Security Communication RootCA
Certification Practice Statement

May 24, 2019
Version 5.12

SECOM Trust Systems Co., Ltd.

Version History		
Version Number	Date	Description
V1.00	2003.09.29	Publication of the first version
V2.00	2004.11.08	Major version upgrade Separation of the Security Communication RootCA1 Certificate Policy (CP)/Certification Practice Statement (CPS) document into the independent CP and CPS documents, with new publication of the Security Communication RootCA1 CPS Revision of the descriptions
V3.00	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."
V4.00	2009.05.29	Major version upgrade Renaming of "Security Communication RootCA1 CPS" to "Security Communication RootCA CPS" and addition of the CA Private Key "Security Communication RootCA2"
V4.10	2012.02.15	"5.6 Key Changeover" - Addition of Certificate Renewal
V4.20	2012.11.09	Amendment associated with commencement of the OCSP server operations
V5.00	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"
V5.10	2017.05.23	Overall revision of the descriptions and styles
V5.11	2018.11.28	Overall revision of the descriptions and styles
V5.12	2019.05.24	Overall revision of the descriptions and styles

Table of Contents

1. Introduction

1.1 Overview

Security Communication RootCA Certification Practice Statement (hereinafter, "this CPS") is a document that defines operational policies for 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"), including the issuance/revocation (hereinafter, "the Services") of the digital certificates (hereinafter, "Certificates") to the subscribers, the administration of the CA Keys, the operation and maintenance procedures for the Public Key Infrastructure (hereinafter, "PKI") based on the Certificates.

The Certificates issued by the CAs prove and certify the unique correspondence between the subjects of the issuance and their public keys. The qualifications (identification and authentication), registrations, and issuance procedures of the CA Certificates are defined in each Certificate Policy (hereinafter, "CP") for each type of the Certificates used by the subscribers.

The CAs conform to the CA/Browser Forum provisions disclosed at https://www.cabforum.org/.
Any provisions in the CP inconsistent with this CPS shall prevail and any provisions in a separate agreement or the like between the subscribers and SECOM inconsistent with this CPS or the relevant CP shall prevail.

This CPS 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 CPS is "Security Communication RootCA Certification Practice Statement". 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 CPS is identified with the Object IDentifier (hereinafter, "OID") given in "Table 1.2-2 OID (This CPS)".

Table 1.2-2 OID (This CPS)

CPS	OID
Security Communication RootCA Certification Practice Statement	1.2.392.200091.100.901.3

This CPS is applied to the CPs indicated in the "Table 1.2-3 OID (CPs)".

Table 1.2-3 OID (CPs)

CP	OID
Security Communication RootCA Subordinate CA Certificate Policy	1.2.392.200091.100.901.1 (Security Communication RootCA1) 1.2.392.200091.100.901.4 (Security Communication RootCA2) 1.2.392.200091.100.901.6 (Security Communication RootCA3) 1.2.392.200091.100.902.1 (Security Communication ECC RootCA1)
Security Communication RootCA Time-Stamp Service Certificate Policy	1.2.392.200091.100.901.2 (Security Communication RootCA1) 1.2.392.200091.100.901.5 (Security Communication RootCA2) 1.2.392.200091.100.901.7 (Security Communication RootCA3) 1.2.392.200091.100.902.2 (Security Communication ECC RootCA1)

The Services may add a new CP in the future, which shall accompany addition of the correspondence between the new CP and the OID in this CPS.

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 application 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 issued Certificates after submitting the Certificate applications to the CAs.

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 assessing the contents of this CPS and the relevant CP in light of the Relying Parties' own purposes of use.

1.3.5 Other Participants

No stipulation

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The CAs are the Root CAs functioning as top of the subordinate CAs and issue Certificates conforming to the CPs described in "1.2 Document Name and Identification" hereof. Relying Parties may authenticate the reliability of such Certificates using the CA Certificates.

1.4.2 Prohibited Certificate Uses

Stipulated in the relevant CP.

1.5 Policy Administration

1.5.1 Organization Administering the Document

This CPS is maintained and administered by SECOM.

1.5.2 Contact Information

Inquiries concerning this CPS 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 CPS as the CAs' practice policy is determined by SECOM's Certification Services Improvement Committee.

1.5.4 Approval Procedure

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

1.6 Definitions and Acronyms

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.

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 Certificate applications, 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 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.

HSM (Hardware Security Module)

The hardware that works as a protecting safe to store private keys used for encryption and digital signing. An HSM computes encryption and digital signing as well as generates private keys and random digits.

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 CPS revision (e.g., the underlined digit [1] of Version 1.02) whose magnitude of the amendment(s) 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 CPS revision (e.g., the underlined digit [02] of Version 1.02) whose magnitude of the amendment(s) is considered to have no or less impact on the use of the Certificates and the CRLs by Subscribers and Relying Parties.

OCSP

OCSP stands for Online Certificate Status Protocol, the protocol used to provide the

real-time Certificates 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 (subjects) to be included in the 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 CPS 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.

Root CA

The Security Communication RootCA described in this CPS is an institute owned and run by SECOM as a Root CA that issues the subordinate CA Certificates and functions as top of the subordinate CAs.

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.

Subordinate CA

A CA trusted and signed by the CAs.

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.

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.

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

The CAs maintain and administer the Repository to allow access by the Subscribers and Relying Parties to the CRL information. The CAs also maintain and administer the OCSP server to allow 24x7 online access by the Subscribers and Relying Parties to the Certificates status. The protocol employed for the Repository access shall be HTTP (HyperText Transfer Protocol) and HTTPS (HTTP + SSL/TLS data encryption function). Information in the repository may be accessed via any commonly used Web interface.

2.2 Publication of Certificate Information

The CAs store the following contents in the Repository to allow online access by the Subscribers and Relying Parties:

- CRLs that contain all revocation records based on this CPS and the relevant CP.
- The self-signed Certificate of the CAs
- The latest version of this CPS and the relevant CP
- Other information pertaining to Certificates issued by the CAs

SECOM will make the Certificates status available online to Subscribers and Relying Parties for browsing on the OCSP server.

2.3 Time or Frequency of Publication

This CPS and the relevant CP are published in the Repository as revised. A CRL containing all information of revocation processed conforming to this CPS and the relevant CP is published in the Repository as issued.

2.4 Access Controls on Repositories

Subscribers and Relying Parties may browse the Repository anytime. However, the Repository may not be available temporarily at times due to maintenance or for any other reason.

3. Identification and Authentication

3.1 Naming

Stipulated in the relevant CP.

3.2 Initial Identity Validation

Stipulated in the relevant CP.

3.3 Identification and Authentication for Re-Key Requests

Stipulated in the relevant CP.

3.4 Identification and Authentication for Revocation Requests

Stipulated in the relevant CP.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application
Stipulated in the relevant CP.

4.2 Certificate Application Processing
Stipulated in the relevant CP.

4.3 Certificate Issuance
Stipulated in the relevant CP.

4.4 Certificate Acceptance
Stipulated in the relevant CP.

4.5 Key Pair and Certificate Usage
Stipulated in the relevant CP.

4.6 Certificate Renewal
Stipulated in the relevant CP.

4.7 Certificate Re-Key
Stipulated in the relevant CP.

4.8 Certificate Modification
Stipulated in the relevant CP.

4.9 Certificate Revocation and Suspension
Stipulated in the relevant CP.

4.10 Certificate Status Services
Stipulated in the relevant CP.

4.11 End of Subscription (Registry)
Stipulated in the relevant CP.

4.12 Key Escrow and Recovery
Stipulated in the relevant CP.

5. Facility, Management, and Operational Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

The systems of the CAs (hereinafter, "CA Systems") are located where they will not be easily damaged by water exposures, earthquakes, fires or any other disasters, and structural measures have been implemented to prevent and protect against such disasters. In addition, the equipment and instruments used in the facility shall be installed in secure locations implementing the anti-disaster/hacking/breaking & entering measures.

5.1.2 Physical Access

The hardware and software used by the CAs employ an appropriate security control combining physical and electronic access controls. Access to the hardware and the software providing the CA Services are continuously monitored and requires permission by the Service Operation Manager(s).

5.1.3 Power and Air Conditioning

The installation room for the CA Systems secure the power source with sufficient capacity to operate the CA Systems and is protected through the power supply from the backup generators during long-lasting power outages. Further, the CA Systems are installed in an air conditioned environment where optimum temperature and humidity can be maintained constantly using air conditioners.

5.1.4 Water Exposures

The installation room for the CA Systems implement the protection against the water exposures, including deployment of the leakage sensors.

5.1.5 Fire Prevention and Protection

The installation rooms for CA Systems are in a fireproof compartment partitioned off by firewalls and equipped with fire alarms as well as fire extinguishing equipment.

5.1.6 Earthquake

The installation room for the CA Systems shall implement anti-seismic measures for protection against tumbling and falling of the machines and fixtures.

5.1.7 Media Storage

Critical storage media containing the archive or backup data are stored in secure locations.

5.1.8 Waste Disposal

Disposal of Private Keys of the CAs (hereinafter, "CA Private Keys") and paper and electronic media containing confidential information shall be conducted with CA Private Keys and the backup media completely initialized or physically destroyed, and with the paper-based media as documents shredded, incinerated, or dissolved.

5.1.9 Off-Site Backup

Measures for remote storage and retrieval of the data, equipment, and any other items required to operate the Services shall be implemented.

5.2 Procedural Controls

5.2.1 Trusted Roles

Individuals involved in the registration, issuance, and revocation practices are acting in the capacity of a trusted role conforming to this CPS and the relevant CP. The CAs do not centrally assign operational roles to a specific individual, but allocate authorities to multiple personnel. The roles in the CAs are listed in "Table 5.2-1 Trusted Roles".

Table 5.2.1 Trusted Roles

Name of role	Primary responsibilities
Certification Services Improvement Committee	- Approves development/amendment/termination of this CPS and the relevant CP. - Directs actions taken as a result of audit deficiency.
Person Responsible for Services	- Supervises the CA management organization. - Approves CA Systems/operational procedure changes
Service Operation Manager	- Gives work instructions to person(s) in charge of operation and observes the operations. - Observes CA Systems and CA Private Key operations on site. - Generally manages other service operations.
CA Administrator	- Registers and issues Certificates - Issues CRLs
Person in Charge of RA	- Accepts Certificate applications - Qualifies (identifies and authenticates) Subscribers
Log Examiner (Log Checker)	- Checks room access, system and other logs.

5.2.2 Number of Persons Required per Task

The CA Systems are designed to physically refuse single-person accesses, which requires operations by at least two persons.

5.2.3 Identification and Authentication for Each Role

The biometric identification control is deployed for entry to the CA Systems installation room, while multiple-person control is deployed for access to CA Private Keys.

5.2.4 Roles Requiring Separation of Duties

The CAs intend to prevent such unwanted actions as misconducts, which can happen through the single-person operations made possible by authority centralization, through decentralization of the authority by not granting authorities/permissions to a specific person. Authorities for system operations, acts of approving, and audits are separated.

5.3 Personnel Controls

Personnel who perform the Trusted Roles bear responsibility for operations and administration of the Services. In providing the Services, personnel management that assures reliability and suitability of these roles as well as the reasonable skills to perform these roles shall be conducted, by which the security is established.

5.3.1 Qualifications, Experience, and Clearance Requirements

Individuals responsible for the Trusted Roles for the Services shall be regular employees hired by SECOM's hiring criteria. Individuals who have undergone specialized training with understanding of the PKI outline and how to operate the PKI systems shall be appointed as the persons in charge of the direct operation of the CA Systems.

5.3.2 Background Check Procedures

Reliability and suitability of the individuals responsible for the Trusted Roles are assessed at the appointment and periodically, conforming to the provisions in this CPS and the relevant CP.

5.3.3 Training Requirements

Individuals responsible for the Trusted Roles have to be properly trained for the jobs upon appointment, and retrained as necessary from then on.

5.3.4 Retraining Frequency and Requirements

SECOM provides the individuals performing the roles listed in "5.2.1 Trusted Roles" hereof with refresher training as needed.

5.3.5 Job Rotation Frequency and Sequence

The CAs conduct job rotations of the personnel for the purpose of securing service quality consistency and improvement as well as prevention of misconducts.

5.3.6 Sanctions for Unauthorized Actions
The provisions concerning penalties in SECOM's Rules of Employment apply.

5.3.7 Independent Contractor Requirements
When the CAs may employ independent contractors for operations of the CA systems in whole or in part, appropriate performance of the operational duties by the contractors shall be ensured through the agreements therewith.

5.3.8 Documentation Supplied to Personnel
The CAs permit the personnel's access only to the documents necessary for the performance of relevant duties.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded
The CAs manually or automatically retrieve audit trails and event logs of the CA Systems, Repository system, and the network devices related to the CAs.

5.4.2 Frequency of Processing Audit Log
The CAs probe the Audit Log on a regular basis.

5.4.3 Retention Period for Audit Log
Audit Logs are retained for at least ten (10) years.

5.4.4 Protection of Audit Log
The CAs implement appropriate controls on Audit Log access to secure sole access by the authorized personnel and to keep the log from the eyes of those unauthorized.

5.4.5 Audit Log Backup Procedure
Audit Logs are backed up onto offline recording media, which are stored in a secure location.

5.4.6 Audit Log Collection System
The Audit Log collection system is included as a function of the CA Systems, collecting Audit Log automatically or manually.

5.4.7 Notification to Event-Causing Subject
The CAs collect Audit Log without notifying the person, system or application that has caused the corresponding event.

5.4.8 Vulnerability Assessments

The CAs conduct assessment addressing the security vulnerabilities in the operational and system behavior aspects as well as review and revision of the security measures as needed, including introduction of the latest security technologies available for implementation.

5.5 Records Archival

5.5.1 Types of Records Archived

The archive of the CAs includes the following records:

- Certificate issuance and revocation histories
- Processing history relating to CRL issuance
- The self-signed Certificate of the CAs
- Subscriber Certificates
- CRL
- OCSP server access log

5.5.2 Retention Period for Archive

Archived records are retained for at least ten (10) years.

5.5.3 Protection of Archive

The media containing the archived records are physically protected and are retained in a facility, to which access is restricted to the authorized personnel. Inspections of the archived records are conducted once a year to ensure no failure or loss of the data.

5.5.4 Archive Backup Procedures

The primary and secondary backup data are taken whenever a change is made in such critical data as may affect the CA operations, including issuance/revocation of Certificates or CRL issuance, while the secondary backup shall be stored in a remote location.

5.5.5 Requirements for Time-Stamping of Records

The CAs properly time synchronize the CA Systems and Time-Stamp the critical information recorded therein.

5.5.6 Archive Collection System

The Archive collection system is included as a function of the CA Systems.

5.5.7 Procedures to Obtain and Verify Archive Information
Storage condition of the archived records is periodically checked and the records shall be copied to fresh media as necessary.

5.6 Key Changeover
Re-Keying of the CAs' own Key Pairs or renewal of Certificates thereof shall be performed basically when their usage periods become shorter than the maximum validity periods of the Certificates issued to Subscribers. When the remaining validity periods of the CAs become shorter than the maximum validity periods of the Certificates issued to Subscribers, the validity periods of the renewed Certificates issued thereto shall be so changed to be within the validity period of the CAs.
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
Should it be determined that CA Private Keys 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 Services, the predetermined plans and procedures are followed to securely resume the Services.

5.7.2 Computing Resources, Software, and/or Data are Corrupted
In the event of damage to any hardware, software or data, the CAs promptly engage in the system recovery efforts using the relevant hardware, software or data that are retained as backup.

5.7.3 Entity Private Key Compromise Procedures
Should a Subscriber determine that a Private Key has or could have been compromised, the Subscriber must promptly make a revocation request to the relevant CA. Following receipt of a revocation request, the relevant CA processes the revocation according to the procedure set forth in "4.9 Certificate Revocation and Suspension" hereof.

5.7.4 Business Continuity Capabilities after a Disaster
Based on SECOM's business continuity policy, the contingency plans to continue the Services by the CAs in the event of situations forcing suspension or significant reliability compromise of the Services have been developed and put in place. In addition, to minimize the suspension length, SECOM implements the contingency plan to procure resources required to recover the Services.

5.8 CA or RA Termination

In the event of termination of the Services by SECOM, the company shall so notify Subscribers and other affected participants three (3) months prior to the termination. All Certificates issued by the CAs 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 Services, the CA Key Pairs are generated on an FIPS140-1 Level 3 conformant HSM. The Key Pair generation operation is jointly performed by at least two authorized individuals under observation by the Service Operation Manager(s).

6.1.2 Private Key Delivery to Subscriber

Being generated by the Subscribers themselves, the Subscriber Key Pairs are possessed only by the Subscribers.

6.1.3 Public Key Delivery to Certificate Issuer

Subscriber Public Keys are verified according to the procedure set forth in "3.2.1 Method to Prove Possession of Private Key" hereof, and are delivered online.

6.1.4 CA Public Key Delivery to Relying Parties

Relying Parties may obtain CA Public Keys by accessing the CA Repository or through a commonly used web browser.

6.1.5 Key Sizes

The Digital Signature scheme of the CA Key Pairs is described in "Table 6.1-1 Digital Signature Scheme".

Table 6.1-1 Digital Signature Scheme

Public Key algorithm	Signature algorithm	CA Key
2048 bit RSA	SHA1	Security Communication RootCA1
2048 bit RSA	SHA256	Security Communication RootCA2
4096 bit RSA	SHA384	Security Communication RootCA3
384 bit ECC	SHA384	Security Communication ECC RootCA1

6.1.6 Public Key Parameters Generation and Quality Checking

The HSM used in the CA systems has the capability to check the quality of the encryption function. Public Key parameters are generated using the encryption function qualified by the quality checking.

6.1.7 Key Usage Purposes

Stipulated in the relevant CP.

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 HSM that has obtained the FIPS140-2 Level 3 conformance.

6.2.2 Private Key Multi-Person Control

Generation of CA Private Keys requires operation by the Service Operation Manager(s) and at least two authorized individuals, who are also required for the post-generation administration of the Private Keys including transfer and disposal of the cryptographic module.

6.2.3 Private Key Escrow

The CAs do not Escrow CA Private Keys.

6.2.4 Private Key Backup

CA Private Keys are backed up onto an HSM that has obtained the FIPS140-2 Level 3 conformance. The same control scheme as in "6.2.2 Private Key Multi-Person Control" hereof applies to the backup operation. The backup files and media are securely controlled as well.

6.2.5 Private Key Archival

The CAs do not archive CA Private Keys.

6.2.6 Private Key Transfer into or from a Cryptographic Module

CA Private Keys are generated inside an HSM and will never be retrieved by other hardware or software.

6.2.7 Private Key Storage on Cryptographic Module

CA Private Keys are stored in an HSM that has obtained the FIPS140-2 Level 3 conformance.

6.2.8 Method of Activating Private Key

Activation of CA Private Keys is jointly performed by at least two authorized individuals as in "6.2.2 Private Key Multi-Person Control" hereof, in the CA rooms.

6.2.9 Method of Deactivating Private Key

CA Private Keys are automatically deactivated after completion of a successful access thereto.

6.2.10 Method of Destroying Private Key
In a situation that requires disposal of CA Private Keys, the HSM storing them are completely initialized or physically destroyed by at least two authorized individuals as in "6.2.2 Private Key Multi-Person Control" hereof, in the CA rooms, while the backup Private Keys are also disposed of, following the same procedure.

6.2.11 Cryptographic Module Rating
An HSM that has obtained the FIPS140-2 Level 3 conformance is used for control of CA Private Keys.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival
Archival of CA Public Keys is covered by "5.5.1 Types of Archives" hereof.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods
The validity period of CA Key Pairs is assumed to be twenty (20) years, which will not be modified.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation
At least two digital keys are used for activation of CA Private Keys.

6.4.2 Activation Data Protection
The keys required for activation are stored in different locations.

6.4.3 Other Aspects of Activation Data
No stipulation

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements
Hardware used by the CAs is protected by the scheme described in "5.1 Physical Controls" hereof and the user authentication is required to log in thereto. Protections against different threats are implemented, including the anti-virus protection.

6.5.2 Computer Security Rating
The CAs conduct the preproduction system tests of all software and hardware to be

employed by the CA Systems in an effort to secure the system reliability. In addition, the CAs constantly collect information on the security vulnerabilities and perform assessments to be able to promptly take proper actions should any vulnerability be detected.

6.6 Life-Cycle Technical Controls

For hardware and software used by the CAs, the latest security technologies are assessed at an appropriate cycle while reviews of this CPS and the relevant CP as well as security checks are conducted as required.

6.6.1 System Development Controls

The CA Systems are configured and maintained in a secure environment. Security is thoroughly assessed and verified when modifying the CA Systems. Further, security checks are performed in order to ensure the security by implementing the latest security technologies at an appropriate cycle.

6.6.2 Security Management Controls

The CAs ensure security by conducting such operational management as administration of the information asset, personnel and permissions, as well as timely updates of the security software such as anti-hacking and anti-virus applications.

6.6.3 Life-Cycle Security Controls

The CAs perform assessments as appropriate to ensure that the CA Systems are developed, operated and maintained properly, to make improvements as needed.

6.7 Network Security Controls

The CA Systems are not connected to any internal or external systems. The Repository system is protected against unauthorized accesses through such implementations as firewalls and unauthorized access detection systems.

6.8 Time-Stamping

Requirements concerning Time-Stamping shall be as stipulated in "5.5.5 Requirements for Time-stamping of Records" hereof.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile
Stipulated in the relevant CP.

7.2 CRL Profile
Stipulated in the relevant CP.

7.3 OCSP Profile
Stipulated in the relevant CP.

8 Compliance Audit and Other Assessments

8.1 Frequency and Circumstances of Assessment

SECOM performs audits once a year or as auditors set forth in "8.2 Identity/Qualifications of Assessor" hereof determine to be necessary to verify whether or not the operation of the Services is in compliance with this CPS and the relevant CP.

8.2 Identity/Qualifications of Assessor

The compliance audits shall be performed by the auditors demonstrating appropriate proficiency with solid and adequate auditing experience.

8.3 Assessor’s Relationship to Assessed Entity

Auditors shall be operationally and organizationally independent of the assessed entity, except for the audit-related aspects. In conducting the audits, the assessed entity shall provide appropriate support to the effort.

8.4 Topics Covered by Assessment

Audits are performed, conforming to the WebTrust for CA standards with respect to the business activities for operation of the CAs.

8.5 Actions Taken as a Result of Deficiency

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

8.6 Communication of Results

The audit results are communicated to SECOM by the auditors. If SECOM Trust Systems is required to disclose the audit results, the company will not externally disclose the audit results unless the requirement is in accordance with relevant laws or made by an associated party based on the agreement therewith, or the disclosure is approved by the Certification Services Improvement Committee.

9. Other Business and Legal Matters

9.1 Fees
Stipulated in the relevant CP.

9.2 Financial Responsibility
Stipulated in the relevant CP.

9.3 Confidentiality of Business Information
Stipulated in the relevant CP.

9.4 Privacy of Personal Information
Stipulated in the relevant CP.

9.5 Intellectual Property Rights
Stipulated in the relevant CP.

9.6 Representations and Warranties
Stipulated in the relevant CP.

9.7 Disclaimers of Warranties
Stipulated in the relevant CP.

9.8 Limitations of Liability
Stipulated in the relevant CP.

9.9 Indemnities
Stipulated in the relevant CP.

9.10 Term and Termination
Stipulated in the relevant CP.

9.11 Individual Notices and Communications with Participants
Stipulated in the relevant CP.

9.12 Amendments

9.12.1 Procedure for Amendment

(1) Critical revisions/amendments

SECOM notifies Subscribers and Relying Parties of amendments of this CPS 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 CPS (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 CPS 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 CPS (including the Version History/Description/Date) in the Repository, while refreshing the Minor Version Number.

9.12.2 Notification Mechanism and Period
If this CPS is revised/amended, the prompt publication of the post-amendment version of this CPS (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 CPS is deemed to be approved by the Subscribers unless any claim is made within the said period.

9.13 Dispute Resolution Provisions
Stipulated in the relevant CP.

9.14 Governing Law
Stipulated in the relevant CP.

9.15 Compliance with Applicable Law
Stipulated in the relevant CP.

9.16 Miscellaneous Provisions
Stipulated in the relevant CP.

9.17 Other Provisions
Stipulated in the relevant CP.