SECOM Digital Certification Infrastructure Certification Practice Statement

Version 2.21

October 23, 2024

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
2.13	2020/03/30	Revised chapters and added some " No Stipulation" content
2.14	2021/03/30	Update of the date and version
2.15	2021/11/30	Overall revision of the descriptions and styles
2.16	2022/06/10	Overall revision of the descriptions and styles
2.17	2022/12/08	Content added to "6.3.2 Certificate Operational Periods and Key Pair Usage Periods"
2.18	2023/05/17	Update “2.3 Time or Frequency of Publication” Change the item name for 5.3.2 as “Background Check Procedures” Update “5.5.1 Types of Records Archived” Update “5.5.2 Retention Period for Archive” Update “5.7.3 Entity Private Key Compromise Procedures”
2.19	2024/04/01	Update “1.1 Overview” Update “1.6 Definitions and Acronyms” Update “5.3.2 Background Check Procedures” Update “6.1.5 Key Sizes” Update “6.1.6 Public Key Parameters Generation and Quality Checking” Update “6.3.2 Certificate Operational Periods and Key Pair Usage Periods” Update “8.4 Topics Covered by Assessment”

2.20	2024/08/21	Update the below: 1.1 Overview 1.3.3 Subscribers 5.2.2 Number of Persons Required per Task 5.2.4 Roles Requiring Separation of Duties 5.4.1 Types of Events Recorded 5.4.3 Retention Period for Audit Log 5.4.5 Audit Log Backup Procedure 5.5.1 Types of Records Archived 5.5.2 Retention Period for Archive 5.7.1 Incident and Compromise Handling Procedures 5.7.3 Entity Private Key Compromise Procedures 6.1.1 Key Pair Generation 6.1.5 Key Sizes 6.2 Private Key Protection and Cryptographic Module Engineering Controls 6.2.7 Private Key Storage on Cryptographic Module 6.3.2 Certificate Operational Periods and Key Pair Usage Periods Add the below: 5.4.1.1 Router and firewall activities logs 5.4.1.2 Types of events recorded for Timestamp Authorities
2.21	2024/10/23	Update the below: 1.5.2 Contact Information 2.1 Repository 2.2 Publication of Certificate Information 6.1.1 Key Pair Generation 6.2.1 Cryptographic Module Standards and Controls 6.2.4 Private Key Backup 6.2.5 Private Key Archival 6.2.6 Private Key Transfer into or from a Cryptographic Module 6.3.2 Certificate Operational Periods and Key Pair Usage Periods 8.7 Self-Audit

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, "CA”) of SECOM Trust Systems as well as the CA of the subscribers of SECOM Trust Systems Private CA Services (hereinafter, "Private CA Subscribers"). The Digital Certification Infrastructure comprises certification infrastructure systems, such as repository servers for publishing revocation information, CA certificates, and other information. 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 required by 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.

CAs that issue certificates whose subordinate CA certificates comply with the "Security Communication RootCA Subordinate CA Certificate Policy", conform to the current version of the standard which is defined by the CA / Browser Forum published at https://www.cabforum.org/ and Application software supplier standard.

Table 1.1-1 List of the standards

Types of certificates issued by subordinate CAs	Standards to comply with
TLS Server Certificate	● Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates (hereinafter, "Baseline Requirements")

	● Guidelines for the Issuance and Management of Extended Validation Certificates (EV Certificate only. hereinafter, " EV Guidelines ") ● 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 (hereinafter, " S/MIME Baseline Requirements") ● 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 (hereinafter, " Baseline Requirements for Code Signing Certificates ") ● Microsoft Trusted Root Program
AATL Document Signing Certificate AATL Timestamp Certificate	● Adobe Approved Trust List Technical Requirements (AATL Technical Requirements)
Microsoft Document Signing Certificate	● Microsoft Trusted Root Program

If any provisions in the CP are inconsistent with this CPS, then the CP shall prevail. And any provisions in a service agreement or the like with SECOM Trust Systems inconsistent with the CP, the service agreement shall prevail.
In the event of any inconsistency between this CPS and the Baseline Requirements, the Baseline Requirements take precedence over this CPS.

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. Certification Authority (CA) is defined in Section 1.6 “Definitions and Acronyms”

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.

If the subordinate CA certificate is a CA which issues a TLS server certificate that complies with the "Security Communication Root CA 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 CA may delegate the performance of all, or any part, of Baseline Requirements 3.2 requirements to a Delegated Third Party, provided that the process as a whole fulfills all of the requirements of Baseline

Requirements 3.2.

Before the CA authorizes a Delegated Third Party to perform a delegated function, the CA shall contractually require the Delegated Third Party to:

(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 this CPS 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 CA has verified complies with Baseline Requirements.

1.3.3 Subscribers

Subscribers shall be any natural person or Legal Entity that receives a Certificate issued by the CA and conforms to the Subscriber Agreement or Term of Use.

1.3.4 Relying Parties

Relying Parties are the entities that authenticate the certificates issued by the CA operated on the Digital Certification Infrastructure. “Relying Party” and “Application Software Supplier” are defined in Section 1.6” Definitions and Acronyms”.

1.3.5 Other parties

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

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

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:

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 CPS 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

The contents of this CPS are determined by SECOM Trust Systems Certification Services Committee.　This CPS shall be reviewed and revised at least annually.

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.

Application Software Supplier
A supplier of Internet browser software or other relying-party application software that displays or uses Certificates and incorporates Root Certificates.

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 (Certification Authority)
CA stands for Certification Authority, an entity that mainly issues, renews and revokes Certificates, generates and protects CA Private Keys, and registers Subscribers. This CPS also includes the Issuing Authority (IA).

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

CP (Certificate Policy)
A document that sets forth provisions pertaining to certificates issued by a CA, including certificate types, 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

The security certification standards developed by the U.S. NIST (National Institute of Standards and Technology) for cryptographic modules.

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.

OCSP

Abbreviation for Online Certificate Status Protocol. A protocol that provides certificate status information in real time.

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.

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

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.

Root CA

Security Communication Root CA in this CPS is an organization owned and operated by SECOM, and is the root CA that issues certificates for Subordinate CAs.
The CA that functions as the top level CA for 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 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.

SHA-2

A hash function of the Secure Hash Algorithm series used for digital signatures, which is an improved version of SHA-1. The bit length of SHA-256 is 256 bits, and the bit length of SHA-384 is 384 bits. By comparing the hash values on the transmitting side and the receiving side of the data, which works to detect whether the original text has been tampered or not during communication.

Time-Stamp

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

WebTrust for CA

Certification system for standards maintained by CPA Canada for the internal controls regarding the reliability of certificate authorities and the safety of electronic commerce.

X.500

A directory standard established by ITU-T for the purpose of providing a wide range of services from name and address search to attribute search. X.500 Distinguished Name is used for X.509 issuer name and subject name.

X.509

X.509 ITU-T certificate and CRL format. In X.509 v3 (Version 3), an extension area for holding arbitrary information has been added.

2. Publication and Repository Responsibilities

2.1 Repository

The CA maintains a Repository to provide Subscribers and Relying Parties with access to CRL information. The CA also maintains an OCSP responder to make online certificate status information available to Subscribers and Relying Parties for 24 x 7 bases. The protocol used to access the repository shall be HTTP (HyperText Transfer Protocol) or HTTPS (a protocol that adds data encryption functionality using SSL/TLS to HTTP). The repository information is accessible through a common web interface.

2.2 Publication of Certificate Information

The CA shall store the following information in the Repository to allow online access on a 24x7 basis thereto by Subscribers and Relying Parties:

- Certificate Revocation List (hereinafter "CRL") containing all revocation information under this CPS and the CP.
- Self-signed certificate of the CA
- Latest version of this CPS and the CP
- Any other relevant information regarding certificates issued by the CA

The CA 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. The CA SHALL host separate Web pages using Subscriber Certificates that are:

i. valid,
ii. revoked, and
iii. expired.

2.3 Time or Frequency of Publication

The CA shall develop, implement, enforce, and annually update 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 the CP and CPS.

2.4 Access Controls on Repository

The CA makes its Repository publicly available in a read-only manner. In the CA, 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

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.

3.2.2.1 Identity

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

3.2.2.2 DBA/Tradename

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

3.2.2.3 Verification of Country

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

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

The CA 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 CA 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 should 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 CA has in place to counter such threats.

Based on the Risk Assessment, the CA 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

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.

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

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 this CPS "5.2.1 Trusted Roles" hereof are performed by independent personnel. However, a Service Operation Manager may concurrently serve as a Log Examiner.

Subordinate CAs issuing EV TLS Server Certificates that comply with the EV Guidelines shall conduct the following:

1. The CA MUST enforce rigorous control procedures for the separation of validation duties to ensure that no one person can single-handedly validate and authorize the issuance of an EV Certificate. The Final Cross-Correlation and Due Diligence steps, as outlined in the EV Guidelines, Section 3.2.2.13, MAY be performed by one

of the persons. For example, one Validation Specialist MAY review and verify all the Applicant information and a second Validation Specialist MAY approve issuance of the EV Certificate.

2. Such controls MUST be auditable.

5.3 Personnel Controls

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 CA, the CA shall verify the identity and trustworthiness of such person.

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.

Prior to the commencement of employment of any person by the CA for engagement in the EV Processes, whether as an employee, agent, or an independent contractor of the CA, the CA MUST:

1. Verify the Identity of Such Person: Verification of identity MUST be performed through:
   A. The personal (physical) presence of such person before trusted persons who perform human resource or security functions,
   B. The verification of well-recognized forms of government-issued photo identification (e.g., passports and/or drivers licenses);
2. Verify the Trustworthiness of Such Person: Verification of trustworthiness SHALL include background checks, which address at least the following, or their equivalent:
   A. Confirmation of previous employment,
   B. Check of professional references;
   C. Confirmation of the highest or most-relevant educational qualification obtained;

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.

The CA 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 CA 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 CA shall document that each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task.

The CA shall require all Validation Specialists to pass an examination provided by the CA on the information verification requirements outlined in these Requirements.

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.

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

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.

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

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:

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;
   5. Generation of Certificate Revocation Lists
   6. Signing of OCSP Responses.
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 ;
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;
2. Logging of all administrative actions performed on routers and firewalls, including configuration changes, firmware updates, and access control modifications;
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 Certificates]

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

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

5.4.3 Retention Period for Audit Log

SECOM Trust Systems retains the following for at least two years:

1. The CA certificate and key lifecycle management event record (as described in the CP "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 (as described in the CP "5.4.1 Types of Events Recorded") after the revocation or expiration of the Subscriber Certificate;
3. Any security event records (described in the CP "5.4.1 Types of Events Recorded") after the event occurred.
4. For Code Signing Certificates, Timestamp Authority data record after the revocation or renewal of the Timestamp Certificate private key (as set forth in this CPS, "5.4.1.2 Types of events recorded for Timestamp Authorities"); and the security event record after the event occurred (as specified in this CPS, " Types of Events Recorded").

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 and stored in a secure off-site environment that is separate from the equipment that generates the Audit Logs.

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 assessments 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.

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 CA has in place to counter such threats.

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:

- Documentation related to the security of the Certificate Systems, Certificate Management Systems, Root CA Systems, and Delegated Third Party Systems;
- Documentation related to the certificate request, certificate verification, issuance,

and revocation.

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 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 "5.4.3 Retention Period for Audit Log" of this CPS, 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"); and
2. All archived documentation relating to the certificate request, certificate verification, issuance, and revocation (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 certificate request, certificate verification, issuance, and revocation; or
   ⅱ. the expiration of the Subscriber Certificates relying upon such records and documentation.

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

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 CA shall have an Incident Response Plan and a Disaster Recovery Plan.

The CA 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 CA is not required to publicly disclose its business continuity plans but shall make its business continuity plan and security plans available to the CA's auditors upon request. The CA 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 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 a Subscriber determine that a Private Key has or could have been compromised, the Subscriber must promptly make a revocation request to the relevant CA. Following receipt of a revocation request, the relevant CA processes the revocation according to the procedure set forth in "4.9 Certificate Revocation and Suspension" of the CP of the CAs operated on the Digital Certification Infrastructure.

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

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

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 (CA that complies with the standards established by the CA/Browser Forum) 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 (CA that complies with the standards established by the CA/Browser Forum).

In all cases, the CA 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 that complies with Baseline Requirements, 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 CP "6.1.5 Key Sizes" or this CP "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 CA is aware of a demonstrated or proven method that exposes the Applicant's Private Key to compromise;
4. The subordinate CA has previously been notified that the Applicant's Private Key has suffered a Key Compromise using the CA's procedure for revocation request as described in the CP "4.9.3 Procedure for Revocation Request" and the CP "4.9.12 Special Requirements Regarding Key Compromise";.
5. The Public Key corresponds to an industry-demonstrated weak Private Key. For requests submitted on or after November 15, 2024, at least the following precautions SHALL be implemented:
    1. In the case of Debian weak keys vulnerability (https://wiki.debian.org/SSLkeys), the CA SHALL reject all keys found at https://github.com/cabforum/Debian-weak-keys/ for each key type (e.g. RSA, ECDSA) and size listed in the repository. For all other keys meeting the requirements of this CPS "6.1.5 Key Sizes", with the exception of RSA key sizes greater than 8192 bits, the CA SHALL reject Debian weak keys.
    2. In the case of ROCA vulnerability, the CA SHALL reject keys identified by the tools available at https://github.com/crocs-muni/roca or equivalent.
    3. In the case of Close Primes vulnerability (https://fermatattack.secvuln.info/), the CA SHALL reject weak keys which can be factored within 100 rounds using Fermat's factorization method. Suggested tools for checking for weak keys can be found here: https://cabforum.org/resources/tools/

If the Subscriber Certificate will contain an extKeyUsage extension containing either the values id-kp-serverAuth [RFC5280] or anyExtendedKeyUsage [RFC5280], the CA SHALL NOT generate a Key Pair on behalf of a Subscriber, and SHALL NOT accept a certificate request using a Key Pair previously generated by the CA.

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

When issuing a TLS server certificate that complies with Baseline Requirements, S/MIME certificate that complies with S/MIME Baseline Requirements, AATL document signing certificate and AATL timestamp certificate, the following confirmation need to be done:

For RSA key pairs the CA shall:

- Ensure that the modulus size, when encoded, is at least 2048 bits, and;
- Ensure that the modulus size, in bits, is evenly divisible by 8.

For ECDSA key pairs the CA shall:

- Ensure that the key represents a valid point on the NIST P-256 or NIST P-384 elliptic curve.

When issuing code signing certificates and timestamp certificates that comply with Baseline Requirements for Code Signing Certificates, the following confirmation need to be done:

For RSA key pairs the CA shall:

- Ensure that the modulus size, when encoded, is at least 3072 bits, and;
- Ensure that the modulus size, in bits, is evenly divisible by 8.

For ECDSA key pairs the CA shall:

- Ensure that the key represents a valid point on the NIST P-256 or NIST P-384 elliptic curve.

Ensure that no other algorithms or key sizes are permitted.

Key pairs for certificates other than those listed above shall have a key size of 1024 bits, 2048 bits, 3072 bits, or 4096 bits for RSA method, and a key size of 256 bits or 384 bits for ECDSA method.

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.

RSA

The CA 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 CA 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 56A: Revision 2].

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

The CA 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 CA 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 operated on the Digital Certification Infrastructure 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

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

6.2.4 Private Key Backup

Backups of the CA private key operated on the Digital Certification Infrastructure 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 issuing CA generated the Private Key on behalf of the Subordinate CA, then the issuing CA SHALL encrypt the Private Key for transport to the Subordinate CA. If the issuing 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 issuing 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

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

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 validity period of the key pair of the CA is not specified, but the validity period of the CA certificate is assumed to be 20 years or less.

TLS server certificates that comply with Baseline Requirements issued after September 1, 2020 SHOULD NOT have a Validity Period greater than 397 days and MUST NOT have a Validity Period greater than 398 days. TLS server certificates issued after 1 March 2018, but prior to 1 September 2020, must not have a Validity Period greater than 825 days. TLS server certificates issued after 1 July 2016 but prior to 1 March 2018 must not have a Validity Period greater than 39 months.

The Validity Period for EV TLS Server Certificates that comply with the EV Guidelines SHALL NOT exceed 398 days.

Code signing certificates that comply with Baseline Requirements for Code Signing Certificates must not have a Validity Period greater than 39 months. The time stamp authority used for code signing certificates must use a new time stamp certificate with a new private key every 15 months to minimize the impact on the subscriber if the private key of the time stamp certificate is compromised. The validity period of the time stamp certificate must not be greater than 135 months.

The Timestamp Certificate Key Pair that complies with the Baseline Requirements for Code Signing Certificates MUST meet the requirements in this CPS “6.1.5 Key Sizes”. Timestamp Authority SHALL NOT use a Private Key associated with a Timestamp Certificate more than 15 months after the notBefore date of a Timestamp Certificate. Effective April 15, 2025, Private Keys associated with Timestamp Certificates issued for greater than 15 months MUST be removed from the Hardware Crypto Module protecting the Private Key within 18 months after issuance of the Timestamp Certificate. For Timestamp Certificates issued on or after June 1, 2024, the CA SHALL log the removal of the Private Key from the Hardware Crypto Module through means of a key deletion ceremony performed by the CA and witnessed and signed‐off by at least two Trusted Role members. The CA MAY also perform a key destruction ceremony, meaning that all copies of that private key are unequivocally/securely destroyed (i.e. without a way to recover the key), including any instance of the key as part of a backup, to satisfy the Baseline Requirements for Code Signing Certificates. The CA MAY maintain existing backup sets containing the Private Key corresponding to a Timestamp Certificate. The CA SHOULD NOT restore the Private Key corresponding to a Timestamp Certificate contained within the backup if the Timestamp Certificate was issued more than 15 months prior to restoration of the backup. If the CA does restore such a Private Key, the CA SHALL only restore the Private Key in a suitable HSM while it’s maintained in a High Security Zone and in an offline state or air‐gapped from all other networks and perform a new key destruction ceremony prior to the HSM being brought to an online state.

S/MIME certificates that comply with the Mozilla Root Store Policy and Apple Root Certificate Program and S/MIME Baseline Requirements issued after April 1, 2022 must not have a Validity Period greater than 825 days.

Subscriber certificates other than the above for which the subordinate CA certificate complies with the "Security Communication RootCA Subordinate CA Certificate Policy" must not have a Validity Period greater than 1827 days.

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

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

Management of the generation and setting of the activation data of the private key of the CA operated on the Digital Certification Infrastructure is 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

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

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

The CA 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 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.

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 the CP "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 CA issues Certificates shall be divided into an unbroken sequence of audit periods. An audit period must not exceed one year in duration.

If the CA has a currently valid Audit Report indicating compliance with an audit scheme listed in the CP, “8.4 Topics Covered by Assessment”, then no pre-issuance readiness assessment is necessary.

If the CA does not have a currently valid Audit Report indicating compliance with one of the audit schemes listed in the CP, “8.4 Topics Covered by Assessment”, then, before issuing Publicly-Trusted Certificates, the CA shall successfully complete a point-in-time readiness assessment performed in accordance with applicable standards under one of the audit schemes listed in the CP, “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 his CP, “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 undergo an audit in accordance with the following WebTrust Standards:

- 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 CA shall obtain an audit report, issued under the auditing standards that underlie the accepted audit schemes found in the CP, “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 CA 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 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.

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 CA shall make the Audit Report publicly available. The CA 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 CA shall provide an explanatory letter signed by the Qualified Auditor.

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 CA 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 CA issues Certificates, the CA 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 Certificates within the selected sample set independently of previous linting performed on the same Certificates.

For S/MIME certificates, 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 this CPS, Section 8.4 "Topics Covered by Assessment", the CA 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 CA 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 CA 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 CA shall internally audit each Delegated Third Party's compliance with these Requirements on an annual basis.

During the period in which a Technically Constrained CA issues Certificates that complies with Baseline Requirements, the CA shall monitor adherence to the CA's Certificate Policy. 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 CA, during the period commencing immediately after the previous audit sample was taken, the CA 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

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

9.1.2 Certificate Access Fee

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

9.1.3 Expiration or Access Fee for Status Information

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

9.1.4 Fees for Other Services

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

9.1.5 Refund Policy

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

9.2 Financial Responsibility

9.2.1 Insurance Coverage

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

9.2.2 Other Assets

No stipulation.

9.2.3 End entity Insurance or Warranty coverage

No stipulation.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

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

9.4.1 Personal Information Protection Plan

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

9.4.2 Information Treated as Personal Information

SECOM Trust Systems treats information defined as personal information based on domestic laws and regulations (such as information collected from subscribers of SECOM authentication services) as personal information and manages it appropriately.

9.4.3 Information that is not considered Personal Information

SECOM Trust Systems treats personal information as specified in “9.4.2 Information Treated as Personal Information”.

9.4.4 Responsibility for protecting Personal Information

SECOM Trust Systems shall not disclose any personal information of the other party that it has learned during the execution and termination of the contract to third parties, whether during or after the contract period. The personal information protection manager shall be appointed in the operation of this CA operated on the Digital Certification Infrastructure, and the personal information protection manager shall have employees engaged in the service comply with internal rules regarding the handling of personal information.

9.4.5 Notice and Consent regarding use of Personal Information

SECOM Trust Systems shall not use personal information for any purpose other than the purpose of obtaining the consent of the certificate subscriber, except as provided by law. The personal number and specific personal information will be used for the purpose of use permitted by law and for the purpose of use with the consent of the certificate subscriber.

9.4.6 Disclosure of Information with Judicial or Administrative Procedures

If disclosure is requested by law, rule, court decision/order, administrative agency order /instruction, etc., the personal information of the certificate subscriber may be disclosed.

9.4.7 Other Information Disclosure Conditions

No stipulation.

9.5 Intellectual Property Rights

Unless otherwise agreed to between SECOM 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

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

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

Even if any provision of the CP, the Service Terms 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 CA operates or issues certificates, the CA 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 CA 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 CA.

The CA 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 CA 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 them 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

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.