SecureSign®

Public Service Standard V1.60

Feb. 24, 2012

Japan Certification Services, Inc.

SecureSign Certificate Policy and Certification Practice Statement (V1.60)

Major revisions to the previous version

1. Additional descriptions for SecureSign server service (Appendix A) - V1.51
2. Additional descriptions for consistency with AccreditedSign public service - V1.51
3. Corrections of certificate validity period (chapter 6) - V1.51
4. Additional OID for signing certificate - V1.52
5. Correction of clerical mistake(chapter A7) - V1.53
6. Additional OID for Time Stumping certificate - V1.54
7. Corrections of errors in writing- V1.55
8. Additional descriptions for Time Stumping certificate - V1.56
9. Update the profile of Web server Certificate –V1.57
10. Part modification of certificate profile of signing certificate and modification of the description regarding private information protection-V1.58
11. Following the change of the local government document electrification, “a copy of corporate register (toukibo touhon)” is replaced by “a certificate of corporate registration information (touki jikou shoumeisho)” -V1.59.
12. Moving to the new office –V1.60.

Table of Contents

1. INTRODUCTION 7
1.1 General 7
1.2 Object Names 8
1.3 Community and Applicability 9
1.3.1 Entities and roles 9
1.3.2 SecureSign services 11
1.3.3 Uses 11
1.3.4 Interoperability and root certificates 12
1.4 Distribution of Service Specification Information 12
2. GENERAL PROVISIONS 13
2.1 Obligations 13
2.1.1 CA obligations 13
2.1.2 RA obligations 13
2.1.3 KRS obligations 14
2.1.4 Subscriber obligations 14
2.1.5 Relying party obligations 15
2.1.6 Repository obligations 16
2.2 Liability 16
2.2.1 JCSI liability 16
2.2.2 Customer liability 17
2.3 Financial Responsibility 18
2.3.1 Responsibility for compensation 18
2.3.2 Fiduciary relationships 18
2.3.3 Accountability 19
2.4 Interpretation and Enforcement 19
2.4.1 Governing law 19
2.4.2 Severability, survival, merger, notice 19
2.4.3 Dispute resolution procedures 19
2.5 Fees 19
2.6 Publication and Repositories 19
2.6.1 Publication of CA information 19
2.6.2 Frequency of publication 19
2.6.3 Access controls 20
2.6.4 Repositories 20
2.7 Compliance audit 20

2.7.1 Frequency of audit 21
2.7.2 Identity/qualifications of the auditor 21
2.7.3 Auditor's relationship to the audited party 21
2.7.4 List of topics covered under the compliance audit 21
2.7.5 Actions taken as a result of a deficiency found during compliance audit 21
2.7.6 Report on compliance audit results 21
2.7.7 Customer audit 21
2.8 Confidentiality 21
2.8.1 Types of information that must be kept confidential 21
2.8.2 Types of information that are not considered confidential 22
2.8.3 Disclosure of certificate revocation information 22
2.8.4 Release to law enforcement officials 22
2.8.5 Release as part of civil procedure 22
2.8.6 Disclosure upon owner’s request 22
2.8.7 Any other circumstances under which confidential information may be disclosed 23
2.9 Intellectual Property Rights 23
2.10 Personal Information Protection 23
3. IDENTIFICATION AND AUTHENTICATION 24
3.1 Initial Registration (Initial Application) 24
3.1.1 Types of names 24
3.1.2 Need for names to be meaningful 25
3.1.3 Rules for interpreting various name forms 25
3.1.4 Uniqueness of names 25
3.1.5 Name claim dispute resolution procedure 25
3.1.6 Recognition, authentication, and role of trademarks 25
3.1.7 Method to prove possession of private keys 26
3.1.8 Authentication of organization identity 26
3.1.9 Authentication of individual identity 26
3.2 Routine Rekey with Certificate Updates 26
3.3 Rekey after Revocation 27
3.4 Revocation Request 27
3.5 Secret Certification Key 27
3.6 Handling of Certification Application Data 28
4. OPERATIONAL REQUIREMENTS 29
4.1 Certificate Application, Issuance and Acceptance 29
4.2 Certificate Suspension and Revocation 33

4.3 Security Audit Procedures....33
4.4 Archiving....33
4.5 Key changeover....34
4.6 Recovery from Compromise....35
4.7 CA Termination....35
5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS....36
5.1 Physical Security Controls....36
5.2 Procedural Security Controls....37
5.3 Personnel Security Controls....38
6. TECHNICAL SECURITY CONTROLS....39
6.1 Key Pair Generation and Installation....39
6.1.1 RCA....39
6.1.2 ICA/SCA....39
6.1.3 Subscriber (Issuance pattern 1)....40
6.1.4 Subscriber (Issuance patterns 2 and 3)....41
6.2 Private Key Protection....42
6.2.1 Standards for cryptographic module....42
6.2.2 Private key (n out of m) multi-person control....42
6.2.3 Private key escrow....42
6.2.4 Private key backup....42
6.2.5 Private key archive....43
6.2.6 Private key entry into cryptographic module....43
6.2.7 Method of activating private key....43
6.2.8 Method of deactivating private key....43
6.2.9 Method of destroying private key....43
6.2.10 Private key recovery....43
6.3 Other Aspects of Key Pair Management....44
6.3.1 Public key archive....44
6.3.2 Usage periods for the public and private keys....44
6.4 Activation Data....45
6.4.1 Activation data generation and installation....45
6.4.2 Activation data protection....45
6.5 Computer Security Controls....45
6.5.1 Specific computer security technical requirements....45
6.5.2 Computer security evaluation....45
6.6 Life Cycle Technical Control....45

6.6.1 System development control 45
6.6.2 Security management control 45
6.7 Network Security Controls 46
6.8 Cryptographic Module Engineering Controls 46
7. CERTIFICATE AND CRL PROFILES FOR PUBLIC SERVICE 47
7.1 Setter and Set Values for Fields 48
7.1.1 Name forms 50
7.1.2 General name (GeneralName) 50
7.1.3 Key usage (KeyUsage) 50
7.1.4 Extended key usage (extendedKeyUsage) 50
7.1.5 Certificate policies (certificatePolicies) 51
7.1.6 Policy mapping (policyMappings) 51
7.1.7 Basic constraints (basicConstraints) 51
7.1.8 Name constraints (nameConstraints) 51
7.1.9 Policy constraints (policyConstraints) 51
7.1.10 CRL distribution points (cRLDistributionPoints) 51
7.1.11 Certification authority information access (authorityInfoAccess) 51
7.1.12 netscape-cert-type 51
7.2 Certificate/CRL Setting Contents Determination Procedures 52
7.2.1 Validity check of application contents 52
7.2.2 Validity check of setting contents of issued certificates 52
7.3 Profiles of Certificates 52
7.3.1 SecureSign public CA certificate 52
7.3.2 SecureSign public subscriber’s certificate 53
8. SPECIFICATION ADMINISTRATION 55
8.1 Specification Change Procedures and Publication/Notification Policies 55
8.2 Publication/Notification Policies 55
8.3 Specification Approval Procedures 55
8.4 Storage of this Document 56
Appendix A. SecureSign Server Service 57
A1 INTRODUCTION 57
A2 GENERAL PROVISIONS 58
A2.1 Obligations 58
A2.1.1 CA obligations 58
A2.1.2 RA obligations 58
A2.1.3 KPS obligations 59
A2.1.4 Subscriber’s obligations 59

A2.1.5 Relying party obligations 60
A2.1.6 Repository obligations 61
A2.2 Liability 61
A2.2.1 JCSI liability 61
A2.2.2 Customer liability 62
A2.3 Financial responsibilities 62
A2.4 Interpretation and Enforcement 62
A2.5 Fees 62
A2.6 Publication and Repositories 62
A2.7 Compliance audit 62
A2.8 Confidentiality 62
A2.9 Intellectual Property Rights 62
A2.10 Personal Privacy Protection 62
A3 IDENTIFICATION AND AUTHENTICATION 63
A3.1 Initial Registration (Initial Application) 63
A3.1.1 Types of names 63
A3.1.2 Need for names to be meaningful 63
A3.1.3 Rules for interpreting various name forms 63
A3.1.4 Uniqueness of names 63
A3.1.5 Name claim dispute resolution procedure 64
A3.1.6 Recognition, authentication, and role of trademarks 64
A3.1.7 Method to prove possesion of private key 64
A3.1.8 Authentication of organization identity 64
A3.1.9 Authentication of individual identity 64
A3.2 Routine Rekey 65
A3.3 Rekey after Revocation 65
A3.4 Revocation request 65
A4 OPERATIONAL REQUIREMENTS 66
A4.1 Certificate Application, Issuance and Acceptance 66
A4.2 Certificate Suspension and Revocation 67
A4.3 Security Audit Procedures 67
A4.4 Archiving 67
A4.5 Key changeover 68
A4.6 Compromise and Disaster Recovery 68
A4.7 CA Termination 68
A5 PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS 69

A5.1 Physical Security Controls 69
A5.2 Procedural Security Controls 69
A5.3 Personnel security controls 71
A6 TECHNICAL SECURITY CONTROLS 71
A7 CERTIFICATE AND CRL PROFILES FOR SecureSign SERVER SERVICE 72
A7.1 Hierarchy of certificates 72
A7.2 Profile and settings of each certificate 72
A7.2.1 Contents of the subscriber's application (remarks) 73
A7.2.2 Validation of the settings in an issued certificate 73
A8 Specification Administration 74

Trademarks

JCSI, PaymentSign, SecureSign,and AccreditedSign are trademarks of Japan Certification Services, Inc.

1. INTRODUCTION

1.1 General

Japan Certification Services, Inc. (JCSI) provides two types of certificate issuing services named SecureSign and AccreditedSign™. SecureSign is established for customers who want to introduce a certificate issuing system based upon the PKI standards into their organization. AccreditedSign™ is established for certification and authorization services accredited under the the Electronic Signature Law of Japan.

JCSI issues the *SecureSign Public Service Standard* (this document) in conformance with the Certificate Policy and Certification Practices Framework developed by the Public Key Infrastructure working group (PKIX) of Internet Engineering Task Force (IETF).

SecureSign provides two types of services: Public Service and Private Service. In Private Service, customers define a certification policy and CPS (Certification Practice Statement) that are disclosed in a network domain required by the customer. In Public Service, on the other hand, JCSI decides on a certificate polity and CPS and discloses them to the public in JCSI's repository. This means that JCSI is the party who issues and signs certificates as part of Public Service (see Section 1.3).

This document describes the policy that JCSI defines regarding certificates JCSI issues as part of SecureSign Public Service as well as the CPS that JCSI applies to certificate issuing operations.

The PKIX defines the certificate policy and CPS as follows: A certificate policy is " a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements." This means that certificate policies are defined for each type of certificates issued. On the other hand, a CPS is defined as "a statement of the practices which a certification authority employs in issuing certificates." Therefore, a CPS is a document necessary for users to evaluate the quality of certificates issued in conformance with that CPS and to judge whether they should use the certificate. In other words, a certificate policy is a message regarding the use of certificates presented by the issuer, and a CPS is a message from the issuer for the user to judge the applicability of the certificate. In summary, a certificate policy and a CPS are two sides of the same coin and complementary to each other.

JCSI defines the contents of this document as the certificate policy for any certificates issued as part of SecureSign Public Service. Different policies for different certificates are indicated where necessary. Furthermore, this document serves as a detailed statement (CPS) regarding the system and practices JCSI employs to assure a high level of security and reliability and to ensure certificate issuing operations. In addition, this document is the rulebook for all entities (persons and objects, including JCSI and subscribers or customers) participating in SecureSign Public Service.

Any part of this document applies to customers who use SecureSign Public Service. Some parts of this document apply to customers who use SecureSign Private Service. Parts applicable to users of SecureSign Private Service are those describing the certification operations carried out by JCSI at its

operation center to issue, on behalf of a customer, certificates under the customer's name. However, other parts of this document will help users of SecureSign Private Service in creating certificate policies and CPSs.

Certificate policies and CPSs will be updated according to changes in the requirements that the SecureSign services should satisfy.

1.2 Object Names

This document shall be titled *SecureSign Public Service Standard*. Table 1-1 lists the object identifiers (OID) assigned to this document and related services.

Table 1-1 OIDs and objects assigned to JCSI

OID	Object
1.2.392.200075	Japan Certification Services, Inc.
1.2.392.200075.2	SecureSign Public Service
1.2.392.200075.2.1	SecureSign CPS (this document)
1.2.392.200075.2.2	SecureSign Policy for Web-server certificate
1.2.392.200075.2.3	SecureSign Policy for Public SSL/TLS server certificate
1.2.392.200075.2.4	SecureSign Policy for Public SSL/TLS client certificate
1.2.392.200075.2.5	SecureSign Policy for Public S/MIME certificate
1.2.392.200075.2.6	SecureSign Policy for Public signing certificate
1.2.392.200075.2.7	SecureSign Policy for Public Time Stamping certificate
1.2.392.200075.2.8	SecureSign Policy for Public Long Term SCA certificate

1.3 Community and Applicability

1.3.1 Entities and roles

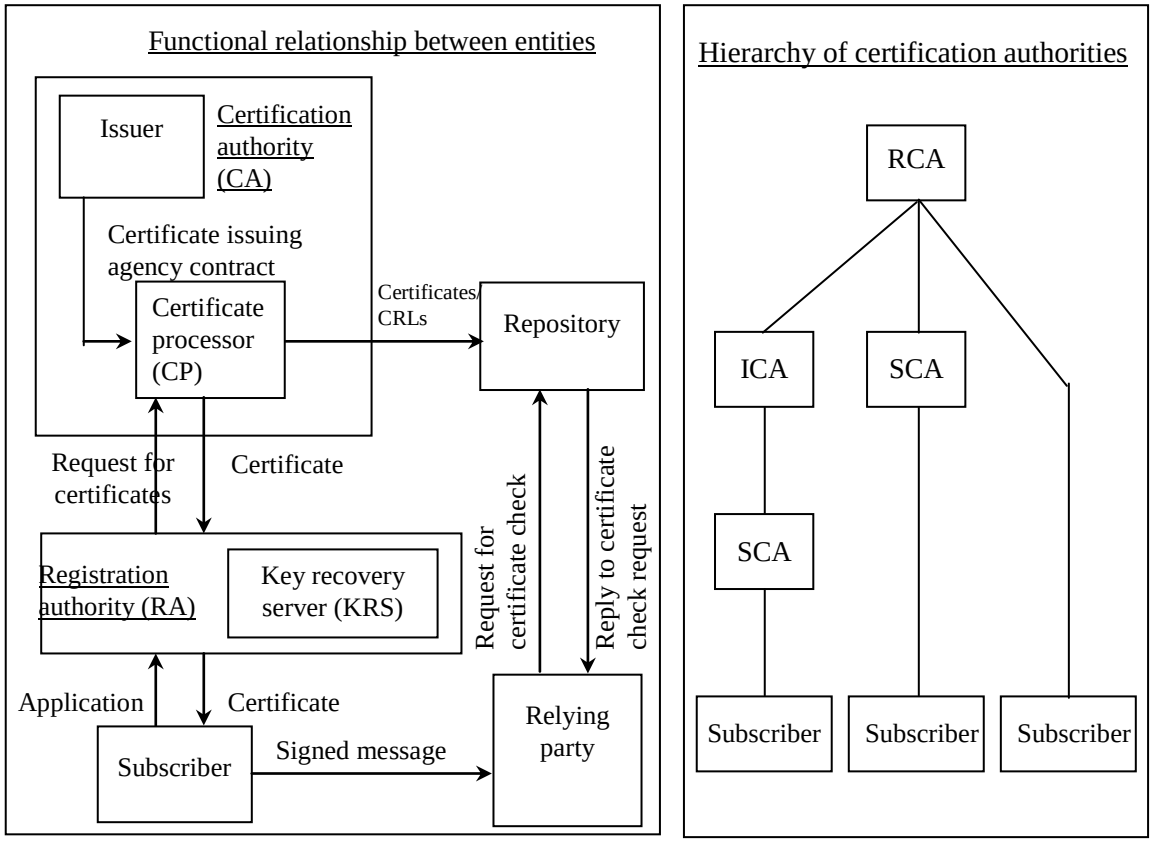
SecureSign contains entities as listed in Table 1-2. Figure 1-1 shows the functional relationship between entities and the hierarchy of certification authorities.

Table 1-2 Entities and their roles

Entity	Roles
Customer	An organization or a person in that organization who takes charge of a contract with JCSI for SecureSign Private or Public Service. In Public Service, the issuer of certificates is JCSI. Customers are delegated by JCSI to conduct RA operations and shall appoint an authorized person(s), or RAO(s), to RA operations. Customers shall adhere to the subscriber's obligations included in the Public Service contract made between the customer and JCSI as well as to the CPS and certificate policy (this document). In Private Service, the issuer of certificates is the customer. Customers shall appoint an appropriate member of their own organization as an RAO.
Subscriber	A person, an organization or object whose public key and subject name are combined in a certificate. A subscriber is a person who belongs to, or has membership of, the customer's organization. In Public Service, terms that the subscriber shall carry out are defined in the contract between the customer and JCSI.
Relying party	A person, an organization or object that relies on a subscriber's certificate and verifies the subscriber's digital signature.
End entity	Both subscribers and relying parties are called end entities.
Issuer	When issuing a certificate, the issuer creates and discloses a certificate policy and a CPS (without breaching the policy of a superior certification authority, if any). The issuer is an organization that signs a certificate with its own private key and thereby authenticates that certificate. The issuer is a managing subject in a certification authority. Its certificates are issued to the certification authority, registration authority, RAOs and subscribers.
Registration authority (RA)	SecureSign assumes that at least one RA exists in each model. An issuer delegates the RA to exercise several functions related to the issuance of certificates. Such functions include: Acceptance of certification applications Applicant identification Request to CA for certificates Delivery of certificates (and private keys) Decision on revocation of certificates and request to the CA for certificate revocation
RA officer (RAO)	A person who manages and operates the RA.
Certificate processor (CP)	An organization that creates certificates with a signature of the issuer and CRLs (certificate revocation lists) on behalf of the issuer according to a certificate issuing agency contract. Upon receiving a request for certificates from the RA, the CP issues individual certificates. The term "Issuing Authority(IA)" is used as the same meaning of "CP".
Repository	A repository is used to store certificates of subscribers, CRLs and other information on the SecureSign services, and reply to queries from relying parties.
Key recovery server (KRS)	As precautions against subscribers' losing or destroying their private keys, the KRS securely stores and recovers them when necessary.
KRS officer (KRO)	A person who manages and operates the KRS.

Certification authority (CA)	An organization that works as an issuer and certificate processor. SecureSign classifies the functions of certification authorities into the above two categories. In Public Service, JCSI acts as a certificate issuer and processor. In Private Service, on the other hand, the customer should act as an issuer, while JCSI as a certificate processor. Consequently, the part of this document describing a role of JCSI as a certificate processor concerns Private Service users. In SecureSign, more than one certification authority can exist hierarchically. They are a root certification authority, an intermediate certification authority and a subordinate certification authority.
Root certification authority (RCA)	The RCA resides at the top of the hierarchy (or at the beginning of a hierarchical certification path) and signs its own certificates and those for certification authorities (ICA or SCA) immediately below it. When no certification authorities exist below the RCA, it signs certificates for subscribers.
Intermediate certification authority (ICA)	ICA certificates are signed by the RCA. The ICA signs SCA certificates. When no SCAs exist below the ICA, it signs certificates for subscribers.
Subordinate certification authority (SCA)	SCA certificates are signed by the certification authority immediately above the SCA (or by the RCA if no ICA exists). The SCA signs the certificates for subscribers.
CA officer (CAO)	A person who manages and operates the CA.

Figure 1-1 Functional relationship between entities and hierarchy of certification authorities



Note: In general, a security domain is defined as a group of subscribers who receive signed certificates from the same issuer and observe the certificate policy developed by that issuer. Certificates of subscribers and CRLs are disclosed in the security domain. In SecureSign Public Service, however, a security domain is defined as a group of: subscribers who come under the root certification authority in SecureSign Public Service, and of relying parties who use certificates of those subscribers. Consequently, the certificates of subscribers and CRLs are disclosed to the public. Customers who use Private Service should determine how they set up a security domain, that is, a disclosure policy of subscriber's certificates and CRLs (disclosing domain and method), and should notify JCSI of such decisions.

JCSI, as an issuer of Public Service certificates, can divide this domain among customers. Customers shall assure uniqueness of the names of subscribers belonging to their respective subdomains. JCSI shall not interfere with any communications between a subscriber and a relying party in different subdomains.

1.3.2 SecureSign services

JCSI provides two types of SecureSign services:

Public Service -- Both the issuer and certification processor are operated by JCSI.

Private Service -- The issuer is operated by the customer, and the certification processor is operated by JCSI.

1.3.3 Uses

This section describes the uses of certificates with such expressions as "uses in a broad sense" and "uses in a narrow sense." Uses in a broad sense refer to cases where certificates are used as a guide to reasonable qualification for participation in a particular community or application. Examples include a case where a certificate is used to permit someone to make transactions involving an amount of money not exceeding a certain limit. On the other hand, uses in a narrow sense refer to cases where the use of a certificate is determined by the settings in the keyUsage and extendedKeyUsage fields within an X.509 certificate.

In Private Service, the operator of the certification authority, that is, the customer, shall define uses in both broad and narrow senses.

In Public Service, JCSI does not define uses in a broad sense. Therefore, JCSI does not present any applications to which issued certificates are applied or which limit uses. However, JCSI prohibits the use of certificates in crimes or other activities violating laws.

As part of Public Service, JCSI issues the following certificates for six uses in a narrow sense (see Chapter 7).

- SecureSign Web-server certificate

- SecureSign SSL/TLS server certificate
- SecureSign SSL/TLS client certificate
- SecureSign S/MIME certificate
- SecureSign Signing certificate
- SecureSign Time Stamping certificate

Both subscribers and relying parties shall not use certificates for any other uses than those in a narrow sense.

Note: Appendix A covers most descriptions of the standard for SecureSign Web-server certificate.

1.3.4 Interoperability and root certificates

Certificates and CRLs JCSI issues are used in an environment that needs a PKI. JCSI verifies the interoperability with more and more typical PKI-conforming products. However, since PKIs are under standardization, interoperability tests should be continued. For the latest information on interoperability, contact our sales department.

JCSI discloses RCA/SCA certificates for SecureSign Public Service in a repository. Users can download and install them as part of software. In distributing software containing RCA certificates to a third party, the user must give written agreement to root certificate installation before downloading.

1.4 Distribution of Service Specification Information

This CPS is disclosed in a repository. RAOs shall visit repositories on a scheduled basis to keep themselves updated about new SecureSign service contents and changes in the service specifications. A subscriber who wants to learn about SecureSign service contents should ask the RAO of his/her organization. RAOs can ask JCSI's help desk, which has been set up to offer help to customers. Inquiries via S/MIME mail are desirable. However, those over the phone will be accepted if they occur within the business hours of JCSI.

For inquiries, contact: Japan Certification Services, Inc.

Akasaka Daiichi Building, 4F, 4-9-17, Akasaka, Minato-ku, Tokyo, 107-0052

System Operations Department

Tel: +3-6804-2480

Fax: +3-6804-2482

Email: securesign@jcsinc.co.jp

2. GENERAL PROVISIONS

2.1 Obligations

As the issuer in SecureSign Public Service, JCSI defines the entity obligations as follows: In Private Service, the customer can set its own entity obligations by referring to the information given below. Obligations of JCSI as a trustee shall be the same as those in Public Service.

2.1.1 CA obligations

A CA shall issue and operate certificates according to the rules listed below. Also, a CA shall meet the conditions described in other parts of this document.

(1) As a certificate processor (CP), the CA shall securely generate and manage the issuer's signature key (private key).

(2) The CA shall issue subscriber's certificates in response to requests from the RA.

(3) The CA shall disclose CRLs, and other information, such as that on issuance of certificates, in a prompt manner in a repository.

(4) The CA shall manage certificate life cycles in cooperation with the RA.

(5) The CA shall revoke subscriber certificates in response to requests from the RA, and issue CRLs.

2.1.2 RA obligations

In this section, the functions of an RA shall include those of its administrator (RAO). Note that obligations regarding RA operations may be described as RAO obligations. In this case, obligations to automatic eligibility check systems without RAO operations shall be included in the RA administrator obligations.

(1) The RA shall properly review certification applications.

(2) The RA shall establish a scheme to identify the certificate applicants in the subdomain of a customer. For example, using personal names as application items may cause confusion if more than one person with the same name exists in the same domain. To prevent this, the RA shall take countermeasures as a subscriber verification (authentication) process.

(3) When the certificate application form contains fields for organization names, group names, etc., it is RAOs' obligation to develop and operate an identification process for organizations.

(4) When it generates public and private keys for subscribers (issuance patterns 2 and 3), the RA has an obligation to distribute certificates and keys to legitimate subscribers.

(5) The RA is obliged to install and operate RA servers in a secure environment.

(6) The RA shall verify (authenticate) that the subscriber whose name is on the certificate application form is the same person as the applicant. SecureSign Public Service requires the use

of “secret certification keys.”

(7) When revoking a subscriber’s certificate, the RA shall check the reasonability of revocation. The check covers applicant identification and confirmation of applicant’s decisions as necessary.

(8) Certificate application data can contain information not set in the certificate. If such information is contained, the RA must handle application data not reflected in the certificate as confidential information.

(9) The RA shall manage certificate life cycles in cooperation with the CA.

2.1.3 KRS obligations

SecureSign can implement a key recovery function as an RA option. If such a function is implemented, the key recovery server (KRS) is obliged to securely store and recover them whenever necessary as precautions against subscribers’ losing or destroying their private keys.

(1) A KRO (Key Recovery Officer) shall determine the keys to be recovered. Actual key recovery operations shall be accomplished through DualControl by the KRO and RAO.

(2) Data containing private keys, stored in the KRS, shall be backed up. The backups shall be securely maintained until the certificate expires.

(3) Upon revocation or expiry of the certificate, the data containing the private key shall be destroyed promptly.

2.1.4 Subscriber obligations

(1) Presentation of precise certification application contents
In acquiring a certificate, a subscriber shall submit a certification application that provides precise information on his/her present conditions.

(2) Limitation on the use of certificates
Certificates are issued according to this document (the customer’s CPS in Private Service) specifying use range, security domain and compensation for damages. Subscribers shall not present certificates for any uses out of the specified range.

(3) Obligation to the use of certificates by relying parties
For ciphertext from a relying party using a subscriber’s certificate, the subscriber shall agree that JCSI does not verify or check that in what transaction the certificate will be used or whether it is suitable for particular uses or circumstances and there are no restrictions imposed on relying parties due to the nature of public service.

(4) Obligation to maintain keys
Subscribers shall generate a pair of keys (private and public keys) using their software and hardware, submit the public key to the RA and receive a certificate from the RA. Alternatively,

they receive a pair of keys generated by the RA (the public key is included in the certificate). In any case, in order to deliver exact information to relying parties, subscribers are obliged to assume the following management:

(a) Management of confidentiality of private keys

Private keys must not be used, copied or backed up by any person other than the subscriber. In this context, subscribers shall manage private information -- such as their PIN, which is required to use a private key -- very carefully so that it will never fall to someone's knowledge. If a subscriber suspects that illegal use, copy or backup might have occurred, he/she must request revocation.

(b) Management of key pair

If a subscriber suspects an illegal relationship between the private key and the public key in the certificate, he/she must request revocation.

(5) Management of certificate contents

Subscribers shall check that the certificate describes their present conditions upon receipt and from time to time before using the certificate. When a subscriber finds that the information contained in the certificate is not (or no longer) true to his/her present conditions, the subscriber shall request revocation.

(6) Prompt revocation request

In the cases above (4)-(a) (b) and (5), subscribers shall promptly request revocation.

(7) Keeping in contact with RAO

In the cases above, subscribers shall follow the instructions of an RAO. Revocation requests shall be made via the RAO. Therefore, subscribers shall keep in contact with the RAO.

2.1.5 Relying party obligations

Relying parties must give consent to the Relying Party Agreement published in a repository. As set forth in the Relying Party Agreement, relying parties shall check the validity of certificates possessed by subscribers as their transacting parties.

(1) Limitation on the use of certificates

Certificates are operated according to this document (the customer's CPS in Private Service) specifying purpose, a range of uses, subscriber certification method and compensation for damages. Relying parties shall understand and agree with these provisions to use certificates. Relying parties shall use certificates presented by their communicating parties within the range of uses described or cited in the certificates.

(2) Obligation to verify the validity of certificates

To use certificates, relying parties shall verify the validity of the certificates. Validity

verification shall include the following:

(a) Check that all the certificates on the certificate path meet the conditions listed below. In Public Service, it is assumed that the JCSI root certificate is trusted.
- Certificates are not tampered.
- Certificates are not expired.
- Certificates are not revoked.
- The purpose of certificate use in (1) above is proper.

(b) Verify the signature on the subscriber's certificate

(c) Items stated in the presented certificates (especially the Subject and Subject Alt Name items) meet the provisions prescribed in Chapter 7.

(3) Installation of SecureSign public root certificates
SecureSign public root certificate is not contained in some PKI application software. To use such application software, SecureSign public root certificate can be installed as trusted certificates. Hash values (SHA-1 and MD5) for SecureSign public root certificate is published on the JCSI Web site. In installing the SecureSign public root certificate, relying parties shall compare the hash values with those of the SecureSign public root certificate to be installed.

2.1.6 Repository obligations

JCSI shall disclose information about the created CRLs in the repositories (see Table 4-2) and help relying parties to retrieve the CRLs in the repositories at any time and to check the validity of subscriber's certificates to determine if they are still available.

JCSI repositories also contain other information about the SecureSign service and disclose it with the method shown in Table 2-1.

2.2 Liability

As a certification authority (CA), JCSI shall be liable for providing customers with SecureSign Public Service, and customers shall be liable for maintaining a registration authority (RA) and its administrator (RAO). These liabilities are defined as follows:

2.2.1 JCSI liability

(1) In SecureSign services, JCSI warrants the following:
- When an RAO identifies a subscriber as per Chapter 3, and requests the issuance of a certificate, JCSI shall issue a certificate that exactly reflects the details (e.g., the subject's distinguished name as in a certificate) of the RA's request for a certificate.

- JCSI shall provide a means of assuring the delivery of a key pair only to the subscriber who should have that key pair. (Issuance patterns 2 and 3)
- As per Chapter 4, JCSI shall register CRLs issued as part of Public Service in JCSI's repositories on a scheduled basis and disclose the revoked certificates in CRLs at all times until those certificates expire, except for suspension due to system maintenance or system shutdown for emergency reasons.
- Upon receiving a revocation request from the RA, JCSI shall revoke the certificates of certain subscribers without fail.
- As per Chapters 5 and 6, JCSI shall operate a certificate issuing system without any private keys of certification authorities being compromised due to a key theft, except for cases where they are inferred or calculated from public keys.
- JCSI warrants that certificates, CRL format and attributes conform to the provisions in Chapter 7 at the time of issuance of the certificates.

(2) When a customer uses RA outsourcing service, JCSI shall operate the service with care of a bona fide administrator.

(3) When a customer uses key recovery service, JCSI shall operate the service with care of a bona fide administrator.

(4) Notwithstanding (1) through (3) above, JCSI shall have a right to temporarily suspend the whole or part of SecureSign Public Service without notice to the customers and subscribers when:

- JCSI performs emergency maintenance of its own facilities for SecureSign Public Service;
- SecureSign Public Service discontinues due to fire or power failure;
- SecureSign Public Service discontinues due to natural disasters including earthquake, eruption, floods or seismic sea wave;
- SecureSign Public Service discontinues due to war, disturbance, riot, civil commotion or labor disputes; or
- JCSI acknowledges the necessity of suspension of SecureSign Public Service for operational, technical or other reasons including the fulfillment of contracts with customers.

(5) The liability of JCSI for customers, subscribers and relying parties regarding SecureSign services is limited to those prescribed by (1) through (4) above.

2.2.2 Customer liability

The provisions for customer liability below assume that the RA consists of an RA server and its administrators (RAOs).

(1) Customers are liable for proper development and operation of a process that performs eligibility checking of and reviews (authenticates) certificate applications as well as verifies the

legitimacy of the contents of certifications.

(2) When customers install and operate an RA server at their own site, they are liable for security of that RA server.

(3) Customers shall make each individual subscriber understand his/her obligations and JCSI's liabilities.

2.3 Financial Responsibility

2.3.1 Responsibility for compensation

(1) When JCSI compensates for damages caused by a breach of the provisions prescribed in Section 2.2.1, the amount of indemnity paid to customers shall be limited to the amount agreed upon in the contract with the customer, and that paid to relying parties shall be limited to the amount agreed upon in the Relying Party Agreement. JCSI shall bear no responsibility for damage and loss of profit caused by reasons not attributable to JCSI or by special circumstances that JCSI may or may not have foreseen.

(2) When JCSI suffers damage due to a customer's failure to fulfill the obligations prescribed in this document or a breach of the provisions prescribed in Section 2.2.2, JCSI shall have a right to claim an indemnity for the relevant damage.

(3) In relation to the limitation on the use of certificates by subscribers prescribed in item (2) of Section 2.1.4, subscribers shall bear full responsibility for any trouble caused by their use of a certificate for uses out of the specified range. When JCSI suffers damage due to such trouble, the subscriber shall compensate JCSI for the damage. In relation to revocation requests prescribed in item (5) of Section 2.1.4, subscribers shall bear full responsibility for any trouble caused by a third party's pretense of being a subscriber or by misjudgment of a relying party, resulting from the subscriber's negligence of a revocation request. When JCSI suffers damage due to such trouble, the subscriber shall compensate JCSI for the damage.

(4) In relation to the limitation on the use of certificates prescribed in item (1) of Section 2.1.5, relying parties shall bear full responsibility for damage caused by the relying party's use of a certificate beyond the specified range. JCSI shall bear no responsibility for such damage. The verification of the validity of certificates by relying parties, prescribed in item (2) of Section 2.1.5, is generally done automatically by the software. However, relying parties shall make final decisions. JCSI shall bear no responsibility for damage resulting from transactions made by the relying party in spite of its failure or negligence of validity verification.

2.3.2 Fiduciary relationships

JCSI does not act as an agent or trustee in terms of finance for customers, subscribers and replying parties of the SecureSign public service. However, notice that JCSI is in cooperation with NEC Corporation, Hitachi, Ltd., and Fujitsu Ltd. These companies manage JCSI as the main stock holders

while JCSI trusts its operations to them.

2.3.3 Accountability

JCSI shall be managed according to the accounting rules under the Commercial Law of Japan.

2.4 Interpretation and Enforcement

2.4.1 Governing law

This documentation shall be interpreted according to Japanese laws and regulations.

2.4.2 Severability, survival, merger, notice

JCSI may segment the SesureSign public service, consolidate the other services to the SecureSign public service or merge the SecureSign public service to the other services.

2.4.3 Dispute resolution procedures

Tokyo District Court shall be the exclusive agreed jurisdictional court for lawsuits and legal acts between customers, subscribers or relying parties and JCSI. Any question arising out of, or in connection with, this document or the contract, or any matter not stipulated therein shall be settled upon consultation between both parties.

2.5 Fees

The basic fees for SecureSign shall be disclosed on the JCSI web site. The other fees shall be disclosed by JCSI sales personnel on demand.

2.6 Publication and Repositories

2.6.1 Publication of CA information

In SecureSign Public Service, JCSI operates repositories to provide repository service to customers.

Caution: Certificates and CRLs issued for SecureSign Private Service are not disclosed to the public domain. In other words, such information is confined in the customer's security domain.

2.6.2 Frequency of publication

(1) Disclosure of this document is defined in Chapter 8.

(2) Revocation information is disclosed in the CRL form on JCSI's repositories within 24 hours after the revocation procedure has been performed.

(3) Revocation information for target certificates is kept disclosed in the CRL form on JCSI's repositories until the expiration dates of the certificates.

(4) Other information is updated and disclosed from time to time at the discretion of JCSI.

2.6.3 Access controls

Information open to the public is disclosed with the method shown in Table 2-1, "Contents of JCSI's repositories."

Note: Anyone involved has access to, but cannot modify this document.

2.6.4 Repositories

(1) JCSI repositories are used to store and disclose the CRLs and other information about the SecureSign services (see Table 2-1).

(2) The CRLs stored on the repositories are disclosed to relying parties.

(3) A means of access to JCSI's repositories and its addresses are available at JCSI Web site (http://www.jcsinc.co.jp).

(4) A JCSI optional service allows customers to duplicate subscribers' certificates and CRLs in repositories that they administrate.

(5) Repositories are operated for 24 hours a day. However, with prior notice on the Web site, repositories may be temporarily unavailable for technical reasons such as system maintenance. In an emergency, repositories may be shut down without notice.

Table 2-1 Contents of JCSI repositories

	Document name	Audience	Disclosure method
			http/https
Standard	*SecureSign Public Service Standard* (CPS)	Any person involved	Yes
Agreement	Relying Party Agreement	Relying parties	Yes
	Root Certification Installation Agreement	Software providers	Yes
ICA/SCA	Public Service Root Certificate	Software providers, subscribers and relying parties	Yes
	CRL	Relying parties	Yes
Notice	Notice from SecureSign	Any person involved	Yes

2.7 Compliance audit

In operating SecureSign Public Service, JCSI periodically self-audits to verify that it conforms to the security provisions including this document.

2.7.1 Frequency of audit

Self-audit is conducted in the following events:

(1) One year after the previous self-audit

(2) Upon an important update on security management

2.7.2 Identity/qualifications of the auditor

JCSI internally appoints experienced personnel with sufficient skills in compliance audit as auditors.

2.7.3 Auditor's relationship to the audited party

Auditors shall belong to a different organization from the certificate operating department.

2.7.4 List of topics covered under the compliance audit

JCSI develops rules and procedures for self-audit and clarifies purpose, auditing organization, schedule, entities to be audited, working procedures and progress in improvement.

2.7.5 Actions taken as a result of a deficiency found during compliance audit

JCSI shall take corrective actions against problems found in audits as soon as possible.

2.7.6 Report on compliance audit results

Although JCSI conducts self-audits, it does not report to an external entity.

2.7.7 Customer audit

Upon customer’s request, JCSI will accept the customer’s audit at its expense.

2.8 Confidentiality

2.8.1 Types of information that must be kept confidential

JCSI and customers shall not disclose or divulge to a third party without written consent from the other party confidential information (including information on subscribers) that in connection with the SecureSign the other party has presented either (i) in a written form with an explicit statement of confidentiality or (ii) orally with an explicit declaration of confidentiality, followed by the verification of the relevant information’s confidentiality in a written form within 14 days of the date of presentation. They also shall not use such information beyond limitations to provide or use the SecureSign services.

2.8.2 Types of information that are not considered confidential

Notwithstanding Section 2.8.1, types of information prescribed by the following items shall not be considered confidential.

(1) Information that should be included in a certificate or CRL except subscriber's distinguished name in the certificate

(2) Information included in this CPS

(3) Information known to the receiving party or in the public domain at the time of disclosure

(4) Information that has become known in the public domain without the receiving party's fault

(5) Information acquired lawfully from any third party without secrecy obligations

(6) Information that has been created through product development by the receiving party, without using the disclosed information

(7) Information disclosed to a third party by the disclosing party without secrecy obligations

2.8.3 Disclosure of certificate revocation information

When a subscriber's certificate is revoked upon a revocation request from a subscriber, a reason code and the date of revocation are included in the CRL. Therefore, the reason code and the revocation date are not considered confidential and will be disclosed to all the relying parties. Other detailed information about revocation is not disclosed.

2.8.4 Release to law enforcement officials

Upon non-forcible inquiry from an investigating authority, court, bar association or other officials with legal authority, JCSI can voluntarily release confidential information, known to JCSI, about customers and subscribers to such law enforcement officials when such release is considered to be a means of lawful self-defense or emergency evacuation.

2.8.5 Release as part of civil procedure

Included in Section 2.8.4.

2.8.6 Disclosure upon owner's request

When the owner of an issued certificate notifies in writing that his or her rights or benefits have been infringed or may be infringed, JCSI or a customer confirms that he or she is the right owner or the trusted agent of the owner, then discloses the following information to him or her via the RAO.

- Certificate application and attached document
- Materials and records used to confirm that the subscriber is right person
- Information listed in the certificate

Except the cases stated in Sections 2.8.4 and 2.8.5, JCSI does not accept the requests submitted by the

relying parties who demand the disclosure of subscriber's information. JCSI discloses only the revocation information of the issued certificate in the CRL for the relying parties unless the certificate expires.

2.8.7 Any other circumstances under which confidential information may be disclosed

When re-entrusting part of its business, JCSI may disclose confidential information to the re-entrusted agent. In this case, to prevent divulgement, JCSI shall include confidentiality obligations in the entrustment contract.

2.9 Intellectual Property Rights

JCSI owns the copyright of this document (CPS) and the software and documents JCSI lends to customers. Customers using SecureSign Private Service may use this document as a guide in creating a certificate policy or their CPS. However, if such certificate policies or CPSs are deemed as a secondary product of this document, JCSI shall reserve the right as the original copyright owner.

2.10 Personal Information Protection

JCSI handles personal information on the basis of the personal information protection policy which is published on JCSI's WEB sight. However during SecureSign service there are also types which do not entry personal information in the certificate. In addition, receiving the trust of the customer, there are times when JCSI issues certificates where private information is entried.

3. IDENTIFICATION AND AUTHENTICATION

JCSI operates a trusted root certificate authority for all certificates issued in SecureSign Public Service. This means that JCSI will guarantee the contents of the certificates JCSI issues. Therefore, JCSI requires RAOs to properly review certificate applications on behalf of JCSI. Proper review requires exact identification information available for reviewing certificate applications and establishment of a verification (authentication) process that compares certificate application contents (application form contents) developed and used by the RAO with identity information contents, as well as a process that verifies (identifies) that the applicant for a certificate is identical to the person whose name is written in the application for a certificate. In other words, the RAO shall recognize that it is an important obligation to exactly design/construct/maintain:

- Identity information contents (including data for identification)
- Certificate application form
- Subscriber verification process (identification and authentication)

and shall be liable for accidents/disputes resulted from negligence of this obligation. The remaining part of this chapter describes various guidelines for identification and authentication, and guidelines for setting values in certificate application forms with a view to the fact that certificate application form contents include information necessary for identification and authentication. When certificates are issued in batches, they are sent to identified subscribers. Although this issuance workflow requires no certificate applications, it is the RAO's obligation to establish/maintain a process to assure delivery of certificates to legitimate subscribers. In SecureSign Private Service, the above obligation shall be imposed upon the RAO by the issuer.

3.1 Initial Registration (Initial Application)

3.1.1 Types of names

In SecureSign Public/Private Service, no certificates are issued to natural persons. Therefore, applicants (subscribers) should belong to a meaningful domain. The following types are possible for the name included in certificate application forms (and also identity information). In determining a domain structure and component types, refer to related rules, such as X.500 directory rules/X.509 certificate's subject distinguished name rules.

(1) Domain name (corporate/association name)

(2) Subdomain name (organization/group name)

(3) Subscriber name (personal name, application name or computer name)

(4) Subscriber alternative name (employee number, MailAdder or URL)

(5) Secret certification key (data for identifying applicants exchanged and shared between the RAO and subscribers outside the PKI)

Note*:* Items (1) through (4) are examples of name types for comparative verification (authentication)

with identity information contents. Item (5) is data for identification verification and essential for SecureSign Public Service.

3.1.2 Need for names to be meaningful

Names contained in certificate application forms have to be meaningful. However, JCSI is not concerned about this. Names shall obey the rules for names in the domain administrated by the RAO. The RAO shall ensure that certificate applicants (subscribers) obey the rules. When a subscriber uses, for example, the "organization name" in the name field on the certificate application form, an identical "organization name" as a matching key exists in the identity information contents. More detailed setting rules are necessary to clarify not only the meaning of the name but also whether the "organization name" is actually the name of a department, section, or a formal or abbreviated name.

3.1.3 Rules for interpreting various name forms

Interpreting various name forms depends on the RAO's setting rules. For example, rules specifying that the space between the first and last names may be either a double byte or a single byte, or whether "ABC Corporation" is equivalent to "ABC Corp." or not.

3.1.4 Uniqueness of names

The name values to distinguish entities (or subjects) shall be unique in the domain the RAO administers. For example, "First Sales Department" as a department type is a unique value and not equivalent to "1st Sales Department." However, since more than one person with the same name may exist in a domain, personal names as identification names must be accompanied by a modifier such as the domain name or subdomain name to associate the entity with the name value. A subscriber's alternative name or secret certification key may be used as a matching key. More precisely, the uniqueness of names must be implemented as a subscriber verification (authentication) process.

3.1.5 Name claim dispute resolution procedure

Name claim dispute shall mean a dispute (e.g., trademark infringement, unfair competition, or use for illegal purposes) about the name the applicant has entered in the certificate application form or the subject distinguished name specified on the certificate issued as the result of authentication.

Basically, name claim disputes that arise in a domain administered by an RAO shall be resolved in that domain. Disputes across multiple domains or those involving a relying party shall be resolved by the parties (the RAO and relying party). In both cases, JCSI is not involved in disputes. However, JCSI shall be a party in disputes arising from an RAO's infringement of the rights of JCSI.

3.1.6 Recognition, authentication, and role of trademarks

It must be guaranteed that the distinguished names of the issuer and subscriber specified on certificates

do not infringe any rights of others including trademarks and trade names. In SecureSign services, the responsibility for the guarantee shall be borne by RAOs, who are liable for eligibility check of application contents, authentication, and proper establishment/operation of a process verifying the validity of certificate contents. JCSI shall be exempted from the responsibilities for any damage resulted from such infringement or obstruction.

3.1.7 Method to prove possession of private keys

(1) Case where the RA server generates keys (issuance patterns 2 and 3)
When the RA server generates public and private keys, customers shall be obliged to deliver certificates and keys to legitimate subscribers. The delivery and reception verification means required must be implemented in the customers as a secure delivery process. JCSI shall bear no responsibility for delivery-related accidents. Secret certification keys as activation data for delivery media that store certificates and private keys are essential (for secret certification keys, see Section 3.5).

(2) Case where the client generates keys
The RA server shall confirm that the certificate applications and public keys to be registered are signed with the private key corresponding to the public key (EX.PKCS#10).

3.1.8 Authentication of organization identity

Even when the certificate application form contains a field for organization names, it is an RAO obligation to develop and operate an identification process of organizations.

3.1.9 Authentication of individual identity

In SecureSign Public Service, secret certification keys must be used to verify (authenticate) that the subscriber whose name is on the certificate application form is the same person as the applicant. The RAO shall require subscribers to enter the secret certification key value delivered beforehand to subscribers into the secret certification key field defined in the certificate application form. The RAO must implement a process verifying that the secret certification key value on a subscriber's certification application matches the secret certification key value held in the subscriber's identity information contents (for secret certification keys, see Section 3.5).

3.2 Routine Rekey with Certificate Updates

Rekey (key regeneration) shall follow certificate updates (re-creation) due to expiration. There is nothing different from the initial registration described above, and the same guidelines for identification and authentication described in the initial registration sections shall apply to the certificate updating procedure. It is essential to generate and deliver new secret certification keys.

3.3 Rekey after Revocation

Rekey (key regeneration) shall follow certificate reissuance (re-creation) due to revocation. There is nothing different from the initial registration described above, and the same guidelines for identification and authentication described in the initial registration sections shall apply to the certificate reissuing procedure. It is essential to generate and deliver new secret certification keys.

Note: JCSI defines the guidelines for certificate updating and reissuing procedures in Sections 3.2 and 3.3 as the same guidelines described in the initial registration sections. If necessary, a procedure different from that for initial registration may be applied (and implemented in the process), but this must be done by the RAO. The work includes development of rules -- for example, applications for certificate update will be accepted from one month before the expiry date, or applications for reissue will not be accepted unless the revocation of the issued certificate is confirmed -- and implementation of a verification process.

3.4 Revocation Request

Processes for verification of application contents (including identification of applicants), starting from the acceptance of a request for revocation of subscriber's certificates, and including revocability check, must be established on the RAO's responsibility. The SecureSign service provides RAOs with only a revocation operation means, not a standard identification or authentication process for revocation applications. Unlike applications for certificates, in applications for revocation, applicants are not necessarily subscribers. The RAO should establish a process that assumes applicants to be subscribers, issuers, relying parties and even third parties.

3.5 Secret Certification Key

A secret certification key is confidential information shared between the subscriber and RAO. Secret certification key must be generated or selected by the RAO or RA server, and delivered to subscribers in some out-of-band method of PKI (e.g., by first-class mail or in-house first-class quasi mail). Secret certification keys must be corresponding and unique to subscribers in the domain the RAO administers. Secret certification keys are used for the purposes listed below. For SecureSign Public Service, JCSI requires the RAO to use and operate secret certification keys.

(1) Data for verifying the identity of applicants

Secret certification keys are used as information to verify that the subscriber whose name is specified on the certificate application is identical to the applicant. This is to eliminate possible applications by someone pretending to be or on behalf of a subscriber (see Section 3.1.9 for actual verification procedure).

(2) Data for activating storage media

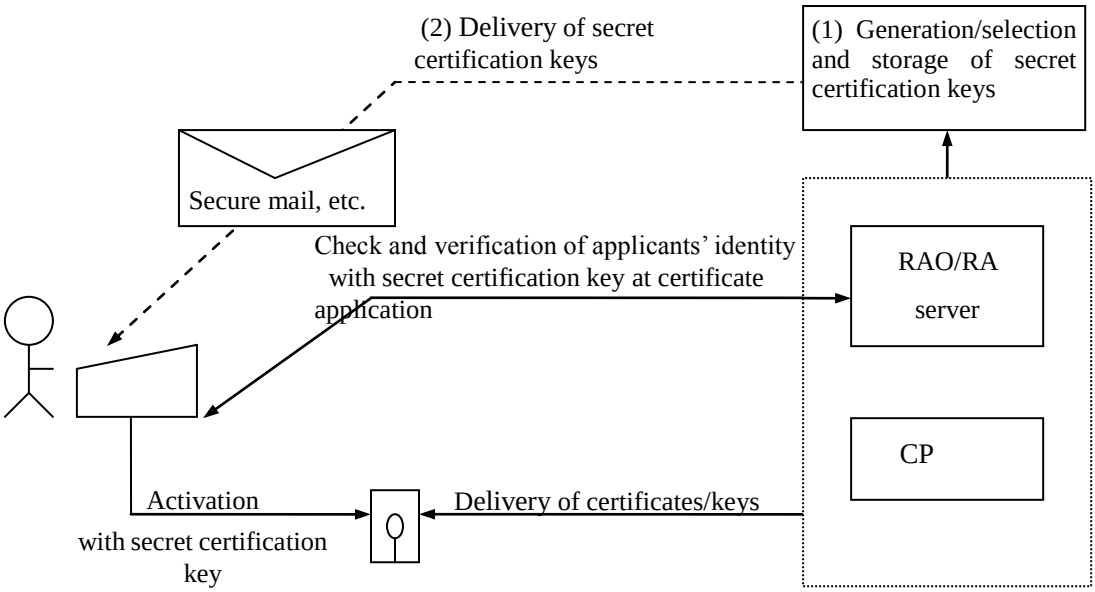
As described in item (1) in Section 3.1.7, when issuance pattern 2 or 3 in SecureSign services is employed, private keys and certificates are contained in storage media such as an FD or IC card and

delivered to subscribers. Activation data such as a PIN or password must be set in the storage media to be delivered. In SecureSign services, activation data is defined and handled as a secret certification key, or information necessary for identifying the legitimate subscriber who should receive a key and certificate. The delivery media and secret certification key should be ed by separate mail or route, since delivering them in one package, if they are delivered to a wrong person, can lead to certificate/key abuse by a third party.

Rule for secret certification key: Eight or more alphanumeric characters long

Figure 3-1 illustrates how secret certification keys are generated and distributed, and their example usage.

Figure 3-1 Generation/delivery of secret certification keys and their example usage



3.6 Handling of Certification Application Data

Certificate application data can contain information not written in the certificate. Information not reflected in certificates should be handled as confidential information as prescribed in Section 2.8.

4. OPERATIONAL REQUIREMENTS

4.1 Certificate Application, Issuance and Acceptance

SecureSign provides a wide range of services to meet various needs of customers who want to outsource certificate-related operations. The services are classified according to type and pattern. SecureSign provides eight types of services.

Types A and B are for Public Service. In type A, the Public Service certification authority, whose certificate issuer is JCSI, directly issues subscriber's certificates. In type B, customer-specific certification authorities (SCAs), whose certificate is signed by the Public Service certification authority and whose certificate issuer is JCSI, issue subscriber's certificates. As part of SecureSign Public Service, JCSI discloses the revocation information (CRL) of subscriber's certificates in the repositories for all customers issued by all CAs under the RCA for Public Service.

Types C and D are for Private Service. In type C, a single customer-specific RCA exists, and in type D, a customer-specific RCA and a customer-specific SCA whose certificate is signed by the RCA exist. In Private Service, repositories are operated by customers. That is, the security domain lies in the customers and is closed against the outside.

SecureSign requires that an RA operated by customers be installed. Each of service types A, B, C and D may or may not be further classified into two subtypes, depending on the needs of the RA installation site. In subtype 1, the RA system is installed in the JCSI center and operated by the RAO stationed in the customer's site. In subtype 2, the RA system, provided by JCSI, is installed in the customer's site and operated by the RAO. JCSI can be entrusted with the key recovery function as an outsourcing service to customers who choose subtype 1. The key recovery function is also available to customers choosing subtype 2. In this case, the customer should install the function in its organization. JCSI specifies a communication protocol between the RA and CA. Customers choosing subtype 2 must observe this communication protocol in communicating with the CA.

Tables 4-1 and 4-2 summarize the service types as a summary of the above explanations.

Table 4-1 List of service types (Part 1: Characteristics of individual service types).

<table>
<tr><th colspan="3">Type</th><th>Issuer and security domain</th><th>Issuing CA (see Figure 1-1)</th><th>RA</th></tr>
<tr><td rowspan="4">Public Service</td><td rowspan="2">JCSI SCA</td><td>A-1</td><td rowspan="4">JCSI is an issuer of certificates.

Based on the trustworthiness of JCSI, all subscriber certificates are trusted by relying parties worldwide.</td><td rowspan="2">JCSI operates RCAs, ICAs and SCAs. Certificates are issued from SCAs.</td><td>Installed at JCSI
(Secure environment and operation become available in a short time.)</td></tr>
<tr><td>A-2</td><td>Installed at the customer
(Linkage to the customer’s mission-critical system facilitates automatic eligibility check.)</td></tr>
<tr><td rowspan="2">Customer SCA</td><td>B-1</td><td rowspan="2">JCSI operates RCAs and ICAs. Certificates are issued from the SCA operated by customers under the ICA.</td><td>Installed at JCSI
(same as above)</td></tr>
<tr><td>B-2</td><td>Installed at the customer
(same as above)</td></tr>
<tr><td rowspan="4">Private Service</td><td rowspan="2">Single CA</td><td>C-1</td><td rowspan="4">The customer issues certificates. JCSI acts as an issuing agent. Subscribers’ certificates are trusted by relying parties specified by the customer (relying parties to whom RCA certificates are distributed).</td><td rowspan="2">Certificates are issued directly from the single RCA operated by the customer.</td><td>Installed at JCSI
(same as above)</td></tr>
<tr><td>C-2</td><td>Installed at the customer
(same as above)</td></tr>
<tr><td rowspan="2">Hierarchical CA</td><td>D-1</td><td rowspan="2">The customer operates an RCA, (ICA) and an SCA. Certificates are issued from the SCA.</td><td>Installed at JCSI
(same as above)</td></tr>
<tr><td>D-2</td><td>Installed at the customer
(same as above)</td></tr>
</table>

Table 4-2 List of service types (Part 2: Installation site and managing subject)

Type			RCA	ICA	SCA	CAO	RA	RAO	Repository	Key recovery
Public Service	JCSI SCA	A-1	*1	*1	*1	*1	*2	*3	*1	Entrusted by JCSI
		A-2					*3			Operated by the customer
	Customer SCA	B-1			*2	*2	*2			Entrusted by JCSI
		B-2					*3			Operated by the customer
Private Service	Single CA	C-1	*2	None	None	*2	*2	*3	*3	Entrusted by JCSI
		C-2					*3			Operated by the customer
	Hierarchical CA	D-1		*2	*2	*2	*2			Entrusted by JCSI
		D-2					*3			Operated by the customer

*1 Installed at JCSI and operated by JCSI

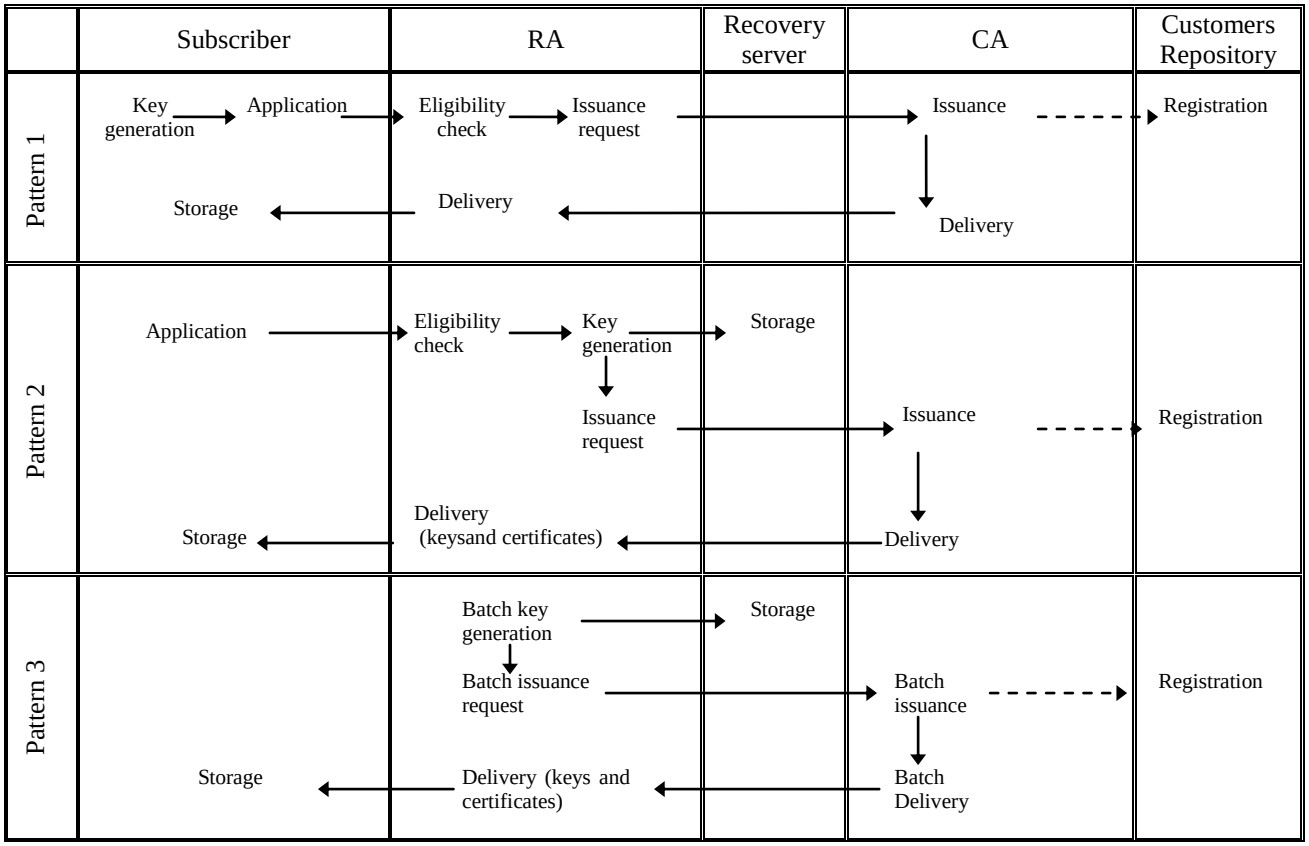
*2 Installed at JCSI and operated by the customer

*3 Installed at the customer and operated by the customer

In SecureSign services, CRLs shall be disclosed in the repositories. In SecureSign Public Service, JCSI operates the (logically) single repository. In Private Service, they may be placed in any place by customers and the CRLs shall be disclosed there by the CA or RA.

SecureSign provides three patterns of certificate issuing as shown in Table 4-3. The key recovery service is available only to issuance patterns 2 and 3, in which the RA generates subscriber's keys.

Table 4-3 Issuance pattern



Issuance pattern	Subscriber's key generation	Trigger for issuance	Eligibility check method		
			Automatic	Advance	Manual
1	Subscriber	Triggered by a subscriber or RAO	Yes	Yes	Yes
2	RA		Yes	Yes	Yes
3		Batch	--	Yes	--

Eligibility checking is carried out automatically, manually or in advance. Details depend on implementation.

- Automatic check: The RA system operates in connection with another system of the customer, and checks applicants for eligibility by accessing the customer's system whenever a subscriber application occurs.
- Advance check: With registration information on (advance-checked) applicants from customers stored beforehand in the RA system (including the RAO terminal), the applicants are checked for eligibility by comparing their application contents with the registration information. In batch issuance (pattern 3), a batch issuance request is made upon the registration information.
- Manual check: The RAO checks subscriber applications one by one for eligibility by verifying

the contents.

4.2 Certificate Suspension and Revocation

In the event of a change in certificate contents such as distinguished name, replacement of that certificate with another, suspension by a subscriber, or compromise of a subscriber's private key or a certificate signature key, the certificate shall be revoked. Under present conditions, no temporary invalidation of certificates (certificate suspension) shall be available.

Normally, revocation procedures shall be initiated upon a subscriber's request. When the RAO admits the necessity of revocation, the CA accepts the request for revocation. Certification revocation lists (CRLs) are updated and disclosed periodically.

4.3 Security Audit Procedures

JCSI administers a system designed to record and audit center operation logs as a means of keeping the environment safe. The CA, RA, and repositories leave audit trail and periodically security-audit them. Audit trail includes:

- Operation and running logs of the CP and RA servers. These include all logs for controlling the CA's private key and all event logs such as; issuing certificates for authorizing the servers and RAOs; startups and stops; registering, issuing, and revoking individual subscriber's certificates;
- Monitoring logs for networks and servers in the rooms where certificate-issuing systems are installed, firewalls and intruder detection systems. These include records of all packets and transactions.
- Operation and running logs of the repositories. Records of all accesses from any parties or parties authenticated and access-controlled, including records of revisions of information in the repositories.
- Running records (including alarm emissions) of motion detectors, monitoring cameras and video units, and entry/exit gate devices covering the rooms where certificate-issuing systems are installed. Alarm emissions are handled as abnormality records in the cases described below.

This audit trail is periodically security-audited. Records regarded as normal are replaced with audit records and thus deleted. Records of erroneously or deliberately produced abnormalities are individually verified. Corrective actions are taken if considered necessary. Security audit records including these records considered as those of abnormalities and records of corrective actions taken are stored with the method set forth in the next clause until a compliance audit (clause 2.7) is conducted, and are verified again. A security audit is conducted at least once a month.

4.4 Archiving

SecureSign public services archive the documents and digital data listed below. In the storage of these documents, provision is made to prevent leakage and tampering. The documents are stored in their originals. For that purpose, such a specified room is used that is divided with partitions and walls and

is equipped with functions proofed against disasters, burglars, fires, and water as well as lockable doors with unlocking events to be recorded in the ledger.

JCSI provides specified parties alone with a specified range of archived and stored information in cases set forth in clauses 2.8.4 through 2.8.7 of this document.

JCSI securely deletes all documents and digital data that are past their storage periods. The documents are shredded or otherwise disposed of, while the digital data is deleted by destroying the mediums containing it or overwriting it with void information, among other methods. Following is data to be archived. The figures in parentheses are storage periods.

- The originals of commissioning agreements for commissioning part of CA business to another party and related documents. (Until the commissioning agreements are terminated.)
- The originals of control information and history of operations concerning personnel engaged in CA business, organization, system, main representatives, and supervisors and directors. (The latest version to be stored permanently, and the old version preceding the revision is to be stored until the next internal audit <compliance audit (clause 2.7 of this document)>.)
- The originals of records of internal audits (compliance audits <clause 2.7 of this document>) and audit reports. (For 10 years.)
- Log data about the issuance of CA certificates corresponding to the administration of CA private keys (key generation, storage, activation/deactivation, backup/restoration, and discarding). (Until the security audit is over. Records of security audits are to be stored until the next internal audit <compliance audit (clause 2.7 of this document)>.)
- Records of security audits (clause 4.3 of this document). (Until the next internal audit <compliance audit (clause 2.7 of this document)>.)
- Records of authorizations and de-authorizations set forth in procedural controls (Chapter 5 of this document). (Until the next internal audit <compliance audit (clause 2.7 of this document)>.)
- Records of facility maintenance, system maintenance, revisions and disorders. (Until the next internal audit <compliance audit (clause 2.7 of this document)>.)
- All certificates and CRLs issued. Certificates and CRLs of the SecureSign public services CA itself, and all certificates and CRLs concerned. (For 10 years after the expiration.)
- This document (SecureSign Public Service Standard), detailed procedures, related regulations for protecting personal information, and their revision records. (The latest version is to be stored permanently, while the old version preceding the revision is to be stored for 10 years after the revision.)

4.5 Key changeover

Before the remainder of the validity period of the CA public key for SecureSign public services becomes shorter than the maximum validity period of the subscriber’s certificate, JCSI suspends the issuance of the new subscriber’s certificate with the related key and generates a new pair of signature

keys with the method set forth in Chapter 6 of this document. The new public key is issued in the format of that certificate from a widely-trusted RCA of JCSI and is disclosed on the JCSI's website.

JCSI does not issue a certificate for a new key with the old key. Nor does it issue a certificate for the old key with the new key.

4.6 Recovery from Compromise

If the CA private key of SecureSign public services is compromised, JCSI revokes that certificate signature key to prevent the circulation of new subscriber's certificates signed with the illegal reproduction of that key, resulting in those illegal certificates being trusted. More specifically, all effective certificates signed with that key are revoked as soon as possible, and their CRLs are signed with the compromised key and disclosed. After that, that certificate signature key is deleted, and a widely trusted RCA of JCSI issues an updated CRL and disclose it. To continue the services, JCSI generates a new certificate signature key as soon as possible. Subscribers can apply for the issuance (or update) of their certificates.

JCSI sets forth another recovery procedure to counter any compromise or damage and provide education and training of recovery procedure according to schedule.

4.7 CA Termination

The SecureSign public services CA is terminated due to the provisions of clauses 2.2 through 2.4 of this document and changes in the business principles of JCSI, along with other reasons. Its termination is publicized on the JCSI's website (or a site succeeding to it) from two months before until six months after the termination, unless it is unavoidable. When the CA is terminated, JCSI initializes completely or destroys physically the CA private key and backup medium, thus discontinuing their use, but does not revoke the CA certificate related to the CA private key. JCSI suspends the issuance of new certificates (and suspends the renewal of such certificates). Certificates issued, still effective at the time, are collectively revoked with the termination of the CA. However, JCSI does not perform the final renewal or disclosure of the CRL that reflects such collective revocation. It makes the URLs in the certificates (CRL distribution points) inaccessible, thus making the verification of certificates by the relying parties unsuccessful. With the termination of the CA, JCSI will delete all documents and digital data regardless of the provisions of clause 4.4.

5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1 Physical Security Controls

JCSI defines security requirements for facilities where a certificate issuing system (CA, including RAs for types A-1, B-1, C-1 and D-1) is installed and operated:

(1) JCSI requires the rooms in the building where a certificate issuing system is installed be classified into multiple security levels and controlled with security regulations regarding movement in and between levels. Actual fulfillment is done by the center.

(2) JCSI prepares the procedures for authorization of access rights at each security level. Each center shall implement the procedures.

(3) The certificate issuing system shall be installed in a secure facility with quakeproof, fireproof, waterproof, burglar prevention and air-conditioning functions.

(4) The certificate issuing system (server, key cryptographic device, F/W and routers) must be installed in a room at the highest security level exclusively reserved for JCSI use.

(5) Personal entry and exit from the facility must be controlled by a security guard. Only persons registered in advance are allowed to enter the facility. Persons entering a security-controlled room must be accompanied by an authorized person for the relevant security level. These entries and exits must be allowed individually and reported at the end of each entry or exit.

(6) Rooms at the highest security level must be monitored by video recording systems and motion detectors at all times. Detection of illegal access sets off an alarm. The cause of the alarm must be promptly identified for proper action.

(7) Persons entering a room at the highest security level must be identified by the biological authentication function, so that they can unlock the electronically locked door. Personal entry and exit from the facility must be authorized by two persons at the same time.

(8) The rooms at the highest security level must be protected with an illegal-access preventive structure.

(9) Monitoring information and personal entry record for the monthly security audit must be kept for three years as audit trail.

(10) Devices important for ensuring confidentiality and security must be supplied with power by a UPS or private electric generator as a precaution against power failure.

(11) Only authorized personnel are allowed to access the media repository or system monitoring room.

(12) Certification authorities must inspect monthly, according to the documented procedure, whether they use their equipment and devices in conformance to this security control concept.

5.2 Procedural Security Controls

JCSI distinguishes the personnel as shown in the table 5-1 below. Personnel at operation centers shall operate the CA, the RA installed at JCSI, and JCSI's repositories.

Table 5-1 Authority of personnel

<table>
<tr><th colspan="2">Personnel classification</th><th>Authorization</th><th>Authorization for access</th><th>Authorization for operation</th><th>Access authority check</th></tr>
<tr><td colspan="2">PKI operation administrator</td><td>Designated and authorized at each center.</td><td colspan="2">–</td><td>–</td></tr>
<tr><td colspan="2">Security administrator</td><td>Same as the above</td><td>Authorized</td><td>–</td><td>ID card system and biological authentication system</td></tr>
<tr><td rowspan="3">Center personnel</td><td>PKI engineers</td><td>Designated by the PKI operation administrator.</td><td rowspan="3">Authorized by the PKI operation administrator based on the consent of the security administrator.</td><td rowspan="3">Authorized by the PKI operation administrator.</td><td>Access by a single person is not allowed. Must be accompanied by a person authorized to access the security system.</td></tr>
<tr><td>System operator</td><td>Designated by the security administrator based on the consent of the PKI operation administrator.</td><td>ID card system and biological authentication system</td></tr>
<tr><td>Maintenance personnel</td><td>Designated by the security administrator or PKI operation administrator.</td><td>Access by a single person is not allowed. Must be accompanied by a person authorized to access the security system</td></tr>
</table>

To ensure security of the installation site of the certificate issuing system, center personnel are authorized to access the site or limited in access to the system room. Based on the consent of the security administrator, the PKI operation administrator of each center must be able to authorize them to access the system room. The security administrator must register or erase the information of the center personnel in the ID card system and biometric authentication system based on the authorization document.

To ensure security of the operation of the certificate issuing system, only a limited number of personnel are authorized to operate specific equipment and devices. The PKI operation administrator of each center must be able to authorize the rights to operate the certificate issuing system. Based on the authorization document, the PKI operation administrator must set (change or erase) the accounts and issue or revoke the operation certificates. In particular, the administrator must rigidly control the accounts with access privileges.

Records of the authorization for access, operation and remote operation must be managed by the PKI operation administrator and stored in a keyed cabinet for at least three years.

The details of authorization for access and commanding system must be stated in the detailed procedure of each center. The PKI operation administrator of each center may be referred to simply as the operation administrator in detailed procedures. To trust some operations, JCSI must direct the trustee to observe the rules stated in this chapter and to create the detailed procedure so that the trusted operations can be performed according to that procedure. Each center must monitor the operations of personnel or trustee to maintain the proper security according to this document.

5.3 Personnel Security Controls

JCSI controls the security of personnel involved in the certificate issuing system to conform to the following requirements:

(1) Personnel who engage in the direct operation of a center system shall sign an annual written pledge that they have not committed a crime for the last 15 years.

(2) Center personnel shall be educated on regulations and procedures necessary for operating the certificate issuing system, and required to sign a written pledge that they will follow them. In the course of education, they should understand the seriousness of compromise or loss of keys.

(3) In split knowledge of private keys (Section 6.2), holders of a key fragment (split key) shall agree to sign a written pledge that they fulfill their control responsibility before receiving a key component.

The members (*1) assigned to the center have enough knowledge and experience (*2) on the related technology.

*1: The number of members must be decided at each center

*2: Members must have experience on the development, operation or consultation of authentication systems over two years and on the development of this standard or the similar standard.

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 RCA

(1) Key pair generation

A pair of private and public keys shall be generated within the cryptographic device with a random-number or a pseudo-random-number generation process prescribed in ISO 9564-1:1991 and ISO 11568-5. This key pair shall be generated by four DualControl members designated by JCSI (or by two or more members designated by customers for Private Service).

(2) Presentation of public key to certificate issuer

A generated public key shall be made into a form of certificate in the RCA without presenting to any external entity.

(3) Distribution of JCSI's RCA public keys to users

- JCSI's RCA public keys are distributed as a preinstalled item in de facto standard applications (products and application programs).
- JCSI's RCA public keys are downloaded to end entities from the JCSI repositories for distribution. End entities shall be required to verify the validity of the downloaded RCA public keys based on the hash value (released by JCSI).
- JCSI's RCA public keys are delivered together when subscriber's certificates are issued to subscribers.

(4) Key size

Key size shall be 2,048 bits conforming to the RSA public-key cryptographic scheme (for Public Service)

(1,024 or 2,048 bits for Private Service)

(5) Use of hardware key

Key pairs are generated with a cryptographic device (hardware).

(6) Key pair installation

Key pair installation is not necessary because the keys are used on the device that generated them.

(7) Hash function

SHA-1

6.1.2 ICA/SCA

(1) Key pair generation

A pair of private and public keys shall be generated within the cryptographic device with a random-number or a pseudo-random-number generation process prescribed in ISO

9564-1:1991 and ISO 11568-5. Key pairs shall be generated by two DualControl members designated by each CA certificate issuer. The generated keys are used only on the cryptographic device on which they were generated.

(2) Derivery of public key to certificate issuer

A generated key is output to a token (for example, an FD or IC card) to request the superior CA to issue certificates.

(3) Distribution of ICA/SCA public key to users

- SCA public keys are preinstalled in the de fact standard applications (products, application programs) for distribution.
- JCSI's ICA/SCA public keys are delivered together when subscriber's certificates are issued to subscribers.

(4) Key size

Key size shall be 1,024 or 2,048 bits conforming to the RSA public-key cryptographic scheme.

(5) Use of hardware key

Key pairs are generated with a cryptographic device (hardware).

(6) Key usage

Using the Extension of X.509 version 3 certificate, keys should be used only to sign and verify certificates and CRLs.

(7) Key pair installation

Key pair installation is not necessary because the keys are used on the device that generated them.

(8) Hash function

SHA-1

6.1.3 Subscriber (Issuance pattern 1)

（1） Key pair generation

A pair of private and public keys shall be generated with a random-number or a pseudo-random-number generation process prescribed in ISO 9564-1:1991 and ISO 11568-5. Generated key pairs shall be securely stored.

(2) Presentation of public key to certificate issuer

A generated public key is submitted as an online request for signing certificates to the CA, via RA, to issue certificates.

(3) Key size

Depending on the software used by the subscriber, key size shall be 512, 768, 1,024 or 2,048 bits conforming to the RSA public-key cryptographic scheme.

(4) Use of hardware key

Key pairs can be generated with a cryptographic device (hardware).

(5) Key usage

The Extension of X.509 version 3 certificate that meets the key usage shall be set. End entities shall use a certificate for a purpose within the specified range of key uses.

(6) Key pair installation

Key pair installation is not necessary because the keys are used on the device that generated them.

(7) Hash function

SHA-1

6.1.4 Subscriber (Issuance patterns 2 and 3)

(1) Key pair generation

A pair of private and public keys shall be generated with a random-number or a pseudo-random-number generation process prescribed in ISO 9564-1:1991 and ISO 11568-5. Key pairs shall be generated at the RA or KRS, based on the approval of two DualControl members of RAOs.

(2) Presentation of public key to certificate issuer

A generated public keys is submitted as an online request for signing certificates to the CA to issue certificates.

(3) Key size

Key size shall be 512, 1,024 or 2,048 bits conforming to the RSA public-key cryptographic scheme.

(4) Use of hardware key

Key pairs are generated without a cryptographic device.

(5) Key usage

The Extension of X.509 version 3 certificate that meets the key usage shall be set. End entities shall use a certificate for a purpose within the specified range of key uses.

(6) Key pair installation

The subscriber shall access the JCSI-designated download page by using the path phrase to download, then install the key pairs in the target application.

- Key pairs must not be used outside of the RA without encryption
- Key pairs must be abandoned soon when key reception by subscribers is checked.

(7) Hash function

SHA-1

6.2 Private Key Protection

6.2.1 Standards for cryptographic module

CA private keys shall be controlled with a cryptographic module conforming to FIPS 140-1 level 3 or the equivalent.

Cryptographic modules used by subscribers should preferably comply with FIPS 140-1.

6.2.2 Private key (n out of m) multi-person control

The private key protection scheme uses both DualControl in which system operations using the private key are done by the consent of multiple persons and SecretShare (SecretSplit) in which the private key is split and shared by multiple persons. Each CA determines which control it uses in the range shown in Table 6-1.

When the number of SecretShare splits equals to the number of shares necessary for signature, the storage media shall be duplicated.

Table 6-1 DualControl and SecretShare

Authoriy	Persons necessary for DualControl	SecretShare splits	Shares necessary for signature
RCA (Public)	2 (server personnel)	4	4
Other than RCA (Public)	2 (server personnel)	2 to 5	2 to 5

NOTE:"server personnel" in this chapter indicates "PKI engineers" or "System operator" in chapter 5.

6.2.3 Private key escrow

No private key escrow services are provided.

6.2.4 Private key backup

Using secret shares, a CA private key is stored as key fragments (split key) in tokens. Holders of the key fragments of a split key shall be designated by the issuer of each CA. In handling the tokens, the holders shall sign "Pledge of Key Control," enclose the token in a tamper-evident envelope, and control and store the token in the fireproof safe responsibility owned by the key fragment (split key) holders.

Private keys must be securely backed up based on the consent of DualControl members of server personnel.

Subscriber private keys shall be securely backed up on the subscriber's responsibility. Keys for the subscriber (issuance patterns 2 and 3) using the key recovery service shall be backed up by the KRS using multiple encryption.

6.2.5 Private key archive

CA private keys are not archived.

6.2.6 Private key entry into cryptographic module

CA private keys shall be entered based on the consent of DualControl members of server personnel. They shall be securely entered into the cryptographic module from split tokens.

Tokens shall be operated by the key fragment (split key) holders who signed the written "Pledge of Key Control" according to the directions given by the server personnel.

6.2.7 Method of activating private key

CA private keys shall be activated based on the consent of DualControl members of server personnel. Once activated, keys remain activated for a period shown in Table 6-2.

Table 6-2 Private key activation period

Authority	Activation period
CA issuing CA certificates	Only when a signature is made
CA issuing subscriber's certificates	At all times (except hardware maintenance time)

6.2.8 Method of deactivating private key

CA private keys shall be deactivated based on the consent of DualControl members of server personnel.

6.2.9 Method of destroying private key

CA private keys shall be destroyed promptly upon expiry or key abandonment (operation at CA termination). Private keys are destructed by fully initializing the cryptographic module. This work shall be done based on the consent of DualControl members of server personnel. Key fragment (split key) tokens shall be physically destroyed. This work shall be done by a key fragment holder while witnessed by a third party authority. The witness and key fragment holder shall sign "Pledge for Key Destruction."

Subscriber's private keys shall be destroyed promptly upon expiry.

6.2.10 Private key recovery

Keys for subscribers (issuance patterns 2 and 3) using the key recovery service shall be recovered based on the consent of DualControl members.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archive

Archiving of CA public keys shall include measures against compromise. Table 6-3 shows archive period.

Table 6-3 Public key archive period

Authority	Archive type	Archive period
RCA	Own certificates	Ten years from the expiry date
	Issued certificates	Ten years from the expiry date
ICA/SCA	Own certificates	Ten years from the expiry date
	Issued certificates	Ten years from the expiry date

6.3.2 Usage periods for the public and private keys

Table 6-4 shows expiry periods of public and private keys.

Table 6-4 Expiry period of keys

Authority	Key type	Public key expiry period	Private key expiry period
RCA	Certificates and CRL signature keys	21 years	10 years
ICA/SCA	Certificates and CRL signature keys	Within 21 years	Within 10 years
Subscriber	Web server certificates	Within 1 year 30 days	1 year
Subscriber	Long Term Certificate	Within 11 years	Within 11 years
Subscriber	(Other than the above)	Within 6 years	Within 6 years

6.4 Activation Data

In CAs, activation data shall be controlled by PINs and passwords.

6.4.1 Activation data generation and installation

PINs and passwords shall be at least 8 characters in length, containing both alphabetical and numeric characters.

6.4.2 Activation data protection

Passwords shall be stored in the system, in a one-way functional ciphertext format. Expiry period of passwords shall be between 2 and 30 days inclusive. Passwords shall be changed periodically. PINs are stored in hardware modules or tokens, and cannot be taken out for external use.

6.5 Computer Security Controls

6.5.1 Specific computer security technical requirements

The computer systems used by the CA shall be in compliance with Level C2 described in the Standard of the US Department of Defense: Trusted Computer System Evaluation Criteria (Orange Book).

6.5.2 Computer security evaluation

Cracking tests shall be performed as nencessary to evaluate the CA’s computer system security.

6.6 Life Cycle Technical Control

6.6.1 System development control

CAs shall use systems that are proven to have been developed and tested by a trusted organization.

6.6.2 Security management control

CAs shall make periodic use of vaccine software to prevent, detect, and recover from virus infection.

6.7 Network Security Controls

CAs issuing CA certificates shall not connect with the network.CAs issuing subscriber's certificates shall connect with the Internet via a firewall. Firewall logs illegal accesses as audit trail. Network attack tests shall be done as necessary by an external organization.

Network-based IDS shall be used to prevent illegal accesses.

6.8 Cryptographic Module Engineering Controls

The hardware cryptographic modules used in CAs shall be compatible with FIPS 140-1 Level 2 or Level 3.

7. CERTIFICATE AND CRL PROFILES FOR PUBLIC SERVICE

Most part of certificate and CRL formats and attribute specifications for SecureSign was developed by referring to the following standard specifications drawn up in global technological standards or by standardization organizations.

(1) ITU-T Recommendation X.509 (1997E)

(2) RFC2459 Internet X.509 PKI Certificate and CRL Profile, January1999

Standard specifications are subject to continuous revision. We are committed to comply with future standard specifications.

Tables 7-1 and 7-2 list certificate and CRL profiles for SecureSign.

Table 7-1 Certificate profile

No.	Field name (Symbolic name)	Object identifier (OID)	Setting *1			Description
			Version 1 CA certificate	Version 3 CA certificate	Version 3 subscriber's certificate	
Certificate Basic Fields						
1	Version (version)	None	v1	v3	v3	
2	Serial number (serialNumber)		⊙	⊙	⊙	
3	Signature (signature)		⊙	⊙	⊙	
4	Issuer (issuer)		⊙	⊙	⊙	
5	Validity period (validity)		⊙	⊙	⊙	
6	Subject (subject)		⊙	⊙	⊙	
7	Subject public key (subjectPublicKeyInfo)		⊙	⊙	⊙	
8	Issuer unique ID (issuerUniqueID)		×	×	×	
9	Subject unique ID (subjectUniqueID)		×	×	×	
Certificate Standard Extensions						
10	Authority key identifier (authorityKeyIdentifier)	2.5.29.35	–	○	⊙	
11	Subject key identifier (subjectKeyIdentifier)	2.5.29.14	–	⊙	○	
12	Key usage (keyUsage)	2.5.29.15	–	⊙	⊙	Usage of public key
13	Extended key usage (extendedKeyUsages)	2.5.29.37	–	○	○	Usage other than KeyUsage
14	Private key expiry period (privateKeyUsagePeriod)	2.5.29.16	–	×	×	Expiry period of private key
15	Certificate policies (certificatePolicies)	2.5.29.32	–	○	○	CA policy
16	Policy mapping (policyMappings)	2.5.29.33	–	○*2	×	Correlation with policies of other certification domains
17	Subject alternative name (subjectAltName)	2.5.29.17	–	○	○	Alternative name of the subject
18	Issuer alternative name (issuerAltName)	2.5.29.18	–	×	×	Alternative name of the issuer
19	Basic constraints (basicConstraints)	2.5.29.19	–	⊙	○	Whether or not the certificate is for CA use
20	Name constraints (nameConstraints)	2.5.29.30	–	○	×	Constraints on the space for name on subordinate certificates
21	Policy constraints (policyConstraints)	2.5.29.36	–	○	×	Constraints on the policy on subordinate certificates
22	CRL distribution points (cRLDistributionPoints)	2.5.29.31	–	○	○	Distribution points of CRLs
23	Subject directory attributes (subjectDirectoryAttributes)	2.5.29.9	–	×	×	Value of Directory Attribute for the subject
Certificate Private Internet Extensions						
24	Certification authority information access (authorityInfoAccess)	1.3.6.1.5.5.7.1.1	–	○	○	Specifies the method of access to issuer information
Certificate Netscape Extensions		2.16.840.1.113730.1				
25	netscape-cert-type	.1	–	○	○	Usage of the certificate

⊙: Mandatory; ○: Optional; ×: Not edited; –: No setting definitions

*1:Settings are classified according to certificate type and version

Version 1 CA certificate: X.509 version 1 CA certificate

Version 3 CA certificate: X.509 version 3 CA certificate

Version 3 subscriber's certificate: X.509 version 3 subscriber's certificate

*2: Mutual authentication certificates only

Table 7-2 CRL profile

No.	Field name (Symbolic name)	Object identifier (OID)	Setting*1			Description
			Version 1 CRL	Version 2 CA CRL	Version 2 subscriber's CRL	
CRL Basic Fields						
1	Version (version)	None	v1	V2	v2	
2	Signature (signature)		⊙	⊙	⊙	
3	Issuer (issuer)		⊙	⊙	⊙	
4	Date of the last update (thisUpdate)		⊙	⊙	⊙	Effective date of the last CRL issued
5	Plan for the next update (nextUpdate)		⊙	⊙	⊙	Plan for the next CRL issuance
6	Revoked certificates (revokedCertificates)		⊙	⊙	⊙	
	Certificate(userCertificate)		⊙	⊙	⊙	Serial number of the revoked certificate
	Revocation date(revocation date)		⊙	⊙	⊙	Revocation date and time
CRL Extensions						
7	Authority key identifier (authorityKeyIdentifier)	2.5.29.35	–	⊙	⊙	
8	Issuer alternative name (issureAltName)	2.5.29.18	–	×	×	Alternative name of the issuer
9	CRL number (cRLNumber)	2.5.29.20	–	⊙	⊙	
10	Delta CRL Indicator (deltaCRLIndicator)	2.5.29.27	–	○	○	Set for delta CRLs only
11	Issuing distribution point (issuingDistributionPoint)	2.5.29.28	–	○	○	
CRL Entry Extensions						
12	Reason code (reasonCode)	2.5.29.21	–	⊙	○	Reason for revocation
13	Hold instruction code (holdInstructionCode)	2.5.29.23	–	×	○	A detailed description code used when the reason for revocation is suspension
14	Invalidity date (invalidityDate)	2.5.29.24	–	○	○	Invalidity date of the certificate (date of last update if skipped)
15	Certificate issuer (certificateIssure)	2.5.29.29	–	×	×	

⊙: Mandatory; ○: Optional; ×: Not edited; –: No setting definitions

*1: Settings are classified according to CRL type and version
Version 1 CA certificate: X.509 version 1 CA certificate
Version 2 CA certificate: X.509 version 3 CA certificate
Version 2 subscriber's certificate: X.509 version 3 subscriber's certificate

7.1 Setter and Set Values for Fields

The details of each certificate/CRL field are set by the RA or CA. The settings are managed for individual certificate types.

Tables 7-3 and 7-4 show the setter and description of settings for each field.

In extensions on version 3 certificates and version 2 CRLs, criticality settings are made for each field. Unless a description is given, a "noncritical" setting is made for the field (ignored when this is not recognized).

The CA shall set up the actual encoding sequence for each extension field on version 3 certificates and version 2 CRLs.

In consideration of the present compatibility of products applied, ASCII-compliant one-byte codes should be used for settings. UNICODE is recommended for Japanese codes and UTF8String for encoding.

Table 7-3 Setter and description of settings in fields on certificates

No.	Field name (Symbolic name)	Setter			Description of setting
		Version 1 CA certificate	Version 3 CA certificate	Version 3 subscriber's certificate	
Certificate Basic Fields (Certificate Basic Fields)					
1	Version (version)	CA	CA	CA	v1 may be set when the CA is an RCA that authenticates a subordinate ICA or SCA. In other cases, v3 should be set.
2	Serial number (serialNumber)	CA	CA	CA	A positive integer up to 128 bits
3	Signature (signature)	CA	CA	CA	RSA with SHA-1, or RSA with MD5
4	Issuer (issuer)	CA	CA	CA	See 7.1.1.
5	Validity period (validity)	CA	CA	RA	Starting and ending dates are set in seconds.
6	Subject (subject)	CA	CA	RA	See 7.1.1.
7	Subject public key (subjectPublicKeyInfo)	CA	CA	RA	RSA public key (512 to 2,048 bits)
8	Issuer unique ID (issuerUniqueID)	×	×	×	
9	Subject unique ID (subjectUniqueID)	×	×	×	
Certificate Standard Extensions (certificate Standard Extensions)					
10	Authority key identifier (authorityKeyIdentifier)	–	CA	CA	SHA-1 of the public key, or DN and serial number of the issuer.
11	Subject key identifier (subjectKeyIdentifier)	–	CA	RA	SHA-1 of the public key
12	Key usage (keyUsage)	–	CA	CA	See 7.1.3.
13	Extended key usage (extendedKeyUsages)	–	CA	CA	See 7.1.4.
14	Private key expiry period (privateKeyUsagePeriod)	–	×	×	
15	Certificate policies (certificatePolicies)	–	CA	CA	See 7.1.5.
16	Policy mapping (policyMappings)	–	CA	×	See 7.1.6.
17	Subject alternative name (subjectAltName)	–	CA	RA	See 7.1.2.
18	Issuer alternative name (issuerAltName)	–	×	×	See 7.1.2.
19	Basic constraints (basicConstraints)	–	CA	CA	See 7.1.7.
20	Name constraints (nameConstraints)	–	CA	×	See 7.1.8.
21	Policy constraints (policyConstraints)	–	CA	×	See 7.1.9.
22	CRL distribution points (cRLDistributionPoints)	–	CA	CA	See 7.1.10.
23	Subject directory attributes (subjectDirectoryAttributes)	–	×	×	
Certificate Private Internet Extensions (certificate Private Internet Extensions)					
24	Certification authority information access (authorityInfoAccess)	–	CA	CA	See 7.1.11.
Certificate Netscape Extensions (Netscape Standard Extensions)					
25	netscape-cert-type	–	CA	CA	See 7.1.12.

CA: Set by CA; RA: Set by RA (for some policies, CA has priority to set in CA policies);

×: Not edited; –: No setting definitions

Table 7-4 Setter and description of settings in fields on CRLs

No.	Field name (Symbolic name)	Setting		Description of setting
		CA CRL	Subscriber's CRL	
CRL Basic Fields				
1	Version (version)	CA	CA	v1 or v2
2	Signature (signature)	CA	CA	RSA with SHA-1, or RSA with MD5
3	Issuer (issuer)	CA	CA	See 7.1.1.
4	Date of the last update (thisUpdate)	CA	CA	
5	Plan for the next update (nextUpdate)	CA	CA	Set in seconds in the UTCTime format
6	Revoked certificates (revokedCertificates)	—	—	
	Certificate (userCertificate)	CA	RA	Serial number of certificate
	Revocation date (revocation date)	CA	CA	Set in seconds in the UTCTime format
CRL Extensions				
7	Authority key identifier (authorityKeyIdentifier)	CA	CA	SHA-1 of the public key, or DN and serial number of the issuer.
8	Issuer alternative name (issureAltName)	×	×	
9	CRL number (cRLNumber)	CA	CA	A positive integer up to 128 bits
10	Delta CRL Indicator (deltaCRLIndicator)	CA	CA	Set for delta CRLs
11	Issuing distribution point (issuingDistributionPoint)	CA	CA	Used for indirect CRLs only.
CRL Entry Extensions				
12	Reason code (reasonCode)	CA	RA	
13	Hold instruction code (holdInstructionCode)	×	RA	
14	Invalidity date (invalidityDate)	CA	CA	
15	Certificate issuer (certificateIssure)	×	×	

CA: Set by CA; RA: Set by RA (for some policies, CA has priority to set in CA policies);

×: Not edited; –: No setting definitions

7.1.1 Name forms

Specified as a distinguished name (DistinguishedName) defined by the ITU X.500 series. In reality, name forms are defined by a combination of PKIX (RFC2459) and attribute definitions defined by FRC of LDAP (RFC2256) (Table 7-5). The CA sets the encoding sequence for attributes.

Table 7-5 Certificate profile

No.	Attribute name (Symbolic name)	Object identifier (OID)	Setting *1		Maximum number of settings	Description
			CA name	Subscriber's name		
1	Country name (CountryName, c=)	2.5.4.6	⊙	⊙	1	Fixed at 'c=JP'
2	State or province name (stateOrProvinceName, st=)	2.5.4.8	×	○	1	
3	Locality name (localityName, l=)	2.5.4.7	×	○	1	
4	Organization name (organizationName, o=)	2.5.4.10	⊙	⊙	1	CA name: Fixed at 'o=Japan Certification Services, Inc.' or 'o=Japan Certification Services' Subscriber's name: Fixed at 'SecureSignN' (N=1, 2, 3) or value designated by subscriber (customer)
5	Organizational unit name (organizationalUnitName, ou=)	2.5.4.11	○	○	5	
6	Common name (CommonName, cn=)	2.5.4.3	⊙	⊙	1	CA name or subscriber's name is set. Settings must be unique values when seen from the superior authority.
7	Email (EmailAddress, e=)	1.2.840.113 549.1.9.1	×	○	1	Since this setting is not recommended by PKIX, this may be set only for smime certificates for subscribers.

⊙: Mandatory; ○: Optional; ×: Not edited; –: No setting definitions

*1: CA setting fields -- The subject/issuer fields of CA certificates
Subscriber setting fields -- The subject field of subscriber's certificates

7.1.2 General name (GeneralName)

General name, which is set to an alternative name, is defined by X.509 as a choice of multiple definitions (ASN.1). Table 7-6 shows this setting. This setting is mandatory for some certificates.

This item is set on subscriber's certificates by the RA.

Table 7-6 General name (GeneralName) setting

No.	ASN.1 definition type (Symbolic name)	Setting	Setter	Description
General name (GenaralName)				
1	otherName type	×	-	
2	rfc822Name type	○	RA	An email address is set.
3	dNSName type	○	RA	A DNS name is set.
4	x400Address type	×	-	
5	directoryName type	○	RA	An LDAP reference is set.
6	ediPartyName type	×	-	
7	uniformResourceIdentifier type	○	RA	A URL is set.
8	iPAddress type	○	RA	An IP address is set.
9	registeredID type	×	-	

○: Optional; ×: Not edited

7.1.3 Key usage (KeyUsage)

At least one bit must be set equal to 1. The keyCertSign can be set (=1) for CA certificates only.

7.1.4 Extended key usage (extendedKeyUsage)

This specifies an RFC2459 definition or industry standard object identifier (OID). Settings that conflict with the key usage are not allowed. The criticality setting may be set to "critical".

7.1.5 Certificate policies (certificatePolicies)

This specifies the object identifiers (OIDs) listed in Table 1-1 and the URL which indicates the location of disclosure of a document prescribing the rules for certificate usage (see Note 1).

Note 1: Though RFC2459 recommends the use of a CPS, for relying parties' convenience, Public Service uses the "Relying Party Agreement" that extracts the user obligations from the CPS.

7.1.6 Policy mapping (policyMappings)

This should be edited for mutual authentication certificates only. This specifies an object identifier pair that establishes mutual correlation.

7.1.7 Basic constraints (basicConstraints)

For CA certificates:	Set cA=TRUE, skip the pathLenConstraint field setting (which specifies an infinite class) or set SCA to 0. Set the criticality setting to "critical". (RFC2459)
For subscriber's certificates:	Skip the settings or set cA=FALSE and skip the pathLenConstraint field settings. Set the criticality setting to "noncritical".

7.1.8 Name constraints (nameConstraints)

For SCAs (issuing subscriber's certificates), this should be set according to the type of subscriber certificates. The setting should conform to RFC2459.

7.1.9 Policy constraints (policyConstraints)

The setting should conform to RFC2459.

7.1.10 CRL distribution points (cRLDistributionPoints)

The setting should conform to RFC2459.

7.1.11 Certification authority information access (authorityInfoAccess)

The setting should conform to RFC2459.

7.1.12 netscape-cert-type

This should conform to the Netscape standard. Settings that conflict with the key usage and extended key usage are not allowed.

7.2 Certificate/CRL Setting Contents Determination Procedures

The setting contents of a certificate are determined in the following steps:

(1) A subscriber enrolls an application of the setting contents to the RA.

(2) Considering the setting contents of the application submitted from the subscriber, the RAO determines the tentative settings for the items whose setter is the RA (described in Section 7.1) and requests the CA for issuance.

(3) Considering the contents of the application requested by the RA server, the CP determines the setting contents for all the items.

The setting contents of a CRL are determined in the following steps:

(1) The RAO determines the certificates to be revoked and determines the tentative settings for the items whose setter is the RA (described in Section 7.1) and requests the CA for issuance.

(2) Considering the contents of the revocation application requested by the RA server, the CP determines the setting contents for all the items. When the certificate is listed in the last CRL issued and is still valid, it should be listed in a next CRL.

7.2.1 Validity check of application contents

RAOs should check, in the light of this document, whether the subscriber's application contents are appropriate for RA settings.

The CP should check the values of RA setting items in the light of this document agreed upon with the issuer (JCSI). The CP then sets RA application values as is, uses new values in their place, or rejects the application itself. The CP may change the setting items defined as those set by the RA in Section 7.1.

7.2.2 Validity check of setting contents of issued certificates

RAOs or subscriber should promptly check whether the authentication contents (setting contents) of the issued certificate conform to the provisions in this document. When they do not accept setting contents, they should immediately request the CA (RA in the case of subscribers) to revoke the relevant certificate.

7.3 Profiles of Certificates

7.3.1 SecureSign public CA certificate

(1) Public RCA certificate

Aiming to assure permanent authenticity generally as a root of certificate verification path, this uses intense encryption (2,048-bit RSA key) in the X.509 version 1 format.

(2) Public ICA certificate

The X.509 version 3 format is used, and the key usage attributes of this certificate are set to the signature of a subordinate CA in extension fields.

(3) Public SCA certificate 1 (CA for common use)

The X.509 version 3 format is used, and the key usage attributes of this certificate are set to the signature of a subscriber's certificate in extension fields. The long term SCA(2,048-bit RSA key) which can issue subscriber's certificates with a long validity priod is included in this kind of certificate.

(4) Public SCA certificate 2 (CA for customer use)

The X.509 version 3 format is used, and the key usage attributes of this certificate are set to the signature of a subscriber's certificate in extension fields.

With JCSI's approval, customers can set customer information in the following fields of certificates.

(a) Validity period

(b) o, ou and cn in the subject field

(c) Others

7.3.2 SecureSign public subscriber's certificate

(1) Public SSL/TLS server certificate

The X.509 version 3 format is used, and the key usage attributes of this certificate are set to the SSL/TLS of a server certificate in extension fields.

Customers can set customer information in the following fields of certificates:

(a) c, st, l, o, ou and cn in the subject field

(b) The RA must set, in cn of the subject field, a DNS name that identifies the server owned by the subject.

(2) Public SSL/TLS client certificate

The X.509 version 3 format is used, and the key usage attributes of this certificate are set to the SSL/TLS of a client certificate in extension fields.

Customers can set customer information in the following fields of certificates:

(a) Validity period

(b) c, st, l, o, ou (up to 5 items) and cn in the subject field

The RA must set, in the subject field, attribute values that the RA can set uniquely to identify the subject.

(3) Public S/MIME certificate

The X.509 version 3 format is used, and the key usage attributes of this certificate are set to the S/MIME of a certificate in extension fields.

Customers can set customer information in the following fields of certificates:

(a) Validity period

(b) c, st, l, o, ou (up to 5 items), cn and e in the subject field

(c) Subject alternative name field

The RA must set the email address of the subject in e (within DN) of the subject field and in the subject alternative name field as an rfc822name type .

(4) Public signing certificate

The X.509 version 3 format is used, and the key usage attributes of this certificate are set to the digitalSignature and(or) nonRepudiation in extension fields.

Customers can set customer information in the following fields of certificates:

(a) Validity period

(b) c, st, l, o, ou (up to 5 items) and cn in the subject field

(c) Subject alternative name field

(5) Public Time Stumping certificate

The X.509 version 3 format is used, and the key usage attributes of this certificate are set to the digitalSignature and nonRepudiation in extension fields. Extended key usage attributes of this certificate are set to the time stamping in extension fields.

Customers can set customer information in the following fields of certificates:

(a) Validity period (6 years and 30 days or 11 years and 30 days)

(b) c, st, l, o, ou (up to 5 items) and cn in the subject field

8. SPECIFICATION ADMINISTRATION

This chapter describes the specification administration for *SecureSign Public Service Standard* (referred to as this Standard in this chapter). Customers shall establish their own specification administration standard for SecureSign Private Service (customers may use this document as a reference and/or a source of quotations).

To maintain the security, JCSL makes efforts to study and acquire the advanced security technologies and revises the specifications of this Standard as necessary.

8.1 Specification Change Procedures and Publication/Notification Policies

JCSI reserves the right to update the Standard without the consent of customers (including RAOs and subscribers) and relying parties. Before updating this Standard, the JCSI Specification Control Group reviews the contents of the update to check for validity. Updating this Standard completes with the disclosure of the updated Standard or the release of a change notice (a collection of updated portions in the Standard) in the JCSI repository. The change notice has the same effects as the actual updated standard and reflected in the next version of the Standard. Revisions/updates of the Standard are identified by the version number representing the revision history, and the date of issue.

Notification of revision shall be done by releasing a change notice or disclosing the updated Standard in the JCSI repository. Effective date of specification changes shall depend on the importance and urgency of the changes. JCSI shall reserve the right to determine the importance/urgency of the changes at its sole discretion. Typically, however, effective dates are set as follows:

(1) Important changes shall take effect after 15 days (notification period) of the notice. Customers (including RAOs and subscribers) and relying parties must periodically visit the JCSI repositories to find additions and changes to the SecureSign service specifications. During notification period, JCSI may withdraw changes by presenting a notice of withdrawal in the JCSI repository.

(2) Urgent and important changes shall take effect immediately after notice. Here, urgent situations refer to cases where part or whole of the SecureSign services would be compromised unless the relevant changes take effect immediately.

(3) Unimportant changes shall take effect immediately after notice..

8.2 Publication/Notification Policies

Included in Section 8.1.

8.3 Specification Approval Procedures

When this Standard has been updated, the new standard disclosed in the JCSI's repositories applies regardless of timings when subscriber’s certificates are issued. Unless customers (including RAOs and

subscribers) apply for certificate revocation, it shall be deemed that they have agreed with all the specification changes JCSI had made. Relying parties who disagree with any change should discontinue the use of the certificates obtained.

8.4 Storage of this Document

JCSI keeps the versions of this Standard so long as SecureSign public service continues.

Appendix A. SecureSign Server Service

A1 INTRODUCTION

SecureSign server service (hereinafter abbreviated as "the Services" in this appendix) is designed to issue electronic certificates verifying the existence of web servers. When a customer applies for the issuance of a server certificate, JCSI checks that the website exists uniquely, then issues an SSL v3-compatible web server certificate to that server. To that end, JCSI provide SCAs under the SecureSign public route CA. According to the definition of SecureSign, the web server which has received an issued certificate is the subscriber, while the user of the server certificate is the relying party. However, in this appendix, "subscriber" refers to the customer him- or herself who is applying for the issuance of a web server certificate (note 1) or the person responsible for the practical administration of the web server in the customer's organization (note 2).

SecureSign public services described in this document are such that the customer administers the RA under commission from JCSI. In the Services, JCSI administers the RA. JCSI sets forth the regulations for the administration of the RA in connection with the Services in this Appendix. JCSI also sets forth the obligations of the subscriber. Under approval of JCSI, a third party as the intermediary of the Service for the subscriber must be able to direct the subscriber to carry out the subscriber’s obligations set forth in this appendix without any modification, on behalf of JCSI.

Note 1: He or she is called a client in the "application for a web server certificate."

Note 2: He or she is called a certification application manager in the "application for a web server certificate."

A2 GENERAL PROVISIONS

A2.1 Obligations

Unlike other SecureSign public service, the Services are such that JCSI bears the obligations of the issuer and RA, while the customer bears the obligations of the subscriber. This clause sets forth the obligations based on these characteristics of the Services.

A2.1.1 CA obligations

A CA shall issue and operate certificates according to the rules listed below. The Service is such that the issuer and the administration of a certificate processor and the administration of the RA (including the RAO) are all conducted by JCSI. The obligations of the CA are therefore the obligations of JCSI.

(1) As a certificate processor (CP), the CA shall securely generate and manage the issuer'signature key (private key).

(2) The CA issues a server certificate upon request from the RA.

(3) The CA shall disclose CRLs, and other information, such as that on issuance of certificates, in a prompt manner in a repository.

(4) The CA shall manage certificate life cycles in cooperation with the RA.

(5) The CA revokes a server certificate upon request from the RA and issues CRL.

A2.1.2 RA obligations

In this section, the functions of an RA shall include those of its administrator (RAO). Note that obligations regarding RA operations may be described as RAO obligations. In the Service, the RA is administered by JCSI. The obligations specified below are therefore those of JCSI.

(1) RAOs shall properly review certification applications.

(2) RAOs must verify the reality of the DNS name, one of the characteristic designations of the subscriber to be specified in the certificate.

(3) RAOs must verify the reasonableness of the organizational information if the application includes an organization name or other detail.

(4) The RA is obliged to install and operate RA servers in a secure environment

(5) RAOs must authenticate the certificate applicant. RAOs must also authenticate the certificate application manager (who is responsible for all processes ranging from the generation of keys to the incorporation of a certificate in the web server) and the certificate applicant (client).

(6) When revoking a subscriber's certificate, RAOs shall check the reasonability of revocation The check covers applicant identification and confirmation of applicant's decisions as necessary.

(7) Certificate application data can contain information not stated in the certificate. If such information is contained, the RA must handle application data not reflected in the certificate as

confidential information.

(8) The RA shall manage certificate life cycles in cooperation with the CA.

A2.1.3 KPS obligations

The Services do not include KRS services.

A2.1.4 Subscriber’s obligations

The Services are such that "subscriber" means the same thing as "customer."

(1) Presentation of precise certification application

In acquiring a certificate, a subscriber shall submit a certification application that provides precise information on his/her present conditions.

(2) Limitation on the use of certificates

Certificates are issued according to this document which specifies the use range, security domain and compensation for damages. Subscribers shall not present certificates for any uses out of the specified range (it must be used only as a server certificate).

(3) Obligation to the use of certificates by relying parties

For ciphertext from a relying party using a subscriber’s certificate, the subscriber shall agree that JCSI does not verify or check that in what transaction the certificate will be used or whether it is suitable for particular uses or circumstances and there are no restrictions imposed on relying parties due to the nature of public service.

(4) Obligation to maintain keys

Subscribers shall generate a pair of keys (private and public keys) using their software and hardware, submit the public key to the RA and receive a certificate from the RA. In order to deliver exact information to relying parties, subscribers are obliged to assume the following management:

(a) Management of confidentiality of private keys

The generated private keys must not be used, copied or backed up by any person other than the subscriber. To prevent such operations, subscribers shall take enough care in, for example, controling the authority of the web server and controlling qualifications. If a subscriber suspect sthat illegal use, copy or backup might have occurred, he/she must request revocation.

(b) Management of key pair

If a subscriber suspects an illegal relationship between the private key and the public key in the certificate, he/she must request revocation.

(5) Management of certificate contents

Subscribers shall check that the certificate describes their present conditions upon receipt and

from time to time before using the certificate. When a subscriber finds that the information contained in the certificate is not (or no longer) true to his/her present conditions, the subscriber shall request revocation.

(6) Prompt revocation request

In the cases above (4)-(a) (b) and (5), subscribers shall promptly request revocation.

(7) Keeping in contact with RAO

In the cases above, subscribers shall follow the instructions of an RAO. Revocation requests shall be made via the RAO. Therefore, subscribers shall keep in contact with the RAO.

A2.1.5 Relying party obligations

Relying parties must give consent to the Relying Party Agreement for the Service published in a repository. As set forth in the Relying Party Agreement, relying parties shall check the validity of certificates possessed by subscribers as their transacting parties.

(1) Limitation on the use of certificates

Certificates are operated according to this document specifying purpose, a range of uses, subscriber certification method and compensation for damages. Relying parties shall understand and agree with these provisions to use certificates. The certificate presented at the website is used for encrypted communications between the site and relying parties and for server authentication for the relying parties. The relying parties must not use the certificate if it is considered to be used for any other purpose.

(2) Obligation to verify the validity of certificates

To use certificates, relying parties shall verify the validity of the certificates. Validity verification shall include the following:

(a) Check that all the certificates on the certificate path meet the conditions listed below. In Public Service, it is assumed that JCSI root certificate is trusted.

- Certificates are not tampered.
- Certificates are not expired.
- Certificates are not revoked. (note)
- The purpose of certificate use in (1) above is proper.

(b) Verify the signature on the server certificate

(c) Items stated in the presented certificates meet the provisions prescribed in Chapter A7.

Note: Revocation information is available from information about CRL distribution points in JCSI repositories.

(3) Installation of SecureSign public root certificates

SecureSign public root certificate is not contained in some PKI application software. To use such application software, SecureSign public root certificates can be installed as a trusted certificates.

Hash values (SHA-1 and MD5) for SecureSign public root certificate is published on the JCSI Web site. In installing the SecureSign public root certificate, relying parties shall compare the hash values with those of the SecureSign public root certificate to be installed.

A2.1.6 Repository obligations

The Services conform to clause 2.1.6 of this document.

A2.2 Liability

JCSI, which is to provide the customers with the Services, must have responsibility as the certification authority (CA) and the registration authority (RA), together with its manager (RAOs). Their responsibilities are specified below.

A2.2.1 JCSI liability

(1) In the Services, JCSI warrants the following:

- JCSI itself identifies a subscriber as per Chapter A3 strictly. After that, JCSI shall issue a certificate that exactly reflects the details of the certificate application (e.g., the subjects' distinguished name as in a certificate) from the subscriber.
- As per Chapter A4, JCSI shall register CRLs issued as part of Public Service in JCSI's repositories on a scheduled basis and disclose the revoked certificates in CRLs at all times until those certificates expire, except for suspension due to system maintenance or system shutdown for emergency reasons.
- JCSI shall examine revocation applications appropriately and revoke the certificates of their subscribers without fail.
- As per Chapters 5 and 6 of this document, JCSI shall operate a certificate issuing system without any private keys of certification authorities being compromised due to a key theft, except for cases where they are inferred or calculated from public keys.
- JCSI warrants that certificates, CRL format and attributes conform to the provisions in Chapters 7 and A7at the time of issuance of the certificates.
- Various documents and papers including those to be used to examine the subscribers must be stored with a method invulnerable to loss, tampering and other damage, for a period specified by JCSI.

(2) Notwithstanding (1) above, JCSI shall have a right to temporarily suspend the whole or part of SecureSign Public Service without notice to the customers and subscribers when:

- JCSI performs emergency maintenance of its own facilities for the Services;
- The Service discontinues due to fire or power failure;
- The Service discontinues due to natural disasters including earthquake, eruption, floods or seismic sea wave;

- The Service discontinues due to war, disturbance, riot, civil commotion or labor disputes; or
- JCSI acknowledges the necessity of suspension of the Service for operational, technical or other reasons including the fulfillment of contracts with customers.

(3) The liability of JCSI for customers, subscribers and relying parties regarding SecureSign services is limited to those prescribed in (1) and (2) above.

A2.2.2 Customer liability

In the Services, "customer" is synonymous with "subscriber." The customer is therefore responsible for carrying out the obligations of the subscriber set forth in clause A2.1.4.

A2.3 Financial responsibilities

The Services conform to clause 2.3 of this document.

A2.4 Interpretation and Enforcement

The Services conform to clause 2.4 of this document.

A2.5 Fees

The Services conform to clause 2.5 of this document.

A2.6 Publication and Repositories

Revocation information is available from information about the CRL distribution points in the JCSI's repositories. Except for the points listed above, the Services conform to clause 2.6 of this document.

A2.7 Compliance audit

The Services conform to clause 2.7 of this document.

A2.8 Confidentiality

The Services conform to clause 2.8 of this document.

A2.9 Intellectual Property Rights

The Services conform to clause 2.9 of this document.

A2.10 Personal Privacy Protection

The Services conform to clause 2.10 of this document.

A3 IDENTIFICATION AND AUTHENTICATION

The procedure starting with applying to the issuance of a certificate ("application for a web server certificate") and leading to its issuance is described in clause A4.2. The inspection and verification of the identity of the website in this series of steps are conducted by JCSI (RAOs). The inspection and verification of identity here are specified as follows by JCSI:

- A check that the certificate application manager is qualified to manage the website.
- A check that the certificate applicant (client) is authenticated by the certificate application manager.
- Verification that the items to be reflected on the certificate in the application (information about the registration of certificate applications) represents the reality of the website (for example, a check of the existence of the subscriber organization and the existence of the DNS name and owner).
- Correspondence between the registered information about the certificate application and the information in the certificate signing request (CSR).

The method of identification and authentication conforms to the internal regulations of JCSI.

Note 1: The "application for a web server certificate" can be downloaded from the JCSI's repositories.

Note 2: When one administers more than one web server with the same Common Name by means of a load distributor or an SSL accelerator, one needs as many server certificates as web servers.

A3.1 Initial Registration (Initial Application)

A3.1.1 Types of names

See the information for registration in the "application for a web server certificate."

A3.1.2 Need for names to be meaningful

The name must represent correctly the reality of the website. For that reason, the subscriber becomes obligated to represent the reality of the site and apply for it in the "application for a web server certificate."

A3.1.3 Rules for interpreting various name forms

As per the configuration rules of the subscriber.

A3.1.4 Uniqueness of names

Each constituent of the distinguished name in the server certificate must represent the reality of the subscriber accurately. The server recognized as the entire distinguished name must be uniquely

recognized.

Note: If, for example, one wishes to obtain more than one server certificate for the same server name (CommonName), one changes the organization name (OrganizationalUnitName) for each server certificate.

A3.1.5 Name claim dispute resolution procedure

Name claim dispute in name requirements shall mean some kind of dispute related to the distinguished name in the server certificate (such as infringement on a right, libel, business obstruction, unfair competition, and unlawful use).

Name claim dispute in the subscriber's domain (the domain to which a server with a server certificate belongs) shall be resolved in that domain. Disputes across multiple domains or those involving a relying party shall be resolved by the parties (subscriber and relying party). In both cases, JCSI is not involved in disputes.

A3.1.6 Recognition, authentication, and role of trademarks

The distinguished name in the server certificate must guarantee that it does not infringe on any trademark or any other intellectual property owned by a third party. The responsibility for the guarantee shall be borne by the subscriber applying to the entries in the certificate, and JCSI shall be exempted from the responsibilities for any damage resulted from such infringement or obstruction.

A3.1.7 Method to prove possesion of private key

The precondition is that the certificate signing request (CSR) has been signed by the private key corresponding to the public key. (A request is as a rule formed with PKCS#10.)

A3.1.8 Authentication of organization identity

To check the entity of an organization to which the subscriber belongs, JCSI (RAO) may require the subscriber to present a certificate of existence and good standing of his or her organization (such as a certificate of its corporate registration information).

A3.1.9 Authentication of individual identity

To check identity described in the introduction of clause A.3, JCSI (RAO) may require the subscriber to present a certificate of the existence and good standing of his or her organization mentioned in clause A.3.1.8, along with a certificate indicating that the certificate application manager belongs to the organization (such as his or her employee card). Another indispensable item in applying to a certificate is the individual (client) responsible for such actual work as the steps ranging from key generation/registration to incorporating a server certificate into the server machine. The verification of

this personal identity is also conducted by JCSI, just like that of the certification application manager.

A3.2 Routine Rekey

The same as initial registration.

A3.3 Rekey after Revocation

The same as initial registration.

A3.4 Revocation request

JCSI (RAO) accepts revocation requests for server certificates from the certificate applicant (client) or certificate application manager alone. To check the identity of the revocation applicant, JCSI may require the revocation applicant to present the certificates specified in clauses A3.1.8 and A3.1.9.

A4 OPERATIONAL REQUIREMENTS

A4.1 Certificate Application, Issuance and Acceptance

The Service differ from every one of the eight types of services (A-1 through D-2) set forth in this document. The types of the Services, repository locations, and issuing patterns are specified below.

Table A4-1 Services of issuing Web-server certificates (locations and operators)

Type	RCA	ICA	SCA	CAO	RA	RAO	Repository	Key restoration
SecureSign server services	Installed by JCSI Operated by JCSI	—	Installed by JCSI Operated by JCSI	Installed by JCSI Operated by JCSI	Installed by JCSI Operated by JCSI	Installed by JCSI Operated by JCSI	Installed by JCSI Operated by JCSI	×

Table A4-2 Repository locations and methods of disclosing and verifying CRLs

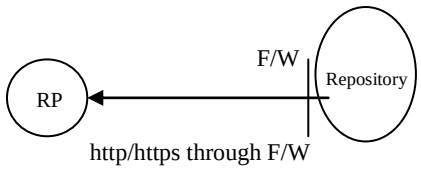
No.	Repository locations	Style overview	Applicable service type	Type of repository	Repository to be referred to by the relying parties for verification
4	JCSI		SecureSign public services including SecureSign server services	SecureSign public repository	Refer directly to the SecureSign public repository by http

Table A4-3 Issuing pattern

	Subscriber	RA	CA	Repository
Pattern 1	Key generation → Application (including revocation) Storage ←	Eligibility check → Issuance request Delivery ←	Issuance Delivery ←	Registration (CRL)

Issuing pattern	Trigger for issuance	Subscriber's key generation	Eligbility check method		
			Automatic	Advance	Manual
1	Certificate: Subscriber trigger CRL: RAO trigger	Subscriber	×	×	○

In the Services, one applies for the issuance of a certificate as follows:

(1) The subscriber applies provisionally for the inquiry page on the JCSI's web.

(2) JCSI examines the contents of the provisional application carefully, and gives orders to present an official application and documents necessary for the application to the subscriber.

(3) The subscriber fills out the web server application (to be downloaded from the JCSI's web) and mail it to JCSI together with the necessary documents.

(4) JCSI examines the web server application and attached documents according to JCSI's standards and, if it is found to be problem-free, JCSI regards that the contract is established. If it is found to be problem-ridden, the subscriber will be required to present a corrected set of documents.

(5) Key generation by the subscriber, then Certification Signing Request (CSR) preparation by the subscriber and then Application from the subscriber to the RAO

(6) Manual check of the Certification Signing Request (CSR) by JCSI (RAOs)

(7) Request for the issuance of a certificate by the JCSI RAO to the CA, then Issuance of a certificate by the CA, and then reception of it by the RAO

(8) The RAO sends the certificate to the subscriber.

A4.2 Certificate Suspension and Revocation

In the service too, the certificate is revoked if the distinguished name or other entry in the certificate is changed, the certificate is replaced with another certificate, it is halted to use by the subscriber, the private key is compromised by the subscriber, the certificate signature key of the SCA is compromised. The suspension of certificates is not part of the current system.

The revocation procedure is usually initiated upon request from the subscriber to the RAO. The RAOs of JCSI examines whether to revoke it, and the request for revocation is accepted and processed by the CA. The certificate revocation list (CRL) is periodically disclosed.

A4.3 Security Audit Procedures

The Services conform to clause 4.3 of this document.

A4.4 Archiving

The Services conform to clause 4.4 of this document, together with the following:

- The original application and attached documents to be filed when the subscriber applies for the issuance of a certificate. (For 10 years after the certificate expires.)
- A complete set of the application form to be filed in applying for revocation of the certificate by the subscriber and other documents used by JCSI or customer to decide whether to revoke it. (For 10 years after the certificate expires.)
- The letter of information and subscriber’s agreement to be disclosed to the subscriber, relying party's agreement to be disclosed to the relying parties, and records of their changes. (The latest version is to be stored permanently, while the old version before the revised one is to be stored for 10 years after the revision.)

A4.5 Key changeover

The Services conform to clause 4.5 of this document.

A4.6 Compromise and Disaster Recovery

The Services conform to clause 4.6 of this document.

A4.7 CA Termination

The Services conform to clause 4.7 of this document.

A5 PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

The Services conform to Chapter 5 of this document, together with the following:

A5.1 Physical Security Controls

In SecureSign services, the server (it means CA, and RA for types A-1, B-1, C-1 and D-1. The same term is used hereinafter in this chapter) is operated outside the secure facilities (from the office of JCSI headquarters). JCSI specifies security for all operations from this JCSI headquarters.

(1) All accesses are client-authenticated by the server.

(2) The client certificate is stored in a Smart Card medium and protected by PIN.

(3) Each medium is provided with a designated owner (RAOs) and information of provision is documented.

(4) All accesses are applied to encrypted communications with a sufficient intensity against tapping.

(5) All operations are applied to DualControl.

(6) All accesses are recorded on the server as audit trails.

(7) The terminal in the JCSI headquarters must be places with access restricted by means of keyed doors. These places are designed to prevent intruders from outside within the range set forth in the Fire Service Law. Accesses to these locations are limited to designated personnel. The doors are locked automatically when closed, and every entry or exit to this room is recorded in the ledger every time such an event happens. These records must then be audited very month by the PKI operation administrator.

A5.2 Procedural Security Controls

JCSI distinguishes the personnel as shown in the table A5-1 below. Personnel at operation centers and JCSI's headquarter shall operate the CA, the RA installed at JCSI, and JCSI's repositories.

Table A5-1 Authority of personnel

<table>
<tr><th colspan="2">Personnel classification</th><th>Authorization</th><th>Authorization for access</th><th>Authorization for operation</th><th>Access authority check</th></tr>
<tr><td colspan="2">PKI operation administrator</td><td>Designated and authorized at each JCSI headquarter and center</td><td colspan="2">—</td><td>—</td></tr>
<tr><td colspan="2">Security adminisstrator</td><td>Same as above</td><td>Authorized</td><td>—</td><td>ID card system and biological authentication system</td></tr>
<tr><td rowspan="3">Center personnel</td><td>PKI engineers</td><td>Designated by the PKI operation administrator</td><td rowspan="3">Authorized by the PKI operation administrator based on the consent of the security administrator</td><td rowspan="4">Authorized by the PKI operation administrator</td><td>Access by a single person is not allowed. Must be accompanied with a person authorized to access the security systems</td></tr>
<tr><td>System operator</td><td>Designated by the security administrator based on the consent of the PKI operation administrator</td><td>ID card system and biological authentication system</td></tr>
<tr><td>Maintenance personnel</td><td>Designated by the security administrator or PKI operation administrator</td><td>Access by a single person is not allowed. Must be accompanied with a person authorized to access the security system</td></tr>
<tr><td>Headquarters’ personnel</td><td>Business operator</td><td>Designated by the PKI operation administrator</td><td>—</td><td>Client certificate for remote access</td></tr>
</table>

To ensure security of the installation site of the certificate issuing system, center personnel are authorized to access the site or limited in access to the system room. Based on the consent of the security administrator, the PKI operation administrator of each center must be able to authorize them to access the system room. The security administrator must register or erase the information of the center personnel in the ID card system and biometric authentication system based on the authorization document.

To ensure security of the operation of the certificate issuing system, only a limited number of personnel are authorized to operate specific equipment and devices. The PKI operation administrator of each center must be able to authorize the rights to operate the certificate issuing system. Based on the authorization document, the PKI operation administrator must set (change or erase) the accounts and issue or revoke the operation certificates. In particular, the administrator must rigidly control the accounts with access privileges.

To ensure security in the remote operation of the certificate issuance system from the JCSI's headquarter, the headquarter personnel are authorized to do remote operation from the JCSI's headquarter for secure operation. The PKI operation administrator can provide the authority of personnel to remotely operate the certificate issuance system.

Records of the authorization for access, operation and remote operation must be managed by the PKI operation administrator and stored in a keyed cabinet for at least three years.

The details of authorization for access and commanding system must be stated in the detailed procedure of each center or JCSI's headquarter. The PKI operation administrator of each center may be referred to simply as the operation administrator in detailed procedures. To trust some operations, JCSI must direct the trustee to observe the rules stated in this chapter and to create the detailed procedure so that the trusted operations can be performed according to that procedure. Each center and JCSI's headquarter must monitor the operations of personnel or trustee to maintain the proper security according to this document.

A5.3 Personnel security controls

The Services conform to clause 5.3 of this document.

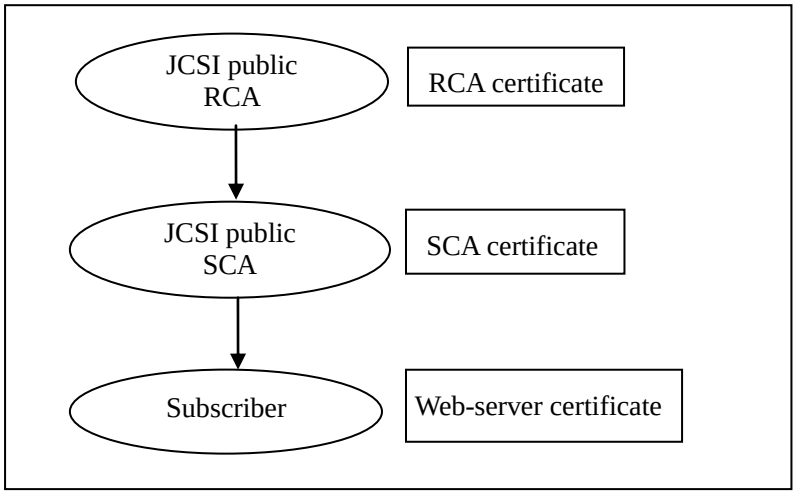
A6 TECHNICAL SECURITY CONTROLS

The Services also conform to Chapter 6 of this document. However, the Web-server certificate is registered/verified/issued via the RAOs with the issuing pattern 1.

A7 CERTIFICATE AND CRL PROFILES FOR SecureSign SERVER SERVICE

A7.1 Hierarchy of certificates

Shown below is the hierarchy of certificates in SecureSign server service.



A7.2 Profile and settings of each certificate

The settings of the SecureSign certificate conform to RFC2459. The settings are configured by the subscriber or JCSI. The settings are individually controlled for each certificate type. The RCA certificate, SCA certificate, and CRL profile conform to the descriptions in Chapter 7 of this document. Here, the profile of the Web-server certificate is specified in Table A7-1.

Table A7-1 Server certificate profile and its setting

No.	Field name (field name)	Setter	c/nc	Description of setting
Certificate Basic Fields				
1	Version (version)	JCSI	—	Fixed to V3
2	Serial number (serialNumber)	JCSI	—	A positive integer up to 128 bits
3	Signature (signature)	JCSI	—	RSA with SHA-1
4	Issuer (issuer)	JCSI	—	c=JP o=Japan Certification Services, Inc. cn=SecureSign PublicCAn (n=1, 2, 3,…)
5	Validity period (validity)	JCSI	—	1 year + 30 days after the application
6	Subject (subject)	Subscriber and JCSI	—	c=JP st=Prefecture name (subscriber setting, optional) l=Municipality (subscriber setting, optional) o=Name of server management organization (subscriber setting, indispensable) ou=Name of server management department (subscriber setting, optional) cn=Server DNS name (subscriber setting, indispensable)
7	Subject public key (subjectPublicKeyInfo)	Subscriber	—	RSA public key (512 to 2,048 bits) *1
Certificate Standard Extensions				
8	Authority key identifier (authorityKeyIdentifier)	JCSI	nc	SHA-1 of the public key, and DN and serial number of the issuer
9	Subject key identifier (subjectKeyIdentifier)	JCSI	nc	SHA-1 of the public key
10	Key usage (keyUsage)	JCSI	nc	digitalsignature,keyEncipherment
11	Extended key usage (extendedKeyUsages)	JCSI	nc	PKIX-IDKP-ServerAuth、PKIX-IDKP-ClientAuth
12	Certificate policy (certificatePolicies)	JCSI	nc	policyOID: 1.2.392.200075.2.2 policyURL: https://cp.jcsinc.co.jp/SecureSigh/1/RPA1.html
13	Basic constraints (basicConstraints)	JCSI	nc	cA: FALSE pathLenConstraint: The field is omitted.
Certificate Netscape Extensions				
14	Netscape-cert-type	JCSI	nc	SSL Client, SSL Server

c/nc: show critical specifications c and nc, respectively. —: No setting definitions

*1: A key 512 bits long may be tolerated as an exception.

A7.2.1 Contents of the subscriber's application (remarks)

(1) Email item in the subject field

The subscriber must not configure this item in a certificate signing request (CSR).

(2) The RAO must verify whether a DNS name is specified in the cn of the subject field that identifies the server owned by the subscriber.

A7.2.2 Validation of the settings in an issued certificate

The subscriber must promptly inspect whether the settings in an issued certificate are valid. If any setting is unacceptable, the subscriber must promptly apply to JCSI for revoking that particular certificate.

A8 Specification Administration

The Services conform to Chapter 8 of this document.