SecureSign® AD

Service Standard (V2.5)

Sept. Feb. 1, 2013

Japan Certification Services, Inc.

Revision history

Version	Date	Content of revision
1.0	January 30, 2009	First edition
1.0.1	January 25, 2010	Update based on Mozilla public discussion result
2.0	April 1, 2010	Addition of client certificates issuing service
2.1	June 7, 2010	Addition of TSA server certificate issuing service
2.2	April 4, 2011	Modification of client certificate profile
2.3	Sept. 30, 2011	3.(2) Sync. with detailed procedure
2.4	Feb. 24, 2012	1.4 Moving to the new office
2.5	Feb. 1, 2013	4.3、5.1、6.7 Quitting the operation of IDS

Table of Contents

1. INTRODUCTION

1.1 General

Japan Certification Services, Inc. (JCSI) provides a certificate issuing service named SecureSign AD (also hereafter referred to as "this service"). With this service, JCSI issues a public key certificate based on PKI standards for a key pair conforming to a Public Key Cryptography that is associated with a "person," "corporation," "device" or "software" of a JCSI customer, and gives proof of the subject of that key pair to third parties (relying parties) to whom the certificate is presented.
JCSI also provides two other types of certificate issuing services: SecureSign and AccreditedSign.
From the start of practice, SecureSign AD must be periodically audited and accredited externally according to the WebTrust for CA standard (the AICPA/CICA WebTrust for Certification Authorities Principles and Criteria) designed by the American Institute of Certified Public Accountants(AICPA) and the Canadian Institute of Chartered Public Accountants(CICPA). Many vendors dealing with globally used browsers, electronic mail and electronic document software accept the WebTrust for CA as a trustworthy audit standard for certification authorities. For users of those products (i.e., parties relying on their certificates) vendors regard the certification authorities approved with WebTrust for CA accreditation as “Trusted Certification Authority” on their products.
The public key certificates issued from the SecureSign AD service cannot be used in procedures for bidding, application, and notification (e.g., tax declaration with the e-Tax system、application for patent and other applications via the Internet) to administrative agencies as this service is not accredited under Electronic Signature Law Japan.
SecureSign AD certificates (or is intended to certificate) multiple types of entities, such as a "person," "corporation," "device" and "software", as the subjects of key pairs (i.e., subscribers to be certificated). At present, JCSI sets the certificate policy for SecureSign AD assuming that the certificates must be used for SSL/TLS server certification, TSA server certification, SSL/TLS client certification, S/MIME mail, and Electronic Document Signature. The certificate policy is defined and described together with the Certification Practice Statement (CPS) in this document.
SecureSign AD is practiced in conformance with various RFC standards such as RFC 5280 developed by the Public Key Infrastructure working group (PKIX) of the Internet Engineering Task Force.
SecureSign AD is part of the certification business in which JCSI functions as the certificate issuer. JCSI may entrust certain parts of its business, such as certification processor server operations and qualification/registration operations concerning specific certificate policies, to agents. This document includes a definition of terms that the entrusted agents must observe.

1.2 Object Names

This document is titled "SecureSign AD Service Standard". Table 1-1 lists the object identifiers (OIDs) assigned to this document and related services.

Table 1-1 OIDs assigned to JCSI and other objects

OID	Object
1.2.392.200075	Japan Certification Services, Inc.
1.2.392.200075.4	SecureSign AD Service
1.2.392.200075.4.1	SecureSign AD CPS (this document)
1.2.392.200075.4.2	SecureSign AD Policy for certificate

1.3 Community and Applicability

1.3.1 Entities and roles

The SecureSign AD service involves the entities listed in Table 1-2.

Table 1-2 Entities and their roles

Entity	Role
Subscriber	A person, organization or object whose public key and subject name are combined in a certificate. A subscriber (or administrator of a subscriber where it is an object) purchases a SecureSign AD certificate from JCSI. The terms that the subscriber shall observe are also defined in the salse contract between the subscriber and JCSI.
Relying party	A person, organization or object that relies on a subscriber's certificate and verifies the subscriber's digital signature.
End entity	Subscribers and relying parties are called end entities.
Issuer (certification authority) (CA)	When issuing a certificate, the issuer creates and discloses a certificate policy and a CPS (without breaching the policy of any superior certification authority、if any). The issuer is an organization that signs a certificate with its own private key, thereby authenticating that certificate. In this service, JCSI is the issuer. The issuer is a managing subject in a certification authority. Its public key certificates are issued not only to subscribers but also to the personnel and devices of the issuing and registration authorities.
Registration authority (RA)	An organization that accepts subscriber’s applications, checks the contents of themt, and registers subscriber’s information before issuing certificates. In this service, JCSI basically performs registration operations, but may entrust those operations to another organization based on a consignment contract

	with JCSI. The registration authority performs the following functions: Acceptance of certificate applications Applicant identification Request to the IA for certificates Delivery of certificates (and private keys) Decision on revocation of certificates and request to the IA for certificate revocation * IA: Issuing Authority
RA officer (RAO)	(1) A person who manages and operates the RA. (2) A person who inputs requests for subscriber certificate issuance and subscriber certificate revocation.
Issuing authority (IA)	An organization that creates certificates and certificate revocation lists (CRLs) with the signature of the issuer according to a consignment contract with JCSI. The IA issues individual certificates upon receiving a request for certificates from the RA, revokes individual certificates according to a request for certificate revocation, and periodically updates and issues CRLs.
IA officer (IAO)	A person who manages and operates the IA.
Repository	A repository is used to store the certificates ofCAs, CRLs and other information on the SecureSign AD service, and reply to queries from relying parties.
Root certification authority (RCA)	The RCA resides at the top of the certification hierarchy (or beginning of the hierarchical certification path, and signs its own certificates and those for subordinate certification authorities (SCAs) immediately below it. Certificates issued fromthe RCA shall be under dual control requiring the consent of multiple persons for issuing each certificate. The RCA does not include any RA. The self-signed certificate may be denoted as “Root Certificate”. * RCA: Root CA
Subordinate certification authority (SCA)	Certificates for an SCA are signed by the root certification authority (RCA) immediately above the SCA. The SCA signs certificates for subscribers and includes RAs that check applicants and registers them as subscribers. * SCA: Subordinate CA

1.3.2 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 using a certificate to permit someone to make transactions involving an amount of money not exceeding a certain limit. Conversely, uses in a narrow sense refer to cases where the use of a certificate is determined by settings in the KeyUsage and extendedKeyUsage fields within an X.509 certificate.

In the SecureSign AD service, JCSI does not define uses in a broad sense. Therefore, JCSI does not present any applications to which issued certificates are appliacable or which limit the use of issued certificates. JCSI, however, prohibits the use of certificates in criminal or other illegal activities. End entities should not make transactions which involve a large amount of money relying on the settings of SecureSign AD certificates.

As part of the SecureSign AD service, JCSI issues the following certificate for uses in a narrow sense (see Chapter 7):

- SecureSign AD Web-server certificate (Web server certificates, TSA server certificates, etc.)
- SecureSign AD client certificate (S/MIME certificates, client certificates, etc.)

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

1.3.3 Interoperability and root certificates

The certificates and CRLs issued by JCSI are used in an environment that calls for a Public Key Infrastructure (PKI). JCSI one after another verifies the interoperability with typical PKI-conforming products. For the latest information on interoperability, contact our sales department.

JCSI discloses RCA/SCA certificates for SecureSign AD in a repository. End entities can download these certificates for installation as part of the software requiringthem. To distribute the software containing RCA certificates to a third party, the end entity must consent to the Root Certification Installation Agreement before downloadingthem.

1.4 Distribution of Service Specification Information

This CPS is disclosed in a repository. End entities shall periodically visit repositories and understand contents regarding to new SecureSign AD service and changes in the service specifications. An end entity that needs to know SecureSign AD service contents can send inquiries to JCSI's help desk. Inquiries via electronic mail are desirable. Inquiries over the phone will also be accepted during JCSI's business hours (9:00 a.m. to 5:00 p.m.).

Note: The business days of JCSI are weekdays (Monday to Friday) other than national holidays and JCSI-specified special holidays and year-end through New Year holidays. JCSI announces its special holidays and year-end through New Year holidays on its Web site (http://www.jcsinc.co.jp).

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 (CA) in the SecureSign AD service, JCSI bears the obligations of the IA, RA and repository, each subscriber bears the obligations of the subscriber, and each relying party bears the obligations of the relying party. JCSI will fulfill some of its obligations by entrusting them to third parties.

2.1.1 IA obligations

An IA shall issue and operate certificates according to the rules below. IA obligations are imposed on JCSI (including entrusted agents).

(1) The IA shall securely generate and manage the issuer's (JCSI's) signature key (private key).
(2) The IA shall issue certificates in response to requests from the RA.
(3) The IA shall manage certificate life cycles in cooperation with the RA.
(4) The IA shall promptly disclose CRLs and other information concerned with the issuance of certificates in a repository.
(5) The IA shall revoke subscriber certificates in response to requests from the RA, and issue CRLs.

2.1.2 RA obligations

Descriptions in this section are based on the assumption that the functions of an RA should include those of its operator - the RA officer (RAO). Note that obligations regarding RA operations may be described as RAO obligations. RA and RAO obligations are imposed on JCSI (including entrusted agents).

(1) The RAO shall properly verify certificate applications.
(2) The RAO shall verify the authenticity of the DNS name, a part of Common name in Subject name specified in the certificate.
(3) If a certificate application includes an organization name or other detail, the RAO shall verify the validity of the organizational information.
(4) The RA is obliged to install and operate RA servers in a secure environment. When the RA generates subscribers' key pairs for S/MIME or client certificates, RA shall set up an adequate protection measures to make someone other than authorized RAO unable to generate the key pairs or to get access to the key pairs.
(5) The RAO shall identify certificate applicants (customers). The RAO shall also identify the certificate application administrator (responsible for all processes from generating keys to installing certificates on the Web server). When the RAO handle subscribers' key pairs for issuing S/MIME or client certificates, the RAO shall set up an adequate protection measures

from leakage or damage of the key pair, shall ensure distinct deliveries to the applicants (customers), and shall promptly delete that key pair in RA after confirming the completion of delivery.

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

(7) A certificate application may include information that is not be set in the certificate. If such information is included, the RA is obliged to handle application information not reflected in the certificate as confidential information.

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

2.1.3 Subscriber obligations

Subscribers to the SecureSign AD service bear the obligations below. If a subscriber corresponds to an object, the administrator of the object bears the obligations below.

(1) Presentation of precise certificate application contents

In acquiring a certificate, the subscriber shall present a certificate application that provides precise information on the subscriber's current conditions to the RA.

(2) Limitation on the use of certificates

Certificates are issued according to this document by specifying the use range, security domain, and compensation for damages. The subscriber shall not use certificates for any uses out of the specified range.

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

The subscriber shall agree that for the cipher text from a relying party using a subscriber's certificate JCSI does not examine or check in what transaction certificate will be used or whether the certificate is suitable for particular uses or circumstances. The subscriber shall also agree that no restrictions are imposed on relying parties due to the nature of public service.

(4) Obligation to maintain keys (for Web server certificates, TSA server certificates)

The subscriber shall generate a pair of keys (private and public keys) with the subscriber's software and hardware, submit the public key to the RA, and then receive a certificate from the RA. In order to deliver exact information to relying parties, the subscriber is obliged to assume the following management:

(a) Management of confidentiality of private keys

Private keys generated by a subscriber must not be used, copied or backed up by any person other than the subscriber. In this context, the subscriber shall also maintain the mannegement process of authority and qualification for using the Web server very carefully. If there is the susupicion of any illegal use, copying or backup, the subscriber

must request revocation.

(b) Management of key pair

If the subscriber suspects an illegal relation between the private key and public key in the certificate, the subscriber must request revocation.

(5) Obligation to maintain keys (for S/MIME certificates, client certificates)

The generation of a key pair is performed in RA. Subscriber shall receive it with a certificate from RA. In order to deliver exact information to relying parties, the subscriber is obliged to assume the following management:

(a) Management of confidentiality of private keys

Private keys received by a subscriber must not be used, copied or backed up by any person other than the subscriber. In this context, the subscriber shall also maintain the mannegement process of authority and qualification for using the PC very carefully. If there is the susupicion of any illegal use, copying or backup, the subscriber must request revocation.

(b) Management of key pair

If the subscriber suspects an illegal relation between the private key and public key in the certificate, the subscriber must request revocation.

(6)Management of certificate contents

The subscriber shall confirm the contents of an issued certificate upon receiving it, and then confirm that the certificate describes the subscriber's present conditions before using the certificate as needed. If the subscriber finds that any information contained in the certificate is not(or no longer) true regarding the subscriber's present conditions, the subscriber shall promptly request revocation.

(7) Prompt revocation request

In case of (4)-(a), (4)-b, (5)-(a), (5)-(b) or (6) above, the subscriber shall promptly request revocation.

(8) Keeping in contact with the RAO

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

2.1.4 Relying party obligations

Each relying party shall consent to the Relying Party Agreement published for this service in a repository. As set forth in the Relying Party Agreement, the relying party shall check the validity of certificates possessed by subscribers who are his/her transacting parties.

(1) Limitation on the use of certificates

Certificates are operated according to this document specifying the purposes, range of uses, subscriber certification method, and compensation for damages. The relying party shall understand and agree with these provisions before using certificates. A certificate presented from a Web site is used for encrypted communications between a Web site and relying parties, as well as server authentication by relying parties.TSA server certificate is used to digitally sign the timestamp tokens. The S/MIME certificate must be attached to the S/MIME mail when it is excaged between a subscriber and a relying party , or be presented by the subscriber to a Web site for client authentication. The client certificate must be attached to the digitally signed electronic document, or be presented by the subscriber to a Web site for client authentication. The relying party must not use the certificate upon determining that the certificate is being used for any other purpose.

(2) Obligation to verify the validity of certificates

The relying party shall verify the validity of certificates when he/she uses them. Validity verification shall include the following:

(a) Confirm that all certificates on the certificate path meet the conditions below. In the SecureSign AD service, it is assumed that the JCSI root certificate is trusted.
- Certificates are not tampered with.
- Certificates are not expired.
- Certificates are not revoked. (Note)
- The certificate is used for a proper purpose as described in (1) above.

(b) Verify the signature on that certificate.

(c) Confirm that the contents of the presented certificate meet the provisions prescribed in Chapter 7.

Note: Revocation information can be acquired from the CRL distribution points in JCSI repositories.

(3) Installation of SecureSign AD root certificate

Some PKI application software does not include the SecureSign AD root certificate. To use such application software, the SecureSign AD root certificate can be installed as a trusted certificate. Hash values (SHA-1) for the SecureSign AD root certificate are disclosed on JCSI's Web site. When installing the SecureSign AD root certificate, the relying party shall verify the hash values of the SecureSign AD root certificate to be installed by comparing them with the disclosed hash values.

2.1.5 Repository obligations

JCSI shall disclose information about created CRLs in repositories with the method prescribed in Section 2.6.2 so that subscribers and relying parties can check the validity of subscriber's certificates

at any time in order to decide whether to use them or not.
JCSI also stores other information about this service in repositories and discloses the information with the method given in Table 2-1.

2.2 Liability

JCSI, which provides subscribers with the SecureSign AD service, shall be responsible for subscribers and relying parties as the issuing authority (IA), registration authority (RA), and registration authority officers (RAOs). Subscribers shall be responsible for fulfilling the subscriber obligations prescribed in Section 2.1.3 for the qualification check and the registration by JCSI. These responsibilities are defined as follows:

2.2.1 JCSI liability

(1) In this service, JCSI warrants the following:

- JCSI shall strictly identify each subscriber as per Chapter 3, and issue a certificate that exactly reflects details (e.g., subject's distinguished name in a certificate) of the certificate application from the subscriber.
- As per Chapter 4, JCSI shall register the CRLs periodically issued as part of the SecureSign AD service in its repositories, and continue disclosing the revoked certificates until they expire, except in case of suspension due to system maintenance or system shutdown due to emergency reasons.
- JCSI shall examine revocation requests appropriately, and revoke subscriber certificates without failure.
- JCSI shall operate the certificate issuing system as per Chapters 5 and 6 without any private keys of CAs being compromised due to key theft, except in cases where private keys 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 the certificates are issued.
- JCSI shall store various documents and papers, including those to be used in examining the subscribers, with a method invulnerable to loss or tampering for a period specified by JCSI.

(2) Notwithstanding (1) above, JCSI shall have the right to temporarily suspend the whole or part of this servicewithout giving prior notice to the subscribers in case of the following:

- JCSI performs emergency maintenance of its own facilities for this service,
- service discontinued due to fire or power failure,
- service discontinued due to a natural disaster (e.g., earthquake, eruption, flood, seismic sea wave),
- service discontinued due to war, disturbance, riot, civil commotion or labor dispute, and

- JCSI acknowledges the need to suspend this service for operational, technical or other reasons, including the fulfillment of contracts with subscribers.

(3) The liability of JCSI for subscribers and relying parties regarding this service shall be limited to those prescribed in (1) and (2) above.

2.2.2 Subscriber liability

Subscribers shall be responsible for fulfilling the subscriber obligations prescribed in Section 2.1.3.

2.3 Financial Responsibilities

2.3.1 Responsibility for compensation

(1) If JCSI compensates for damages caused by a breach of the provisions prescribed in Section 2.2.1, the amount of indemnity paid to a subscriber shall be limited to the amount agreed upon in the contract with the subscriber, and that paid to a relying party shall be limited to the amount agreed upon in the Relying Party Agreement. JCSI shall bear no responsibility for any 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) If JCSI suffers damage due to a subscriber's failure to fulfill the obligations prescribed in this document or a subscriber's breach of the provisions in Section 2.2.2, JCSI shall have the right to claim indemnity for the relevant damage.

(3) In relation to the limitation on the use of certificates by subscribers prescribed in Item (2) of Section 2.1.3, subscribers shall bear full responsibility for any trouble caused by their use of a certificate for any uses out of the specified range. If JCSI suffers any damage due to such trouble, the subscriber shall compensate JCSI for the damage. In relation to revocation requests prescribed in Item (7) of Section 2.1.3, 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. If JCSI suffers any damage due to such trouble, the subscriber shall compensate JCSI for the damage.

(4) In relation to the limitation on the use of certifications prescribed in Item (1) of Section 2.1.4, the relying parties shall bear full responsibility for any damage caused by their use of a certificate for any uses out of the specified range. JCSI shall bear no responsibility for the damage. The validity of certificates used by relying parties, prescribed in Item (2) of Section 2.1.4, is generally verified automatically by the software. The relying parties shall be responsible, however, for their final decisions. JCSI shall bear no responsibility for any damage resulting from transactions made by a relying party in spite of its failure or negligence to verify validity.

2.3.2 Fiduciary relationships

JCSI does not act as an agent or trustee in terms of finance for subscribers and relying parties of the SecureSign AD service. However, JCSI does cooperate with NEC Corporation, Hitachi, Ltd., and Fujitsu Limited. These companies participate in the managment of JCSI as its main stockholders, while JCSI entrusts its operations to them.

2.3.3 Accounting principles

JCSI is managed according to corporate accounting principles under the Commercial Law of Japan.

2.4 Interpretation and Enforcement

2.4.1 Governing law

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

2.4.2 Severability, survival, merger, and notice

JCSI may segment the SecureSign AD service, consolidate other services to the SecureSign AD service, or merge the SecureSign AD service with other services.

2.4.3 Dispute resolution procedures

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

2.5 Fees

JCSI shall disclose the basic fees for the SecureSign AD service on its Web site. Other fees will be disclosed by the sales department of JCSI on demand.

2.6 Publication and Repositories

2.6.1 Publication of CA information

In the SecureSign AD service, JCSI operates repositories to provide information to subscribers and relyig parties.

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 repositories within 12 hours after the revocation procedure is performed.

(3) The information about revoked certificates in CRLs is kept disclosed on JCSI repositories until the revoked certificates expire.
(4) Other information is updated and disclosed from time to time at the discretion of JCSI.

2.6.3 Access control

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

Note: Anyone involved is allowed to access this document, but must not modify it.

2.6.4 Repositories

(1) JCSI repositories are used to store and disclose CRLs and other information about the SecureSign AD service. (See Table 2-1.)
(2) The CRLs of unexpired certificates are stored on the repositories, and disclosed to relying parties.
(3) The method of accessing JCSI repositories and their addresses are available on JCSI's Web site (http://www.jcsinc.co.jp).
(4) Subscribers can make copies of subscriber certificates and CRLs on servers managed by the subscribers.
(5) Repositories are operated for 24 hours a day. However, repositories may be temporarily shut down with prior notice given on the Web site for system maintenance or other technical reasons. 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 AD Service Standard (CPS)	Any person involved	Yes
Agreement	Relying Party Agreement	Relying parties	Yes
	Root Certification Installation Agreement	Software providers	Yes
Certificate, etc.	SecureSign AD Service Root Certificate	Software providers, subscribers and relying parties	Yes
	CRL	Relying parties	Yes
Notice	Notice from JCSI	Any person involved	Yes

2.7 Compliance audit

In operating the SecureSign AD service, JCSI periodically undergoes an external audit to verify its conformance to the security provisions, including this document.

2.7.1 Frequency of audit

An external audit is conducted in the following events in compliance with the WebTrust for CA audit standard:

(1) One year after the previous external audit

(2) Upon an important update related to security

2.7.2 Auditor identity and qualification

JCSI appoints a Japanese audit corporation qualified for WebTrust for CA audit as the external auditor. At present, Ernst & Young ShinNihon LLC is appointed as the external auditor.

2.7.3 Auditor's relationship to the audited party

The auditor shall belong to a different organization independent of the certificate operating department.

2.7.4 List of topics covered under the compliance audit

To undergo an external audit, JCSI, together with the auditor, defines the purpose of the audit, auditing organization, schedule, entities to be audited, and working procedures.

2.7.5 Actions taken against problems found in audits

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

2.7.6 Report on compliance audit results

JCSI submits a report on WebTrust for CA audit results to AICPA so as to be certified with WebTrust for CA accreditation. This association will publicly announce that the SecureSign AD service is accredited. JCSI may disclose the audit report to individual vendors who desire to preinstall the SecureSign AD Service Root Certificate in their products on demand.

2.8 Confidentiality

2.8.1 types of information to be kept confidential

JCSI and subscribers shall not disclose or divulge to a third party, without written consent from the other party, any confidential information (including information on subscribers) that, in connection with the SecureSign AD service, 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 verification of the relevant information's confidentiality in a written form within 14 days after the date of presentation. JCSI and subscribers also shall not use such confidential information beyond the limitations to provide or use the SecureSign AD service.

2.8.2 type of information not considered confidential

Notwithstanding Section 2.8.1, the types of information prescribed below shall not be considered confidential.

(1) Information that should be included in a certificate or CRL, except the subscriber's distinguished name in the certificate
(2) Information included in this CPS
(3) Information already known to the receiving party or publicly known at the time of disclosure
(4) Information that that has become publicly known after disclosure for reasons not attributable to the receiving party
(5) Information acquired lawfully from any third party without secrecy obligations
(6) Information that has been created by the receiving party on its own terms 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 in response to a revocation request, the CRL corresponding to the certificate includes the reason code and the date of revocation. Therefore, the reason code and date of revocation are not considered confidential, and will be disclosed to all relying parties. Other detailed information about revocation will not be 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 subscribers to such law enforcement officials when such release is considered 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 certificate owner's request

If the owner of an issued certificate reports in writing that his/her rights or benefits have been or may be infringed, JCSI shall verify that he/she is the rightful owner or a trusted agent of the owner, and then disclose the following information to him/her via the RAO:

- Certificate application and attached documents
- Materials and records used to authenticate the subscriber
- Certificate contents

Except in the cases stated in Sections 2.8.4 and 2.8.5, JCSI shall not accept requests from relying parties for disclosing subscriber information. JCSI will disclose to relying parties only the revocation information about issued certificates in CRLs unless the certificates expire.

2.8.7 Any other circumstances under which confidential information may be disclosed

Upon entrusting some part of its business to an agent, JCSI may disclose confidential information to the entrusted agent. In such cases, JCSI shall include confidentiality obligations in the entrustment contract in order to deter divulgement.

2.9 Intellectual Property Rights

JCSI owns the copyright to this document (CPS), as well as the software and documents that it lends

to subscribers.

2.10 Personal Information Protection

JCSI shall handle personal information on the basis of the personal information protection policy published on JCSI's Web site.

3. IDENTIFICATION AND AUTHENTICATION

Section 4.1 describes the procedural steps from application for the issuance of a certificate (with a Web server certificate application or order sheet) through its issuance in this service. In this sequence of steps, JCSI (i.e., the RAO) verifies and authenticates the identity of Web site, S/MIME mail address owner, or signer. JCSI defines the verification and authentication of Web site identity as follows:

(1) Web server certificate, TSA server certificate

・A check to confirm that the certificate application manager is qualified to manage the relevant Web site

・A check to confirm that the certificate applicant (customer) is authenticated by the certificate application manager

・A check to verify that the items to be reflected in the certificate (registration information on the certificate application) being applied for represent an authentic Web site.

・As to CN=, DNS lookup for existence check, issuing Whois command (and the "Domain name consent agreement" issued by domain owner to the certificate application manager if not the same) for domain name ownership or control check.

Note: For TSA server certificate, CN= value is not verified as domain name.

・As to O=, L=, and ST=, Whois command info or "Domain name consent agreement" for the accuracy of organization name and address. If some info lacks, we request the certified copy of the register (database entry of the system of commercial and corporate registration by Japanese government), as described in Section 3.1.8

・A check to verify the correspondence between registration information on the certificate application described in the application form and information in the certificate signing request (CSR) and so on

(2) S/MIME certificate, client certificate

・A check to confirm the exisistence of the subscriber and the subscriber’s intension of application by the signature of the order sheet

・A check to confirm the exisistence of the organization to which the subscriber belongs by Whois command response using the e-mail address domain part (S/MIME certificate only), published enterprise database, or the Web site pages of that organization

・A check to verify that the declared items to be reflected in the certificate (registration information on the certificate application) represent the rality of the subscriber

・As to O=, L=, and ST=, confirm their accuracy using Whois command info or "Domain name consent agreement" information. The "Agreement for certificate issuing application " must be included in the order, in case of proxy ordering.

・As to e-mail address set into the certificate, confirm its accuracy by sending confirmation mail

to that address, guiding how to reply in that mail contents, and checking the proper reply mail, in case of S/MIME certificate.

•

Note: S/MIME certificates and client certificates are issued to those who belong to some organization. The domain part of E-mail address must be owned or controlled by that organization in case of S/MIME certificate. JCSI does not issue S/MIME certificates to the e-mail address issued by network service providers.

The method of identification and authentication will conform to JCSI's internal policies.

Note 1: An application form for these certificates can be downloaded from JCSI's Web site.

3.1 Initial Registration (Initial Application)

3.1.1 Types of names

The types of names are defined as registration information on the certificate application in the certificates application form.

3.1.2 Necessity of meaningful names

Names must correctly represent the authenticity of the relevant Web site, e-mail account owner, or signer. Therefore, the subscriber is obligated to reflect the authenticity of the Web site, e-mail account owner, or signer in the application form when applying for the certificate.

3.1.3 Rules for interpreting various name forms

The rules set by the subscriber shall apply.

3.1.4 Uniqueness of names

Every item constituting the distinguished name other than OU in the Web server, TSA server, S/MIME, or client certificate must accurately represent the authenticity of the subscriber. Web server, e-mail account, or signer name recognized by a fully distinguished name must be recognized uniquely.

Note: For example, if the subscriber intends to obtain multiple server certificates for the same server name (CommonName), the subscriber must vary the organizational unit name (OrganizationalUnitName) for every server certificate.

3.1.5 Procedure for resolving name claim disputes

A name claim dispute refers to any kind of dispute (e.g., infringement on a right, libel, business obstruction, unfair competition, unlawful use) related to the distinguished name described in the server, or S/MIME certificate.

Name claim disputes in the subscriber's domain (to which a server implemented a server certificate belongs) shall be resolved in principle within the domain. Name claim disputes across multiple domains or those involving a relying party shall be resolved in principle by the parties concerned (i.e., subscriber and relying party). JCSI shall not be involved in any such disputes.

3.1.6 Recognition, authentication, and role of trademarks

The distinguished name of a server, or e-mail address in the certificate must guarantee that it does not infringe on any trademark or any other intellectual property rights of a third party. The responsibility for this guarantee shall be placed on the subscriber who applies for setting values in the certificate. JCSI shall be exempt from the responsibility for any damage resulting from such infringement or obstruction.

3.1.7 Method to prove possession of private key

The certificate signing request (CSR) for Web server or TSA server certificate is based on the premise that it has been signed with a private key corresponding to a public key (and the request must be made with PKCS#10, in principle). In case of S/MIME or client certificate, RA generates subscriber’s key pair and sends it to the subscriber.

3.1.8 Authentication of organization identity

To check the entity of the organization to which the subscriber belongs, JCSI (i.e., the RAO) may require the subscriber to present a certificate authenticating the organization (such as a certificate of its corporate registration information).

3.1.9 Authentication of individual identity

For the identification described in the introduction of Chapter 3, JCSI (i.e., the RAO) may require the subscriber to present a certificate authenticating the subscriber's organization as described in Section 3.1.8, as well as a certificate attesting that the certificate application manager belongs to the organization (such as the manager’s employee card). Another indispensable item in application is the person responsible for actual work in steps from generating/registering keys to installing Web server / TSA server certificates on server machines, and from accepting keys and S/MIME / client certificates to installing them on the PC. JCSI authenticates the identity of individual persons similar to how it identifies the certificate application manager.

3.2 Routine Rekey with Certificate Updates

Same as provisions for initial registration in Section 3.1.

3.3 Rekey after Revocation

Same as provisions for initial registration in Section 3.1.

3.4 Identification upon Revocation Request

JCSI (i.e., the RAO) only accepts revocation requests for Web server / TSA server certificates from the certificate application manager, and for S/MIME / client certificates from theperson who placed the order. To verify the identity of the revocation applicant, JCSI may require the applicant to present the documents specified in Sections 3.1.8 and 3.1.9.

3.5 Handling of Certification Application Data

Certification application data may include information not to be set in the certificate. The certification application data not to be reflected in certificates shall be handled as confidential information as prescribed in Section 2.8.

4. OPERATIONAL REQUIREMENTS

4.1 Certificate Application, Issuance, and Acceptance

In this service, an application for the issuance of a Web server / TSA server certificate follows the procedure below.

(1) The subscriber fills out the application form (to be downloaded from JCSI's Web site), and then mails it together with necessary documents to JCSI.

(2) JCSI examines the application and attached documents according to this standard, and upon finding no inconformity, regards that a contract is concluded. If any inconformity is found, JCSI will request the subscriber to resubmit the documents concerned.

(3) The subscriber generates keys, prepares a certification signing request (CSR), and then makes an application to JCSI (i.e., the RAO).

(4) JCSI (i.e., the RAO) manually checks the certificate signing request (CSR).

(5) JCSI (i.e., the RAO) requests the IA to issue a certificate, and then the IA issues the certificate, which is received by the RAO.

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

In this service, an application for the issuance of a S/MIME / client certificate follows the procedure below.

(1) The subscriber fills out the order form (to be downloaded from JCSI's Web site), and then mails it together with certificate value data and necessary documents to JCSI.

(2) JCSI examines the order form and attached documents according to this standard, and upon finding no inconformity, regards that a contract is concluded. If any inconformity is found, JCSI will request the subscriber to resubmit the documents concerned.

(3) JCSI (i.e., the RAO) manually generates subscriber’s keys in the RA server, and prepares a certification signing request (CSR) from certificate items value data.

(4) JCSI (i.e., the RAO) manually checks the certificate signing request (CSR).

(5) JCSI (i.e., the RAO) requests the IA to issue a certificate, and then the IA issues the certificate.

(6) JCSI (i.e., the RAO) receives the key and certificate (PKCS#12 format file) and sends it to the subscriber.

(7) JCSI (i.e., the RAO) receives the PIN of the PKCS#12 format file and sends it to the subscriber. After subscriber receives them, JCSI (i.e., the RAO) deletes PKCS#12 format file and PIN promptly.

In this service, the issuance of a certificate from the RCA to an SCA follows the procedure below.

(1) The SCA is checked to determine whether it meets the requirements of JCSI, and then the issuance of a certificate is decided.

(2) The CSR is obtained from the SCA in a secure manner, predetermined DualControl members

restore the RCA signature key in the HSM, the RCA is activated, and then the RCA issues the certificate in response to the CSR from the SCA.

(3) The RCA sends the issued certificate to the SCA in a secure manner, and waits until the SCA accepts the certificate.

(4) Upon receiving the notice of acceptance completion, the RCA is deactivated and the RCA signature key in the HSM is then deleted.

(5) A check is made to confirm that the certificate was issued to the SCA in conformity with the decision made.

4.2 Certificate Suspension and Revocation

In this service, a certificate shall be revoked if the distinguished name or other setting values in the certificate are changed, the certificate is replaced with another certificate, the subscriber cancels use of the certificate, or the subscriber's private key or SCA certificate signature key is compromised.
In this service, the certificate is not suspended.
The revocation procedure is usually initiated upon request from the subscriber to the RAO. The RAO examines whether to revoke the certificate, and then the IAaccepts the revocation request.
JCSI periodically discloses the Certification Revocation List (CRL).
In this service, the application for revocation is accepted when the applicant either mails or brings the Web server /TSA server / S/MIME / client certificate revocation request to the RAO.
Identification of the applicant follows the procedure below.

(1) Identification of the revocation applicant (when the revocation request is mailed or brought with the applicant)

When the revocation applicant can be identified by the method below, JCSI determines that the result of identification check is true. If the applicant cannot be identified, JCSI determines that the result of identification check is false.

(a) Information in the server certificate application form or S/MIME / client certificate order form stored at JCSI

- Veriy whether the information (i.e., name of application manager, organization name, department name, job title, seal impression) provided by the subscriber corresponds to applicant information in the certificate revocation request.

4.3 Security Audit Procedure

JCSI shall operate a system designed to record and audit center operation logs as a means of keeping the environment safe. The IA, RA, and repositories shall leave audit trails and periodically audit them from a standpoint of security. Audit trails include the following:

Frequency	Audit item	Target audit trail	Product
Weekly	Check on normal operation of entry/exit control system (for rooms)	Entry/exit history stored in entry/exit control system Monitoring record (HDDR)	Monthly inspection report on entry/exit control system HDDR check sheet
Monthly	Cross-check of entry/exit control system records and manual records	Monthly inspection report on entry/exit control system, Statement of direction for operation, storage/retrieval control form, Irregular work/troubleshooting record	Audit practice record
	Management of entry/exit control (for personnel)	Vein sensor data registration/ updating/deletion application, Testimony	Same as the above
	Audit log	Firewall log, IA/RA audit log, Server system logs	Same as the above

- Operation and running logs of the IA and RA servers. These include all logs of such events as the control of the CA's private key, certificate issuance for authorizing the servers and RAOs, server startups and shutdowns, and the registration, issuance and revocation of individual subscriber's certificates.
- Monitoring logs for firewalls, networks in the room where certificate issuing systems are installed and servers. These logs include the records of all packets and transactions saved as the audit log.
- Operation and running logs of repositories. These logs are records of all accesses from any parties or the authenticated parties under access control, including modification records of repository information.

- Running records (including alarm emissions) of passive sensors, monitoring cameras, monitoring video units and entry/exit gate devices that cover rooms where certificate issuing systems are installed. Alarm emissions are treated as abnormality records.
- Forms used in this service (retention priod/storage place)
  (1) Monthly inspection report on entry/exit control system (1 year/an area in JCSI)
  (2) HDDR check sheet (1 year/an area in JCSI)
  (3) Fireproof cabinet storage/retrieval control form (1 year/an area in JCSI)
  (4) Irregular work/troubleshooting record (1 year/an area in JCSI)
  (5) Periodic audit record (1 year/an area in JCSI)
  (6) Application form of veint sensor data registration/updating/deletion (3 years after expiration/an area in JCSI)
  (7) Request/approval for lending the physical key to space under the roof (1 year/an area in JCSI)
  (8) Key usage report (1 year/an area in JCSI)
  (9) Statement of direction for operation (copy) (1 year/an area in JCSI)

These audit trails are periodically audited from a standpoint of security. These records regarded as normal are replaced by audit records and thus deleted. Records of erroneously or deliberately produced abnormalities are individually verified. Corrective action will be taken as considered necessary. Security audit records including records considered abnormality records and the records of corrective action taken are stored whith the method prescribed in the next section until a compliance audit (Section 2.7) is conducted. The security audit records stored are verified again at the time of the compliance audit. The security audit is conducted at least once a month.

4.4 Archiving

In the SecureSign AD service, the documents and digital data listed below are archived. For storage, JCSI takes measures to prevent leakage and tampering. The documents and data are therefore stored in a special fireproof media repository divided by partitions and walls, and equipped with functions to eliminate electromagnetic effects on storage media.
As per the provisions in Sections 2.8.4 to 2.8.7, JCSI shall only provide the specified parties with a specified range of archived and stored information.
JCSI will securely delete all documents and digital data after the prescribed retention period expires. The documents will be shredded and disposed of, while digital data will be deleted by destroying the storage media or otherwise overwriting with null code. The following lists the data to be archived with retention period indicated in parentheses.

- Originals of the entrustment agreements for entrusting some part of this service to other parties and documents related to those agreements. (To be stored until the entrustment agreements are

terminated)

- Originals of the management information and history data on personnel, organizations, systems, administration, and the chain of command system of this service. (The latest version to be stored permanently and the old version preceding a revision to be stored until the next compliance audit [Section 2.7])
- Originals of the records of compliance audits (Section 2.7) and audit reports. (To be stored for 10 years)
- Log data about CA private key management (key generation, storage, activation/deactivation, backup/restoration, and discarding) and the issuance of RCA/SCA certificates associated with CA private key. (Log data to be stored until the end of a security audit and the security audit record to be stored until the next compliance audit [Section 2.7])
- Records of security audits (Section 4.3). (To be stored until the next compliance audit [Section 2.7])
- Records of authorizations and de-authorizations prescribed in provisions of procedural security control (Chapter 5). (To be stored until the next compliance audit [Section 2.7])
- Records of facility maintenance, system maintenance, updates and disorders. (To be stored until the next compliance audit [Section 2.7])
- All certificates and CRLs issued including the SecureSign AD service RCA/SCA certificates and CRLs and all related public key certificates. (To be stored for 10 years after expiration)
- This document (SecureSign AD Service Standard), detailed procedures, related regulations for personal information protection, and their revision histories. (The latest version to be stored permanently and the old version preceding a revision to be stored for 10 years after revision)
- Originals of certification application forms, order forms and attached documents submitted from subscribers (To be stored till certificate expiration)
- Complete sets of application forms for certificate revocation requests submitted from subscribers. Those documents are used by JCSI to decide upon revocation. (To be stored till certificate expiration)
- Guidbook and subscriber agreements disclosed to subscribers, relying party agreements disclosed to relying parties, and their revision histories. (The latest version to be stored permanently and the old version preceding a revision to be stored for 10 years after revision)

4.5 Key Changeover

Before the remaining validity period of the CA public key for the SecureSign AD service becomes shorter than the maximum validity period of the subscriber's certificate, JCSI shall suspend the issuance of new subscriber's certificates with the related CA public key, and generate a new pair of signature keys by the method prescribed in Chapter 6. New public key of RCA shall be self-signed,

and that of SCA shall be signed by RCA of this service, and disclosed in the form of the certificates on JCSI's Web site.
Note : that JCSI does not issue a certificate for a new key with an old key. Nor does it issue a certificate for an old key with a new key.

4.6 Recovery from Compromise

If the CA private key for the SecureSign AD service is compromised,(Note 1) JCSI shall revoke that certificate signature key to prevent new subscriber's certificates signed with an illegal reproduction of that key from being circulated and trusted. Specifically, JCSI shall revoke all valid certificates signed with the compromised key as soon as possible, and disclose their CRLs signed with the compromised key. The certificate signature key shall then be deleted, and an updated CRL being issued from the RCA of this service and disclosed. To continue this service, JCSI also generates a new certificate signature key as soon as possible. Subscribers can apply for the issuance (or updating) of their certificates.
JCSI shall otherwise define a procedure for recovery against compromise or damage, and implement education and training for the recovery procedure according to a settled schedule.
Note 1: The condition of compromise: illegal intrusion, illegal operation, password leakage, loss of private key fragment.

4.7 CA Termination

The SecureSign AD service shall be terminated due to the provisions of Sections 2.2 to 2.4 or a change in the business policy of JCSI. CA termination will be publicized on JCSI's Web site (or another site on behalf of JCSI's Web site) from two months prior until six months after termination, except for cases under unavoidable circumstances. When terminating the CA, JCSI fully initializes or physically destroys the CA private key and backup medium to discontinue their use, but does not revoke CA certificates related to the CA private key. JCSI suspends the issuance of new certificates (as well as the renewal of certificates). All already issued certificates that are still valid at the time of CA termination are collectively revoked when the CA is terminated. JCSI, however, does not make the final update and disclose the CRL that reflects collective revocation. JCSI disables access to the URLs in the certificates(CRL distribution point) in order to prevent relying parties from verifying the certificates. At CA termination, JCSI shall delete all documents and digital data regardless of the provisions in Section 4.4.

5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

This service conforms to Chapter 5 and the additional provisions below.

5.1 Physical Security Controls

JCSI defines security requirements for facilities where the certificate issuing system (IA and RA) is installed and operated as follows:

(1) JCSI shall divide the internal space of the building in which the certificate issuing system is installed into multiple rooms at different security levels, and define security regulations concerning movement in and between those levels. This requirement is actually implemented by the entrusted center.

(2) JCSI shall divide the networks as system components and the other networks to be connected to the system into segments as shown below, and individually control communications via respective networks with firewalls.

Segment name	Equipment to be connected
Internet	Router, firewall
DMZ	Web gateway/repository
Secure	IA/RA server, monitoring server, operation management server, dedicated operation terminal

(3) JCSI shall document the procedures for authorization of access at each security level. This requirement is actually implemented by the entrusted center.

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

(5) The certificate issuing system (i.e., server, hardware security module(HSM), firewall, routers) shall be installed in a room exclusively used by JCSI and at the highest security level. The records must be audited monthly by the Project manager defined in Section 5.2 Table 5-1.

(6) Security guards shall control the entry and exit of persons into and from the facility. Only those persons registered in advance are allowed to enter the facility. Anyone entering a security-controlled room must be accompanied by an authorized person for the relevant security level. This entry and exit with an authorized person must be allowed on an individual basis, and reported at the end of each entry or exit. Access to the room where an operation terminal is installed must be limited to designated personnel only. The doors of the room must lock automatically when closed, and every entry into or exit from the room is recorded in a ledger. The records must be audited monthly by the Project manager defined in Section 5.2 Table 5-1.

(7) Rooms at the highest security level shall be always monitored by video recording systems and

passive sensors. The detection of illegal access must trigger an alarm. The cause of alarm must be promptly identified, and proper action shall be taken.

(8) Persons entering a room at the highest security level shall be identified by a biometric authentication function, and after identification the electronically locked door shall be unlocked. The entry and exit of persons into and from the room shall be authorized concurrently by two persons.

(9) The rooms at the highest security level shall be protected by an illegal-access preventive structure.

(10) Monitoring information and personal entry/exit records shall be audited from a standpoint of security every month, and stored as audit trails for three years.

(11) Devices important for ensuring confidentiality and security shall be supplied with power by a UPS or private electric generator in case of power failure.

(12) Only authorized persons shall be allowed to access the media repository or system monitoring room.

5.2 Procedural Security Controls

JCSI classifies personnel as shown in Table 5-1, 5-2. Personnel at the operation center and JCSI headquarter operate the IA, RA, the RAO terminal installed at JCSI, and JCSI repositories.

Table 5-1 Center Authority of personnel

<table>
<tr><th>Personnel classification</th><th>Designation</th><th>Authorization for access</th><th>Authorization for operation</th><th>Access authority check</th></tr>
<tr><td>Project Manager (daily operation manager)</td><td>The person responsible to the operation entrusted to the center</td><td colspan="2">—</td><td>—</td></tr>
<tr><td>Project Controller</td><td>Designated by the Project manager</td><td rowspan="4">Authorized by the Project manager</td><td rowspan="4">Authorized by the Project manager</td><td>Biometric authentication system</td></tr>
<tr><td>Project member</td><td>Designated by the Project manager</td><td>Biometric authentication system</td></tr>
<tr><td>CSE (in charge of system operation)</td><td>Designated by the CSE team manager on behalf of the Project manager</td><td>Biometric authentication system</td></tr>
<tr><td>Maintenance personnel</td><td>-</td><td>Access by a single person is not allowed. Access is allowed when accompanied by a person authorized to access the security system.</td></tr>
</table>

Table 5-2 Headquater Authority of personnel

Role	Designator	Authorization for access	Authorization for operation	Remarks
Business Manager	Board of Directors	No		Access is allowed when accompanied by a person authorized to access the security system.
Operation Manager	Business Manager	No		Access is allowed when accompanied by a person authorized to access the security system.
Security Manager		Yes	No	
System Administrator	Operation Manager	Yes		
RA Operator	Business Manager	Yes		Granted the registration operation

To ensure security of the site where the certificate issuing system is installed, center personnel must be authorized to access the site or limited to accessing the system room. The Project manager of entrusted operation center must be eligible to authorize center personnel to access the system room on the basis of consent granted by the Project controller. The Project controller must register or delete center personnel information in the biometric authentication system according to documents stating the authorization for access.

To ensure the security of certificate issuing system operation, only a limited number of personnel must be authorized to operate specific devices and equipment. The Project manager of entrusted operation center must be eligible to authorize personnel to operate the certificate issuing system. The Project manager or designated project member must set (change or delete) the accounts of operatin, and issue or revoke certificates for operation, according to documents stating the authorization for access. In particular, those accounts for equipments and/or devices accompanying privileges must strictly be controled.

To ensure the security of remote operation of the certificate issuing system from JCSI headquarter,

the personnel there must be authorized to perform daily operations. The Project manager must be eligible to authorize the personnel to remotely operate the certificate issuing system.
Records of the authorization for access, operation and remote operation must be managed by the Project manager, and stored in a key-locked cabinet for at least three years.
Details of authorization and the supervising system must be specified in the detailed procedures at the operation center and JCSI headquarters. In the detailed procedures, the Project manager of the center may be referred to simply as the business manager of that center. When entrusting some part of operations to an agent, JCSI shall require the agent to observe the provisions of this Chapter, prepare detailed procedures, and perform operations according to those detailed procedures. The center and JCSI headquarters must supervise the operations of personnel and entrustee in order to maintain proper security according to this document.

5.3 Personnel Security Controls

JCSI controls the security of personnel involved in operations of the certificate issuing system in conformity with the following requirements:

(1) Personnel who directly engage in center system operation shall be checked using one of the methods below to ensure that they have not committed any crimes in the past two years resulting in imprisonment.
   ・Individual personnel must sign an annual written pledge stating that they have committed no such crimes in the past two years.
   ・The company to which the personnel belong makes it clear in writing that the company sets this requirement as a condition for employment in its work regulations.

(2) Center personnel shall be given security education on regulations and procedures necessary for operating the certificate issuing system, and must sign a written pledge to follow the regulations and procedures on starting his/her mission. In the course of education, they should particularly understand the seriousness of compromise and loss of keys. Center personnel must be obligated to receive education periodically to gain a thorough understanding. Such education must be implemented almost every year, and education reports are informed to the Project manager.

(3) The backup token of the CA private keys and its physical keys are splitted to the center personnel and JCSI personnel. Holders of those components shall agree to sign a storage control ledger to fulfill their control responsibility before storing those components.

Center personnel must include an appropriate number of members(Note 2) considered to possess sufficient knowledge and experience(Note 1) in related technical fields.

Note 1: The members must have at least two years' experience not only in authentication systems development, operation or consultation, but also in the development of this document or a similar standard.

Note 2: The number of members must be specified at the entrusted operation center.

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 a cryptographic device using a random-number generation or pseudo-random-number generation process prescribed in ISO 9564-1: 1991 and ISO 11568-5. Key pair generation shall be performed by three or more DualControl members designated by JCSI.

(2) Presentation of public key to certificate issuer

A generated public key shall be made in the form of a self-signed certificate in the RCA without being presented to any external entity.

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

・JCSI's RCA public keys are distributed as items preinstalled in de-facto standard applications (i.e., products or application programs).

・JCSI's RCA public keys are downloaded to end entities from JCSI repositories for distribution. End entities are obliged to verify the validity of downloaded RCA public keys of JCSI based on hash values (released by JCSI).

・JCSI's RCA public keys are delivered along with certificates issued to subscribers.

(4) Key size

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

(5) Use of hardware key

Key pairs shall be generated by a cryptographic device (hardware).

(6) Key pair installation

Key pairs need not be installed because the keys are used on the device that generated them.

(7) Hash function to be used

SHA-1

6.1.2 SCA

(1) Key pair generation

A key pair shall be generated within a cryptographic device in the certification facility room by using a random-numuber or pseudo-random-number generation process. Three DualControl members shall perform key pair generation. The generated certificate signature key shall be used only within the cryptographic device.

(2) Delivery of public key to certificate issuer

A generated public key shall be hand-delivered in the form of CSR to the RCA, and a certificate issued from the RCA shall be received.

(3) Size of public and private keys

The key size shall be 2,048 bits conforming to the RSA public-key cryptographic scheme.

(4) Delivery of SCA public keys to subscribers and relying parties

Self-signed SCA public keys shall be delivered in the form of an SCA certificate issued from the RCA using either of the following methods:

・SCA certificates are downloaded to subscribers and relying parties from JCSI repositories for delivery. Subscribers and relying parties are obliged to verify the validity of downloaded SCA certificates based on fingerprints disclosed in the repositories.

・SCA certificates are delivered along with the subscriber's key pairs delivered to subscribers.

(5) Use of hardware key

Key pairs shall be generated by a cryptographic device (hardware).

(6) Key usage

By using the standard Extension fields of the X.509 version 3 certificate, the usage of keys shall be limited to electronic signature on certificates (subscriber certificates, operation certificates, mutual authentication certificates and link certificates) and CRLs.

(7) Key pair installation

Key pairs need not be installed because the keys are used on the device that generated them.

(8) Hash function to be used

SHA-1

6.1.3 Subscriber (key pair generation by subscriber)

(1) Key pair generation

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

(2) Presentation of public key to certificate issuer

A generated public key shall be submitted as an online request for signing certificates to the IA via the RA to request the CA to issue certificates.

(3) Key size

The key size shall be 2,048 bits conforming to the RSA public-key cryptographic scheme, depending on the software used by the subscriber.

(4) Use of hardware key

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

(5) Key usage

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

(6) Key pair installation

Key pairs need not be installed when the keys are used on the device that generated them.

(7) Hash function to be used

SHA-1

6.1.4 Subscriber (key pair generation by JCSI)

(1) Key pair generation

A pair of private and public keys shall be generated using a pseudo-random-number generation process. Generation is performed in the RA server under two DualControl members (RAO's) administration.

(2) Presentation of public key to certificate issuer

A generated public key shall be submitted as an online request for signing certificates to the IA to request the CA to issue certificates.

(3) Key size

The key size is 2,048 bits conforming to the RSA public-key cryptographic scheme.

(4) Use of hardware key

The cryptographic device (hardware) is not used for subscriber key pair generation.

(5) Key usage

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

(6) Key pair installation

Key pairs and certificate are sent to the subscriber in the form of PKCS#12 file and its PIN separately. Subscriber installes the key pair and certificate to the target PKI application when he/she recived. Subscriber must keep the condition below.

・Key pair must not exist out of the RA server when it is not encrypted.

・Key pair resides in the RA server must be destroyed promptly after receipt by subscriber.

(7) Hash function to be used

SHA-1

6.2 Private Key Protection

6.2.1 Standards for cryptographic device

CA private keys shall be controlled with a cryptographic device authorized to conform to FIPS PUB 140-2 Level 3. The cryptographic device may be used in partitions. However, the partition allocated to this service must not be accessible by any other certification service.
The cryptographic modules used by subscribers should preferably comply with FIPS PUB 140-2.

6.2.2 Multi-person control of private keys

This service implements both DualControl where system operations using a private key are performed upon the consent of multiple persons and SecretShare (SecretSplit) where a private key is split and shared by multiple persons. Table 6-1 lists the numbers of persons, splits, and shares to be applied to these controls.

Table 6-1 DualControl and SecretShare

CA	Persons necessary for DualControl	SecretShare splits	Shares necessary for private key restoration
RCA	2-3	3	3
SCA	2-3	3	3

6.2.3 Private key escrow

No private key escrow service is provided.

6.2.4 Private key backup

A private key shall be stored in (backup) tokens by presenting and referencing multiple physical keys to implement secret shares.
The issuer shall designate the holders of tokens and multiple physical keys who will handle the tokens and multiple physical keys (this activity shall be recorded as work item), enclose the tokens and multiple physical keys in a tamper-evident envelope, and then store it in a fireproof safe at their own responsibility.
Private key backup shall be performed in the certification facility room based on the consent of DualControl members of JCSI headquarters personnel (i.e., the system administrator) and center personnel (i.e., the system administrator).

6.2.5 Private key archiving

Private keys shall not be archived.

6.2.6 Private key entry into cryptographic module (backup recovery)

Private keys shall be entered in the certification facility room based on the consent of DualControl members of JCSI headquarters personnel (i.e., the system administrator) and center personnel (i.e., the system administrator). Private keys are restored from tokens by presenting and referencing multiple physical keys, and entered into the cryptographic device. The tokens and physical keys shall be operated by designated holders.

6.2.7 Method of activating private keys

Private keys shall be activated in the certification facility room based on the consent of DualControl members of center personnel (system administrators). Once activated, private keys remain activated for the periods shown in Table 6-2.

Table 6-2 Private key activation period

CA	Activation period
RCA	While a signature is made only
SCA	At all times (except at hardware maintenance)

6.2.8 Method of deactivating private keys

Private keys shall be deactivated in the certification facility room based on the consent of DualControl members of center personnel (system administrators). Note that when a private key is deactivated at the RCA, the private key in the cryptographic device is deleted (fully erased) by presenting and referencing multiple physical keys, but the physical keys and tokens are retained.

6.2.9 Method of destroying private keys

Private keys shall be promptly destroyed upon falling into disuse due to the updating of RCA or SCA certificates, or when abandoned (at termination of this service). Destroying private keys in the cryptographic device shall refer to their deletion involving the full initialization of the partition used for private keys. This initialization shall be performed based on the consent of DualControl members of JCSI headquarters personnel (i.e., the system administrator) and center personnel (i.e., the system administrator). In case a private key is abandoned (at termination of this service), the tokens and multiple physical keys for the private key shall be physically destroyed. If tokens and multiple physical keys must be discarded for other reasons, the tokens shall be initialized. This operation shall be performed in the certification facility room by holders of the tokens and multiple physical keys and witnessed by center personnel (i.e., the system administrator). This activity shall be recorded as work item.

Subscribers shall promptly destroy (delete) their own private keys upon the expiry of corresponding key pairs.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archiving

The archiving of CA public keys shall involve measures against tampering. Table 6-3 shows the archiving periods.

Table 6-3 Period of CA public key archiving

Authority	Archive type	Archiving period
RCA	Own certificate	10 years from certificate expiry date
	Issued certificate	10 years from certificate expiry date
SCA	Own certificate	10 years from certificate expiry date
	Issued certificate	10 years from certificate expiry date

6.3.2 Usage periods for public and private keys

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

Table 6-4 Expiry periods of keys

Authority	Key type	Public key expiry period	Private key expiry period
RCA	Certificate and CRL signature keys	20 years	10 years
SCA	Certificate and CRL signature keys	Within 20 years	Within 10 years
Subscriber	Web server certificate	1 month Within 1 year and 1 month Within 3 year and 1 month Within 5 year and 1 month	-
Subscriber	TSA server certificate	Within 11 year and 1 month	
Subscriber	S/MIME certificate	Within 3 year and 1 month	-
Subscriber	Client certificate	Within 3 year and 1 month	-

6.4 Activation Data

The data to be used to activate and deactivate hardware cryptographic devices shall be handled as

activation data, and passwords shall be used as the activation data.

6.4.1 Activation data generation and installation

Passwords shall be handled as activation data. A password shall be at least six characters in length.

6.4.2 Activation data protection

Passwords shall be stored in hardware cryptographic devices or tokens, and cannot be taken out for external use.

6.5 Computer Security Controls

6.5.1 Technical requirements for specific computer security

The IA and RA shall use computer systems with proven high reliability and security.

6.5.2 Computer security evaluation

The security of computer systems in the certification facilities shall occasionally be evaluated, with corrective action appropriately taken based on the evaluation results.

6.6 Technical Life Cycle Controls

6.6.1 System development control

The IA and RA servers shall use systems that can be proven to have been developed and tested by a trusted organization.

6.6.2 Security management control

Vaccine software shall be periodically run on the IA and RA servers to prevent, detect, and recover from virus infection.

6.7 Network Security Controls

The communication protocol (https) used by JCSI headquarters for daily operations shall be configured to enable communications with the access source limited to the relevant host (or a proxy server).

The RCA shall not be connected to the Internet. SCAs shall be connected to the Internet via firewalls. The firewalls shall log illegal accesses as audit trails.

6.8 Cryptographic Module Engineering Controls

The hardware cryptographic modules used in IAs shall comply with FIPS PUB 140-2 Level 3.

7. CERTIFICATE AND CRL PROFILES FOR THIS SERVICE

This chapter describes the profiles of the RCA certificates, SCA certificates, Web server certificates, and CRLs issued in this service.

7.1 Certificate Profiles

7.1.1 Version number

X.509 V3 certificates are issued in this service.

7.1.2 Certificate standard extensions

In this service, the extensions to use vary depending on the type of certificate to be issued. For details, refer to the individual certificate profiles in Section 7.1.9.

7.1.3 Algorithm OIDs

The algorithm names and OIDs used in the certificates issued in this service are as follows:
Subscriber's public key (subjectPublicKeyInfo): RSA public key (OID = 1 2 840 113549 1 1 1)
Signature (signature): sha1WithRSAEncryption (OID = 1 2 840 113549 1 1 5)

7.1.4 Name forms

Refer to Section 7.1.9 for the issuer and subject names and detailed name forms that are applied to the certificates and CRLs issued in this service.

7.1.5 Name constraints

No name constraint extensions are configured for certificates issued in this service.

7.1.6 Certificate policy OIDs

For the certificate policy OIDs used in this service, refer to the individual certificate profiles in Section 7.1.9.

7.1.7 Use of policy constraint extensions

No policy constraint extensions are configured for certificates issued in this service.

7.1.8 Policy modifiers

In this service, the usage of policy modifiers varies depending on the type of certificate. For details, refer to the next section.

7.1.9 Certificate profiles

This section describes details of the profiles of certificates issued in this service. Note that the set values shown in the Setter and Criticality columns of subsequent tables have the meanings explained below. These set values also have the same meanings in the tables for CRL profiles inserted later. Certificate contents are encoded with PrintableString syntax unless otherwise specified.

Setter IA: The IA sets a value.
RA: The RA sets a value.
EE: The subscriber sets a value when preparing the CSR
×: No value is set.

Criticality T: The value is "true."
F: The value is "false."
－: No value can be set or is set.

(1) RCA certificate profile

Name			Setter	Criti-cality	Set value
Certificate Basic Fields					
	version		IA	－	V3
	serialNumber		IA	－	128-bit or shorter positive integer
	signature		IA	－	sha1WithRSAEncryption (OID = 1 2 840 113549 1 1 5)
	issuer		IA	－	C = JP, O = Japan Certification Services, Inc., CN = SecureSign Root CA11 * Encoded as PrintableString
	validity				
		notBefore	IA	－	20 years
		notAfter	IA	－	* Set by UTCTime.
	subject		IA	－	C = JP, O = Japan Certification Services, Inc., CN = SecureSign Root CA11 * Encoded as PrintableString
	subjectPublicKeyInfo				
		algorithmIdentifier	IA	－	rsaEncryption (OID = 1 2 840 113549 1 1 1)
		public key	IA	－	2048-bit value

Certificate Standard Extensions					
	subjectKeyIdentifier		IA	F	SHA-1 value (hash value) for public key
	keyUsage		IA	T	Set keyCertSign and cRLSign to ON; set other items to OFF.
	basicConstraints		IA	T	
		cA	IA		TRUE
		pathLenConstraint			NULL

(2) SCA certificate profile

				Setter	Criti-cality	Set value
Certificate Basic Fields						
	version			IA	—	V3
	serialNumber			IA	—	128-bit or shorter positive integer
	signature			IA	—	sha1WithRSAEncryption (OID = 1 2 840 113549 1 1 5)
	issuer			IA	—	C = JP, O = Japan Certification Services, Inc., CN = SecureSign Root CA11 * Encoded as PrintableString
	validity					
		notBefore		IA	—	20 years
		notAfter		IA	—	* Set by UTCTime.
	subject			IA	—	C = JP, O = Japan Certification Services, Inc., CN = SecureSign Public CA11 * Encoded as PrintableString
	subjectPublicKeyInfo					
		algorithmIdentifier		IA	—	rsaEncryption (OID = 1 2 840 113549 1 1 1)
		public key		IA	—	2048-bit value
Certificate Standard Extensions						
	subjectKeyIdentifier			IA	F	SHA-1 value (hash value) for public key
	keyUsage			IA	T	Set keyCertSign and cRLSign to ON; set other items to OFF.
	certificatePolicies			IA	F	
		policyIdentifier				
			certPolicyId			1 2 392 200075 4 2

		policyQualifiers				
			policyQualifierId			1 3 6 1 5 5 7 2 1 (id-qt-cps)
			qualifier			https://cp.jcsinc.co.jp/SecureSign/AD/RPA.html (URL for the agreement)
	basicConstraints			IA	T	
		cA		IA		TRUE
		pathLenConstraint		×		Not to be set
	cRLDistributionPoints			IA	F	Set the following as URLs for "distributionPoint.fullName.URI": http://ssignadcrl01.jcsinc.co.jp/repository/crl/rca.crl http://ssignadcrl02.jcsinc.co.jp/repository/crl/rca.crl

(3) Web server certificate profile

Name			Setter	Criti-cality	Set value
Certificate Basic Fields					
	version		IA	―	V3
	serialNumber		IA	―	128-bit or shorter positive integer
	signature		IA	―	sha1WithRSAEncryption (OID = 1 2 840 113549 1 1 5)
	issuer		IA	―	C = JP, O = Japan Certification Services, Inc., CN = SecureSign Public CA11 * Encoded as PrintableString
	validity				
		notBefore	RA	―	13 months, 37 month, or 61 month
		notAfter	RA	―	* Set by UTCTIme.

	subject		EE	—	C = JP, ST = Subscriber's address (prefecture) (optional), L = Subscriber's address (county, city, town, village, and other details) (optional), O = Subscriber's organization name (optional), OU = Subscriber's department name (up to five names) (optional), CN = Server FQDN, E = E-mail address (optional), * Only the value of C is encoded as PrintableString, while other values are encoded as PrintableString or BMPString.
	subjectPublicKeyInfo				
		algorithmIdentifier	IA	—	rsaEncryption (OID = 1 2 840 113549 1 1 1)
		public key	EE	—	A 2048-bit key to be generated by subscriber
Certificate Standard Extensions					
	authorityKeyIdentifier		IA	F	
		keyIdentifier			SHA-1 value (hash value) for public key
		authorityCertIssuer			Unused
		authCertSerialNumber			Unused
	subjectKeyIdentifier		IA	F	SHA-1 value (hash value) for public key
	keyUsage		IA	F	Set digitalSignature and keyEncipherment to ON; set other items to OFF.
	extendKeyUsage		IA	F	Set PKIX-IDKP-ServerAuth and PKIX-IDKP-ClientAuth to ON; set other items to OFF.
	certificatePolicies		IA	F	
		policyIdentifier			
			certPolicyId		1 2 392 200075 4 2
		policyQualifiers			
			policyQualifierId		1 3 6 1 5 5 7 2 1(id-qt-cps)
			qualifier		https://cp.jcsinc.co.jp/SecureSign/AD/RPA.html (URL for the agreement)
	basicConstraints		IA	F	
		cA			FALSE
		pathLenConstraint			NULL

	cRLDistributionPoints	IA	F	Set the following as URLs for "distributionPoint.fullName.URI": http://ssignadcrl01.jcsinc.co.jp/repository/crl/sca1.crl http://ssignadcrl02.jcsinc.co.jp/repository/crl/sca1.crl

(4) TSA server certificate profile

Name			Setter	Criti-cality	Set value
Certificate Basic Fields					
	version		IA	—	V3
	serialNumber		IA	—	128-bit or shorter positive integer
	signature		IA	—	sha1WithRSAEncryption (OID = 1 2 840 113549 1 1 5)
	issuer		IA	—	C = JP, O = Japan Certification Services, Inc., CN = SecureSign Public CA11 * Encoded as PrintableString
	validity				
		notBefore	RA	—	133 months * Set by UTCTIme.
		notAfter	RA	—	
	subject		EE	—	C = JP, ST = Subscriber's address (prefecture) (optional), L = Subscriber's address (county, city, town, village, and other details) (optional), O = Subscriber's organization name (optional), OU = Subscriber's department name (up to five names) (optional), CN = Server FQDN, E = E-mail address (optional), * Only the value of C is encoded as PrintableString, while other values are encoded as PrintableString or BMPString.
	subjectPublicKeyInfo				
		algorithmIdentifier	IA	—	rsaEncryption (OID = 1 2 840 113549 1 1 1)
		public key	EE	—	A 2048-bit key to be generated by subscriber
Certificate Standard Extensions					
	authorityKeyIdentifier		IA	F	

		keyIdentifier			SHA-1 value (hash value) for public key
		authorityCertIssuer			Unused
		authCertSerialNumber			Unused
	subjectKeyIdentifier		IA	F	SHA-1 value (hash value) for public key
	keyUsage		IA	F	Set digitalSignature and keyEncipherment to ON; set other items to OFF.
	extendKeyUsage		IA	F	Set PKIX-IDKP-timeStamping to ON; set other items to OFF.
	certificatePolicies		IA	F	
		policyIdentifier			
		certPolicyId			1 2 392 200075 4 2
		policyQualifiers			
		policyQualifierId			1 3 6 1 5 5 7 2 1(id-qt-cps)
		qualifier			https://cp.jcsinc.co.jp/SecureSign/AD/RPA.html (URL for the agreement)
	basicConstraints		IA	F	
		cA			FALSE
		pathLenConstraint			NULL
	cRLDistributionPoints		IA	F	Set the following as URLs for "distributionPoint.fullName.URI": http://ssignadcrl01.jcsinc.co.jp/repository/crl/sca1.crl http://ssignadcrl02.jcsinc.co.jp/repository/crl/sca1.crl

(5) S/MIME certificate profile

Name		Setter	Criti-cality	Set value
Certificate Basic Fields				
	version	IA	—	V3
	serialNumber	IA	—	128-bit or shorter positive integer
	signature	IA	—	sha1WithRSAEncryption (OID = 1 2 840 113549 1 1 5)
	Issuer	IA	—	C = JP, O = Japan Certification Services, Inc., CN = SecureSign Public CA11 * Encoded as PrintableString
	validity			

		notBefore	RA	—	37 month
		notAfter	RA	—	* Set by UTCTIme.
	subject		EE	—	C = JP, O = Subscriber's organization name, OU = Subscriber's department name (optional), CN = Subscriber's full name, E = E-mail address, * Only the value of C is encoded as PrintableString, while other values are encoded as PrintableString or BMPString.
	subjectPublicKeyInfo				
		algorithmIdentifier	IA	—	rsaEncryption (OID = 1 2 840 113549 1 1 1)
		public key	RA	—	A 2048-bit key to be generated by RA
Certificate Standard Extensions					
	authorityKeyIdentifier		IA	F	
		keyIdentifier			SHA-1 value (hash value) for public key
		authorityCertIssuer			Unused
		authCertSerialNumber			Unused
	subjectKeyIdentifier		IA	F	SHA-1 value (hash value) for public key
	keyUsage		IA	F	Set digitalSignature and keyEncipherment to ON; set other items to OFF.
	certificatePolicies		IA	F	
		policyIdentifier			
			certPolicyId		1 2 392 200075 4 2
		policyQualifiers			
			policyQualifierId		1 3 6 1 5 5 7 2 1(id-qt-cps)
			qualifier		https://cp.jcsinc.co.jp/SecureSign/AD/RPA.html (URL for the agreement)
	subjectAltName		EE	F	
		rfc822name			E-mail address
	basicConstraints		IA	F	
		cA			FALSE
		pathLenConstraint			NULL

	cRLDistributionPoints	IA	F	Set the following as URLs for "distributionPoint.fullName.URI": http://ssignadcrl01.jcsinc.co.jp/repository/crl/sca1.crl http://ssignadcrl02.jcsinc.co.jp/repository/crl/sca1.crl

(6) client certificate profile

Name			Setter	Criti-cality	Set value
Certificate Basic Fields					
	version		IA	—	V3
	serialNumber		IA	—	128-bit or shorter positive integer
	signature		IA	—	sha1WithRSAEncryption (OID = 1 2 840 113549 1 1 5)
	issuer		IA	—	C = JP, O = Japan Certification Services, Inc., CN = SecureSign Public CA11 * Encoded as PrintableString
	validity				
		notBefore	RA	—	37 month * Set by UTCTIme.
		notAfter	RA	—	
	subject		EE	—	C = JP, ST = Subscriber's address (prefecture) (optional), L = Subscriber's address (county, city, town, village, and other details) (optional), O = Subscriber's organization name, OU = Subscriber's department name (optional), CN = Subscriber’s full name, * Only the value of C is encoded as PrintableString, while other values are encoded as PrintableString or BMPString.
	subjectPublicKeyInfo				
		algorithmIdentifier	IA	—	rsaEncryption (OID = 1 2 840 113549 1 1 1)
		public key	RA	—	A 2048-bit key to be generated by RA
Certificate Standard Extensions					
	authorityKeyIdentifier		IA	F	
		keyIdentifier			SHA-1 value (hash value) for public key
		authorityCertIssuer			Unused

	authCertSerialNumber				Unused
subjectKeyIdentifier			IA	F	SHA-1 value (hash value) for public key
keyUsage			IA	F	Set digitalSignature and keyEncipherment to ON; set other items to OFF.
certificatePolicies			IA	F	
	policyIdentifier				
		certPolicyId			1 2 392 200075 4 2
	policyQualifiers				
		policyQualifierId			1 3 6 1 5 5 7 2 1(id-qt-cps)
		qualifier			https://cp.jcsinc.co.jp/SecureSign/AD/RPA.html (URL for the agreement)
subjectAltName			EE	F	
	directoryName				C=JP, O= Subscriber's organization name (Japanese), OU= Subscriber's department name (Japanese) (optional), CN= Subscriber’s full name (Japanese), * Only the value of C is encoded as PrintableString, while other values are encoded as PrintableString or BMPString.
basicConstraints			IA	F	
	cA				FALSE
	pathLenConstraint				NULL
cRLDistributionPoints			IA	F	Set the following as URLs for "distributionPoint.fullName.URI": http://ssignadcrl01.jcsinc.co.jp/repository/crl/sca1.crl http://ssignadcrl02.jcsinc.co.jp/repository/crl/sca1.crl

7.2 CRL Profiles

7.2.1 Version number

X.509 V 2 CRLs are issued in this service.

7.2.2 CRL entry extensions

In this service, only the reason code (reasonCode) is used among items that can be set in these extension fields.

7.2.3 CRL profiles

This section describes details of the profiles of CRLs issued in this service. Note that CRL contents are encoded with PrintableString syntax unless otherwise specified.

(1) SCA CRL profile

Name	Setter	Criti-cality	Set value
Certificate Basic Fields			
version	IA	—	V2
signature	IA	—	sha1WithRSAEncryption (OID = 1 2 840 113549 1 1 5)
issuer	IA	—	C = JP, O = Japan Certification Services, Inc., CN = SecureSign Root CA11 * Encoded as PrintableString
thisUpdate	IA	—	CRL issuance date and time (Set by UTCTime.)
nextUpdate	IA	—	thisUpdate + 99days+999hours (Set by UTCTime.)
RevokedCertificates			
userCertificate	RA	—	Serial number
revocationDate	IA	—	Revocation date and time
crlEntryExtensions	IA		
reasonCode	RA		Set a reason code.
Certificate Standard Extensions			
authorityKeyIdentifier	IA	F	
keyIdentifier			SHA-1 value (hash value) for public key
authorityCertIssuer			DN of the issuer
authCertSerialNumber			Serial number
cRLNumber	IA	F	128-bit or shorter positive integer

(2) EE CRL profile

Name	Setter	Criti-cality	Set value
Certificate Basic Fields			
version	IA	—	V2
signature	IA	—	sha1WithRSAEncryption (OID = 1 2 840 113549 1 1 5)

	issuer		IA	—	C = JP, O = Japan Certification Services, Inc., CN = SecureSign Public CA11 * Encoded as PrintableString
	thisUpdate		IA	—	CRL issuance date and time (Set by UTCTime.)
	nextUpdate		IA	—	thisUpdate + 36 hours (Set by UTCTime.)
	RevokedCertificates				
		userCertificate	RA	—	Serial number
		revocationDate	IA	—	Revocation date and time
	crlEntryExtensions		IA		
		reasonCode	RA		Set a reason code.
Certificate Standard Extensions					
	authorityKeyIdentifier		IA	F	
		keyIdentifier			SHA-1 value (hash value) for public key
		authorityCertIssuer			DN of the issuer
		authCertSerialNumber			Serial number
	cRLNumber		IA	F	128-bit or shorter positive integer

8. SPECIFICATION ADMINISTRATION

In order to maintain security, JCSI makes positive efforts to stay abreast of cutting-edge security technologies and reflect them in the specifications of this standard as needed.

8.1 Specification Change Procedures and Publication/Notification Policies

JCSI shall reserve the right to update this standard without the prior consent of subscribers and relying parties. Before updating this standard, the JCSI Specification Control Group shall review the contents of the update to check for validity. Updating of this standard shall be completed upon disclosure of the updated standard or release of a change notice (i.e., collection of updated portions of this standard) in JCSI repositories. The change notice has the same effect as that of the actual update of this standard, and is reflected in the next version of this standard. Revisions and updates of this standard are identified by version numbers representing the revision history and dates of issue.

Revisions shall be notified by releasing a change notice or disclosing the updated standard in JCSI repositories. The effective date of specification changes shall depend on the importance and urgency of those changes. JCSI shall reserve the right to determine the importance and urgency of said changes at its sole discretion. However, effective dates are typically defined as follows:

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

(2) Urgent and important changes shall take effect immediately after notification. Here, urgent situations refer to cases where the SecureSign AD service might be compromised, in whole or in part, unless the relevant changes take effect immediately.

(3) Unimportant changes shall also take effect immediately after notification.

8.2 Publication and Notification Policies

Included in Section 8.1

8.3 Specification Approval Procedures

When this standard has been updated, the new standard disclosed in JCSI repositories shall apply regardless of when subscriber's certificates are issued. Customers (including RAOs and subscribers) shall be deemed as agreeing to all specification changes made by JCSI, unless they apply for revocation of their certificates. Relying parties who disagree with any specification changes should discontinue use of the certificates they have obtained.

8.4 Storage of This Document

JCSI shall store every version of this standard as long as the SecureSign AD service continues.

