SECOM Passport for Web SR
Certification Authority Certificate Policy

Version 2.92

March 30, 2020

SECOM Trust Systems Co., Ltd.

Version History		
Version Number	Date	Description
1.00	2008/02/25	Publication of the first version
1.10	2008/09/19	Contact information change
1.20	2009/05/13	Addition of the certificate validity period of five (5) years
1.30	2012/02/15	"5.6 Key Changeover" - Addition of Certificate Renewal - Addition of the validity period of the CA keys
1.40	2012/11/09	Amendment associated with commencement of the OCSP server operations Addition of SubjectAltName to the Certificate Profile
2.00	2013/12/02	Major version upgrade Renaming of "SECOM Passport for Web SR2.0 CA Certificate Policy" to "SECOM Passport for Web SR CA Certificate Policy" and addition of the CA Private Key "SECOM Passport for Web SR3.0 CA"
2.10	2014/01/15	Revision of the descriptions
2.20	2014/09/25	Removal of Basic Constraints in "Certificate Profile" Addition of the certificate validity period of three (3) years Revision of the descriptions
2.30	2015/04/15	Addition of the CAA description
2.40	2015/12/25	Addition of the "Authentication of Domain Name" provisions
2.50	2017/05/23	Removal of "SECOM Passport for Web SR2.0 CA" Revision of the acceptance and issuance dates for Renewal/Re-Keying requests Overall revision of the descriptions and styles
2.60	2017/09/07	Correction of the "CAA Records" description.
2.70	2018/03/01	Revision of the retention period for Archive Removal of the certificate validity period of three (3) years
2.80	2018/03/29	Addition of the Certificate Transparency Extension descrpition Registration of the OV identifier

2.90	2018/08/01	Correction of description about Authentication of Domain. Revision of the descriptions
2.91	2019/05/24	Overall revision of the descriptions and styles
2.92	2020/03/30	Revised chapters and added some " No Stipulation" content

Table of Contents

1. Introduction

1.1 Overview

SECOM Passport for Web SR Certification Authority Certificate Policy (hereinafter, "this CP") defines the policy on certificates issued by SECOM Passport for Web SR 3.0 CA (hereinafter, "the CA"), which are operated by SECOM Trust Systems Co., Ltd. (hereinafter, "SECOM Trust Systems"), by specifying the purpose of use, the scope of application and user procedures concerning the Certificates. Various procedures regarding the operation and maintenance of the CA are stipulated in the SECOM Digital Certification Infrastructure Certification Practice Statement (hereinafter, "CPS").

Unilateral cross-certificate by Security Communication RootCA2 has been issued to the CA.
Certificates issued by the CA shall be valid for six (6) month, one (1) year, or two (2) years, as the case may be.

Certificates issued by the CA are used for server authentication and data encryption in the communication routing. The parties to whom Certificates may be issued (Certificate subjects) are set forth in the SECOM Passport for Web SR Service Terms (hereinafter, "Service Terms").
A party seeking to obtain Certificates from the CA must examine its usage purposes against this CP, the Service Terms and the CPS, and agree to all three prior to getting the Certificates issued.
The CA conforms to the Baseline Requirements of the CA/Browser Forum disclosed at https://www.cabforum.org/.

In the event of a conflict between this CP and the Service Terms or the CPS, the order of precedence in the application thereof shall be the Service Terms, this CP, and the CPS. Any provisions set forth in a separate contract or the like between SECOM Trust Systems and an organization, a group or any other party, with which it has a contractual relationship that are inconsistent with the Service Terms, this CP, and the CPS, shall prevail.

This CP shall be revised as necessary in order to reflect any technical or operational developments or improvements pertaining to the CA

This CP conforms to the RFC3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" advocated by the IETF as a CA practice framework.

1.2 Document Name and Identification

The official name of this CP is "SECOM Passport for Web SR Certification Authority Certificate Policy".

This CP is identified with the Object IDentifier (hereinafter, "OID") given in "Table 1.2-1 OID (This CP)"

Table 1.2-1 OID (This CP)

CP	OID
SECOM Passport for Web SR 3.0 CA (sha256)	1.2.392.200091.100.751.1

The OID of the CPS associated with this CP is given in Table 1.2-2 OID (The CPS)

Table 1.2-2 OID (The CPS)

CPS	OID
SECOM Digital Certification Infrastructure Certification Practice Statement	1.2.392.200091.100.401.1

1.3 PKI Participants

1.3.1 CA

A CA mainly issues or revokes Certificates, publishes CRLs (Certificate Revocation Lists), provides information on Certificate status using the OCSP server, and maintains and manages the Repository. The operating body of the CAs on the Digital Certification Infrastructure is SECOM Trust Systems.

1.3.2 RA

An RA mainly performs identification and authentication of applicants requesting the issuance or revocation of Certificates as well as the registration thereof.

1.3.3 Subscribers

Subscribers shall be corporations or any other organizations that submit Certificate Application to SECOM Trust Systems, as well as any independent contractors concluding such individual agreements as sales consignment therewith to conduct as

agencies for the application procedure, administration of the servers and storage of Certificates thereon.

1.3.4 Relying Parties

Relying Parties signify individuals, corporations or any other organizations that authenticate the identity of Subscribers and the validity of Public Keys. They also signify individuals, corporations or any other organizations that trust and use CPs and CPSes for the purpose of conducting encrypted communication with web servers owned by Subscribers using said Public Keys.

1.3.5 Other Parties

Other Parties include auditors, and companies or organizations that have service contracts with SECOM Trust Systems, and companies that perform system integration.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

Certificates issued by the CA may be used for server authentication and data encryption in the communication routing.

1.4.2 Prohibited Certificate Uses

Certificates issued by the CA may not be used for purposes other than server authentication and data encryption in the communication routing.

1.5 Policy Administration

1.5.1 Organization Administering the Document

This CP is maintained and administered by SECOM Trust Systems.

1.5.2 Contact Information

Inquiries concerning this CP should be directed to:

CA Support Center, SECOM Trust Systems Co., Ltd.
Address: 2-7-8 Mejirodai, Bunkyo-ku, Tokyo 112-0015
E-mail address: ra-support@secom.co.jp

1.5.3 Person Determining CP Suitability for the Policy

The Certification Services Improvement Committee determines the suitability of the contents of this CP.

1.5.4 Approval Procedure

This CP is prepared and revised by SECOM Trust Systems and goes into effect upon approval by the Certification Services Improvement Committee.

1.6 Definitions and Acronyms

Archive

Information obtained for the purpose of preserving history for legal or other reasons.

Audit Log

Behavioral, access and other histories pertaining to the CA systems which are recorded for inspection of access to and unauthorized operation of the CA systems.

Baseline Requirements

A document issued by the CA/Browser Forum (available at cabforum.org.) that integrates a set of fundamental requirements for Certificate issuance/administration.

CA (Certification Authority)

An entity that mainly issues, renews and revokes Certificates, generates and protects CA Private Keys, and registers Subscribers.

CAA (Certificate Authority Authorization)

A function to prevent false issuance of Certificates by an unintended CA, by including the CA information for the domain ownership/control rights to grant the Certificate issuance for the specific domain, in the DNS record.

CA/Browser Forum

An NPO organized by CAs and Internet browser vendors that works to define and standardize the Certificate issuance requirements.

CP (Certificate Policy)

A document that sets forth provisions pertaining to Certificates issued by a CA, including Certificate types, usage and application procedure.

CPS (Certification Practices Statement)

A document that sets forth provisions pertaining to the practices of CAs, including procedures for the CA operations and the security standards.

CRL (Certificate Revocation List)

A list of information on Certificates which were revoked prior to their expiration due to reasons such as changes to the information provided in the Certificates and loss of the relevant Private Key.

CT (Certificate Transparency)

Certificate Transparency, stipulated in RFC 6962, is an open framework for monitoring/auditing the records of the issued Certificates by registering and publishing them on the log servers.

Digital Certificate

Digital data certifying that a public key is owned by the party specified, validity of which is certified by the digital signature of the relevant CA affixed thereto. Digital Certificate is referred to as "Certificate" hereinafter.

Escrow

Escrow means the placement (entrustment) of an asset in the control of an independent third party.

FIPS140-2

The security certification standards developed by the U.S. NIST (National Institute of Standards and Technology) for cryptographic modules, defining four security levels, the lowest 1 through the highest 4.

IA (Issuing Authority)

An entity which, of the duties of a CA, mainly handles the issuance, renewal and revocation of Certificates, generation and protection of CA Private Keys, and the maintenance and management of repositories.

Key Pair

A pair of keys comprising a private key and a public key in the public key cryptosystem.

OCSP (Online Certificate Status Protocol)

A protocol for real-time provision of information on Certificate status.

OID (Object Identifier)

A unique numeric identifier registered by the international registration authority, in a framework to maintain and administer the uniqueness of the mutual connectivity, services and other aspects of the networks.

PKI (Public Key Infrastructure)

An infrastructure for use of the encryption technology known as the public key cryptosystem to realize such security technologies as digital signature, encryption and certification.

Private Key

A key of a Key Pair that is possessed by the holder of the corresponding public key.

Public Key

A key of a Key Pair used in the public key cryptosystem. A Public Key corresponds to the Private Key and is published to and shared with the recipient.

RA (Registration Authority)

An entity which, of the duties of a CA, mainly performs assessment of application submissions, registration of necessary information for issuance of the Certificates, and requests Certificate signing to CAs.

Repository

A (online) database for storing and providing access to CA certificates, CRLs and the like.

RFC3647 (Request for Comments 3647)

A document defining the framework for CP and CPS published by the IETF (The Internet Engineering Task Force), an industry group which establishes technical

standards for the Internet.

RSA

One of the most standard encryption technologies widely used in the Public Key cryptosystem.

SHA-1 (Secure Hash Algorithm 1)

A hash function used in digital signing. A hash function is a computation technique for generating a fixed-length string from a given text. The hash length is 160 bits.
The algorithm works to detect any alterations in the original message during the transmission by comparing the hash values transmitted and received.

SHA-256 (Secure Hash Algorithm 256)

A hash function used in digital signing. The hash length is 256 bits.
The algorithm works to detect any alterations in the original message during the transmission by comparing the hash values transmitted and received.

Time-Stamp

Data recording such date and time of creating an electronic file or running a system process.

WebTrust for Baseline Requirements

Audit standards established by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) defining the rules for the reviews/authentications by the CAs for issuance of SSL Certificates and on the Certificates themselves.

WebTrust for CA

Standards of internal control and a certification framework based thereon established by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) regarding the reliability of CAs, the security of electronic commerce transactions, and other relevant matters.

WHOIS

An Internet browsing service for information about the registrants of IP addresses and domain names.

X.500

A series of computer network standards regarding the decentralized directory service.

2. Publication and Repository Responsibilities

2.1 Repository

SECOM Trust Systems maintains and manages a Repository in order to allow Subscribers and Relying Parties to access CRL information 24x7. Further, it manages an OCSP server to allow Subscribers and Relying Parties to check online the status of Certificates 24x7. However, the Repository and the OCSP server may not be available temporarily at times due to maintenance or for any other reason.

2.2 Publication of Certificate Information

SECOM Trust Systems stores the following information in the Repository to allow the online access thereto by Subscribers and Relying Parties:

- CRL
- The CA Certificates
- The latest versions of this CP and the CPS
- Other information pertaining to Certificates issued by the CA

SECOM Trust Systems will make the Certificate status available online to Subscribers and Relying Parties for browsing on the OCSP server. Additionally, SECOM Trust Systems hosts the test Web pages that allow vendors to perform verifications, as part of the publication.

2.3 Time or Frequency of Publication

This CP and the CPS are published in the Repository as revised. A CRL containing information of revocation processed conforming to this CP is published in the Repository as issued. Certificates with expired validity period shall be removed from the CRL.

2.4 Access Controls on Repository

Subscribers and Relying Parties may access the Repository at any time. The protocols used to access the Repository shall be HTTP (Hyper Text Transfer Protocol) and HTTPS (HTTP + SSL/TLS data encryption function). Information in the Repository may be accessed via any commonly used Web interface.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

The name of the CA indicated in a Certificate as the issuer and the name of the issuance subject Subscriber are configured according to the X.500 Distinguished Name (DN) format.

The following information shall be included in a Certificate issued by the CA:

1. [Country Name (C)] shall be JP.
2. "Organization Name" (O) shall be the name of the relevant organization in the form of a legal person, corporation, or other form of a legal person. For a sole proprietor, the name shall be that of the individual proprietor.
3. [Organizational Unit Name (OU)] shall be an optional field. The OU field is used to distinguish departments (e.g., Human Resources, Marketing, or Development).
4. [Common Name (CN)] shall be the hostname of the web server on which the Certificates issued by the CA will be installed.

3.1.2 Need for Names to Be Meaningful

The Common Name used in a Certificate issued by the CA shall be meaningful when the hostname used in the web server DNS for which the relevant Subscriber plans to install the Certificate is assigned.

3.1.3 Anonymity or Pseudonymity of Subscribers

An anonymous or pseudonymous name may not be registered as the Organization Name or the Common Name in the Certificate issued by the CA.

3.1.4 Rules for Interpreting Various Name Forms

Rules concerning the interpretation of various name forms are governed by the X.500 Series DN rules.

3.1.5 Uniqueness of Names

The DN indicated in any Certificate issued by the CA shall be uniquely attributable to the web server for which the Certificate is issued.

3.1.6 Recognition, Authentication, and Roles of Trademarks

SECOM Trust Systems does not verify intellectual property rights for the names indicated in Certificate applications. Subscribers may not submit any registered trademark or other trademark-related names of a third party. SECOM Trust Systems will not arbitrate or engage itself in the resolution of any dispute between Subscribers and third parties over the registered trademark or any alike. SECOM Trust Systems reserves the right to reject a Subscriber Certificate Application or revoke an issued Certificate due to the dispute.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

A Subscriber proves possession of the relevant Private Key in accordance with the following method.

The signature on the relevant Certificate Signing Request (hereinafter, "CSR") is authenticated to prove that said CSR is signed with the Private Key corresponding to the Public Key.

3.2.2 Authentication of Organization Identity

SECOM Trust Systems authenticates the identity of organizations based on official documents issued by national or local governments, investigations conducted, or databases owned by third parties that SECOM Trust Systems trusts, or through other means deemed equally trustworthy by the Certification Services Improvement Committee.

3.2.3 Authentication of Individual Identity

SECOM Trust Systems authenticates the identity of individuals based on official documents issued by national or local governments, investigations conducted, or databases owned by third parties that SECOM Trust Systems trusts, or through other means deemed equally trustworthy by the Certification Services Improvement Committee.

3.2.4 Non-Verified Subscriber Information

SECOM Trust Systems verifies all information specified in BR, such as the trade name, name, and location of the certificate subscriber included in the certificate's distinguished name. In addition, in providing the service, there is a case where it is

requested to provide information necessary for office procedures such as billing information.

3.2.5 Validation of Authority

When an entity submits a Certificate-related application, legitimacy of authority for such request is authenticated by SECOM Trust Systems in accordance with "3.2.2 Authentication of Organization Identity" and "3.2.3 Authentication of Individual Identity" hereof. In the event a third party other than a Subscriber makes the request and the intent to make said request cannot be confirmed directly with the Subscriber, a letter of proxy is required certifying that said third party is an agent of the Subscriber.

*As used in this clause, "Subscriber" signifies an individual, a corporation, or any other organization that uses the hostname indicated as the Common Name populated in the Certificates as stipulated in "3.1.1 Types of Names" hereof.

3.2.6 Criteria for Interoperation

Unilateral cross-certificate by Security Communication RootCA2 has been issued to the CA.

3.2.7 Authentication of Domain Name

To authenticate a Subscriber's ownership of or control over the requested Domain Name(s), SECOM Trust Systems implements the following method:

1. Examine the Subscriber's control over or right to use the required FQDN by sending randomized values to e-mail addresses with 'admin', "administrator', 'webmaster', 'hostmaster' or 'postmaster' in the local portion and with the authenticated Domain Name following "@"; and by receiving the confirming reply containing the randomized values;
2. Examine the Subscriber's control over or right to use the required FQDN by sending randomized values to the domain administrator's e-mail address registered under the WHOIS registry service, and by receiving the confirming reply containing the randomized values; and
3. Use other reasonable methods conforming to the Baseline Requirements.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

Subscribers shall be identified and authenticated for Re-Keying in the same manner as set forth in "3.2 Initial Identity Validation" hereof.

3.3.2 Identification and Authentication for Re-Key after Revocation

A routine Re-Key after Revocation is not supported. The (Re-Keying) application for a Certificate shall be treated as a new submission, and the applicant Subscriber shall be identified and authenticated in the same manner as set forth in "3.2 Initial Identity Validation" hereof.

3.4 Identification and Authentication for Revocation Requests

Accepting a Revocation Request via a website accessible only by the Subscriber, SECOM Trust Systems identifies and authenticates the applicant Subscriber.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who May Submit a Certificate Application

An application for a Certificate may be filed by a corporation using the Certificate, an Authorized Person, as specified in the Client Organization-Based Document Submission Criteria [SECOM Passport for Web SR] (hereinafter, "Client Organization-Based Document Submission Criteria"), of a non-Subscriber corporation, or an agent appointed by of a corporation or other form of a legal person.

4.1.2 Enrollment Process and Responsibilities

In submitting a Certificate Application, a Subscriber or an agent entrusted by the Subscriber shall agree to the provisions of Each Regulatory Document before proceeding with the application, as well as certify that the information submitted is accurate.

The method for Certificate Application is to submit required documents to Trust Systems following the “Application Procedure” published on its website.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Once accepted, the Certificate Application is authenticated by SECOM Trust Systems in accordance with "3.2 Initial Identification and Authentication" hereof.

4.2.2 Approval or Rejection of Certificate Applications

SECOM Trust Systems issues a Certificate corresponding to any application that it approves following the review and authentication, subsequently notifying the relevant Subscriber of the completion thereof and the issuance of the Certificate. Should a Certificate Application be inadequate or deficient, SECOM Trust Systems shall notify the relevant Subscriber of the reason therefor and ask for re-submission of the documents and any other information required.

4.2.3 Time to Process Certificate Applications

SECOM Trust Systems promptly issues a Certificate corresponding to any approved Certificate Application.

4.2.4 Confirmation of CAA Records

The CA shall check the CAA records during the review and authentication of the Certificate Application and the submitted information. The domain name of the CA to be included in the CAA record shall be [secomtrust.net].

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

Upon completion of the review and authentication of a Certificate Application, SECOM Trust Systems issues the corresponding Certificate and makes it available for download via a website accessible only by the Subscriber or send the Certificate to the Subscriber.

4.3.2 Notifications to Subscriber of Certificate Issuance

SECOM Trust Systems notifies the relevant Subscriber of the fact that the Subscriber Certificate is ready for download via a website accessible only by the Subscriber via e-mail. Download of the Certificate is made available to the Subscriber upon receiving the e-mail notice from the CA. The notification shall be also deemed complete when the Certificate is sent to the Subscriber.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Certificate acceptance shall be deemed complete when the Subscriber Certificate has been downloaded from the website accessible only by the subscriver. When the Certificate is sent to the Subscriber, the acceptance thereof shall be deemed complete if no such claim by the Subscriber as wrong descriptions on the Certificate is made within a week from the delivery.

4.4.2 Publication of the Certificate by the CA

The CA does not publish Subscriber Certificates.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

SECOM Trust Systems will not send a notice of Certificate issuance to entities other than the person in charge, who was registered at the time of the Certificate

Application submission.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers shall use Private Keys and Certificates for the server authentication and data encryption in the communication routing. Subscribers shall use the relevant Certificates and corresponding Private Keys only for the purposes approved by the CA and for no other purpose.

4.5.2 Relying Party Public Key and Certificate Usage

Relying Parties shall acknowledge and agree to the provisions of this CP and the CPS before using the CA Certificates.
Relying Parties may use the CA Certificates for assessment of Subscriber Certificates.

4.6 Certificate Renewal

The CA recommends generating a new Key Pair when Subscribers renew a Certificate.

4.6.1 Circumstances for Certificate Renewal

No stipulation

4.6.2 Who May Request Renewal

No stipulation

4.6.3 Processing Certificate Renewal Requests

No stipulation

4.6.4 Notification of New Certificate Issuance to Subscriber

No stipulation

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

No stipulation

4.6.6 Publication of the Renewal Certificates by the CA

No stipulation

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation

4.7 Certificate Re-Key

4.7.1 Circumstances for Certificate Re-Key

A Certificate may be Re-Keyed when its validity period is about to expire. A revoked or expired Certificate cannot be Re-Keyed.

Certificate Re-Key applications shall be accepted 90 days prior to the expiry of the validity periods.

4.7.2 Who May Request Certification of a New Public Key

The provisions of "4.1.1 Who Can Submit a Certificate Application" hereof shall apply.

4.7.3 Processing Certificate Re-Keying Requests

The provisions of "4.3.1 CA Actions during Certificate Issuance" hereof shall apply.

4.7.4 Notification of New Certificate Issuance to Subscriber

The provisions of "4.3.2 Notifications to Subscriber of Certificate Issuance" hereof shall apply.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

The provisions of "4.4.1 Conduct Constituting Certificate Acceptance" hereof shall apply.

4.7.6 Publication of the Re-Keyed Certificate by the CA

The provisions of "4.4.2 Publication of the Certificate by the CA" hereof shall apply.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

The provisions of "4.4.3 Notification of Certificate Issuance by the CA to Other Entities" hereof shall apply.

4.8 Certificate Modification

Should modification be required in any information registered in a Certificate, the CA shall revoke the relevant Certificate and issue a new Certificate.

4.8.1 Circumstances for Certificate Modification

No stipulation

4.8.2 Who May Request Certificate Modification

No stipulation

4.8.3 Processing Certificate Modification Requests

No stipulation

4.8.4 Notification of New Certificate Issuance to Subscriber

No stipulation

4.8.5 Conduct Constituting Acceptance of Modified Certificate

No stipulation

4.8.6 Publication of the Modified Certificates by the CA

No stipulation

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Certificate Revocation

A Subscriber must promptly request SECOM Trust Systems to revoke a Certificate in the event of any of the following:

- There has been a change in information populated in the Certificate;
- The Private Key has or may have been compromised for any reason, including the theft, loss, unauthorized disclosure or unauthorized use thereof;
- the Certificate is incorrectly populated or not being used for authorized purposes; or
- the use of the Certificate is being terminated.

SECOM Trust Systems may revoke the Subscriber Certificate at its discretion if:

- the Subscriber is not performing the obligations thereof under the Service Terms, this CP, the CPS, relevant agreements or laws;

- it is determined that the CA Private Key has or could have been compromised; or
- The Secret Key of the Subscriber and CA is compromised, and the reasonable evidence is found, which shows that the key isn't complying with the algorithm type and the requirement for the key size as standard, or the certificate is abused by some other way;
- It is recognized that the Certificate is not issued in compliance with BR, this CP or CPS;
- Based on the law of the CA's jurisdiction, the reasonable evidence is found that shows the Subscriber's name is blacklisted as the rejected party, or banned person;
- SECOM Trust Systems recognizes any other situation deemed to necessitate revocation.

4.9.2 Who Can Request Revocation

A request for revocation of a Certificate may be made by the Certificate user corporation, an Authorized Person, as specified in the Client Organization-Based Document Submission Criteria, of a non-user corporation, or an agent appointed by representatives of a corporation or other form of a legal person.

4.9.3 Procedure for Revocation Request

A Subscriber shall submit a Revocation Request by selecting the relevant Certificate information on the website accessible only by the Subscriber.

4.9.4 Revocation Request Grace Period

Should a Subscriber determine that a Private Key has or could have been compromised, the Subscriber must promptly make a revocation request.

4.9.5 Time within Which CA Shall Process the Revocation Request

Upon receipt of a valid Revocation Request, SECOM Trust Systems will promptly process the request and reflect the relevant Certificate information in the CRL.

4.9.6 Revocation Checking Requirements for Relying Parties

The URLs of the CRL storage destination and the OCSP server are indicated on the Certificates issued by the CA.

CRLs and the OCSP server may be accessed using a commonly available Web Interface. CRLs do not contain expired Certificate information.

Relying Parties must authenticate the validity of a Subscriber's Certificate. The validity of a Certificate may be verified by using the CRL posted on the Repository site or the OCSP server.

4.9.7 CRL Issuance Frequency

The CRL is updated every twenty four (24) hours regardless of whether there has been a Revocation processed. If there has been one, the CRL is updated as of the Revocation.

4.9.8 Maximum Latency for CRLs

The CRLs issued by the CA are immediately reflected onto the Repository.

4.9.9 On-Line Revocation/Status Checking Availability

The On-Line Certificate Status service is provided on the OCSP server. The Certificate Revocation Status is updated every twenty four (24) hours whether there has been a Revocation processed. If there has been one, the Certificate Revocation Status is updated and made available through the OCSP server.

4.9.10 On-Line Revocation/Status Checking Requirements

Relying Parties must authenticate the validity of Subscriber Certificates. When not using the CRL posted on the Repository to check for the Revocation registration of a Certificate, the Relying Parties must confirm the Certificate status available through the OCSP server.

4.9.11 Other Forms of Revocation Advertisements Available

The CA can distribute OCSP responses using stapling in accordance with RFC4366. In this case, the CA ensures that the subscriber includes the OCSP response of the certificate in the TLS process. The CA will comply with this requirement for the subscriber after the Service Terms or the contract with the subscriber, or after the technical confirmation by the CA and the approval of the service manager.

4.9.12 Special Requirements Regarding Key Compromise

Refer to “4.9.1 Circumstances for Certificate Revocation”.

4.9.13 Circumstances for Suspension

The CA will not suspend Certificates.

4.9.14 Who Can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

Certificate status is available to Subscribers and Relying Party for confirmation through the OCSP server.

4.10.2 Service Availability

The CA maintains and manages the OCSP server in order to allow 24x7 access to the Certificate status for confirmation. However, the OCSP server may not be available temporarily at times due to maintenance or for any other reason.

4.10.3 Optional Features

No stipulation

4.11 End of Subscription (Registry)

Subscribers may end the certificate issuing service provided by the CA (hereinafter "The Service") by submitting a Certificate Revocation Request or naturally letting it expire.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

The CA does not Escrow Subscriber Private Keys.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5. Facility, Management, and Operational Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

Relevant provisions are stipulated in the CPS.

5.1.2 Physical Access

Relevant provisions are stipulated in the CPS.

5.1.3 Power and Air Conditioning

Relevant provisions are stipulated in the CPS.

5.1.4 Water Exposures

Relevant provisions are stipulated in the CPS.

5.1.5 Fire Prevention and Protection

Relevant provisions are stipulated in the CPS.

5.1.6 Media Storage

Relevant provisions are stipulated in the CPS.

5.1.7 Waste Disposal

Relevant provisions are stipulated in the CPS.

5.1.8 Off-Site Backup

Relevant provisions are stipulated in the CPS.

5.2 Procedural Controls

5.2.1 Trusted Roles

Relevant provisions are stipulated in the CPS.

5.2.2 Number of Persons Required per Task

Relevant provisions are stipulated in the CPS.

5.2.3 Identification and Authentication for Each Role
Relevant provisions are stipulated in the CPS.

5.2.4 Roles Requiring Separation of Duties
Relevant provisions are stipulated in the CPS.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements
Relevant provisions are stipulated in the CPS.

5.3.2 Background Check Procedures
Relevant provisions are stipulated in the CPS.

5.3.3 Training Requirements
Relevant provisions are stipulated in the CPS.

5.3.4 Retraining Frequency and Requirements
Relevant provisions are stipulated in the CPS.

5.3.5 Job Rotation Frequency and Sequence
Relevant provisions are stipulated in the CPS.

5.3.6 Sanctions for Unauthorized Actions
Relevant provisions are stipulated in the CPS.

5.3.7 Independent Contractor Requirements
Relevant provisions are stipulated in the CPS.

5.3.8 Documentation Supplied to Personnel
Relevant provisions are stipulated in the CPS.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded
Relevant provisions are stipulated in the CPS.

5.4.2 Frequency of Processing Audit Log

Relevant provisions are stipulated in the CPS.

5.4.3 Retention Period for Audit Log

Relevant provisions are stipulated in the CPS.

5.4.4 Protection of Audit Log

Relevant provisions are stipulated in the CPS.

5.4.5 Audit Log Backup Procedure

Relevant provisions are stipulated in the CPS.

5.4.6 Audit Log Collection System

Relevant provisions are stipulated in the CPS.

5.4.7 Notification to Event-Causing Subject

Relevant provisions are stipulated in the CPS.

5.4.8 Vulnerability Assessments

Relevant provisions are stipulated in the CPS.

5.5 Records Archival

5.5.1 Types of Records Archived

SECOM Trust Systems stores the following information in addition to the CA-related system logs specified in "5.4.1 Types of Events Recorded" in the CPS, as Archive:

- Certificates and CRLs issued;
- processing history relating to CRL issuance;
- CPS
- Documents governing the CA business practices, developed in compliance with the CPS
- documents associated with agreements of subcontracting if the certification services are outsourced;
- records of audit results and the audit reports;
- application documentary submissions from Subscribers; and

- OCSP server access log.

5.5.2 Retention Period for Archive

SECOM Trust Systems retains its Archive for a minimum of seven (7) years.

5.5.3 Protection of Archive

The Archive is retained in a facility, to which access is restricted to the authorized personnel.

5.5.4 Archive Backup Procedures

The Archive is backed up whenever a change is made in such critical data pertaining to the CA-related systems as Certificate issuance/revocation or CRL issuance.

5.5.5 Requirements for Time-Stamping of Records

SECOM Trust Systems uses the NTP (Network Time Protocol) to time synchronize systems related to the CA and Time-Stamps critical information recorded therein.

5.5.6 Archive Collection System

The Archive collection system is included as a function of the systems related to the CA.

5.5.7 Procedures to Obtain and Verify Archive Information

The Archive shall be retrieved from the secure storage by designated personnel with the appropriate access permission for periodic checks of the storage conditions of the media. Further, the Archive is copied to new media as appropriate to maintain their integrity and confidentiality.

5.6 Key Changeover

Renewal of Key-Pairs or Certificates of the CA, as a general rule, shall be made before their remaining validity periods become shorter than the maximum validity periods of the Certificates issued to Subscribers.

When the remaining validity period of the CA becomes shorter than the maximum validity periods of the Certificates issued to Subscribers, the validity periods of the Certificates issued thereto shall be so changed to be within the validity period of the CA.

The validity period of CA Private Keys is assumed to be twenty (20) years.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

SECOM Trust Systems establishes measures against incidents and compromises, including the following, to ensure the prompt recovery of the CA-related systems and relevant operations thereafter:

- CA Private Key compromise
- damages to or malfunction of computing resources, software, and/or data; and
- fires, earthquakes and other disasters.

5.7.2 Computing Resources, Software, and/or Data are Corrupted

In the event of damage to any hardware, software or data of a CA-related system, SECOM Trust Systems promptly engages in the system recovery efforts using the relevant hardware, software or data that it retains as backup.

5.7.3 Entity Private Key Compromise Procedures

Should it be determined that the Private Keys of the CA using the CA-related system have been or may be compromised or should a disaster or any other unexpected incidents result in a situation that may lead to interruptions or suspensions of the operation of the CA-related system, SECOM Trust Systems follows the predetermined plans and procedures to securely resume the operation.

5.7.4 Business Continuity Capabilities after a Disaster

In order to ensure prompt recovery to be implemented in the event of an unforeseen circumstance, SECOM Trust Systems deploys preventive measures for the fastest possible recovery of the CA-related systems, including securing of replacement/backup hardware, continual data backups for recovery, and establishment of the recovery procedures.

5.8 CA or RA Termination

In the event of termination of the CA by SECOM Trust Systems, the company shall so notify Subscribers and other affected participants three (3) months prior to the termination. All Certificates issued by the CA are revoked prior to the termination thereof.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

In the certification infrastructure system, CA Key Pairs are generated on an FIPS140-2 Level 3 conformant cryptographic module. The Key Pair generation operation is jointly performed by at least two authorized individuals.
Subscriber Key Pairs are generated by Subscriber.
The method recommended by the CA for Key Pair generation on a web server is posted on the SECOM Trust Systems website.

6.1.2 Private Key Delivery to Subscriber

The CA does not deliver Private Keys to Subscribers.

6.1.3 Public Key Delivery to Certificate Issuer

A Subscriber Public Key may be delivered online to the CA, the communication routing of which is encrypted by SSL/TLS.

6.1.4 CA Public Key Delivery to Relying Parties

Relying Parties may obtain CA Public Keys by accessing the CA Repository.

6.1.5 Key Sizes

The length of a CA Key Pair shall be 2048 bits in the RSA format.
The length of a Subscriber Key Pair shall be 2048 bits in the RSA format.
Certification Applications shall be accepted for the different Key Sizes with RSA due to the dependency on the web servers Subscribers use.

6.1.6 Public Key Parameters Generation and Quality Checking

Parameter generation and parameter strength assessment for CA Public Keys are performed using the function implemented in the cryptographic module used to generate the Key Pairs.
This CP does not provide for the parameter generation and quality check of Subscriber Public Keys.

6.1.7 Key Usage Purposes

Usage Purposes of the CA and the Certificates issued by the CA shall be as follows:

Table 6.1-1 Key Usage Purposes

	The CA	The Certificates issued by the CA
digital Signature	-	yes
nonRepudiation	-	-
keyEncipherment	-	yes
dataEncipherment	-	-
keyAgreement	-	-
keyCertSign	yes	-
cRLSign	yes	-
encipherOnly	-	-
decipherOnly	-	-

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The generation, storage and signing operations of the CA Private Keys are performed using an FIPS140-2 Level 3 conformant cryptographic module.
This CP does not provide for the cryptographic module standards and controls of Subscriber Private Keys.

6.2.2 Private Key Multi-Person Control

Activation, deactivation, backup and other operations relating to CA Private Keys are jointly performed by at least two authorized individuals in a secure environment.
Activation, deactivation, backup and other operations relating to Subscriber Private Keys must be performed securely under the control of the relevant Subscribers.

6.2.3 Private Key Escrow

The CA does not Escrow CA Private Keys.
The CA does not Escrow Subscriber Private Keys.

6.2.4 Private Key Backup

Backup of Private Keys of the CA is jointly performed by at least two authorized individuals and is stored in a secure room as encrypted.

The backup of Subscriber Private Keys must be securely stored under the control of the relevant Subscribers.

6.2.5 Private Key Archival

The CA does not archive CA Private Keys.
This CP does not provide for the cryptographic module standards and controls of Subscriber Private Keys.

6.2.6 Private Key Transfer into or from a Cryptographic

The transfer of Private Keys of the CA into and from an cryptographic module is performed in a secure room while encrypted.
This CP does not provide for the cryptographic module standards and controls of Subscriber Private Keys.

6.2.7 Private Key Storage on Cryptographic Module

Private Keys of the CA operated on the Digital Certification Infrastructure are stored within the cryptographic module.
This CP does not provide for the cryptographic module standards and controls of Subscriber Private Keys.

6.2.8 Method of Activating Private Key

The CA Private Key is jointly activated by at least two authorized individuals in a secure room.
This CP does not provide for the cryptographic module standards and controls of Subscriber Private Keys.

6.2.9 Method of Deactivating Private Key

The CA Private Key is jointly deactivated by at least two authorized individuals in a secure room.
This CP does not provide for the cryptographic module standards and controls of Subscriber Private Keys.

6.2.10 Method of Destroying Private Key

Private Keys of the CA are jointly destroyed by at least two authorized individuals by means of complete initialization or physical destruction. The Private Key backups are also destroyed in the same manner.

This CP does not provide for the cryptographic module standards and controls of Subscriber Private Keys.

6.2.11 Cryptographic Module Rating

The quality standards to be applied to the cryptographic modules used by the CA are as specified in "6.2.1 Cryptographic Module Standards and Controls" hereof.
This CP does not provide for the cryptographic module standards and controls of Subscriber Private Keys.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The provisions for CA Public Keys are stipulated in "6.2.1 Cryptographic Module Standards and Controls" of the CPS.
This CP does not provide for the cryptographic module standards and controls of Subscriber Private Keys.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The validity period of the CA Private Key and Public Key shall not exceed twenty (20) years.
This CP does not provide for the validity period of Subscriber Private Keys.
The validity period of Subscriber Certificates issued by the CA shall be one (1) year or two (2) years, as the case may be.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Relevant provisions are stipulated in the CPS.

6.4.2 Activation Data Protection

Relevant provisions are stipulated in the CPS.

6.4.3 Other Aspects of Activation Data

Relevant provisions are stipulated in the CPS.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

Relevant provisions are stipulated in the CPS.

6.5.2 Computer Security Rating

Relevant provisions are stipulated in the CPS.

6.6 Life-Cycle Technical Controls

6.6.1 System Development Controls

Relevant provisions are stipulated in the CPS.

6.6.2 Security Management Controls

Relevant provisions are stipulated in the CPS.

6.6.3 Life-Cycle Security Controls

Relevant provisions are stipulated in the CPS.

6.7 Network Security Controls

Relevant provisions are stipulated in the CPS.

6.8 Time-Stamping

Relevant provisions are stipulated in the CPS.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

Certificates issued by the CA conform to RFC5280, the profile of which are indicated in the tables below.

Table 7.1-1 SECOM Passport for Web SR 3.0 CA Server Certificate Profile

Basic Fields		Settings	critical
Version		Version 3	-
Serial Number		e.g.) 0123456789	-
Signature Algorithm		sha256 With RSA Encryption	-
Issuer	Country	C=JP	-
	Organization	O=SECOM Trust Systems CO.,LTD.	-
	Common Name	CN= SECOM Passport for Web SR 3.0 CA	-
Validity	NotBefore	e.g.) 2018/3/1 00:00:00 GMT	-
	NotAfter	e.g.) 2019/3/1 00:00:00 GMT	-
Subject	Country	C=JP (Fixed value)	-
	State Or Province	Required	-
	Locality	Required	-
	Organization	Required	-
	Organizational Unit	Optional	-
	Common Name	Server name (Required)	-
Subject Public Key Info		Subject Public Key 2048 bits	-
Extension Fields		Settings	critical
keyUsage		digitalSignature, keyEncipherment	y
extendedKeyUsage		serverAuth	n
Subject Alt Name		dNSName=Server Name	n
CertificatePolicies		[1]policyIdentifier OID=1.2.392.200091.100.751.1 policyQualifiers policyQualifierId=CPS qualifiier=https://repo1.secomtrust.net/spcpp/pfw/pfwsr3ca/	n

	[2]policyIdentifier=2.23.140.1.2.2	
CRL Distribution Points	http://repo1.secomtrust.net/spcpp/pfw/pfwsr3ca/fullcrl2.crl	n
Authority Information Access	accessMethod ocsp (1 3 6 1 5 5 7 48 1) accessLocation http://sr30.ocsp.secomtrust.net	n
Authority Key Identifier	SHA-1 hash value of authority Public Key (160 bits)	n
Subject Key Identifier	SHA-1 hash value of the subject Public Key (160 bits)	n
Certificate Transparency Extension (1.3.6.1.4.1.11129.2.4.2)	SignedCertificateTimestampList value	n

Table 7.1-2 SECOM Passport for Web SR 3.0 CA Server Certificate Profile

Basic Fields		Settings	critical
Version		Version 3	-
Serial Number		e.g.) 0123456789	-
Signature Algorithm		sha256 With RSA Encryption	-
Issuer	Country	C=JP	-
	Organization	O=SECOM Trust Systems CO.,LTD.	-
	Common Name	CN= SECOM Passport for Web SR 3.0 CA	-
Validity	NotBefore	e.g.) 2018/3/1 00:00:00 GMT	-
	NotAfter	e.g.) 2019/3/5 00:00:00 GMT	-
Subject	Country	C=JP (Fixed value)	-
	Organization	SECOM Trust Systems CO.,LTD. (Fixed value)	-
	Common Name	OCSP Server name (Required)	-
Subject Public Key Info		Subject Public Key 2048 bits	-
Extension Fields		**Settings**	**critical**
keyUsage		digitalSignature	y
extendedKeyUsage		OCSPSigning	n
OCSP No Check		null	n
CertificatePolicies		policyIdentifier	n

	OID=1.2.392.200091.100.751.1 policyQualifiers policyQualifierId=CPS qualifiier=https://repo1.secomtrust.net/spcpp/pfw/pfwsr3ca/	
Authority Key Identifier	SHA-1 hash value of authority Public Key (160 bits)	n
Subject Key Identifier	SHA-1 hash value of the subject Public Key (160 bits)	n

7.1.1 Version Number(s)

This CA applies version 3.

7.1.2 Certificate Extension

Certificates issued by this CA use certificate extension fields.

7.1.3 Algorithm Object Identifier

The algorithm OID used in this service is as follows:

Algorithm	Object Identifier
sha256 With RSA Encryption	1.2.840.113549.1.1.11
RSA Encryption	1 2 840 113549 1 1 1

7.1.4 Name Format

This CA and the subscribers are uniquely identified by the DN defined according to the X.500 distinguished name.

7.1.5 Name Constraints

Set in the CA as necessary.

7.1.6 Certificate Policy Object Identifier

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

7.1.7 Use of Policy Constraint Extensions

Not set.

7.1.8 Policy Qualifier Syntax and Semantics

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

7.1.9 How to interpret Critical Certificate Policy Extensions

Not set.

7.2 CRL Profile

CRLs issued by the CA conform to RFC5280, the profile of which are indicated in the tables below.

Table 7.2-1 SECOM Passport for Web SR 3.0 CA CRL Profile

Basic Fields		Settings	critical
Version		Version 2	-
Signature Algorithm		SHA256 with RSAEncryption	-
Issuer	Country	C=JP	-
	Organization	O= SECOM Trust Systems CO.,LTD.	-
	Common Name	CN= SECOM Passport for Web SR 3.0 CA	-
This Update		e.g.) 2018/3/1 00:00:00 GMT	-
Next Update		e.g.) 2018/3/5 00:00:00 GMT Update interval =24H, Validity period =96H	-
Revoked Certificates	Serial Number	e.g.) 0123456789	-
	Revocation Date	e.g.) 2018/3/1 00:00:00 GMT	-
	Reason Code	Circumstances of revocation (unspecifiled, etc.)	-
Extension Fields		Settings	critical
CRL Number		CRL number	n
Authority Key Identifier		SHA-1 hash value of authority Public Key (160 bits)	n

7.2.1 Version Number(s)

The CA applies CRL version 2.

7.2.2 Certificate Revocation Lists and CRL Entry Extensions

Use the CRL extension field issued by this CA.

7.3 OCSP Profile

The CA operates the OCSP server in compliance with RFC5019 and 6960.

7.3.1 Version Number(s)

The CA uses OCSP Version 1.

7.3.2 OCSP Extensions

Refer to “7.1 Certificate Profile”.

8. Compliance Audit and Other Assessments

The CA performs audits from time to time to examine if the operation thereof is in compliance with this CP and the CPS. Provisions for the compliance verification audits thereof are set forth in this CP and the CPS.

8.1 Frequency and Circumstances of Assessment

SECOM Trust Systems performs compliance audits at least once a year to examine if the operation of the services is in compliance with this CP and the CPS.

8.2 Identity/Qualifications of Assessor

The compliance audits of the CA shall be performed by auditors with solid proficiency in the CA operations.
The audit of the WebTrust-certified CA shall be performed by an auditing firm.

8.3 Assessor's Relationship to Assessed Entity

Auditors to be appointed shall be those who have no special interests in SECOM Trust Systems.

8.4 Topics Covered by Assessment

Audits are performed with respect to business activities for operation of the CA.
Audits may also be performed, conforming to the standards for CA set forth in WebTrust for CA and WebTrust for BR.

8.5 Actions Taken as a Result of Deficiency

SECOM Trust Systems promptly implements corrective measures with respect to the deficiencies identified in the audit report.

8.6 Communication of Results

Audit reports are reported to the Certification Services Improvement Committee. Audit reports are retained and managed to allow access only by the authorized parties.
Verification reports based on WebTrust for CA and WebTrust for BR are made available on a specific website conforming to the rules thereof.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Fees for Issuing or Renewing Certificates

Stipulated separately in contracts.

9.1.2 Certificate Access Fee

No stipulation.

9.1.3 Expiration or Access Fee for Status Information

No stipulation.

9.1.4 Fees for Other Services

No stipulation.

9.1.5 Refund Policy

Stipulated separately in contracts.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

SECOM Trust Systems shall maintain a sufficient financial resources for the operation and maintenance of the CA.

9.2.2 Other Assets

No stipulation.

9.2.3 End entity Insurance or Warranty coverage

No stipulation.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

Relevant provisions are stipulated in the CPS.

9.3.2 Information Not Within the Scope of Confidential Information

Relevant provisions are stipulated in the CPS.

9.3.3 Responsibility to Protect Confidential Information

Relevant provisions are stipulated in the CPS.

9.4 Privacy of Personal Information

9.4.1 Personal Information Protection Plan

Relevant provisions are stipulated in the CPS.

9.4.2 Information Treated as Personal Information

Relevant provisions are stipulated in the CPS.

9.4.3 Information that is not considered Personal Information

Relevant provisions are stipulated in the CPS.

9.4.4 Responsibility for protecting Personal Information

Relevant provisions are stipulated in the CPS.

9.4.5 Notice and Consent regarding use of Personal Information

Relevant provisions are stipulated in the CPS.

9.4.6 Information Disclosure with Judicial or Administrative Procedures

Relevant provisions are stipulated in the CPS.

9.4.7 Other Information Disclosure Conditions

Relevant provisions are stipulated in the CPS.

9.5 Intellectual Property Rights

The following copyrighted materials are the property of SECOM Trust Systems.

- this CP;
- SECOM Trust Systems stickers and the sticker certification pages

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

SECOM Trust Systems bears the obligation to perform the following in the execution of its duties as a CA:

- Secure generation and management of CA Private Keys
- accurate issuance, revocation and administration of Certificates reflecting the issuance requests by the RA;
- management and operational monitoring of the systems;
- issuance and publication of CRLs;
- provision of access to the OCSP server; and
- maintenance and administration of the Repository.

9.6.2 RA Representations and Warranties

SECOM Trust Systems bears the obligation to perform the following in the execution of its duties as an RA:

- Installation and operation of registration terminals in a secure environment;
- accurate review of Certificate Applications, including identification and authentication, in issuing Certificates;
- Provision of prompt and accurate instructions on issuance, revocation and other Certificate-related actions

9.6.3 Subscriber Representations and Warranties

Subscribers shall bear obligations to:

- provide accurate and complete information in submitting a Certificate Application;
- promptly notify SECOM Trust Systems of any change in the information provided therein;
- protect their own Private Keys against compromise;
- use the Certificates conforming to the provisions of the Service Terms and this CP; and
- promptly request SECOM Trust Systems to revoke the Subscriber Certificate in case the Subscriber determines that the Private Key corresponding to the Public Key indicated therein has or may have been compromised, or there has been a change in the registered information.

9.6.4 Relying Party Representations and Warranties

Relying Parties shall bear the obligations to:

- authenticate the validity of the CA Certificate;
- authenticate the validity of the Subscriber Certificate by checking the validity period thereof to ensure that it has not expired and that it is not registered as a revoked Certificate in the CRL or on the OCSP server; and
- determine whether or not to trust the Subscriber information on their own responsibilities.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimer of Warranties

SECOM Trust Systems is not liable for any direct, special, incidental or consequential damages arising in connection with the warranties stipulated in "9.6.1 CA Representations and Warranties" and "9.6.2 RA Representations and Warranties" hereof, or for lost earnings, loss of data, or any other indirect or consequential damages.

9.8 Limitations of Liability

SECOM Trust Systems is not liable for the provisions of "9.6.1 CA Representations and Warranties" and "9.6.2 RA Representations and Warranties" hereof in any of the following cases:

- Any damage arising from unlawful conduct, unauthorized use, negligence or any other cause not attributable to SECOM Trust Systems;
- any damage attributable to the failure of a Subscriber to perform its obligations;
- any damage attributable to a Subscriber system;
- damages attributable to the defect or malfunction or any other behavior of the Subscriber environment (hardware or software);
- damages caused by information published in a Certificate, a CRL or on the OCSP server due to the reasons not attributable to SECOM Trust Systems;
- any damage incurred in an outage of the normal communication due to reasons not attributable to SECOM Trust Systems;
- any damage arising in connection with the use of a Certificate, including transaction debts;
- damages attributable to improvement, beyond expectations at this point in time, in hardware or software type of cryptographic algorithm decoding skills; and

- any damage attributable to the suspension of the CA's operations due to force majeure, including, but not limited to, natural disasters, earthquakes, volcanic eruptions, fires, tsunami, floods, lightning strikes, wars, civil commotion and terrorism.

9.9 Indemnities

SECOM Trust Systems shall compensate a Subscriber for the damages incurred thereby for reasons attributable to a Certificate in an amount not to exceed the contract fees received and equal to the fees for the remaining months of the contract period (period of less than one month is rounded off) and shall not be liable in any other way.

9.10 Term and Termination

9.10.1 Term

This CP goes into effect upon approval by the Certification Services Improvement Committee.

This CP will not be invalidated under any circumstances prior to the termination stipulated in "9.10.2 Termination" hereof.

9.10.2 Termination

This CP loses effect as of the termination hereof by SECOM Trust Systems with the exception of the provisions stipulated in "9.10.3 Effect of Termination and Survival".

9.10.3 Effect of Termination and Survival

Even in the event of termination of the use of a Certificate by a Subscriber or the termination of a service provided by SECOM Trust Systems, provisions that should remain in effect, due to the nature thereof, shall survive any such termination, regardless of the reasons therefor, and remain in full force and effect with respect to any Subscriber and the CA.

9.11 Individual Notices and Communications with Participants

SECOM Trust Systems provides the necessary notices to Subscribers and Relying Parties through its website, e-mail or in other written forms.

9.12 Amendments

9.12.1 Procedure for Amendment

This CP shall be revised by SECOM Trust Systems as appropriate and goes into effect upon approval by its Certification Services Improvement Committee.

9.12.2 Notification Method and Timing

Whenever this CP is modified, the prompt publication of the modified CP shall be deemed as the notification thereof to the participants.

9.12.3 Circumstances under Which OID Must Be Changed

OID shall be changed if the Certification Service Improvement Committee determines that it is necessary.

9.13 Dispute Resolution Procedures

A party seeking to file a lawsuit, request arbitration or take any other legal action against SECOM Trust Systems for the resolution of a dispute relating to a Certificate issued by the CA, said party shall notify SECOM Trust Systems to this effect in advance. As regards the location for arbitration and court proceedings, a dispute settlement institution located within Tokyo shall have exclusive jurisdiction.

9.14 Governing Law

The laws of Japan will apply to any dispute concerning the interpretation or validity of this CP and the CPS, as well as the use of the Certificates.

9.15 Compliance with Applicable Law

The CA shall handle cryptographic hardware and software in compliance with relevant export regulations of Japan.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

SECOM Trust Systems comprehensively stipulates the obligations of Subscribers and Relying Parties and other relevant matters in this CP, the Service Terms and CPS, for provision of the services. Any agreement otherwise, whether oral or written, shall have no effect.

9.16.2 Assignment

When assigning the services to a third party, SECOM Trust Systems may assign its responsibilities and other obligations specified in this CP, the Service Terms and CPS.

9.16.3 Severability

Even if any provision of this CP, the Service Terms and CPS is deemed invalid, all other provisions stipulated therein shall remain in full force and effect.

9.16.4 Enforcement

Disputes regarding this service shall be governed by the Tokyo District Court, and SECOM Trust Systems may request the parties for compensation and attorney's fees for disputes arising from the contractual provisions of the respective regulatory documents, damages, losses and costs related to the parties' actions.

9.16.5 Irresistible Force

SECOM Trust Systems shall not be liable for any damages caused by natural disasters, earthquakes, eruptions, fires, tsunamis, floods, lightning strikes, disturbances, terrorism, or any other force majeure, whether or not foreseeable. If it becomes impossible to provide this CA, SECOM Trust Systems may suspend this CA until the situation stops.

9.17 Other Provisions

No stipulation