Security Communication RootCA

Time-Stamp Service Certificate Policy

September 29, 2020
Version 5.04

SECOM Trust Systems Co., Ltd.

Version History		
Version Number	Date	Description
V1.00	2004.11.08	Publication of the first version
V2.00	2006.05.22	"SECOM TrustNet" was renamed to "SECOM Trust Systems" after the merger. "SECOM TrustNet Security Policy Committee" was renamed as "Certification Services Improvement Committee."
V3.00	2009.05.29	Major version upgrade Renaming of "Security Communication RootCA1 Time-Stamp Service Certificate Policy" to "Security Communication RootCA Time-Stamp Service Certificate Policy" and addition of the CA Private Key "Security Communication RootCA2"
V4.00	2016.06.01	Major version upgrade Addition of the CA Private Key "Security Communication RootCA3" Addition of the CA Private Key "Security Communication ECC RootCA1"
V5.00	2017.01.20	Amendment associated with commencement of the OCSP server operations Overall revision of the styles
V5.01	2018.11.28	Overall revision of the descriptions and styles
V5.02	2019.05.24	Overall revision of the descriptions and styles
V5.03	2020.03.30	Revised chapters and added some " No Stipulation" content
V5.04	2020.09.29	Revision of CRL basic area

Table of Contents

1. Introduction

1.1 Overview

Security Communication RootCA Time-Stamp Service Certificate Policy (hereinafter, "this CP") is a document that defines operational policies for the TA (Time Authority) certificates and TSA (Time-Stamping Authority) certificates (hereinafter collectively, "Certificates") issued by Security Communication RootCA1, Security Communication RootCA2, Security Communication RootCA3 as well as Security Communication ECC RootCA1 (hereinafter collectively, "the CAs") that are all operated by SECOM Trust Systems Co., Ltd. (hereinafter, "SECOM"), by specifying the purpose of use, the scope of application and the user procedures for the Certificates. Various procedures regarding the operation and maintenance of the CAs are stipulated in the Security Communication RootCA Certification Practice Statement (hereinafter, "CPS").

SECOM provides the certification services as the CAs, including the CA key administration as well as issuance/revocation of Certificates (hereinafter, "the Services"). The Certificates issued by the CAs prove and certify the unique correspondence between the subjects of the issuance and their public keys.
The CAs conform to the CA/Browser Forum provisions disclosed at https://www.cabforum.org/.

Any provisions in this CP inconsistent with the CPS shall prevail and any provisions in a separate agreement or the like between the subscribers and SECOM inconsistent with this CP or the CPS shall prevail.

This CP shall be revised as necessary in order to reflect any technical or service developments or improvements pertaining to the CA operations.
This CPS 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 "Security Communication RootCA Time-Stamp Service Certificate Policy". SECOM, which is the provider and operational body of the Services, uses the Object IDentifier (hereinafter, "OID") assigned by ISO, given in the Table "1.2-1 OID (SECOM)" below.

Table 1.2-1 OID (SECOM)

Name of organization	OID
SECOM Trust Systems Co., Ltd.	1.2.392.200091

This CP is identified with the Object IDentifier (hereinafter, "OID") given in "Table 1.2-2 OID (This CP)"

Table 1.2-2 OID (This CP)

CP	OID
Security Communication RootCA1	1.2.392.200091.100.901.2
Security Communication RootCA2	1.2.392.200091.100.901.5
Security Communication RootCA3	1.2.392.200091.100.901.7
Security Communication ECC RootCA1	1.2.392.200091.100.902.2

The OID of the CPS associated with this CP is given in Table 1.2-3 OID (The CPS)

Table 1.2-3 OID (The CPS)

CPS	OID
Security Communication RootCA Certification Practice Statement	1.2.392.200091.100.901.3

1.3 PKI Participants

1.3.1 Certification Authorities

A CA mainly issues or revokes Certificates, publishes CRLs (Certificate Revocation Lists), and stores and provides information on Certificate status using the OCSP server.

1.3.2 Registration Authorities

An RA mainly performs identification, authentication, as well as assessment of the operation rules of the Certificate applicant organizations or institutions when such a Certificate request as issuance or revocation is submitted.

1.3.3 Subscribers

Subscribers are organizations or institutions that generate Key Pairs in their own rights, to which Certificates are issued by the CAs. They are qualified as Subscribers upon accepting the Certificates issued by the CAs after submitting the Certificate applications thereto. Subscribers must assess this CP and the CPS in light of their usage purposes, and agree thereto.

1.3.4 Relying Parties

Relying Parties are the entities that authenticate the validity of Certificates issued by the CAs. Relying Parts are assumed to be performing the authentication and placing trust upon confirming and agreeing to the contents of this CP and the CPS in light of the Relying Parties' own purposes of use.

1.3.5 Other Participants

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

The CAs are the Certification Authorities functioning as top of the Subordinate CAs and issue the Certificates (TA, TSA) as Subscriber certificates. Relying Parties that trust and use the Certificates may authenticate the reliability of such Certificates using the CA public key Certificates.

1.4.2 Prohibited Certificate Uses

Certificates issued by the CAs may not be used for purposes other than those set forth in this CP.

1.5 Policy Administration

1.5.1 Organization Administering the Document

This CP is maintained and administered by SECOM.

1.5.2 Contact Information

Inquiries concerning this CP should be directed to:

	CA Support Center, SECOM Trust Systems Co., Ltd.
Address:	8-10-16 Shimorenjaku, Mitaka-shi, Tokyo 181-8528
E-mail Address	ca-support@secom.co.jp

1.5.3 Person Determining CP Suitability for the Policy

Suitability of this CP as the CAs' practice policy is determined by SECOM's Certification Services Improvement Committee.

1.5.4 Approval Procedure

This CP shall be published in the repository as developed and revised under approval of the SECOM Certification Services Improvement Committee.

1.6 Definitions and Acronyms

A～Z

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.

CA

CA stands for Certification Authority, an entity that mainly issues, renews and revokes Certificates, generates and protects CA Private Keys, and registers Subscribers.

CA/Browser Forum

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

Certificate

The word "Certificate" is simply used to indicate a digital certificate in this CPS, which is the electronic data certifying that a public key is owned by the party specified therein. The validity of a Certificate is certified by the digital signature of the relevant CA affixed thereto.

Certification Services Improvement Committee

The decision making body for the operational policy of the Services, including administration of this CP and modification reviews.

CP

CP stands for Certificate Policy, a document that sets forth the policy regarding the Certificates.

CPS

CPS stands for Certification Practice Statement, which sets forth provisions to be followed in providing and subscribing to the Services, including applications of digital Certificates, application reviews, and issuance/revocation/storage/publication of Certificates by the CAs.

CRL

CRL stands for Certificate Revocation List, which records the list of Certificates revoked by the CAs.

CSR

CSR stands for Certificate Signing Request, a data file on which the digital certificate issuance is based. A CSR contains the public key of the entity requesting the

Certificate signing, to which the issuer's digital signature is affixed upon the issuance thereof.

Digital Signature/Signing

A digital data to prove that a specific individual is the author of a specific digital documentation. It is a signature representing that the reliability of the information contained in such documentation is certified by the author.

Escrow

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

Key Pair

A Key Pair consists of a private key and a public key in the public key cryptosystem.

Major Version Number

A number to be given to a revision of this CP (e.g., the underlined digit [1] of Version 1.02) whose magnitude of the amendment(s) thereof is considered to have an obvious impact on the use of the Certificates and the CRLs by Subscribers and Relying Parties.

Minor Version Number

A number to be given to a revision of this CP (e.g., the underlined digit [02] of Version 1.02) whose magnitude of the amendment(s) thereof is considered to have no or less impact on the use of the Certificates and the CRLs by Subscribers and Relying Parties.

OCSP (Online Certificate Status Protocol)

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

OID

OID stands for Object IDentifier. OIDs are registered in the registration institutions (ISO and ITU) as globally unique IDs. The IDs registered as OIDs are used for such parameters as algorithms used in the PKI, types (attributes like [Country name]) of the names (subject) to be included in the digital Certificates.

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 comprising a Key Pair used in the public key cryptosystem, which corresponds to a public key and is possessed only by the relevant Subscriber.

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.

RA

RA stands for Registration Authority, an entity that conducts qualifications (identification and authentication) among the CA operations in the Services.

Repository

The storage for such data as Certificates issued by the CAs. The Repository is a mechanism to allow access by the users or applications to the Certificates from any point in the network. CRLs as well as this CP are also stored in the Repository.

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-2

A Secure Hash Algorithm family function used in digital signing and the improved version of SHA-1. The size of the SHA-256 and SHA-384 described in this CP are respectively 256 and 384 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

Information containing digital data and the clock time information that may be used as the instrument of proof or the information leading to the evidence that the data existed before that time (proof of existence) and that the data have not been modified or falsified between the stamped time and the authenticated time (proof of authenticity).

In the Services, Certificates are issued to TSA (Time-Stamping Authority), and to TA (Time Authority) that conducts delivery of standard time and time audits to TSA.

X.500

X.500 is a series of directory standards that was developed by ITU-T in order to provide a range of services from the name and address lookup to the query by attribute value. The X.500 Distinguished Names (DN) will be used for the names of the X.509 Issuers and Subjects.

X.509

The Certificate and CRL formats set forth by X.509 ITU-T. With [X.509 v3 (Version 3)], extension fields were additionally defined for storage of optional data.

2. Publication and Repository Responsibilities

2.1 Repository
Stipulated in the CPS.

2.2 Publication of Certificate Information
Stipulated in the CPS.

2.3 Time or Frequency of Publication
Stipulated in the CPS.

2.4 Access Controls on Repositories
Stipulated in the CPS.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

The Certificate issuer name and the name of the issuance subject Subscriber are configured according to the X.500 Distinguished Name (DN) format as well as provisions in "7.1.4 Name Forms" hereof.

3.1.2 Need for Names to Be Meaningful

The Distinguished Names assigned to Subscribers shall be meaningful, and the Subjects' names specified in Certificates shall have association with the organizations or the institutions to an appropriate extent.
Subscribers shall not submit Certificate applications with third parties' trademarks or associated names to the CAs.

3.1.3 Anonymity or Pseudonymity of Subscribers

No anonym nor pseudonym shall be used as Subject names specified in Certificates.

3.1.4 Rules for Interpreting Various Name Forms

DNs are interpreted as defined in "3.1.1 Types of Names" and "3.1.2 Need for Names to Be Meaningful" hereof.

3.1.5 Uniqueness of Names

The uniqueness of each subject name in Certificates shall be enforced across the Certificates issued by the CAs.

3.1.6 Recognition, Authentication, and Roles of Trademarks

Rights to use the trademarks shall be reserved by the trademark owners. The CAs may, as necessary, require the trademark owners to present such official documentation as the submission for the trademark.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The signature on the relevant CSR made by a Certificate applicant is authenticated to prove that such CSR is signed with the Private Key corresponding to the Public Key contained therein. In addition, the fingerprint of the CSR is inspected to identify the Public Key owner.

3.2.2 Authentication of Organization Identity

Certificate applicants shall provide the CAs with the following information in submitting a Certificate Application:

- Certificate Application Form;
- records or information to prove the (legal) existence of the organization or institution;
- CSR; and
- other documentation required by SECOM.

The CAs use the provided information to make sure that there is no inaccuracy or missing information in the application.

3.2.3 Authentication of Individual Identity

The CAs will not issue Certificates to individuals.

3.2.4 Non-Verified Subscriber Information

The CAs will not verify "Organizational Unit" with the documentary submission of the Certificate application by Subscribers and the CSR information.

3.2.5 Validation of Authority

Representatives, employees or agents of Certificate applicant organizations or institutions who submit information about such organizations or institutions are authenticated by the CAs to prove that they have the legitimate authority to do so.

3.2.6 Criteria for Interoperation

This CA issues a unilateral cross-certificate to the CA identified and authenticated by this CA based on this CP.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

The procedure set forth in "3.2 Initial Identity Validation" hereof shall be followed.

3.3.2 Identification and Authentication for Re-Key after Revocation

The procedure set forth in "3.2 Initial Identity Validation" hereof shall be followed.

3.4 Identification and Authentication for Revocation Requests

When a Certificate revocation request is accepted, legitimacy of the request is authenticated by the CAs based on the submitted Subscriber information.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

A Certificate Application can be submitted by representatives, employees or agents of the applicant organizations or institutions.

4.1.2 Enrollment Process and Responsibilities

Applicants shall follow the procedure notified by the CAs in advance in submitting the Certificate Applications. In doing so, the applicants are assumed to have agreed to the provisions in this CP, the CPS, and other documents disclosed by the CAs.
The applicants must certify that the Certificate Application information submitted to the CAs is accurate.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Accepting the applications by the Certificate applicants, the documentary submissions as well as the CSR are authenticated by the CAs in accordance with "3.2 Initial Identification and Authentication" hereof.

4.2.2 Approval or Rejection of Certificate Applications

The CAs decide approval or rejection of the Certificate Applications according to the prescribed authentication procedure for the Certificate applicant submissions, and notify the applicants of the results thereof.

4.2.3 Time to Process Certificate Applications

The CAs promptly issue Certificates once the CSRs submitted by the Certificate applicants are approved.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

The CAs issue Certificates containing the CA Private Key signature for the Public Key of the CSR submitted by the Certificate applicants conforming to "7.1 Certificate Profile" hereof.

4.3.2 Notifications to Subscriber of Certificate Issuance

After completing the issuance of Certificates for approved Certificate Applications, the

CAs store the issued Certificates on such external memory media, seal them together with the receipts, and then personally deliver or just send them to the Subscriber applicants.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Subscribers must send the receipts to the CAs upon confirming how the Certificate is populated and no deficiency therein, while the CAs assume the Certificate Acceptance is complete upon receiving such receipts. The Certificate applicants must promptly notify the CAs if any deficiency is found in how the Certificate is populated. Any claims thereon must be made within fourteen (14) days of the date the Certificate is sent.

4.4.2 Publication of the Certificate by the CA

The Certificates issued by the CAs are published in the Repository.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

The CAs will not issue Certificates to individuals.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

The usage of Certificates issued by the CAs and Private Keys possessed by Subscribers is restricted to those specified for the services and products provided by the Subscribers of the CAs having contractual relationship with SECOM. Certificates issued by the CAs shall not be used otherwise.

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 and authenticating the Certificates issued by the CAs.

4.6 Certificate Renewal

The CAs do not accept Certificate Renewal without Subscriber Key Pair re-keying. In renewing a Certificate, a new Key Pair shall be generated, following the procedure set forth in "4.7 Certificate Re-Key".

4.6.1 Circumstances for Certificate Renewal

Refer to this CP "4.7.1 Circumstances for Certificate Re-Key ".

4.6.2 Who May Request Renewal
Refer to this CP "4.7.2 Who May Request Certification of a New Public Key ".

4.6.3 Processing Certificate Renewal Requests
Refer to this CP "4.7.3 Processing Certificate Re-Keying Requests ".

4.6.4 Notification of New Certificate Issuance to Subscriber
Refer to this CP "4.7.4 Notification of New Certificate Issuance to Subscriber ".

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate
Refer to this CP "4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate ".

4.6.6 Publication of the Renewal Certificates by the CA
Refer to this CP "4.7.6 Publication of the Re-Keyed Certificate by the CA ".

4.6.7 Notification of Certificate Issuance by the CA to Other Entities
Refer to this CP "4.7.7 Notification of Certificate Issuance by the CA to Other Entities ".

4.7 Certificate Re-Key

4.7.1 Circumstances for Certificate Re-Key
A Certificate is Re-Keyed when the validity period of the Certificate is about to expire or when the Certificate is revoked due to the key compromise.

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 "4.2 Certificate Application Processing" 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

4.8.1 Circumstances for Certificate Modification
If any of the descriptions in a Certificate has to be modified, the Subscriber must promptly submit a Certificate Modification application. Procedures for the revocation and initial issuance shall be followed as the procedure for re-issuance by the modification.

4.8.2 Who May Request Certificate Modification
The provisions of "4.9.2 Who Can Request Revocation" and "4.1.1 Who Can Submit a Certificate Application" hereof shall apply.

4.8.3 Processing Certificate Modification Requests
The provisions of "4.9.3 Procedure for Revocation Request" and "4.2 Certificate Application Processing" hereof shall apply.

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

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

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

4.8.7 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.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Certificate Revocation
Subscribers may request a Certificate Revocation based on their own decisions, provided that they must always request the revocation to the CAs in any of the following cases:

- There has been a change in information populated in the Certificate;
- the Private Key has or may have been compromised or no longer reliable for any reason, including the theft, loss, unauthorized disclosure or unauthorized use thereof;
- the Private Key has or may have been compromised to have lost the privacy or confidentiality.
- the Certificate is incorrectly populated or not being used for authorized purposes; or
- the use of the Certificate is being terminated.

The CAs may revoke the Certificate with or without the Subscriber's revocation request when the CAs are aware of the following situations:

- The Subscriber is not performing the obligations thereof under this CP, the CPS, relevant agreements or laws;
- SECOM terminates the Services;
- it is determined that the CA Private Key has or could have been compromised; or
- the CAs recognize any other situation deemed to necessitate revocation.

4.9.2 Who Can Request Revocation

Certificate Revocation can be requested by representatives, employees or agents of the applicant organizations or institutions.

4.9.3 Procedure for Revocation Request

Certificate Revocation Request shall be submitted by post-mailing the information required for the revocation to the CAs. However, e-mail submission is allowed as an alternative in an emergency or when the said submission option is not available.

4.9.4 Revocation Request Grace Period

Revocation Requests due to other than Private Key compromise shall be submitted to the CAs five (5) operational days prior to the desired revocation date. However, should a Subscriber determine that a Private Key has or could have been compromised, the Subscriber must promptly make a revocation request after identifying the compromise.

4.9.5 Time within Which CA Shall Process the Revocation Request

The CAs promptly revoke a Certificate upon accepting a valid Certificate Revocation Request.

4.9.6 Revocation Checking Requirements for Relying Parties

Before placing trust and using a Certificate issued by the CAs, Relying Parties must confirm that the Certificate has not been revoked by checking the CRLs or the OCSP server.

4.9.7 CRL Issuance Frequency
A new CRL is issued within a year from the latest CRL issuance as well as when a Certificate issuance or revocation is made.

4.9.8 Maximum Latency for CRLs
A new CRL is promptly issued upon issuance or revocation of a Certificate and is published in the Repository.
The CAs publishes the revocation reason together with the CRL in the Repository.

4.9.9 On-Line Revocation/Status Checking Availability
Certificate status information is provided online via the OCSP server.

4.9.10 On-Line Revocation/Status Checking Requirements
Before placing trust and using a Certificate issued by the CAs, Relying Parties must confirm the validity of the Certificate. If registered revocation is not confirmed with the CRL in the Repository, the Certificate Status provided through the OCSP server shall be checked.

4.9.11 Other Forms of Revocation Advertisements Available
This 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 usage rules 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 this CP "4.9.1 Circumstances for Certificate Revocation ".

4.9.13 Circumstances for Suspension
The CAs 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 Parties for confirmation through the OCSP server.

4.10.2 Service Availability

The CAs maintain and manage 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)

In terminating subscription of the Services, Subscribers are required to proceed with the service subscription termination procedure set forth in the relevant agreement therefor or the like.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

The CAs will not Escrow the CA 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

5.1.1Site Location and Construction
Stipulated in the CPS.

5.1.2 Physical Access
Stipulated in the CPS.

5.1.3 Power and Air Conditioning
Stipulated in the CPS.

5.1.4 Water Exposures
Stipulated in the CPS.

5.1.5 Fire Prevention and Protection
Stipulated in the CPS.

5.1.6 Media Storage
Stipulated in the CPS.

5.1.7 Waste Disposal
Stipulated in the CPS.

5.1.8 Off-Site Backup
Stipulated in the CPS.

5.2 Procedural Controls

5.2.1 Trusted Roles
Stipulated in the CPS.

5.2.2 Number of Persons Required per Task
Stipulated in the CPS.

5.2.3 Identification and Authentication for Each Role
Stipulated in the CPS.

5.2.4 Roles Requiring Separation of Duties
Stipulated in the CPS.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements
Stipulated in the CPS.

5.3.2 Background Check Procedures
Stipulated in the CPS.

5.3.3 Training Requirements
Stipulated in the CPS.

5.3.4 Retraining Frequency and Requirements
Stipulated in the CPS.

5.3.5 Job Rotation Frequency and Sequence
Stipulated in the CPS.

5.3.6 Sanctions for Unauthorized Actions
Stipulated in the CPS.

5.3.7 Independent Contractor Requirement
Stipulated in the CPS.

5.3.8 Documentation Supplied to Personnel
Stipulated in the CPS.

5.4 Audit Logging Procedures

5.4.1Types of Events Recorded
Stipulated in the CPS.

5.4.2 Frequency of Processing Audit Log
Stipulated in the CPS.

5.4.3 Retention Period for Audit Log
Stipulated in the CPS.

5.4.4 Protection of Audit Log
Stipulated in the CPS.

5.4.5 Audit Log Backup Procedure
Stipulated in the CPS.

5.4.6 Audit Log Collection System
Stipulated in the CPS.

5.4.7 Notification to Event-Causing Subject
Stipulated in the CPS.

5.4.8 Vulnerability Assessments
Stipulated in the CPS.

5.5 Records Archival

5.5.1 Types of Records Archived
Stipulated in the CPS.

5.5.2 Retention Period for Archive
Stipulated in the CPS.

5.5.3 Protection of Archive
Stipulated in the CPS.

5.5.4 Archive Backup Procedures
Stipulated in the CPS.

5.5.5 Requirements for Time-Stamping of Records
Stipulated in the CPS.

5.5.6 Archive Collection System
Stipulated in the CPS.

5.5.7 Procedures to Obtain and Verify Archive Information
Stipulated in the CPS.

5.6 Key Changeover
Stipulated in the CPS.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

Stipulated in the CPS.

5.7.2 Hardware, Software, and/or Data are Corrupted

Stipulated in the CPS.

5.7.3 Entity Private Key Compromise Procedures

Stipulated in the CPS.

5.7.4 Business Continuity Capabilities after a Disaster

Stipulated in the CPS.

5.8 CA or RA Termination

Stipulated in the CPS.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation
Stipulated in the CPS.

6.1.2 Private Key Delivery to Subscriber
Stipulated in the CPS.

6.1.3 Public Key Delivery to Certificate Issuer
Stipulated in the CPS.

6.1.4 CA Public Key Delivery to Relying Parties
Stipulated in the CPS.

6.1.5 Key Sizes
Stipulated in the CPS.

6.1.6 Public Key Parameters Generation and Quality Checking
Stipulated in the CPS.

6.1.7 Key Usage Purposes
Stipulated in the CPS.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls
Stipulated in the CPS.

6.2.2 Private Key Multi-Person Control
Stipulated in the CPS.

6.2.3 Private Key Escrow
Stipulated in the CPS.

6.2.4 Private Key Backup
Stipulated in the CPS.

6.2.5 Private Key Archive
Stipulated in the CPS.

6.2.6 Private Key Transfer into or from a Cryptographic Module
Stipulated in the CPS.

6.2.7 Private Key Storage on Cryptographic Module
Stipulated in the CPS.

6.2.8 Method of Activating Private Key
Stipulated in the CPS.

6.2.9 Method of Deactivating Private Key
Stipulated in the CPS.

6.2.10 Method of Destroying Private Key
Stipulated in the CPS.

6.2.11 Cryptographic Module Rating
Stipulated in the CPS.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival
Stipulated in the CPS.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods
Stipulated in the CPS.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation
Stipulated in the CPS.

6.4.2 Activation Data Protection
Stipulated in the CPS.

6.4.3 Other Aspects of Activation Data
Stipulated in the CPS.

6.5 Computer Security Controls
Stipulated in the CPS.

6.5.1 Specific Computer Security Technical Requirements
Stipulated in the CPS.

6.5.2 Computer Security Rating
Stipulated in the CPS.

6.6 Life-Cycle Technical Controls

6.6.1 System Development Controls
Stipulated in the CPS.

6.6.2 Security Management Controls
Stipulated in the CPS.

6.6.3 Life-Cycle Security Controls
Stipulated in the CPS.

6.7 Network Security Controls
Stipulated in the CPS.

6.8 Time-Stamping
Stipulated in the CPS.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

Certificates issued by the CAs are generated in the X.509 Certificate Format, using the fields specified in Table 7.1-1 Basic Certificate Profile Fields.

Table 7.1-1 Basic Certificate Fields

Field	Description
Version (Version number)	Certificate Format Number *1
SerialNumber (Serial number)	Unique numbers across the CAs *2
Signature (Digital Signature algorithm identifier)	Identifier of the Digital Signature algorithm used in the Services *3
Issuer (Name of the issuer)	Information about the issuer (specified by the CAs)
Validity (Operational/validity period)	Operational or validity period of the Certificate (From/to dates)
Subject (Name of the Subscriber)	Subscriber information
SubjectPublicKeyInfo (Information of the Subscriber Public Key)	The Public Key algorithm identifier and the Public Key data of the Subscriber
Extensions (Extension fields)	See "7.1.2 Certificate Extensions" hereof.

*1 The Certificate format number is set to Version3.

*2 Appended by a CA server when a Certificate is newly created.

*3 Used when digitally signing a Certificate.

7.1.1 Version Number(s)

The X.509 Format version number of Certificates issued by the CAs is Version3.

7.1.2 Certificate Extensions

TSA Certificates issued by the CAs use the X.509 Certificate Extension fields specified in:

Table "7.1-2 Security Communication RootCA1 Certificate Extensions";

Table "7.1-3 Security Communication RootCA2 Certificate Extensions";

Table "7.1-4 Security Communication RootCA2 OCSP Server Certificate Extensions";

Table "7.1-5 Security Communication RootCA3 Certificate Extensions";

Table "7.1-6 Security Communication RootCA3 OCSP Server Certificate Extensions";

Table "7.1-7 Security Communication ECC RootCA1 Certificate Extensions"; and

Table "7.1-8 Security Communication ECC RootCA1 OCSP Server Certificate Extensions".

Table 7.1-2 Security Communication RootCA1 Certificate Extensions

Field	Description
authorityKeyIdentifier (2.5.29.35)	A 160-bit SHA-1 hash for CA Public Key
subjectKeyIdenrifier (2.5.29.14)	A 160-bit SHA-1 hash for Subscriber Public Key
keyUsage (2.5.29.15)	digitalSignature (Other usages than [keyCertSign] and [CRLSign] may be specified by the CAs as necessary.)
extendedKeyUsage (2.5.29.37)	timestamping(1.3.6.1.5.5.7.3.8) (Specified only with TSA)
certificatePolicies (2.5.29.32)	certPolicyId=1.2.392.200091.100.901.2 policyQualifierID=id-qt-cps qualifier=CPS=https://repository.secomtrust.net/SC-Root1/
cRLDistributionPoints (2.5.29.31)	URI:http://repository.secomtrust.net/SC-Root1/ SCRoot1CRL.crl (CRL distribution location in the directory)

Table 7.1-3 Security Communication RootCA2 Certificate Extensions

Field	Description
authorityKeyIdentifier (2.5.29.35)	A 160-bit SHA-1 hash for CA Public Key
subjectKeyIdenrifier (2.5.29.14)	A 160-bit SHA-1 hash for Subscriber Public Key
keyUsage (2.5.29.15)	digitalSignature (Other usages than [keyCertSign] and [CRLSign] may be specified by the CAs as necessary.)
extendedKeyUsage (2.5.29.37)	timestamping(1.3.6.1.5.5.7.3.8) (Specified only with TSA)
certificatePolicies (2.5.29.32)	certPolicyId=1.2.392.200091.100.901.5 policyQualifierID=id-qt-cps qualifier=CPS=https://repository.secomtrust.net/SC-Root2/
cRLDistributionPoints (2.5.29.31)	URI:http://repository.secomtrust.net/SC-Root2/ SCRoot2CRL.crl (CRL distribution location in the directory)
Authority Information Access(1.3.6.1.5.5.7.1.1)	OCSP - URI:http://scrootca2.ocsp.secomtrust.net (OCSP server's access address) * This field can be activated/deactivated per Certificate Application.

Table 7.1-4 Security Communication RootCA2 OCSP Server Certificate Extensions

Field	Description
authorityKeyIdentifier (2.5.29.35)	A 160-bit SHA-1 hash for CA Public Key
subjectKeyIdentifier (2.5.29.14)	A 160-bit SHA-1 hash for Subscriber Public Key

Field	Description
keyUsage (2.5.29.15)	digitalSignature (Usage purpose of Subscriber Public Key)
extendedKeyUsage (2.5.29.37)	OCSPSigning
OCSP No Check (1.3.6.1.5.5.7.48.1.5)	null
certificatePolicies (2.5.29.32)	certPolicyId=1.2.392.200091.100.901.5 policyQualifierID=id-qt-cps qualifier=CPS=https://repository.secomtrust.net/SC-Root2/

Table 7.1-5 Security Communication RootCA3 Certificate Extensions

Field	Description
authorityKeyIdentifier (2.5.29.35)	A 160-bit SHA-1 hash for CA Public Key
subjectKeyIdenrifier (2.5.29.14)	A 160-bit SHA-1 hash for Subscriber Public Key
keyUsage (2.5.29.15)	digitalSignature (Other usages than [keyCertSign] and [CRLSign] may be specified by the CAs as necessary.)
extendedKeyUsage (2.5.29.37)	timestamping(1.3.6.1.5.5.7.3.8) (Specified only with TSA)
certificatePolicies (2.5.29.32)	certPolicyId=1.2.392.200091.100.901.7 policyQualifierID=id-qt-cps qualifier=CPS=https://repository.secomtrust.net/SC-Root3/
cRLDistributionPoints (2.5.29.31)	URI:http://repository.secomtrust.net/SC-Root3/ SCRoot3CRL.crl (CRL distribution location in the directory)
Authority Information Access(1.3.6.1.5.5.7.1.1)	OCSP - URI:http://scrootca3.ocsp.secomtrust.net (OCSP server's access address) * This field can be activated/deactivated per Certificate Application.

Table 7.1-6 Security Communication RootCA3 OCSP Server Certificate Extensions

Field	Description
authorityKeyIdentifier (2.5.29.35)	A 160-bit SHA-1 hash for CA Public Key
subjectKeyIdentifier (2.5.29.14)	A 160-bit SHA-1 hash for Subscriber Public Key
keyUsage (2.5.29.15)	digitalSignature (Usage purpose of Subscriber Public Key)
extendedKeyUsage (2.5.29.37)	OCSPSigning
OCSP No Check	null

Field	Description
(1.3.6.1.5.5.7.48.1.5)	
certificatePolicies (2.5.29.32)	certPolicyId=1.2.392.200091.100.901.7 policyQualifierID=id-qt-cps qualifier=CPS=https://repository.secomtrust.net/SC-Root3/

Table 7.1-7 Security Communication ECC RootCA1 Certificate Extensions

Field	Description
authorityKeyIdentifier (2.5.29.35)	A 160-bit SHA-1 hash for CA Public Key
subjectKeyIdenrifier (2.5.29.14)	A 160-bit SHA-1 hash for Subscriber Public Key
keyUsage (2.5.29.15)	digitalSignature (Other usages than [keyCertSign] and [CRLSign] may be specified by the CAs as necessary.)
extendedKeyUsage (2.5.29.37)	timestamping(1.3.6.1.5.5.7.3.8) (Specified only with TSA)
certificatePolicies (2.5.29.32)	certPolicyId=1.2.392.200091.100.902.2 policyQualifierID=id-qt-cps qualifier=CPS=https://repository.secomtrust.net/SC-ECC-Root1/
cRLDistributionPoints (2.5.29.31)	URI:http://repository.secomtrust.net/SC-ECC-Root1/ SCECCRoot1CRL.crl (CRL distribution location in the directory)
Authority Information Access(1.3.6.1.5.5.7.1.1)	OCSP - URI:http://sceccrootca1.ocsp.secomtrust.net (OCSP server's access address) * This field can be activated/deactivated per Certificate Application.

Table 7.1-8 Security Communication ECC RootCA1 OCSP Server Certificate Extensions

Field	Description
authorityKeyIdentifier (2.5.29.35)	A 160-bit SHA-1 hash for CA Public Key
subjectKeyIdentifier (2.5.29.14)	A 160-bit SHA-1 hash for Subscriber Public Key
keyUsage (2.5.29.15)	digitalSignature (Usage purpose of Subscriber Public Key)
extendedKeyUsage (2.5.29.37)	OCSPSigning
OCSP No Check (1.3.6.1.5.5.7.48.1.5)	null
certificatePolicies	certPolicyId=1.2.392.200091.100.902.2

Field	Description
(2.5.29.32)	policyQualifierID=id-qt-cps qualifier=CPS=https://repository.secomtrust.net/SC-ECC-Root1/

7.1.3 Algorithm Object Identifiers

The Algorithm OIDs used in the Services are as follows:

Algorithm	OID
Sha1 With RSA Encryption	1 2 840 113549 1 1 5
sha256 With RSA Encryption	1.2.840.113549.1.1.11
RSA Encryption	1 2 840 113549 1 1 1

Table 7.1-10 Security Communication RootCA2 Algorithm OIDs

Algorithm	OID
sha256 With RSA Encryption	1.2.840.113549.1.1.11
RSA Encryption	1 2 840 113549 1 1 1

Table 7.1-11 Security Communication RootCA3 Algorithm OIDs

Algorithm	OID
sha384 With RSA Encryption	1.2.840.113549.1.1.12
RSA Encryption	1 2 840 113549 1 1 1

Table 7.1-12 Security Communication ECC RootCA1 Algorithm OIDs

Algorithm	OID
ecdsa-with-SHA384	1.2.840.10045.4.3.3
ecPublicKey	1.2.840.10045.2.1
secp384r1	1.3.132.0.34

7.1.4 Name Forms

The CAs and the Subscribers are uniquely identified by the DNs defined conforming to the X.500 Distinguished Name.

Valid characters are specified in Table "7.1-13 Valid Characters".

Table 7.1-13 Valid Characters

Alphabets	Numbers	Symbols
[A] through [Z], [a] through [z]	[0] through [9]	[:], [-], [.], and [blank]

7.1.5 Name Constraints

No stipulation

7.1.6 Certificate Policy Object Identifier

Policy OID of the Certificates issued by the CA are as indicated in the Table "1.2-2 OID (This CP)".

7.1.7 Usage of Policy Constraints Extension

No stipulation

7.1.8 Policy Qualifiers Syntax and Semantics

Policy Qualifiers store the URL of the web pages on which this CP and the CPS are published.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation

7.2 CRL Profile

CRLs issued by the CAs are generated in the X.509 CRL Format, using the fields specified in Table 7.2-1 Basic CRL Profile Fields.

Table 7.2-1 Basic CRL Profile Fields

Field	Description
Version (Version number)	CRL Format Number *1
Signature (Digital Signature algorithm identifier)	Identifier of the Digital Signature algorithm used by the CAs *2
Issuer (Name of the issuer)	Information about the issuer (specified by the CAs)
ThisUpdate (Date of update)	Date of CRL issuance
NextUpdate (Date of next update)	Date of next CRL update
RevokedCertificates (CRL)	Information about the revoked Certificates; SerialNumber (serial number); and RevocationDate (date of revocation) Reason code（reason for revocation）shall be specified.

*1 The CRL format number is set to Version2.

*2 Used when digitally signing a CRL.

7.2.1 Version Number(s)

The X.509 Format version number of CRLs issued by the CAs is Version2.

7.2.2 CRL and CRL Entry Extensions

The CRLs issued by the CAs use the X.509 CRL Extension field specified in the Table "7.2-2 CRL Extension".

Table 7.2-2 CRL Extension

Field	Description
AuthorityKeyIdentifier (CA Key identifier)	A 160-bit SHA-1 hash for CA Public Key

7.3 OCSP Profile

The CAs operates the OCSP server in compliance with RFC2560 and 5019.

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

8.1 Frequency and Circumstances of Assessment

Stipulated in the CPS.

8.2 Identity/Qualifications of Assessor

Stipulated in the CPS.

8.3 Assessor’s Relationship to Assessed Entity

Stipulated in the CPS.

8.4 Topics Covered by Assessment

Stipulated in the CPS.

8.5 Actions Taken as a Result of Deficiency

Stipulated in the CPS.

8.6 Communication of Results

Stipulated in the CPS.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

Stipulated separately in contracts.

.

9.1.2 Certificate Access Fees

No stipulation

9.1.3 Revocation or Status Information Access Fees

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 in providing this CA.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

Information on individuals and organizations in the possession of SECOM as the CAs are subject to confidentiality with the exception of those that were explicitly published as a part of a Certificate, a CRL, this CP, or the CPS. SECOM does not disclose such information externally unless it is required by law or there is a prior consent of the relevant Subscriber. SECOM may disclose the information subject to confidentiality to a legal counsel or a financial adviser who provides advice in connection with such legal,

judicial, administrative or other procedures required by law. It may also disclose information subject to confidentiality to an attorney, an accountant, a legal institution or any other specialist who provides advice on corporate mergers, acquisitions or restructuring.
Subscriber Private Keys are deemed to be information to be kept confidential by the Subscriber's own responsibility. The Services in no circumstances provide access to these Keys.
Information contained in Audit Log and the Audit Reports themselves are subject to the confidentiality and within the Scope of Confidential Information. SECOM will not disclose such information to any external party in other situation than a case stipulated in "8.6 Communication of Results" of the CPS or unless it is required by law.

9.3.2 Information Not Within the Scope of Confidential Information
Information populated in Certificates and CRLs is not considered confidential. In addition, the following information shall not be subject to the confidentiality provisions herein:

- Information that is or came to be known through no fault of SECOM;
- information that was or is made known to SECOM by a party other than SECOM without confidentiality requirements;
- information independently developed by SECOM; or
- information approved for disclosure by the relevant Subscriber.

9.3.3 Responsibility to Protect Confidential Information
SECOM may disclose confidential information retained as the CAs when required by law or there is a prior consent of the relevant Subscriber. In the event of the foregoing, the party having come to acquire the information may not disclose said information to a third party due to contractual or legal constraints.

9.4 Privacy of Personal Information

9.4.1 Personal Information Protection Plan
SECOM will use the personal information collected from the subscribers of our authentication service to the extent necessary for the operation of this CA, such as confirming the application details, sending necessary documents, etc., and confirming who is authorized. SECOM's privacy policy will be announced on SECOM's website (http://www.secomtrust.net).

9.4.2 Information Treated as Personal Information
SECOM treats information defined as personal information based on domestic laws and regulations (such as information collected from subscribers of SECOM authentication

services) as personal information and manages it appropriately.

9.4.3 Information that is not considered Personal Information
SECOM treats personal information as specified in "9.4.2 Information Treated as Personal Information".

9.4.4 Responsibility for protecting Personal Information
SECOM shall not disclose any personal information of the other party that it has learned during the execution and termination of the contract to third parties, whether during or after the contract period. The personal information protection manager shall be appointed in the operation of this CA, and the personal information protection manager shall have employees engaged in the service comply with internal rules regarding the handling of personal information.

9.4.5 Notice and Consent regarding use of Personal Information
SECOM will not use personal information for any purpose other than the purpose of obtaining the consent of the certificate subscriber, except as provided by law. The personal number and specific personal information will be used for the purpose of use permitted by law and for the purpose of use with the consent of the certificate subscriber.

9.4.6 Disclosure of Information with Judicial or Administrative Procedures
If disclosure is requested by law, rule, court decision/order, administrative agency order /instruction, etc., the personal information of the certificate subscriber may be disclosed.

9.4.7 Other Information Disclosure Conditions
No stipulation.

9.5 Intellectual Property Rights
Unless otherwise agreed to between SECOM and Subscribers, the following informative materials and data pertaining to the Services shall belong to the parties specified as below:

Subscriber Certificate	An asset belonging to SECOM
CRL	An asset belonging to SECOM
Distinguished Name (DN)	An asset belonging to an entity to which the Name is assigned as long as the fee for the Subscriber Certificate is properly paid
Subscriber Private Key	An asset belonging the possessor of the Private Key that completes a Key Pair with the Public Key, regardless of how it is stored or who possesses the storage medium

Subscriber Public Key	An asset belonging the possessor of the Private Key that completes a Key Pair, regardless of how it is stored or who possesses the storage medium
This CP and the CPS	An asset (including the copyrights) belonging to SECOM

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

SECOM provides certification services including authentication of the Certificate applicants and registration/issuance/revocation of Certificates conforming to the provisions of this CP and the CPS, and secures the reliability of the certification practice including that of the CA Private Keys.

The foregoing warranties by SECOM set forth in this CP and the CPS are in lieu of all other warranties, express or implied, or otherwise.

9.6.2 RA Representations and Warranties

The provisions of "9.6.1 CA Representations and Warranties" hereof shall apply.

9.6.3 Subscriber Representations and Warranties

Subscribers to the CAs shall bear obligations to:

- Provide the CAs with as accurate and complete information as possible that Subscribers may know of and promptly notify the CAs of any change in the information provided therein;
- protect their own Private Keys from being compromised;
- restrict the Certificate usage to those set forth in this CP and the CPS without violating any laws and regulations; and
- promptly request the CAs 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 of the CA Services shall bear obligations to:

- Trust Certificates issued by the CAs for use with the intended usage purposes of the CAs set forth in this CP and the CPS;
- ensure that the Certificate has not been revoked by checking the CRLs in the Repository or the OCSP server in attempting to trust the Certificate;
- check the validity period of the Certificate to ensure that it has not expired in attempting to trust the Certificate;

- ensure that the Certificate signature can be authenticated by the CA Certificate in attempting to trust the Certificate issued by the CAs; and
- agree to bear responsibility as the Relying Party defined in this CP and the CPS in trusting and using the CA Certificates.

9.6.5 Representations and Warranties of Other Participants
No stipulation

9.7 Disclaimers of Warranties
SECOM 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 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;
- any damage attributable to the failure of a Subscriber or Relying Party to perform its obligations;
- any damage attributable to a Subscriber or Relying Party system;
- damages attributable to the defect or malfunction or any other behavior of SECOM's, Subscriber's, or Relying Party's hardware or software;
- any damage during the period that a Subscriber neglected to pay the subscription fee as set forth in the agreement thereof;
- damages caused by information published in a Certificate, a CRL or on the OCSP server due to the reasons not attributable to SECOM;
- any damage incurred in an outage of the normal communication due to reasons not attributable to SECOM;
- 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 Services, including that of the CAs, 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

Each Subscriber and Relying Party shall indemnify and hold harmless SECOM and its related organizations upon applying for, accepting, and trusting Certificates issued by the CAs. Incidents subject to the foregoing include loss, damage, lawsuit, as well as misconduct, omission, act, delay or default that are attributable to any kinds of cost burden, which could have been caused by failure of the Subscriber to provide the latest and accurate information to the CAs. Such incidents also include various liabilities, loss, damage, lawsuit, as well as misconduct, omission, act, delay or default by each Subscriber or Relying Party that are attributable to any kinds of cost burden.

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 in no way lose effect 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 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, 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 CAs.

9.11 Individual Notices and Communications with Participants

The CAs provide the necessary notices to Subscribers and Relying Parties through e-mail or in other written forms.

9.12 Amendments

9.12.1 Procedure for Amendment

(1) Critical revisions/amendments

SECOM notifies Subscribers and Relying Parties of amendments of this CP if the amendments thereof are determined to have an obvious impact on the activities for use of Certificates or CRLs by the Subscribers and Relying Parties, by publishing the post-amendment version of this CP (including the Version History/Description/Date) in the Repository, while refreshing the Major Version Number.

(2) Non-critical revisions/amendments

SECOM notifies Subscribers and Relying Parties of amendments of this CP if the amendments thereof are determined to have no or less impact on the activities for use of Certificates or CRLs by the Subscribers and Relying Parties, by publishing the post-amendment version of this CP (including the Version History/Description/Date) in the Repository, while refreshing the Minor Version Number.

9.12.2 Notification Mechanism and Period

If this CP is revised/amended, the prompt publication of the post-amendment version of this CP (including the Version History/Description/Date) in the Repository is deemed to be the notification thereof to Subscribers and Relying Parties. Subscribers may make claims within a week of such notification, while the post-amendment version of this CP is deemed to be approved by the Subscribers unless any claim is made within the said period.

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 Provisions

A party seeking to file a lawsuit, request arbitration, or take any other legal action against SECOM for the resolution of a dispute relating to the Services provided by the CAs, shall notify SECOM to this effect in advance.

9.14 Governing Law

Regardless of the locations of the CAs, Subscribers, or Relying Parties, the laws of Japan will apply to any dispute concerning the interpretation or validity of this CP and the CPS. Regarding the location for arbitration and court proceedings, the parties hereto submit to the exclusive jurisdiction of a dispute settlement institution located within Tokyo.

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 comprehensively stipulates its policy, warranties as well as the Subscriber and Relying Party obligations and other relevant matters in this CP, the CPS and the

agreements for provision of the Services, and any agreement otherwise, whether oral, written, or implied, shall have no effect.

9.16.2 Assignment

When SECOM assigns the Services to a third party, SECOM may also assign its responsibilities and other obligations specified in this CP and the CPS.

9.16.3 Severability

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

9.16.4 Enforcement

Indemnities and attorneys 'fees may be sought from parties for disputes arising from the contractual provisions of each prescribed document, damages, losses and costs relating to the parties' actions.

9.16.5 Force Majeure

SECOM 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 may suspend this CA until the situation ceases.

9.17 Other Provisions

No stipulation