Security Communication RootCA
Certification Practice Statement
Version 6.05

October 23, 2024

SECOM Trust Systems Co., Ltd.

Version History		
Version Number	Date	Description
1.00	2003/09/29	Publication of the first version
2.00	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
3.00	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."
4.00	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"
4.10	2012/02/15	"5.6 Key Changeover" - Addition of Certificate Renewal
4.20	2012/11/09	Amendment associated with commencement of the OCSP server operations
5.00	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"
5.10	2017/05/23	Overall revision of the descriptions and styles
5.11	2018/11/28	Overall revision of the descriptions and styles
5.12	2019/05/24	Overall revision of the descriptions and styles
5.13	2020/03/30	Revised chapters and added some " No Stipulation" content
5.14	2021/03/30	Update of the date and version
5.15	2021/11/30	Overall revision of the descriptions and styles
5.16	2022/06/10	Overall revision of the descriptions and styles

6.00	2023/01/16	Major version upgrade Addition of the CA Private Key "SECOM TLS RSA Root CA 2023" Addition of the CA Private Key "SECOM RSA Root CA 2023" Addition of the CA Private Key "SECOM Document Signing RSA Root CA 2023"
6.01	2023/02/10	Addition of SECOM TLS RSA Root CA 2023 Fingerprint Addition of SECOM RSA Root CA 2023 Fingerprint Addition of SECOM Document Signing RSA Root CA 2023 Fingerprint
6.02	2023/05/17	Update “2.3 Time or Frequency of Publication” Update “5.5.2 Retention Period for Archive” Update “5.7.3 Entity Private Key Compromise Procedures”
6.03	2024/01/24	Addition of the CA Private Key SECOM TLS RSA Root CA 2024 Addition of the CA Private Key SECOM TLS ECC Root CA 2024 Addition of the CA Private Key SECOM SMIME RSA Root CA 2024 Deletion of the CA Private Key SECOM TLS RSA Root CA 2023 Update “1.1 Overview” Update “1.2 Document Name and Identification” Update “1.6 Definitions and Acronyms” Update “6.1.5 Key Sizes” Update “8.4 Topics Covered by Assessment”
6.04	2024/04/01	Update “1.1 Overview”

6.05	2024/10/23	Update the below: 1.5.2 Contact Information 5.4.1 Types of Events Recorded 5.4.1.1 Router and firewall activities logs 5.4.1.2 Types of events recorded for Timestamp Authorities 5.4.3 Retention Period for Audit Log 5.5.1 Types of Records Archived 5.5.2 Retention Period for Archive 5.5.3 Protection of Archive 5.5.4 Archive Backup Procedures 6.1.1 Key Pair Generation 6.2.1 Cryptographic Module Standards and Controls 6.2.2 Private Key Multi-Person Control 6.2.4 Private Key Backup 6.2.5 Private Key Archival 6.2.6 Private Key Transfer into or from a Cryptographic Module 6.2.7 Private Key Storage on Cryptographic Module 6.2.11 Cryptographic Module Rating 6.3.2 Certificate Operational Periods and Key Pair Usage Periods 8.7 Self-Audit

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 Root CA (hereinafter "the CA") that is 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.

CAs that issue certificates whose subordinate CA certificates comply with the "Security Communication RootCA Subordinate CA Certificate Policy" shall conform to the latest versions of the standards established by the CA/Browser Forum (hereinafter referred to as Baseline Requirements) published at https://www.cabforum.org/ and Application Software Supplier Requirements.

Table 1.1-1 List of Standards

Types of certificates issued by Subordinate CA	Standards to comply with
TLS Server Certificate	● Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates ● Guidelines for the Issuance and Management of Extended Validation Certificates (TLS EV Certificate only) ● Apple Root Certificate Program ● Chrome Root Program Policy ● Microsoft Trusted Root Program ● Mozilla Root Store Policy
TLS Client Authentication Certificate	● Apple Root Certificate Program ● Microsoft Trusted Root Program

S/MIME Certificate	● Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates ● Apple Root Certificate Program ● Microsoft Trusted Root Program ● Mozilla Root Store Policy
Code Signing Certificate Timestamp Certificate for Code Signing Certificate	● Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates ● Microsoft Trusted Root Program
AATL Document Signing Certificate AATL Timestamp Certificate	● Adobe Approved Trust List Technical Requirements (AATL Technical Requirements)
Microsoft Compliant Document Signing Certificate	● Microsoft Trusted Root Program

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. In the event of any inconsistency between this CPS and Baseline Requirements, Baseline Requirements take precedence over this CPS.

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.

This CPS shows the root CA certificate of the CAs in Table "1.1-2 Root CA Certificate".

Table 1.1-2 Root CA Certificate

Distinguished Name（DN）	SHA256 Fingerprint
C = JP, O = SECOM Trust Systems CO.,LTD., OU = Security Communication RootCA2	513B2CECB810D4CDE5DD85391ADFC6C2DD60D87BB736D2B521484AA47A0EBEF6
C = JP, O = SECOM Trust Systems CO.,LTD., CN = Security Communication RootCA3	24A55C2AB051442D0617766541239A4AD032D7C55175AA34FFDE2FBC4F5C5294
C = JP, O = SECOM Trust Systems CO.,LTD., CN = Security Communication ECC	E74FBDA55BD564C473A36B441AA799C8A68E077440E8288B9FA1E50E4BBACA11

RootCA1	
C = JP, O = SECOM Trust Systems Co., Ltd., CN = SECOM RSA Root CA 2023	2C154235528D701790B675AFF6E19708 27B10ED665E913835BF46E3460FD5C8 4
C = JP, O = SECOM Trust Systems Co., Ltd., CN = SECOM Document Signing RSA Root CA 2023	46219BBF9148F00E8B7A4C619B57CF7 602701FF81348400718870FABD31FC5B E
C = JP O = SECOM Trust Systems Co., Ltd. CN = SECOM TLS RSA Root CA 2024	1435F225C5D252D7A21948CC3CE62AE CFA88001E3DD72D1CC3555100EB372F 93
C = JP O = SECOM Trust Systems Co., Ltd. CN = SECOM TLS ECC Root CA 2024	6AB2AB75F51CB4F4F0156203FBF6F64 6232F514BE059F62833308B82B4D72DB 1
C = JP O = SECOM Trust Systems Co., Ltd. CN = SECOM SMIME RSA Root CA 2024	3629E7188E00A7CB3232C4426BC84912 F1218B1A9AE676C0B0ABE1DBFE2182 B5

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 RootCA2 Subordinate CA CP	1.2.392.200091.100.901.4
Security Communication RootCA2 Time-Stamp Service CP	1.2.392.200091.100.901.5
Security Communication RootCA3 Subordinate CA CP	1.2.392.200091.100.901.6
Security Communication RootCA3 Time-Stamp Service CP	1.2.392.200091.100.901.7
SECOM RSA Root CA 2023 Subordinate CA CP	1.2.392.200091.100.901.9
SECOM Document Signing RSA Root CA 2023 Subordinate CA CP	1.2.392.200091.100.901.10
SECOM TLS RSA Root CA 2024 Subordinate CA CP	1.2.392.200091.100.901.11
SECOM SMIME RSA Root CA 2024 Subordinate CA CP	1.2.392.200091.100.901.12
Security Communication ECC RootCA1 Subordinate CA CP	1.2.392.200091.100.902.1
SECOM TLS ECC Root CA 2024 Subordinate CA CP	1.2.392.200091.100.902.3

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 responder.

CA is defined in "1.6 Definitions and Acronyms".

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.

If the subordinate CA certificate is a CA that issues a TLS server certificate that complies with the "Security Communication RootCA Certificate Policy for Subordinate CAs", with

the exception of domain name and IP address validation tasks required by Baseline Requirements 3.2.2.4 and 3.2.2.5, the CAs may delegate the performance of all, or any part, of Baseline Requirements 3.2 to a Delegated Third Party, provided that the process as a whole fulfills all of the Baseline Requirements 3.2.

(1) Meet the qualification requirements of this CPS "5.3.1 Qualifications, Experience, and Clearance Requirements" when applicable to the delegated function;
(2) Retain documentation in accordance with this CPS "5.5.2 Retention Period for Archive";
(3) Abide by the other provisions of these Requirements that are applicable to the delegated function; and
(4) Comply with the CA's Certificate Policy/Certification Practice Statement or the Delegated Third Party's practice statement that the CAs have verified complies with Baseline Requirements.

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.
"Relying parties" and "Application Software Suppliers" are defined in "1.6 Definitions and Acronyms".

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 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:Contact Information	CA Support Center, SECOM Trust Systems Co., Ltd.
Address	8-10-16 Shimorennjaku, Mitaka-shi, Tokyo 181-8528

Inquiry details	Inquiries for this CP Except for Certificate Problem Report
E-mail	ca-support@secom.co.jp
Business hours	9:00-18:00 (except Saturdays, Sundays, national holidays, and year-end and New Year holidays)

The Subscribers, Relying Parties, Application Software Suppliers, and other third parties can report suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates. The CA revokes certificates when it is determined that it needs to be revoked.

Inquiry details	Certificate Problem Report
URL	https://www.secomtrust.net/sts/cert/report_entry.html
Business hours	24x7

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. This CPS will be reviewed and revised at least annually.

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

Application Software Supplier

A supplier of Internet browser software or other relying party application software that displays or uses a certificate and incorporates a root CA certificate.

Attestation Letter

A letter attesting that Subject Information is correct, which is written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information.

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.

Relying Party

Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such Supplier merely displays information relating to a Certificate.

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.

Root CA

Root CA 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.

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 bit length of SHA-256 is 256 bits, and the bit length of SHA-384 is 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 maintained by CPA Canada 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 24x7 online access by the Subscribers and Relying Parties:

- Certificate Revocation List (hereinafter, "CRL") 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

The CAs shall host test Web pages that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate. At a minimum, the CAs shall host separate Web pages using Subscriber Certificates that are i valid, ii. revoked, and iii. expired.

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

The CA shall develop, implement, enforce, and annually update a CP and CPS that describes in detail how the CA implements the latest version of the Baseline Requirements. The CA shall indicate conformance with the Baseline Requirements by incrementing the version number and adding a dated changelog entry, even if no other changes are made to a CP and CPS.

2.4 Access Controls on Repositories

The CAs make their Repository publicly available in a read-only manner. In the CAs, only the authorized CA administrators can perform operations such as adding, deleting, modifying, and publishing Repositories.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names
Stipulated in the relevant CP.

3.1.2 Need for Names to Be Meaningful
Stipulated in the relevant CP.

3.1.3 Anonymity or Pseudonymity of Subscribers
Stipulated in the relevant CP.

3.1.4 Rules for Interpreting Various Name Forms
Stipulated in the relevant CP.

3.1.5 Uniqueness of Names
Stipulated in the relevant CP.

3.1.6 Recognition, Authentication, and Roles of Trademarks
Stipulated in the relevant CP.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key
Stipulated in the relevant CP.

3.2.2 Authentication of Organization Identity
Stipulated in the relevant CP.

3.2.2.1 Identity
Stipulated in the relevant CP.

3.2.2.2 DBA/Tradename
Stipulated in the relevant CP.

3.2.2.3 Verification of Country
Stipulated in the relevant CP.

3.2.3 Authentication of Individual Identity
Stipulated in the relevant CP.

3.2.4 Non-Verified Subscriber Information
Stipulated in the relevant CP.

3.2.5 Validation of Authority
Stipulated in the relevant CP.

3.2.6 Criteria for Interoperation
Stipulated in the relevant CP.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for routine Re-Key Requests
Stipulated in the relevant CP.

3.3.2 Identification and Authentication for Re-Key after Revocation
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

4.1.1 Who May Submit a Certificate Application
Stipulated in the relevant CP.

4.1.2 Enrollment Process and Responsibilities
Stipulated in the relevant CP.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions
Stipulated in the relevant CP.

4.2.2 Approval or Rejection of Certificate Applications
Stipulated in the relevant CP.

4.2.3 Time to Process Certificate Applications
Stipulated in the relevant CP.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance
Stipulated in the relevant CP.

4.3.2 Notifications to Subscriber of Certificate Issuance
Stipulated in the relevant CP.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance
Stipulated in the relevant CP.

4.4.2 Publication of the Certificate by the CA
Stipulated in the relevant CP.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities
Stipulated in the relevant CP.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage
Stipulated in the relevant CP.

4.5.2 Relying Party Public Key and Certificate Usage
Stipulated in the relevant CP.

4.6 Certificate Renewal

4.6.1 Circumstances for Certificate Renewal
Stipulated in the relevant CP.

4.6.2 Who May Request Renewal
Stipulated in the relevant CP.

4.6.3 Processing Certificate Renewal Requests
Stipulated in the relevant CP.

4.6.4 Notification of New Certificate Issuance to Subscriber
Stipulated in the relevant CP.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate
Stipulated in the relevant CP.

4.6.6 Publication of the Renewal Certificates by the CA
Stipulated in the relevant CP.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities
Stipulated in the relevant CP.

4.7 Certificate Re-Key

4.7.1 Circumstances for Certificate Re-Key
Stipulated in the relevant CP.

4.7.2 Who May Request Certification of a New Public Key
Stipulated in the relevant CP.

4.7.3 Processing Certificate Re-Keying Requests
Stipulated in the relevant CP.

4.7.4 Notification of New Certificate Issuance to Subscriber
Stipulated in the relevant CP.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate
Stipulated in the relevant CP.

4.7.6 Publication of the Re-Keyed Certificate by the CA
Stipulated in the relevant CP.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities
Stipulated in the relevant CP.

4.8 Certificate Modification

4.8.1 Circumstances for Certificate Modification
Stipulated in the relevant CP.

4.8.2 Who May Request Certificate Modification
Stipulated in the relevant CP.

4.8.3 Processing Certificate Modification Requests
Stipulated in the relevant CP.

4.8.4 Notification of New Certificate Issuance to Subscriber
Stipulated in the relevant CP.

4.8.5 Conduct Constituting Acceptance of Modified Certificate
Stipulated in the relevant CP.

4.8.6 Publication of the Modified Certificates by the CA
Stipulated in the relevant CP.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities
Stipulated in the relevant CP.

4.9 Certificate Revocation and Suspension

4.9.1 Reason for Certificate Revocation
Stipulated in the relevant CP.

4.9.2 Who Can Request Revocation
Stipulated in the relevant CP.

4.9.3 Procedure for Revocation Request
Stipulated in the relevant CP.

4.9.4 Revocation Request Grace Period
Stipulated in the relevant CP.

4.9.5 Time within Which CA Shall Process the Revocation Request
Stipulated in the relevant CP.

4.9.6 Revocation Checking Requirements for Relying Parties
Stipulated in the relevant CP.

4.9.7 CRL Issuance Frequency
Stipulated in the relevant CP.

4.9.8 Maximum Latency for CRLs
Stipulated in the relevant CP.

4.9.9 On-Line Revocation/Status Checking Availability
Stipulated in the relevant CP.

4.9.10 On-Line Revocation/Status Checking Requirements
Stipulated in the relevant CP.

4.9.11 Other Forms of Revocation Advertisements Available
Stipulated in the relevant CP.

4.9.12 Special Requirements Regarding Key Compromise
Stipulated in the relevant CP.

4.9.13 Circumstances for Suspension
Stipulated in the relevant CP.

4.9.14 Who Can Request Suspension
Stipulated in the relevant CP.

4.9.15 Procedure for Suspension Request
Stipulated in the relevant CP.

4.9.16 Limits on Suspension Period
Stipulated in the relevant CP.

4.10 Certificate Status Services

4.10.1 Operational Characteristics
Stipulated in the relevant CP.

4.10.2 Service Availability
Stipulated in the relevant CP.

4.10.3 Optional Features
Stipulated in the relevant CP.

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

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices
Stipulated in the relevant CP.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices
Stipulated in the relevant CP.

5. Facility, Management, and Operational Controls

The CA/Browser Forum's "Network and Certificate System Security Requirement" is fully incorporated into this document by reference.

The CAs shall develop, implement, and maintain a comprehensive security program designed to:

1. Protect the confidentiality, integrity, and availability of Certificate Data and Certificate Management Processes;
2. Protect against anticipated threats or hazards to the confidentiality, integrity, and availability of the Certificate Data and Certificate Management Processes;
3. Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of any Certificate Data or Certificate Management Processes;
4. Protect against accidental loss or destruction of, or damage to, any Certificate Data or Certificate Management Processes; and
5. Comply with all other security requirements applicable to the CAs by law.

The Certificate Management Process MUST include:

1. Physical security and environmental controls;
2. System integrity controls, including configuration management, integrity maintenance of trusted code, and malware detection/prevention;
3. Network security and firewall management, including port restrictions and IP address filtering;
4. User management, separate trusted-role assignments, education, awareness, and training; and
5. Logical access controls, activity logging, and inactivity time-outs to provide individual accountability.

The CA's security program must include the following annual risk assessments:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;
2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CAs have in place to counter such threats.

Based on the Risk Assessment, the CAs shall develop, implement, and maintain a security plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of the Certificate Data and Certificate Management Processes. The security plan must include administrative,

organizational, technical, and physical safeguards appropriate to the sensitivity of the Certificate Data and Certificate Management Processes. The security plan must also take into account then-available technology and the cost of implementing the specific measures, and shall implement a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

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 Media Storage

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

5.1.7 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.

5.1.8 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

5.1.9 Earthquake

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

5.2 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	- Checks room access, system and other logs.

Checker)	

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.

The CA Private Key shall be backed up, stored, and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment.

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

Prior to the engagement of any person in the Certificate Management Process, whether as an employee, agent, or an independent contractor of the CAs, the CAs shall verify the identity and trustworthiness of such person.

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.

The CAs shall provide all personnel performing information verification duties with skills-training that covers basic Public Key Infrastructure knowledge, authentication and vetting policies and procedures (including the CA's Certificate Policy and/or

Certification Practice Statement), common threats to the information verification process (including phishing and other social engineering tactics), and these Requirements.
The CAs shall maintain records of such training and ensure that personnel entrusted with Validation Specialist duties maintain a skill level that enables them to perform such duties satisfactorily.
The CAs shall document that each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task.
The CAs shall require all Validation Specialists to pass an examination provided by the CAs on the information verification requirements outlined in these Requirements.

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.
All personnel in Trusted Roles shall maintain skill levels consistent with the CA's training and performance programs.

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.
The CAs shall verify that the Delegated Third Party's personnel involved in the issuance of a Certificate meet the training and skills requirements of this CPS "5.3.3 Training Requirements" and this CPS "5.4.1 Types of Events Recorded".

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.
The CA shall record at least the following events:

1. CA certificate and key lifecycle events, including:
   1. Key generation, backup, storage, recovery, archival, and destruction;
   2. Certificate requests, renewal, and re-key requests, and revocation;
   3. Approval and rejection of certificate requests;
   4. Cryptographic device lifecycle management events;
   5. Generation of Certificate Revocation Lists and OCSP entries;
   6. Signing of OCSP Responses
   7. Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.
2. Subscriber Certificate lifecycle management events, including:
   1. Certificate requests, renewal, and re-key requests, and revocation;
   2. All verification activities stipulated in these Requirements and the CA's Certification Practice Statement;
   3. Approval and rejection of certificate requests;
   4. Issuance of Certificates; and
   5. Generation of Certificate Revocation Lists and OCSP entries.
3. Security events, including:
   1. Successful and unsuccessful PKI system access attempts;
   2. PKI and security system actions performed;
   3. Security profile changes;
   4. Installation, update and removal of software on a Certificate System;
   5. System crashes, hardware failures, and other anomalies;
   6. Relevant router and firewall activities (as described in this CPS "5.4.1.1 Router and firewall activities logs". Applies to CAs for TLS server certificates and S/MIME certificates); and
   7. Entries to and exits from the CA facility.

Log records MUST include the following elements:

1. Date and time of record;
2. Identity of the person making the journal record; and
3. Description of the record.

5.4.1.1 Router and firewall activities logs

Logging of router and firewall activities necessary to meet the requirements of this CPS "5.4.1, Types of Events Recorded" 3.6 MUST at a minimum include (Applies to CAs for TLS server certificates and S/MIME certificates):

1. Successful and unsuccessful login attempts to routers and firewalls; and
2. Logging of all administrative actions performed on routers and firewalls, including

configuration changes, firmware updates, and access control modifications; and
3. Logging of all changes made to firewall rules, including additions, modifications, and deletions; and
4. Logging of all system events and errors, including hardware failures, software crashes, and system restart.

5.4.1.2 Types of events recorded for Timestamp Authorities
[Code Signing Certificate]
The Timestamp Authority MUST log the following information and make these records available to its Qualified Auditor as proof of the Timestamp Authority's compliance with Baseline Requirements for Code Signing Certificates:

1. Physical or remote access to a timestamp server, including the time of the access and the identity of the individual accessing the server,
2. History of the timestamp server configuration,
3. Any attempt to delete or modify timestamp logs,
4. Security events, including:
   a. Successful and unsuccessful Timestamp Authority access attempts;
   b. Timestamp Authority server actions performed;
   c. Security profile changes;
   d. System crashes, and other anomalies; and
   e. Firewall and router activities.
5. Revocation of a timestamp certificate,
6. Major changes to the timestamp server's time, and
7. System startup and shutdown.

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 shall be retained for at least two (2) years:

1. The CA certificate and key lifecycle management event record (described in this CPS "5.4.1 Types of Events Recorded") shall be retained after any of the following have occurred:
   1. The destruction of the CA Private Key; or
   2. The revocation or expiration of the final CA Certificate in that set of Certificates that have an X.509v3 basicConstraints extension with the cA field set to true and which share a common Public Key corresponding to the CA Private Key;
2. Subscriber Certificate lifecycle management event records (described in this CPS "5.4.1 Types of Events Recorded") after the revocation or expiration of the Subscriber Certificate;

3. Any security event records (described in this CPS "5.4.1 Types of Events Recorded") after the event occurred.
4. For code signing certificates, the time stamp authority data record after the revocation or renewal of the time stamp certificate private key (specified in this CPS "5.4.1.2 Types of Events Recorded by the Time Stamp Authority"), and the security event record after the event occurred (specified in this CPS "5.4.1 Types of Events Recorded").

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 assessments 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.

Additionally, the CA's security program must include an annual Risk Assessment that:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;
2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CAs have in place to counter such threats.

5.5 Records Archival

5.5.1 Types of Records Archived

The CA stores the following information in addition to the CA system log specified in this CPS "5.4.1 Types of Events Recorded" hereof, as Archive:

- Documentation related to the security of their Certificate Systems, Certificate Management Systems, Root CA Systems, and Delegated Third Party Systems; and
- Documentation related to their verification, issuance, and revocation of certificate requests and Certificates.

Archive information specific to CAs operated on the Digital Certification Infrastructure is specified in the CP.

5.5.2 Retention Period for Archive

Archived audit logs (as set forth in this CPS “5.5.1 Types of Records Archived” SHALL be retained for a period of at least two (2) years from their record creation timestamp, or as long as they are required to be retained per this CPS “5.4.3 Retention Period for Audit Log”, whichever is longer. Additionally, the CA and each Delegated Third Party SHALL retain, for at least two (2) years:

1. All archived documentation related to the security of Certificate Systems, Certificate Management Systems, Root CA Systems and Delegated Third Party Systems (as set forth in this CPS “5.5.1 Types of Records Archived”);
2. All archived documentation relating to the verification, issuance, and revocation of certificate requests and Certificates (as set forth in this CPS “5.5.1 Types of Records Archived”) after the later occurrence of:

   i. such records and documentation were last relied upon in the verification, issuance, or revocation of certificate requests and Certificates; or

   ii. the expiration of the Subscriber Certificates relying upon such records and documentation.

5.5.3 Protection of Archive

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

5.5.4 Archive Backup Procedures

If there are any changes to important data related to the Certification Infrastructure system, such as certificate issuance, revocation, or CRL issuance, an archive backup shall be obtained in a timely manner.

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.

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.

The CAs shall have an Incident Response Plan and a Disaster Recovery Plan.

The CAs shall document a business continuity and disaster recovery procedures designed to notify and reasonably protect Application Software Suppliers, Subscribers, and Relying Parties in the event of a disaster, security compromise, or business failure. The CAs are not required to publicly disclose its business continuity plans but shall make their business continuity plan and security plans available to the CA's auditors upon request. The CAs shall annually test, review, and update these procedures.

The business continuity plan must include:

1. The conditions for activating the plan,
2. Emergency procedures,
3. Fallback procedures,
4. Resumption procedures,
5. A maintenance schedule for the plan;
6. Awareness and education requirements;

7. The responsibilities of the individuals;
8. Recovery time objective (RTO);
9. Regular testing of contingency plans.
10. The CA's plan to maintain or restore the CA's business operations in a timely manner following interruption to or failure of critical business processes.
11. A requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location;
12. What constitutes an acceptable system outage and recovery time
13. How frequently backup copies of essential business information and software are taken;
14. The distance of recovery facilities to the CA's main site; and
15. Procedures for securing its facility to the extent possible during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site.

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 CAs. 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" of Security Communication RootCA Subordinate CA Certificate Policy or Security Communication RootCA Time-Stamp Service Certificate Policy.

In the event that the operation of the system related to the CA is interrupted or stopped, the CA shall notify the relevant parties, including the application software supplier, in accordance with the predetermined plans and procedures to safely resume operation.

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, including Application Software Suppliers, 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

The following management is performed for the key pair of the root CA:

1. Prepare and follow a Key Generation Script,
2. Have a Qualified Auditor witness the CA Key Pair generation process, and
3. Have a Qualified Auditor issue a report opining that the CA followed its key ceremony during its Key and Certificate generation process and the controls used to ensure the integrity and confidentiality of the Key Pair.

The following management is performed for the key pair of the subordinate CA.

1. Prepare and follow a Key Generation Script and
2. Have a Qualified Auditor witness the CA Key Pair generation process.

In all cases, the CAs shall:

1. Generate the CA Key Pair in a physically secured environment as described in the CA's Certificate Policy and/or Certification Practice Statement;
2. Generate the CA Key Pair using personnel in trusted roles under the principles of multiple person control and split knowledge;
3. Generate the CA Key Pair within cryptographic modules meeting the applicable technical and business requirements as disclosed in the CA's Certificate Policy and/or Certification Practice Statement; The key pair of this CA is generated on a hardware security module (hereinafter referred to as "HSM") compliant with this CPS "6.2.7 Private Key Storage on Cryptographic Module".
4. Log its CA Key Pair generation activities; and
5. Maintain effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in its Certificate Policy and/or Certification Practice Statement and (if applicable) its Key Generation Script.

For key pair generation of subscriber certificates for TLS server certificates, the subordinate CA must reject the certificate request if one or more of the following conditions are met: The subordinate CA shall perform the following:

1. The key pair does not meet the requirements described in this CPS "6.1.5 Key Sizes" or this CPS "6.1.6 Public Key Parameters Generation and Quality Checking";
2. There is clear evidence that the specific method used to generate the Private Key was flawed;
3. The CAs are aware of a demonstrated or proven method that exposes the Applicant's Private Key to compromise;
4. The subordinate CA has previously been made aware that the Applicant's Private Key has suffered a Key Compromise, such as through the provisions of the CP "4.9.1 Reason for Certificate Revocation".
5. The Subordinate CA is aware of a demonstrated or proven method to easily compute the Applicant's Private Key based on the Public Key (such as a Debian weak key, see https://wiki.debian.org/SSLkeys).

6.1.2 Private Key Delivery to Subscriber

The private key is owned only by the subscriber, and the private key will not be sent from the CAs.

6.1.3 Public Key Delivery to Certificate Issuer

Subscriber Public Keys are verified according to the procedure set forth in the CP "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

CA Key	Public Key Algorithm	Signature Algorithm
Security Communication RootCA2	RSA2048 bit	sha256WithRSAEncryption
Security Communication RootCA3	RSA4096 bit	sha384WithRSAEncryption
Security Communication ECC RootCA1	ECC 384 bit (secp384r1)	ecdsa-with-SHA384
SECOM RSA Root CA 2023	RSA4096 bit	sha384WithRSAEncryption
SECOM Document Signing RSA Root CA 2023	RSA4096 bit	sha384WithRSAEncryption

SECOM TLS RSA Root CA 2024	RSA4096 bit	sha384WithRSAEncryption
SECOM TLS ECC Root CA 2024	ECC 384 bit (secp384r1)	ecdsa-with-SHA384
SECOM SMIME RSA Root CA 2024	RSA4096 bit	sha384WithRSAEncryption

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.

【RSA】

The CAs shall confirm that the value of the public exponent is an odd number equal to 3 or more. Additionally, the public exponent should be in the range between 2^16+1 and 2^256 - 1. The modulus should also have the following characteristics: an odd number, not the power of a prime, and have no factors smaller than 752. [Source: Section 5.3.3, NIST SP 800-89].

【ECDSA】

The CAs should confirm the validity of all keys using either the ECC Full Public Key Validation Routine or the ECC Partial Public Key Validation Routine. [Source: Sections 5.6.2.3.2 and 5.6.2.3.3, respectively, of NIST SP 800-56A: Revision 2].

6.1.7 Key Usage Purposes

Private Keys corresponding to Root Certificates must not be used to sign Certificates except in the following cases:

1. Self-signed Certificates to represent the Root CA itself;
2. Certificates for Subordinate CAs and Cross Certificates;
3. Certificates for infrastructure purposes (administrative role certificates, internal CA operational device certificates); and
4. Certificates for OCSP Response verification.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The CAs shall implement physical and logical safeguards to prevent unauthorized certificate issuance. Protection of the CA Private Key outside the validated system or device specified above must consist of physical security, encryption, or a combination of both, implemented in a manner that prevents disclosure of the CA Private Key. The CAs shall encrypt its Private Key with an algorithm and key-length that, according to the state of the art, are capable of withstanding cryptanalytic attacks for the residual life of the encrypted key or key part.

6.2.1 Cryptographic Module Standards and Controls
The HSM used for generating, storing, and signing CA private keys shall be a product that complies with this CPS "6.2.7 Private Key Storage on Cryptographic Module ".

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
The CAs do not Escrow CA Private Keys.

6.2.4 Private Key Backup
Backups of the CA private key shall be performed in accordance with this CPS "5.2.2 Number of Persons Required per Task".

6.2.5 Private Key Archival
Parties other than the Subordinate CA SHALL NOT archive the Subordinate CA Private keys without authorization by the Subordinate CA.

6.2.6 Private Key Transfer into or from a Cryptographic Module
If the CA generated the Private Key on behalf of the Subordinate CA, then the CA SHALL encrypt the Private Key for transport to the Subordinate CA. If the CA becomes aware that a Subordinate CA's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subordinate CA, then the CA SHALL revoke all certificates that include the Public Key corresponding to the communicated Private Key.

6.2.7 Private Key Storage on Cryptographic Module
The CA's private key shall be stored in an encrypted form in an HSM that meets FIPS 140-2 level 3, FIPS 140-3 level 3, Common Criteria Protection Profile or Security Target, EAL 4 or higher.

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
The HSM used to manage the CA's key pairs shall be a product that complies with this CPS "6.2.7 Private Key Storage on Cryptographic Module ".

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 the key pair and CA certificate of the CAs is assumed to be 8 years or more and 25 years or less. The private key or subject name should not be reused.
The validity period of the key pair of the subordinate CA is not specified, but the validity period of the certificate is assumed to be 20 years or less.

OCSP Certificates MUST NOT have a Validity Period greater than 125 days.

For the purpose of calculations, a day is measured as 86,400 seconds. Any amount of time greater than this, including fractional seconds and/or leap seconds, shall represent an additional day. For this reason, Subscriber Certificates should not be issued for the maximum permissible time by default, in order to account for such adjustments.

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
Management of the generation and setting of the activation data of the private key of the CAs are performed by the persons described in “5.2.1. Trusted Roles” of this CPS.

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.
The CAs shall enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.

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

7.1.1 Version Number(s)
Stipulated in the relevant CP.

7.1.2 Certificate Extension
Stipulated in the relevant CP.

7.1.3 Algorithm Object Identifier
Stipulated in the relevant CP.

7.1.4 Name Format
Stipulated in the relevant CP.

7.1.5 Name Constraints
Stipulated in the relevant CP.

7.1.6 Certificate Policy Object Identifier
Stipulated in the relevant CP.

7.1.7 Use of Policy Constraint Extensions
Stipulated in the relevant CP.

7.1.8 Policy Qualifier Syntax and Semantics
Stipulated in the relevant CP.

7.1.9 How to interpret Critical Certificate Policy Extensions
Stipulated in the relevant CP.

7.2 CRL Profile

7.2.1 Version Number(s)
Stipulated in the relevant CP.

7.2.2 Certificate Revocation Lists and CRL Entry Extensions
Stipulated in the relevant CP.

7.3 OCSP Profile

7.3.1 Version Number(s)

Stipulated in the relevant CP.

7.3.2 OCSP Extensions

Stipulated in the relevant CP.

8. Compliance Audit and Other Assessments

The CAs shall at all times:

1. Issue Certificates and operate its PKI in accordance with all law applicable to its business and the Certificates it issues in every jurisdiction in which it operates;
2. Comply with these Requirements;
3. Comply with the audit requirements specified in the CP; and
4. Be licensed as a CA in each jurisdiction where it operates, if licensing is required by the law of such jurisdiction for the issuance of Certificates.

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.
Certificates that are capable of being used to issue new certificates MUST either be Technically Constrained in line with the CP "7.1.5 Name Constraints" and audited in line with this CPS "8.7 Self-Audit" only, or Unconstrained and fully audited in line with all remaining requirements from this section. A Certificate is deemed as capable of being used to issue new certificates if it contains an X.509v3 basicConstraints extension, with the cA boolean set to true and is therefore by definition a Root CA Certificate or a Subordinate CA Certificate.
The period during which the CAs issue Certificates shall be divided into an unbroken sequence of audit periods. An audit period must not exceed one year in duration.
If the CAs have a currently valid Audit Report indicating compliance with an audit scheme listed in this CPS “8.4 Topics Covered by Assessment”, then no pre-issuance readiness assessment is necessary.
If the CAs do not have a currently valid Audit Report indicating compliance with one of the audit schemes listed in this CPS, “8.4 Topics Covered by Assessment”, then, before issuing Publicly-Trusted Certificates, the CAs shall successfully complete a point-in-time readiness assessment performed in accordance with applicable standards under one of the audit schemes listed in this CPS, “8.4 Topics Covered by Assessment”. The point-in-time readiness assessment shall be completed no earlier than twelve (12) months prior to issuing Publicly-Trusted Certificates and shall be followed by a complete audit under such scheme within ninety (90) days of issuing the first Publicly-Trusted Certificate.

8.2 Identity/Qualifications of Assessor

The CA’s audit shall be performed by a Qualified Auditor. A Qualified Auditor means a natural person, Legal Entity, or group of natural persons or Legal Entities that collectively possess the following qualifications and skills:

1. Independence from the subject of the audit;
2. The ability to conduct an audit that addresses the criteria specified in an Eligible

Audit Scheme (see this CPS, "8.4 Topics Covered by Assessment");

3. Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;
4. (For audits conducted in accordance with the WebTrust standard) licensed by WebTrust;
5. Bound by law, government regulation, or professional code of ethics; and
6. Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage.

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 CA shall be audited as appropriate in accordance with the WebTrust Standards below:

- WebTrust for CAs
- WebTrust for CAs SSL Baseline with Network Security
- WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL
- WebTrust Principles and Criteria for Certification Authorities - Network Security
- WebTrust Principles and Criteria for Certification Authorities – Publicly Trusted Code Signing Certificates
- WebTrust Principles and Criteria for Certification Authorities - S/MIME

It must incorporate periodic monitoring and/or accountability procedures to ensure that its audits continue to be conducted in accordance with the requirements of the scheme.
The audit must be conducted by a Qualified Auditor, as specified in this CPS "8.2 Identity/Qualifications of Assessor".
For Delegated Third Parties which are not Enterprise RAs,, then the CAs shall obtain an audit report, issued under the auditing standards that underlie the accepted audit schemes found in this CPS, "8.4 Topics Covered by Assessment", that provides an opinion whether the Delegated Third Party's performance complies with either the Delegated Third Party's practice statement or the CA's Certificate Policy and/or Certification Practice Statement. If the opinion is that the Delegated Third Party does not comply, then the CAs shall not allow the Delegated Third Party to continue performing delegated functions.

The audit period for the Delegated Third Party shall not exceed one year (ideally aligned with the CA's audit).

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.

The Audit Report shall state explicitly that it covers the relevant systems and processes used in the issuance of all Certificates that assert one or more of the policy identifiers listed in the CP, "7.1.6 Certificate Policy Object Identifier". The CAs shall make the Audit Report publicly available. The CAs must make its Audit Report publicly available no later than three months after the end of the audit period. In the event of a delay greater than three months, the CAs shall provide an explanatory letter signed by the Qualified Auditor.

The Audit documentation must contain at least the following clearly-labelled information:

1. Name of the organization being audited;
2. Name and address of the organization performing the audit;
3. name of the lead auditor and qualifications of the team performing the audit;
4. The SHA-256 fingerprint of all Roots and Subordinate CA Certificates, including Cross Certificates, that were in-scope of the audit;
5. Audit criteria, with version number(s), that were used to audit each of the certificates (and associated keys);
6. A list of the CA policy documents, with version numbers, referenced during the audit;
7. Whether the audit assessed a period of time or a point in time;
8. The start date and end date of the Audit Period, for those that cover a period of time;
9. The point in time date, for those that are for a point in time;
10. The date the report was issued, which will necessarily be after the end date or point in time date.
11. all incidents disclosed by the CA, discovered by the auditor, or reported by a third party, that, at any time during the audit period, occurred or were open in Bugzilla; and

12. the CA locations that were or were not audited.

An authoritative English language version of the publicly available audit information must be provided by the Qualified Auditor and the CAs shall ensure it is publicly available.

The Audit Report must be available as a PDF, and shall be text searchable for all information required. Each SHA-256 fingerprint within the Audit Report must be uppercase letters and must not contain colons, spaces, or line feeds.

8.7 Self-Audit

During the period in which the CAs issue Certificates, the CAs shall monitor adherence to its Certificate Policy, Certification Practice Statement and these Requirements and strictly control its service quality by performing self-audits on at least a quarterly basis against a randomly selected sample of the greater of one certificate or at least three percent of the Certificates (six percent for EV TLS Server Certificate) issued by it during the period commencing immediately after the previous self-audit sample was taken.

Effective 2025-03-15, the CA SHOULD use a Linting process to verify the technical accuracy of TLS server Certificates within the selected sample set independently of previous linting performed on the same Certificates.

Regarding with S/MIME Certificate, during the period in which the CA issues Certificates, the CA SHALL monitor adherence to its CP and/or CPS and S/MIME Baseline Requirements and control its service quality by performing self-audits on at least a quarterly basis against a randomly selected sample including a minimum of the greater of thirty (30) Certificates or three percent (3%) of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.

Except for Delegated Third Parties that undergo an annual audit that meets the criteria specified in Section 8.4 “Topics Covered by Assessment”, the CAs shall strictly control the service quality of Certificates issued or containing information verified by a Delegated Third Party by having a Validation Specialist employed by the CAs perform ongoing quarterly audits against a randomly selected sample of at least the greater of one certificate or three percent of the Certificates (six percent for EV TLS Server Certificate) verified by the Delegated Third Party in the period beginning immediately after the last sample was taken. The CAs shall review each Delegated Third Party’s practices and procedures to ensure that the Delegated Third Party is in compliance with these Requirements and the relevant Certificate Policy and/or Certification Practice Statement.

The CAs shall internally audit each Delegated Third Party’s compliance with these Requirements on an annual basis.

During the period in which a Technically Constrained Subordinate CA issues Certificates, the CAs which signed the Subordinate CA shall monitor adherence to the CA’s Certificate

Policy and the Subordinate CA's Certification Practice Statement. On at least a quarterly basis, against a randomly selected sample of the greater of one certificate or at least three percent of the Certificates (six percent for EV TLS Server Certificate) issued by the Subordinate CA, during the period commencing immediately after the previous audit sample was taken, the CAs shall ensure all applicable CP are met.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Fees for Issuing or Renewing Certificates
Stipulated in the relevant CP.

9.1.2 Certificate Access Fee
Stipulated in the relevant CP.

9.1.3 Expiration or Access Fee for Status Information
Stipulated in the relevant CP.

9.1.4 Fees for Other Services
Stipulated in the relevant CP.

9.1.5 Refund Policy
Stipulated in the relevant CP.

9.2 Financial Responsibility

9.2.1 Insurance Coverage
Stipulated in the relevant CP.

9.2.2 Other Assets
Stipulated in the relevant CP.

9.2.3 End entity Insurance or Warranty coverage
Stipulated in the relevant CP.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information
Stipulated in the relevant CP.

9.3.2 Information outside the scope of confidential information
Stipulated in the relevant CP.

9.3.3 Responsibility to Protect Confidential Information
Stipulated in the relevant CP.

9.4 Privacy of Personal Information

9.4.1 Personal Information Protection Plan
Stipulated in the relevant CP.

9.4.2 Information Treated as Personal Information
Stipulated in the relevant CP.

9.4.3 Information that is not considered Personal Information
Stipulated in the relevant CP.

9.4.4 Responsibility for protecting Personal Information
Stipulated in the relevant CP.

9.4.5 Notice and Consent regarding use of Personal Information
Stipulated in the relevant CP.

9.4.6 Disclosure of Information with Judicial or Administrative Procedures
Stipulated in the relevant CP.

9.4.7 Other Information Disclosure Conditions
Stipulated in the relevant CP.

9.5 Intellectual Property Rights
Stipulated in the relevant CP.
This CPS may be reproduced provided that the original document is properly referenced. It is published under the Creative Commons license Attribution-NoDerivatives (CC-BY-ND) 4.0.

https://creativecommons.org/licenses/by-nd/4.0/

9.6 Representations and Warranties

9.6.1 CA Representation and Warranties
Stipulated in the relevant CP.

9.6.2 RA Representations and Warranties
Stipulated in the relevant CP.

9.6.3 Subscriber Representations and Warranties
Stipulated in the relevant CP.

9.6.4 Relying Party Representations and Warranties
Stipulated in the relevant CP.

9.6.5 Representations and Warranties of Other Participants
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

9.10.1 Term
Stipulated in the relevant CP.

9.10.2 Termination
Stipulated in the relevant CP.

9.10.3 Effect of Termination and Survival
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.

9.12.3 Circumstances under Which OID Must Be Changed
Stipulated in the relevant CP.

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

9.16.1 Entire Agreement
Stipulated in the relevant CP.

9.16.2 Assignment
Stipulated in the relevant CP.

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

In the event of a conflict between Baseline Requirements and a law, regulation or government order (hereinafter 'Law') of any jurisdiction in which the CAs operate or issue certificates, the CAs may modify any conflicting requirement to the minimum extent necessary to make the requirement valid and legal in the jurisdiction.
This applies only to operations or certificate issuances that are subject to that Law. In such event, the CAs shall immediately (and prior to issuing a certificate under the modified requirement) include in the CA's CPS a detailed reference to the Law requiring a modification of Baseline Requirements under this section, and the specific modification to Baseline Requirements implemented by the CAs.
The CAs must also (prior to issuing a certificate under the modified requirement) notify the CA/Browser Forum of the relevant information newly added to the CA's CPS by sending a message to questions@cabforum.org and receiving confirmation that it has been posted to the Public Mailing List and is indexed in the Public Mail Archives available at https://cabforum.org/pipermail/public/ (or such other email addresses and links as the Forum may designate), so that the CA/Browser Forum may consider possible revisions to Baseline Requirements accordingly.
Any modification to the CAs practice enabled under this section must be discontinued if and when the Law no longer applies, or Baseline Requirements are modified to make it possible to comply with both Baseline Requirements and the Law simultaneously. An appropriate change in practice, modification to the CA's CPS and a notice to the CA/Browser Forum, as outlined above, must be made within 90 days.

9.16.4 Enforcement
Stipulated in the relevant CP.

9.16.5 Irresistible Force
Stipulated in the relevant CP.

9.17 Other Provisions
Stipulated in the relevant CP.