SECOM Digital Certification Infrastructure Certification Practice Statement

Version 2.12

May 24, 2019

SECOM Trust Systems Co., Ltd.

Version History		
Version Number	Date	Description
1.00	2006/03/23	Publication of the first version
2.00	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."
2.10	2017/05/23	Overall revision of the descriptions and styles
2.11	2018/11/28	Revision of the descriptions and styles
2.12	2019/05/24	Overall revision of the descriptions and styles

Table of Contents

1. Introduction

1.1 Overview

The SECOM Digital Certification Infrastructure Certification Practice Statement (hereinafter, "this CPS") stipulates the rules for operating the Digital Certification Infrastructure provided by SECOM Trust Systems Co., Ltd. (hereinafter, "SECOM Trust Systems).

The Digital Certification Infrastructure hereunder, which is operated by SECOM Trust Systems, is a platform used for the operation of the certification authority (hereinafter, "Private CA users") of SECOM Trust Systems as well as the CA of the users of SECOM Trust Systems Private CA Services.
The Digital Certification Infrastructure comprises certification infrastructure systems, such as repository servers for publishing revocation information, CA certificates, and other information, as a CA, as well as other servers on which the applications for transmitting certificate signing requests from an RA (Registration Authority) to an IA (Issuing Authority) are installed.
An organization or any other entity serving as operator of a CA may achieve a highly reliable and extremely secure CA by building the CA server on the Digital Certification Infrastructure.

Any CA operated on the Digital Certification Infrastructure has to provide for the types and usages of the certificates to be issued, as well as respective rules of practice specific to that particular CA, as the certificate policy (hereinafter, "CP"). The CA operated on the Digital Certification Infrastructure must comply with this CPS and the CP in conducting the operation.

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

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 "SECOM Digital Certification Infrastructure Certification Practice Statement" and a registered and unique Object Identifier (hereinafter, "OID") is assigned to this CPS, as follows:

CPS	OID
SECOM Digital Certification Infrastructure Certification Practice Statement	1.2.392.200091.100.401.1

OIDs respectively assigned to CAs operated on the Digital Certification Infrastructure are respectively stipulated in the CP.

1.3 PKI Participants

1.3.1 CA

A CA is a Certification Authority issuing certificates, which performs issuance or revocation of Certificates, disclosure of CRL（Certificate Revocation List）and operation maintenance of repository. The operating body of the CAs on the Digital Certification Infrastructure is SECOM Trust Systems or Private CA users. CA activities are operated by SECOM Trust Systems.

1.3.2 RA

An RA mainly performs identification and authentication of applicants requesting the issuance or revocation of Certificates as well as the registration thereof. RA activities for CAs operated on the Digital Certification Infrastructure are operated by SECOM Trust Systems or Private CA users.

1.3.3 Subscribers

Subscribers are entities to which the certificates will be issued by the CA operated on the Digital Certification Infrastructure.

1.3.4 Relying Parties

Relying Parties are the entities that authenticate the certificates issued by the CA operated on the Digital Certification Infrastructure.

1.3.5 Other parties

No stipulation

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

1.4.2 Prohibited Certificate Uses

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

1.5 Policy Administration

1.5.1 Organization Administering the Document

This CPS is maintained and administered by SECOM Trust Systems.

1.5.2 Contact Information

Inquiries concerning this CPS should be directed to:

CA Support Center, Secom Trust Systems Co., Ltd.
TEL: +81-(0)422-76-2072

1.5.3 Person Determining CP Suitability for the Policy

The contents of this CPS are determined by SECOM Trust Systems Certification Services Committee.

1.5.4 Approval Procedure

This CPS is prepared and revised by SECOM Trust Systems and goes into effect upon approval by its Certification Services Committee.

1.6 Definitions and Acronyms

Archive

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

Audit Log

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

CA (Certification Authority)
An entity that mainly issues, renews and revokes certificates, generates and protects CA private keys, and registers Subscribers.

CP (Certificate Policy)
A document that sets forth provisions pertaining to certificates issued by a CA, including certificate types, subject, usage, application procedure and issuance criteria.

CPS (Certification Practices Statement)
A document that sets forth provisions pertaining to the practices of CAs, including procedures for the CA operations and the security standards.

CRL (Certificate Revocation List)
A list of information of the certificates which were revoked prior to their expiration due to reasons such as changes to the information provided in the certificates and compromise of the relevant private key.

Digital Certificate
An electronic data that proves the binding between a public key and an identity, validity of which is certified by the digital signature of a CA affixed thereto. Digital Certificate is referred to as "Certificate" hereinafter.

Digital Certification Infrastructure
A platform for operating the CA of SECOM Trust Systems and of the users of the Private CA users.

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

FIPS140-2
The security certification standards developed by the U.S. NIST (National Institute of

Standards and Technology) for cryptographic modules, defining four security levels, the lowest 1 through the highest 4.

HSM (Hardware Security Module)
A tamper resistant cryptographic module used to ensure the security mainly in generation, storage and usage of private keys.

IA (Issuing Authority)
An entity which, of the duties of a CA, mainly handles the issuance/ renewal/ revocation of Certificates, generation and protection of CA private keys, and the maintenance and management of repositories.

NTP (Network Time Protocol)
A protocol for correctly adjusting the internal clocks of computers via the networks.

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

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

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 CA Services
The name of the certification services provided by SECOM Trust Systems.

Private Key
A key of a Key Pair used in the public key cryptosystem. A Private Key is possessed by the holder of the corresponding public key.

Public Key

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

RA (Registration Authority)

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

Repository

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

RFC3647 (Request for Comments 3647)

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

RSA

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

SHA-1 (Secure Hash Algorithm 1)

A hash function used in digital signings. A hash function is an algorithm that generates a fixed-length string from a given text data.
The algorithm works to detect any alterations in the original message during the transmission by comparing the hash values transmitted and received.

Time-Stamp

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

2. Publication and Repository Responsibilities

2.1 Repository

SECOM Trust Systems provides a Repository for the CA operated on the Digital Certification Infrastructure. The Repository is maintained and administered so as to allow 24x7 access. However, such factors as system maintenance and requirements by respective CAs may suspend the access even during the normal operating hours.

2.2 Publication of Certificate Information

SECOM Trust Systems stores this CP in the Repository to allow online access thereto by Subscribers and Relying Parties.

Information specific to the CA operated on the Digital Certification Infrastructure to be published are stipulated in the CP thereof.

2.3 Time or Frequency of Publication

This CPS shall be published in the Repository as revised.

The timing and frequency of communicating the information specific to the CA operated on the Digital Certification Infrastructure to be published are stipulated in the CP thereof.

2.4 Access Controls on Repository

Provisions for Access Controls on Repository are stipulated in the CP of the CA operated on the Digital Certification Infrastructure.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

3.1.2 Need for Names to Be Meaningful

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

3.1.3 Anonymity or Pseudonymity of Subscribers

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

3.1.4 Rules for Interpreting Various Name Forms

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

3.1.5 Uniqueness of Names

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

3.1.6 Recognition, Authentication, and Roles of Trademarks

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

3.2.2 Authentication of Organization Identity

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

3.2.3 Authentication of Individual Identity

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

3.2.4 Non-Verified Subscriber Information

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

3.2.5 Validation of Authority

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

3.2.6 Criteria for Interoperation

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

3.3.2 Identification and Authentication for Re-Key after Revocation

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

3.4 Identification and Authentication for Revocation Requests

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who May Submit a Certificate Application

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.1.2 Enrollment Process and Responsibilities

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.2.2 Approval or Rejection of Certificate Applications

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.2.3 Time to Process Certificate Applications

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.3.2 Notifications to Subscriber of Certificate Issuance

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance
Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.4.2 Publication of the Certificate by the CA
Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities
Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage
Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.5.2 Relying Party Public Key and Certificate Usage
Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.6 Certificate Renewal

4.6.1 Circumstances for Certificate Renewal
Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.6.2 Who May Request Renewal
Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.6.3 Processing Certificate Renewal Requests
Relevant provisions are stipulated in the CP of the CAs operated on the Digital

Certification Infrastructure.

4.6.4 Notification of New Certificate Issuance to Subscriber
Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate
Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.6.6 Publication of the Renewal Certificates by the CA
Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities
Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.7 Certificate Re-Key

4.7.1 Circumstances for Certificate Re-Key
Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.7.2 Who May Request Certification of a New Public Key
Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.7.3 Processing Certificate Re-Keying Requests
Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.7.4 Notification of New Certificate Issuance to Subscriber
Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.7.6 Publication of the Re-Keyed Certificate by the CA

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.8 Certificate Modification

4.8.1 Circumstances for Certificate Modification

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.8.2 Who May Request Certificate Modification

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.8.3 Processing Certificate Modification Requests

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.8.4 Notification of New Certificate Issuance to Subscriber

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.8.6 Publication of the Modified Certificates by the CA

Relevant provisions are stipulated in the CP of the CAs operated on the Digital

Certification Infrastructure.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Certificate Revocation

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.9.2 Who Can Request Revocation

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.9.3 Procedure for Revocation Request

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.9.4 Revocation Request Grace Period

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.9.5 Time within Which CA Shall Process the Revocation Request

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.9.6 Revocation Checking Requirements for Relying Parties

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.9.7 CRL Issuance Frequency

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.9.8 Maximum Latency for CRLs

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.9.9 On-Line Revocation/Status Checking Availability

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.9.10 On-Line Revocation/Status Checking Requirements

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.9.11 Other Forms of Revocation Advertisements Available

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.9.12 Special Requirements Regarding Key Compromise

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.9.13 Circumstances for Suspension

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.9.14 Who Can Request Suspension

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.9.15 Procedure for Suspension Request

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.9.16 Limits on Suspension Period

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.10.2 Service Availability

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.10.3 Optional Features

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.11 End of Subscription (Registry)

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

5. Facility, Management, and Operational Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

SECOM Trust Systems has its certification infrastructure system installed within a secure data center. The data center is constructed on a premise hardly vulnerable to water exposures, earthquakes, fires or any other disasters, while structural measures have also been implemented to prevent and protect against such disasters.

5.1.2 Physical Access

SECOM Trust Systems implements appropriate security controls, combining physical and electronic access controls according to the critical level of the certification infrastructure system. In addition, access to the certification infrastructure systems is monitored through the installed surveillance cameras and other sensors.

5.1.3 Power and Air Conditioning

The data center is equipped with uninterruptible power supplies and backup generators as a measure of securing the power supply to enable uninterrupted operation of the certification infrastructure systems even during momentary or extended power outages. Additionally, the 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

SECOM Trust Systems installs the certification infrastructure systems on the second or a higher floor of the building for the flood control purpose, also deploying the water leakage sensors in the rooms housing the systems for protection against other water exposures.

5.1.5 Fire Prevention and Protection

The rooms in which the certification infrastructure systems are installed are fireproof compartments partitioned off by firewalls and equipped with fire alarms as well as fire extinguishing equipment.

5.1.6 Media Storage

SECOM Trust Systems stores archive, backup and other data and information critical to the performance of the certification services in a vault inside a room with proper access controls, deploying the measures to prevent potential damage and loss.

5.1.7 Waste Disposal

SECOM Trust Systems initializes and/or shreds sensitive paper documents and electronic media containing confidential information before disposal.

5.1.8 Off-Site Backup

SECOM Trust Systems implements measures for remote storage and retrieval/procurement of the data, equipment, and any other items required to operate the certification infrastructure systems.

5.2 Procedural Controls

5.2.1 Trusted Roles

SECOM Trust Systems defines the roles necessary for the operation of its certification infrastructure systems as follows:

(1) Person Responsible for Services

- Manages the Digital Certification Infrastructure.
- Approves modifications/revisions of the certification infrastructure systems and operational procedures.

(2) Service Operation Manager

- Gives work instructions to person(s) in charge of operation.
- Observes CA Private Key operations on site.
- Manages overall service operations.

(3) CA Administrator

- Maintains and manages CA servers, Repository servers and other certification infrastructure systems.
- Conducts activation and deactivation of CA Private Keys.

(4) Person in Charge of RA

- Controls registration and removal of the information of the customers performing the RA services using the certification infrastructure systems.
- Performs the RA services for CAs operating under the services provided by SECOM Trust Systems through the certification infrastructure systems.

(5) Log Examiner (Log Checker)

・ Checks room access, system and other logs.

5.2.2 Number of Persons Required per Task

With the exception of Service Operation Manager, SECOM Trust Systems deploys at least two persons performing the roles listed in "5.2.1 Trusted Roles" hereof to avoid disruptions in the provision of services. Critical operations, such as those related to the CA Private Key, are jointly performed by at least two persons.

5.2.3 Identification and Authentication for Each Role

With regard to any access to the certification infrastructure systems, SECOM Trust Systems shall conduct identification and authentication of the access-permitted individuals as well as the validity of the access to be an authorized action, through physical or logical means.

5.2.4 Roles Requiring Separation of Duties

As a general rule, individual roles listed in "5.2.1 Trusted Roles" hereof are performed by independent personnel. However, a Service Operation Manager may concurrently serve as a Log Examiner.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

Personnel to be deployed for the roles listed in "5.2.1 Trusted Roles" hereof shall be the employees who were hired conforming to the recruitment standards of SECOM Trust Systems.

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 certification infrastructure systems.

5.3.2 Background Check Procedures

SECOM Trust Systems assesses the reliability and suitability of the individuals responsible for the roles listed in "5.2.1 Trusted Roles" hereof at the time of appointment and on a regular basis thereafter.

5.3.3 Training Requirements

SECOM Trust Systems provides its personnel with the training necessary for the

operation of the certification infrastructure systems prior to their assumption of the roles and as needed thereafter in accordance with their respective roles. In the event of any change in the operational procedures, SECOM Trust Systems provides training for said change.

5.3.4 Retraining Frequency and Requirements

SECOM Trust Systems provides the individuals responsible for the roles listed in "5.2.1 Trusted Roles" hereof with refresher training as needed.

5.3.5 Job Rotation Frequency and Sequence

SECOM Trust Systems conducts 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 set forth in SECOM Trust Systems Rules of Employment apply.

5.3.7 Independent Contractor Requirement

When SECOM Trust Systems may employ independent contractors for operations of the certification infrastructure systems in whole or in part, the company ensures through the agreements therewith that the operational duties are duly performed by the contractors.

5.3.8 Documentation Supplied to Personnel

SECOM Trust Systems permits 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

SECOM Trust Systems records the following as the Audit Log:

(1) CA System Log

- Private Key operations by CAs
- Startup/shutdown of CA systems
- Database operations

- Permission granting history
- Certificate issuance and revocation histories
- CRL issuance history

(2) Room and Network Access Logs

- Record of accesses to the rooms in which the certification infrastructure systems are installed
- Record of unauthorized accesses to the certification infrastructure systems

Audit Log contains the following records:

- Date
- Time
- Subject causing the event
- Description of the event

5.4.2 Frequency of Processing Audit Log

SECOM Trust Systems probes the Audit Log on a regular basis.

5.4.3 Retention Period for Audit Log

SECOM Trust Systems retains the Audit Logs on the certification systems as Archive for a minimum of ten (10) years. Logs of the room entries/exits and network are retained for a minimum of one (1) year.

5.4.4 Protection of Audit Log

SECOM Trust Systems implements 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 certification infrastructure systems.

5.4.7 Notification to Event-Causing Subject

SECOM Trust Systems collects Audit Log without notifying the person, system or application that has caused the corresponding event.

5.4.8 Vulnerability Assessments

SECOM Trust Systems conducts assessment addressing the security vulnerabilities in the operational and system behavior aspects as well as reviews and revises 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

SECOM Trust Systems stores the following information in addition to the CA system log specified in "5.4.1 Types of Events Recorded" hereof, as Archive:

- Certificates and CRLs issued;
- This CPS
- documents governing the CA business practices, developed in compliance with this CPS;
- documents associated with agreements of subcontracting if the certification services are outsourced; and
- records of audit results and the audit reports;

Information specific to the CA operated on the Digital Certification Infrastructure to be archived are stipulated in the CP.

5.5.2 Retention Period for Archive

SECOM Trust Systems retains its Archive for a minimum of ten (10) years.

5.5.3 Protection of Archive

Archives are retained in a facility, access to which is restricted to the authorized personnel.

5.5.4 Archive Backup Procedures

The Archive is backed up whenever a change is made in such critical data pertaining to certification infrastructure system functions as Certificate issuance/revocation or CRL issuance.

5.5.5 Requirements for Time-Stamping of Records

SECOM Trust Systems uses the NTP (Network Time Protocol) to time-synchronize the certification infrastructure systems and Time-Stamps the critical data recorded therein.

5.5.6 Archive Collection System

The Archive collection system is included as a function of the certification infrastructure systems.

5.5.7 Procedures to Obtain and Verify Archive Information

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

5.6 Key Changeover

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

SECOM Trust Systems establishes measures against incidents and compromises, including the following, to ensure the prompt recovery of the certification infrastructure systems and relevant operations thereafter.

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

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

In the event of damage to any hardware, software or data of the certification infrastructure systems, SECOM Trust Systems promptly engages in the certification infrastructure systems recovery efforts using the relevant hardware, software or data retained as backup.

5.7.3 Entity Private Key Compromise Procedures

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

5.7.4 Business Continuity Capabilities after a Disaster

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

5.8 CA or RA Termination

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

Per this topic, this CPS provides for the Key controls by the CAs operated on the Digital Certification Infrastructure. The CP provides for the Key controls by such other participants as Subscribers.

6.1.1 Key Pair Generation

An FIPS140-2 Level 3 conformant HSM is used to generate Key Pairs for the CAs operated on the Digital Certification Infrastructure. The Key Pair generation is jointly performed by at least two authorized individuals.

6.1.2 Private Key Delivery to Subscriber

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

6.1.3 Public Key Delivery to Certificate Issuer

The Subscriber Public Keys may be delivered online to the CA operated on the Digital Certification Infrastructure, with the communication routing encrypted with SSL/TLS.

6.1.4 CA Public Key Delivery to Relying Parties

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

6.1.5 Key Sizes

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

6.1.6 Public Key Parameters Generation and Quality Checking

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

6.1.7 Key Usage Purposes

Relevant provisions are stipulated in the CP of the CAs operated on the Digital

Certification Infrastructure.

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 Private Keys of the CAs operated on the Digital Certification Infrastructure are performed using an FIPS140-2 Level 3 conformant HSM.

6.2.2 Private Key Multi-Person Control

Activation, deactivation, backup and other operations relating to Private Keys of the CAs operated on the Digital Certification Infrastructure are jointly performed by at least two authorized individuals in a secure environment.

6.2.3 Private Key Escrow

Private Keys of the CA operated on the Digital Certification Infrastructure are not escrowed.

6.2.4 Private Key Backup

Backup of Private Keys of the CAs operated on the Digital Certification Infrastructure is jointly performed by at least two authorized individuals and is stored in a secure room as encrypted.

6.2.5 Private Key Archival

Private Keys of the CAs operated on the Digital Certification Infrastructure are not archived.

6.2.6 Private Key Transfer into or from a Cryptographic Module

The transfer of Private Keys of the CAs operated on the Digital Certification Infrastructure into and from an HSM is performed in a secure room while encrypted.

6.2.7 Private Key Storage on Cryptographic Module

Private Keys of the CAs operated on the Digital Certification Infrastructure are stored within the HSM while encrypted.

6.2.8 Method of Activating Private Key

Private Keys of the CAs operated on the Digital Certification Infrastructure are jointly activated by at least two authorized individuals in a secure room.

6.2.9 Method of Deactivating Private Key

Private Keys of the CAs operated on the Digital Certification Infrastructure are jointly deactivated by at least two authorized individuals in a secure room.

6.2.10 Method of Destroying Private Key

Private Keys of the CAs operated on the Digital Certification Infrastructure are jointly destroyed by at least two authorized individuals by means of complete initialization or physical destruction. The Private Key backups are also destroyed in the same manner.

6.2.11 Cryptographic Module Rating

The quality standards to be applied to the HSMs used in certification infrastructure systems are as specified in "6.2.1 Cryptographic Module Standards and Controls" hereof.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Archival of Public Keys of the CAs operated on the Digital Certification Infrastructure is covered by "5.5.1 Types of Archives" hereof.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The maximum key usage period for Private Keys of the CAs operated on the Digital Certification Infrastructure shall not exceed twenty (20) years.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The activation data required to use Private Keys of the CAs operated on the Digital Certification Infrastructure are jointly generated by at least two authorized individuals and are stored on a digital medium.

6.4.2 Activation Data Protection

The digital media storing the data required for activation of Private Keys of the CAs operated on the Digital Certification Infrastructure are stored under control in a secure room.

6.4.3 Other Aspects of Activation Data
No stipulation

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements
SECOM Trust Systems conducts detailed inspections of the quality, stability, safety and other aspects of any hardware or software to be implemented in the certification infrastructure systems before making the decision to implement.

6.5.2 Computer Security Rating
SECOM Trust Systems conducts the preproduction system tests of all software and hardware to be employed by the certification infrastructure systems in an effort to secure the system reliability. In addition, SECOM Trust Systems constantly collects information on the security vulnerabilities of the certification infrastructure systems and performs assessments to be able to promptly take proper actions should any vulnerability be detected.

6.6 Life-Cycle Technical Controls

6.6.1 System Development Controls
Certification infrastructure systems are configured and maintained in a secure environment. Security is thoroughly assessed and verified when modifying a certification infrastructure system. 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
SECOM Trust Systems ensures security by conducting operational administration, such as management 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

SECOM Trust Systems performs assessments as appropriate to ensure that the certification infrastructure systems are developed, operated and maintained properly, and to make improvements as needed.

6.7 Network Security Controls

SECOM Trust Systems implements firewalls, IDS and other measures as protection against unauthorized access through the network to the certification infrastructure 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

7.1.1 Version Number(s)

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

7.1.2 Certificate Extensions

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

7.1.3 Algorithm Object Identifiers

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

7.1.4 Name Forms

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

7.1.5 Name Constraints

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

7.1.6 Certificate Policy Object Identifier

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

7.1.7 Use of Policy Constraints Extension

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

7.1.8 Policy Qualifiers Syntax and Semantics

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

7.2 CRL Profile

7.2.1 Version Number(s)

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

7.2.2 CRL and CRL Entry Extension

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

7.3 OCSP Profile

7.3.1 Version Number(s)

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

7.3.2 OCSP Extensions

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

8. Compliance Audit and Other Assessments

8.1 Frequency and Circumstances of Assessment

SECOM Trust Systems conducts audits from time to time to examine if the operations of the Digital Certification Infrastructure are in compliance with this CPS or not.

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

The primary scope of the audit shall be the compliance with this CPS in the operations of the Digital Certification Infrastructure.

8.5 Actions Taken as a Result of Deficiency

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

8.6 Communication of Results

Compliance audit results shall be reported to SECOM Trust Systems by the auditor(s).

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

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

9.2 Financial Responsibility

SECOM Trust Systems shall maintain adequate financial resources for the operation and maintenance of the Digital Certification Infrastructure.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

Information on individuals and organizations in the possession of SECOM Trusts Systems are subject to confidentiality with the exception of those that were explicitly published as a part of a Certificate, a CRL, this CPS, or a relevant CP. SECOM Trust Systems does not disclose such information externally unless it is required by law or there is a prior consent of the relevant Subscriber. SECOM Trust Systems 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.

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 Trust Systems;
- information that was or is made known to SECOM Trust Systems by a party other than SECOM Trust Systems without confidentiality requirements;
- information independently developed by SECOM Trust Systems; or
- information approved for disclosure by the relevant Subscriber.

9.3.3 Responsibility to Protect Confidential Information

SECOM Trust Systems may disclose confidential information 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

SECOM Trust Systems uses the personal information collected from Subscribers to its Certification and Private CA users to the extent necessary for the operation of CAs established on the Digital Certification Infrastructure, such as authentication of the application details, post-mailing or transmission of the required documents and the like, and authentication of the persons to be authorized. The personal information protection policy (privacy policy) of SECOM Trust Systems is published on its website (http://www.secomtrust.net).

9.5 Intellectual Property Rights

Unless otherwise agreed to between SECOM Trust Systems and the relevant Subscriber or a contracting party, the copyright and other rights pertaining to this CPS shall belong to SECOM Trust Systems. Information specific to a CA are stipulated in the relevant CP.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

9.6.2 RA Representations and Warranties

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

9.6.3 Subscriber Representations and Warranties

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

9.6.4 Relying Party Representations and Warranties

Relevant provisions are stipulated in the CP of the CAs operated on the Digital

Certification Infrastructure.

9.6.5 Representations and Warranties of Other Participants

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

9.7 Disclaimer of Warranties

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

9.8 Limitations of Liability

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

9.9 Indemnities

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

9.10 Term and Termination

9.10.1 Term

This CPS goes into effect upon approval by the Certification Services Improvement Committee. This CPS 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 CPS loses effect as of the termination of the Digital Certification Infrastructure by SECOM Trust Systems, with the exception of the provisions stipulated in "9.10.3 Effect of Termination and Survival" hereof.

9.10.3 Effect of Termination and Survival

Even in the event of termination of the use of a Certificate by a Subscriber, termination of the agreement between SECOM Trust Systems and the other party thereto, or the termination of the services provided by SECOM Trust Systems, provisions that should remain in effect, due to the nature thereof, shall survive any such termination, regardless of the reasons therefor, and remain in full force and

effect with respect to any Subscriber, Relying Party, entity in a contractual relationship with SECOM Trust Systems, and SECOM Trust Systems itself.

9.11 Individual Notices and Communications with Participants

SECOM Trust Systems provides necessary notifications to Subscribers, Relying Parties and contracting parties through its website, e-mail, or in a written form or otherwise.

9.12 Amendments

9.12.1 Procedure for Amendment

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

9.12.2 Notification Method and Timing

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

9.12.3 Circumstances under Which OID Must Be Changed

No stipulation

9.13 Dispute Resolution Procedures

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

9.14 Governing Law

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

9.15 Compliance with Applicable Law

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

9.16.2 Assignment

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

9.16.3 Severability

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

9.16.4 Enforcement

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

9.16.5 Irresistible Force

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.

9.17 Other Provisions

Relevant provisions are stipulated in the CP of the CAs operated on the Digital Certification Infrastructure.