treated as confidential information.

- Information that has become known through no negligence on the part of JPNIC.
- Information that has been provided to JPNIC from another source with no confidential restrictions attached.
- Information that has been independently developed by JPNIC.
- Information that has been confirmed by persons or organizations related to the subject of the released information.

9.3.3. Liability for Protecting Confidential Information

Concerning the information handled by the Certification Authority, in the situation where a request is received for information disclosure based on the legal authority of an investigative agency or court, JPNIC can disclose the information to the legal enforcing institution according to law. Further, regarding the information handled by the Certification Authority, in the case where an optional disclosure request is received from a court, lawyer, or other person with legal authority concerning arbitration, litigation, mediation, and other legal, judicial, or administrative processes, JPNIC can disclose the relevant information relating to the request. Additionally, concerning information received from contract/resource administrators relating to the certificate subject administered by the contract/resource administrator, in the situation where a request is received that violates or has a danger of violating the subject's rights or interests, the Certification Authority will confirm the relationship between the contract/resource administrator and the disclosure request subject information. The Certification Authority can then disclose the information received from the contract/resource administrator concerning the certificate subject and the information described in the certificate.

In the situation where a part of the practices are commissioned, JPNIC Certification Authority may disclose confidential information to the commissioned entity. However, the commissioning agreement incorporates an obligation to maintain the confidentiality of the information.

With the exceptions of the situations mentioned previously, JPNIC Certification Authority will not disclose confidential information. In the case where confidential information is leaked, the liability will be borne by the person leaking the information.

Note that handling concerning the protection of personal data is specified in “9.4. Protection of Personal Data Privacy” in this CPS.

9.4. Protection of Personal Data Privacy

9.4.1. Privacy Policy

The Certification Authority recognizes the importance of personal data protection. In addition to handling personal data in the same way as “9.3.3. Liability for Protecting Confidential Information” in this CPS, the following policy is strictly observed.

(1) An administrator responsible will be appointed to carry out appropriate administration of personal data.

(2) In the situation where personal data is collected, the purpose for collecting the data will be notified, and collection will be conducted only of information that falls within the necessary scope of purpose using legal and fair means.

(3) Personal data received through submission by certificate subjects will only be used for the following purposes:
- To allow smooth operation of IP address administration practices
- To allow fulfillment of responsibilities regarding certification services for certificates
- For other purposes relating to certification practices

(4) With the exception of situations where the agreement of the certificate subject has been received or in cases when legally obligated, personal data will not be disclosed to third parties apart from commissioned practices entities. When disclosing personal data to commissioned practices entities, the commissioned practices entities concerned will be obliged to follow the same conditions as this document.

(5) The personal data administrator responsible for the personal data will strive to protect the personal data using appropriate security measures to prevent improper access, loss, corruption, alterations, or leaks.

(6) In situations where requests are received for disclosure of personal data from the certificate subjects themselves, in order to prevent disclosure of personal data to third parties JPNIC will only disclose the certificate subject personal data stored in JPNIC Certification Authority to the subject themselves after confirming the identity of the subject. Further, in the situation where there is an error or changes in the certificate subject personal data, incorrect data or old information will be swiftly revised or deleted over the logical range based on the notification received from the certificate subject. In a situation where the certificate subject requests disclosure from JPNIC Certification Authority, JPNIC Certification Authority will carry out the application following the specified method.

(7) JPNIC Certification Authority will implement education activities relating to personal data protection for employees carrying out the certification practices.

(8) Regarding the personal data of certificate subjects, in addition to strictly observing the applicable laws and regulations, the personal data protection policy will be revised whenever necessary for improvement to maintain appropriate personal data protection.

9.4.2. Information treated as Privacy

Not stipulated

9.4.3. Information not considered as Privacy

Not stipulated

9.4.4. Liability for Protecting Personal Data

JPNIC Certification Authority will bear liability for the protection of personal data according to “9.4.1. Privacy Policy” in this CPS.

9.4.5. Notification and Agreement to Individuals relating to Use of Personal Data

Not stipulated

9.4.6. Disclosure based on Judicial Procedures and Administrative Procedures

Not stipulated

9.4.7. Other Information Disclosure Situations

Not stipulated

9.5. Intellectual Property Rights

Providing there has been no particular agreement made, intellectual property rights will be treated as follows:

- Certificates and CRLs issued by JPNIC Certification Authority are the property of JPNIC.
- This CPS is the property of JPNIC.
- JPNIC Certification Authority private key and public key is the property of JPNIC.
- Software, hardware, and other documents and information loaned from JPNIC Certification Authority are the property of JPNIC.

9.6. Representation Warranties

9.6.1. Issuing Authority Representation Warranty

JPNIC Issuing Authority will fulfill the following obligations concerning the performance of JPNIC Issuing Authority practices:

- Secure generation and administration of JPNIC Issuing Authority certificate signing keys
- Correct certificate issue and revocation administration following requests from JPNIC Registration Authority.
- JPNIC Issuing Authority system operation audit and operation
- CRL issue and disclosure
- Repository maintenance and administration
- Receipt of questions relating to this CPS during the reception opening times.

9.6.2. Registration Authority Representation Warranty

JPNIC Registration Authority will fulfill the following obligations regarding the performance of JPNIC Registration Authority practices:

- Installation and operation of a secure environment for registration terminals
- Correct information transfer to JPNIC Issuing Authority of applications for certificate issuing and revocation.
- Swift information transfer to JPNIC Issuing Authority during operation times for certificate revocation applications.

9.6.3. Local Registration Authority Representation Warranty

The Local Registration Authority will fulfill the following obligations regarding the performance of the Local Registration Authority practices:

- Verification that the certificate subject and the certificate subscriber are the same.
- Correct application information transfer to JPNIC Registration Authority.
- Resource subscriber education for certificate use.
- Precise certificate distribution to the correct certificate subscriber
- Appropriate confirmation of certificate revocation
- Strict observance of other operations conforming with the agreement with JPNIC.

9.6.4. Subject Representation Warranty

The certificate subject will fulfill the following obligations regarding the holding of the certificate:

- Understanding and agreement with this CPS and other documentation (such as certificate subject agreements) shown by the Certification Authority.
- Obligations stipulated in “4.5.1. Subject Private Key and Certificate Use” in this CPS.

9.6.5. Relying Party Representation Warranty

The certificate relying party will fulfill the obligations stipulated in “4.5.2. Relying Party Public Key and Certificate Use” in this CPS.

9.6.6. Other Related Person Representation Warranty

Not stipulated

9.7. Limitations of Warranty

JPNIC will not bear liability for any indirect damages, special damages, accompanying damages and secondary damages relating to the warranty specified in “9.6.1. Issuing Authority Representation Warranty” together with “9.6.2. Registration Authority Representation Warranty” in this CPS.

9.8. Limitations of Liability

Concerning the contents of “9.6.1. Issuing Authority Representation Warranty” together with “9.6.2. Registration Authority Representation Warranty” in this CPS, JPNIC will not bear liability in the following situations:

- All damages occurring due to illegal actions, improper use, or negligence not caused by JPNIC.
- Damages occurring due to negligence of the Local RA or certificate subject in fulfilling their obligations.
- Damages occurring due to Local RA or certificate subject computer terminal software defects, problems, or other actions themselves.
- Damages caused by information disclosed in certificates and CRLs for reasons that can not be attributed to JPNIC.
- All damages caused by conditions where normal communications cannot be carried out for reasons that can not be attributed to JPNIC.
- Damages caused by improvement in hardware or software encryption algorithms that are not possible to be foreseen at the current time.
- All damages caused by suspension of Certification Authority practices due to acts of God, earthquakes、volcanic eruptions, fires, tidal waves, water damage, lightning, wars, riots, terrorism, and other irresistible forces.
- Damage caused by practices carried out by Local RA such as in individual authentication procedures for certificate issue applications.

9.9. Indemnity

At the point of time that the certificate issued by the Certification Authority is applied for, received, and trusted, damage liability and protection liability is created for JPNIC regarding the certificate subject and the relying party. Among the liability phenomena covered will be mistakes, negligent actions, various actions, delays in implementation, and non-fulfillment caused by the certificate subscriber not supplying the latest and correct information to the Certification Authority when applying for the certificate, resulting in various liabilities, loss, damage, and litigation, and any kind of financial burden. In addition, certificate subject and relying party actions, negligent actions, various actions and non-fulfillment resulting in various liabilities, loss, damage, and litigation, and any kind of financial burden will also be covered.

9.10. Periods of Validity and Termination

9.10.1. Periods of Validity

Documents including this CPS, contracts, and agreements are valid from the time they are issued based on appropriate approved procedures until the time they are amended based on appropriate approved procedures.

9.10.2. Termination

In the situation where all or parts of documentation including this CPS, contracts, and other agreements become invalid, or if specified conditions make the documents invalid for particular related persons, the parts concerned will be terminated.

9.10.3. Effect of Termination and Effect Continuation

Even in the situation where changes or terminations occur in this CPS, contracts, or agreements, the Certification Authority will endeavor to continue taking responsibility for the agreed items.

9.11. Individual Notification and Contact between Related Persons

Not stipulated

9.12. Amendments

9.12.1. Amendment Procedure

In the situation where it becomes necessary to amend this CPS over an extent that will not radically influence the certificate policy, warranties and obligations, the Certification Authority may amend this CPS whenever necessary without giving prior notice to certificate subjects and relying parties. Note that in the situation where no objections are received during the period between the amendment notification and the amendment becoming valid, this will be taken to signify agreement with the amendment. Related persons who do not agree with the amendment should immediately stop using the certificates issued by the Certification Authority.

9.12.2. Notification Method and Period

The Certification Authority will give notification of the amendment to certificate subjects and related persons by disclosing the amended CPS together with the amendment history on the repository more than 10 working days before the amendment is due to become valid.

9.12.3. Situation where Object Identifier must be Changed

Not stipulated

9.13. Dispute Resolution Procedures

For disputes arising relating to certificates issued by the Certification Authority, in the situation where legal means such as litigation or arbitration are to be used to solve the dispute this fact should be notified to JPNIC beforehand. All parties concerned agree that the arbitration and court location will be within the Tokyo metropolitan wards under the exclusive jurisdiction of a dispute handling institution. Further, regarding the situation where questions arise about items not determined in this CPS or in agreements, or about the interpretation of the documentation, all parties will resolve the issues through sincere discussions.

9.14. Governing Law

Regardless of the location of the Certification Authority, certificate subject, or relying party, Japanese laws will apply regarding the interpretation of this CPS, the validity, and disputes relating to the issue of certificates by the Certification Authority.

9.15. Compliance with Applicable Laws

The Certification Authority will strictly observe the various export restrictions, and will handle cryptographic hardware and software.

9.16. Miscellaneous Regulations

9.16.1. Entire Agreement

The agreed items in this CPS, contracts and agreements will have priority over all other agreed items until amended or terminated.

9.16.2. Transfer of Rights

Not stipulated

9.16.3. Severability

In this CPS, certificate subject agreements, and agreements provided by the Certification Authority, even of one part of the provisions is invalid, the other provisions described in the document concerned will continue to remain valid.

9.16.4. Enforcement

Not stipulated

9.17. Other Provisions

Not stipulated