Secom Passport for Member 2.0 PUB Certificate Policy

Version 6.07

May 17, 2024

SECOM Trust Systems Co., Ltd.

Version History		
Version Number	Date	Description
1.00	2008/04/28	Publication of the first version
1.10	2009/03/19	Revision of Certificate Profile (extendedKeyUsage).
2.00	2009/10/13	Addition of the Policy OID Overall revision of the styles
3.00	2013/11/27	Addition of the revised Policy OID associated with the addition of Sha256 Addition of the RootCA repository information
4.00	2014/05/29	Revision associated with the additional use of server authentication Addition of the Policy OID
5.00	2017/01/20	Addition of the Policy OID Revision associated with the start of OCSP server operation Overall revision of the styles
5.01	2020/02/19	Removal of the Certificate policy for server certificate Addition/revision of contents in BR for Code Signing Overall revision of the descriptions and styles
5.02	2020/03/30	Review of "No stipulation"
5.03	2020/06/15	Addition of Extended Key Usage to CA certificate (sha256) profile Addition of Extended Key Usage to Subscriber certificate (sha256) profile
5.04	2020/07/30	From Extended Key Usage of CA certificate (sha256), remove OCSP Signing, change OU, change CP URL From Subscriber certificate (sha256), change OU, change URL of CP, change OCSP URL of AIA, etc.
5.05	2020/09/29	Revision of Reason code for CRL profile
5.06	2021/06/15	Addition of Email Account Authentication
6.00	2021/08/03	Addition of CA Private Key Security Communication Root CA3 Modified Public Key information in Certificate Policy for Code Signing
6.01	2022/06/10	Overall revision of the descriptions and styles

6.02	2022/12/08	Added requirement for Code Signing Certificate to "6.1.5 Key Sizes" Added requirement for Code Signing Certificate to "6.2.7 Private Key Storage on Cryptographic Module" “7.1 Certificate Profile” Modified: “Table 7.1-1 CA certificate (sha1) profile” “Table 7.1-2 CA Certificate (sha256) Profile” “Table 7.1-3 CA certificate (sha384) profile” “Table 7.1-5 Subscriber Certificate (sha256) Profile”
6.03	2023/02/17	Modified the description for “1.1 Overview” Added CP/OID, modified the description for “1.2 Document Name and Identification” Modified the description for “1.4.1 Appropriate Certificate Uses” Added the definition for “1.6 Definitions and Acronyms” Added the description for “3.2.3 Authentication of Applicant and Individual Identity” Added Root CA for “3.2.6 Criteria for Interoperation” Modified the description for “4.3.1 CA Actions during Certificate Issuance” Modified the description for “6.1.1 Key Pair Generation” Modified the description for “6.1.2 Private Key Delivery to Subscriber” Added the description for “6.2.1 Cryptographic Module Standards and Controls” Added the description for “6.2.7 Private Key Storage on Cryptographic Module” Modified the description, added profiles for “7.1 Certificate Profile” Added Root CAs for “7.1.3 Algorithm Object Identifier” Modified the description, added profiles for “7.2 CRL Profile” Modified the description, added profiles for “7.3 OCSP Profile”
6.04	2023/05/17	Update “1.1 Overview” Update “1.2 Document Name and Identification”

		Update “1.6 Definitions and Acronyms” Update “2.3 Time or Frequency of Publication” Update “3.2.2 Authentication of Organization Identity” Update “3.2.6 Criteria for Interoperation” Update “3.2.7 Reliability of verification sources ” Update “4.1.2 Enrollment Process and Responsibilities” Update “4.2.1 Performing Identification and Authentication Functions” Update “4.9.1 Circumstances for Certificate Revocation” Update “4.9.2 Who Can Request Revocation” Update “4.9.3 Procedure for Revocation Request” Update “4.9.5 Time within Which CA Shall Process the Revocation Request” Update “4.9.7 CRL Issuance Frequency” Update “4.9.9 On-Line Revocation/Status Checking Availability” Update “4.9.10 On-Line Revocation/Status Checking Requirements” Update “4.9.11 Other Forms of Revocation Advertisements Available” Update “4.10.2 Service Availability” Update “5.5.1 Types of Records Archived” Update “5.5.2 Retention Period for Archive” Update “5.5.3 Protection of Archive” Update “5.5.4 Archive Backup Procedures” Update “5.5.5 Requirements for Time-Stamping of Records” Update “5.5.6 Archive Collection System” Update “5.5.7 Procedures to Obtain and Verify Archive Information” Update “5.7.1 Incident and Compromise Handling Procedures” Update “5.7.2 Computing Resources, Software, and/or Data are Corrupted” Update “5.7.3 Entity Private Key Compromise Procedures” Update “5.7.4 Business Continuity Capabilities after a Disaster”

		Update “6.1.2 Private Key Delivery to Subscriber” Update “6.1.6 Public Key Parameters Generation and Quality Checking” Update “7.1 Certificate Profile” Update “7.1.4 Name Format” Update “7.1.6 Certificate Policy Object Identifier Update “7.2 CRL Profile” Update “7.3 OCSP Profile”
6.05	2023/08/28	Update “4.9.1 Circumstances for Certificate Revocation” Update “7.1 Certificate Profile” Update “7.3 OCSP Profile” Update “9.6.1 CA Representation and Warranties” Update “9.6.3 Applicant and Subscriber Representations and Warranties”
6.06	2024/04/01	Update “1.1 Overview “ Update “1.6 Definitions and Acronyms” Update “3.2.3 Authentication of Applicant and Individual Identity ” Update “3.2.6 Criteria for Interoperation” Update “4.9.8 Maximum Latency for CRLs” Update “6.1.1 Key Pair Generation Update “6.1.5 Key Sizes” Update “6.2.1 Cryptographic Module Standards and Controls” Update “7.1 Certificate Profile” Update “7.1.3 “Algorithm Object Identifier” Update “7.2 “CRL Profile” Update “7.2.2 “Certificate Revocation Lists and CRL Entry Extensions” Update “7.3 OCSP Profile” Update “8.1 Frequency and Circumstances of Assessment” Update “8.2 Identity/Qualifications of Assessor” Update “8.3 Assessor’s Relationship to Assessed Entity” Update “8.4 Topics Covered by Assessment” Update “8.5 Actions Taken as a Result of Deficiency” Update “8.6 Communication of Results”

6.07	2024/05/17	Update the below: "3.2.3 Authentication of Applicant and Individual Identity" "4.2.1 Performing Identification and Authentication Functions" "7.1 Certificate Profile" "7.2 CRL Profile" "7.3 OCSP Profile"

Table of Contents

1. Introduction

1.1 Overview

SECOM Passport for Member 2.0 PUB Certificate Policy (hereinafter, "this CP") defines the policy on certificates issued by SECOM Passport for Member 2.0 PUB CA (hereinafter, "the CA"), which are operated by SECOM Trust Systems Co., Ltd. (hereinafter, "SECOM Trust Systems"), by specifying the purpose of use, the scope of application and user procedures concerning the Certificates. Various procedures regarding the operation and maintenance of the CA are stipulated in the SECOM Digital Certification Infrastructure Certification Practice Statement (hereinafter, "CPS").

A party seeking to obtain Certificates from the CA must examine its usage purposes against this CP and the CPS, and agree to the both prior to getting the Certificates issued.

This CP shall be revised as necessary in order to reflect any technical or operational developments or improvements pertaining to the CA.

This CP 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.

The CA shall conform to the latest versions of the standard established by the CA/Browser Forum (hereinafter referred to as Baseline Requirements) published at https://www.cabforum.org/ and Application Software Supplier standard.

Table 1.1-1 List of Standards

Types of certificates issued by subordinate CAs	Standards to comply with
TLS Client Authentication Certificate	● Apple Root Certificate Program ● Microsoft Trusted Root Program
S/MIME Certificate	● Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates ● Apple Root Certificate Program

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

In the event of a conflict between this CP and the CPS, the order of precedence in the application thereof shall be this CP, and the CPS. Any provisions set forth in a separate contract or the like between SECOM Trust Systems and an organization, a group or any other party, with which it has a contractual relationship that are inconsistent with this CP or the CPS, shall prevail. In the event of any inconsistency between this CP and the Baseline Requirements, the Baseline Requirements take precedence over this CP.

1.2 Document Name and Identification

The official name of this CP is "SECOM Passport for Member 2.0 PUB Certificate Policy". This CP is assigned a registered unique object identifier (hereinafter referred to as “OID”) for each use of the issued certificate. The OID of this CP and that of the CPS herein referenced are as follows:

CP/CPS	OID
Client Certificate Policy (Signature Algorithm: SHA1)	1. 2. 392. 200091. 100. 381. 1
Client Certificate Policy (Signature Algorithm: SHA256)	1. 2. 392. 200091. 100. 381. 4
Certificate Policy for Data Signing (Signature Algorithm: SHA1)	1. 2. 392. 200091. 100. 381. 2
Certificate Policy for Data Signing (Signature Algorithm: SHA256)	1. 2. 392. 200091. 100. 381. 5
Certificate Policy for Code Signing	1. 2. 392. 200091. 100. 381. 8

(Signature Algorithm: SHA256)	
OCSP Responder Certificate Policy (Signature Algorithm: SHA256)	1. 2. 392. 200091. 100. 381. 9
Certificate Policy for AATL Document Signing	1. 2. 392. 200091. 100. 382. 1
Certificate Policy for S/MIME	1. 2. 392. 200091. 100. 383. 1
SECOM Digital Certification Infrastructure Certification Practice Statement	1. 2. 392. 200091. 100. 401. 1

1.3 PKI Participants

1.3.1 CA

CA performs administration of the CA's private key, issuance/revocation of Certificates, publication of CRLs (Certificate Revocation Lists), provision of certificate status information by OCSP (Online Certificate Status Protocol) Responder, and maintenance/administration of the repository. The operating body of the CA on the Digital Certification Infrastructure is SECOM Trust Systems.

1.3.2 RA

The RA is an entity that performs the examination of LRA (Local Registration Authority) and certificate subscribers, and the registration work for issuing and revoking certificates. In the CA operated on the Digital Certification Infrastructure, the operation of RA is performed by SECOM Trust Systems.

The LRA is the entity that performs, on behalf of the RA, verification of the existence of the certificate subscriber and verification of the identity, registration of the certificate for issuing and revoking the certificate, and the like. A special organization or entity that has been reviewed by the RA in advance and confirmed by the RA can play that role.

The LRA, like the RA, shall comply with the matters stipulated in this CP. Note that the LRA may perform a task only when a client certificate policy or a data signature certificate policy is applied.

1.3.3 Applicants and Subscribers

Applicants shall mean an individual, corporations or any other organizations, etc. that applies to RA or LRA for issuance or revocation of a certificate, and certificate subscribers shall refer to an individual, corporations or any other organizations that receives a certificate issued by the CA and uses the certificate.

1.3.4 Relying Parties

Relying Parties are an individual, corporations or any other organizations that verifies the validity of a certificate issued by the CA.

1.3.5 Other Parties

Other Parties include auditors that check the compliance of the CA, companies and organizations that have service contracts with SECOM Trust Systems, and companies that perform system integration(hereinafter "SIer").

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The certificate issued by the CA based on this CP can be used for the purposes specified in the Key Usage and Extended Key Usage fields in the certificate.

1.4.2 Prohibited Certificate Uses

Certificates issued by the CA based on this CP must not be used for any purpose other than those described in "1.4.1 Appropriate Certificate Uses".

1.5 Policy Administration

1.5.1 Organization Administering the Document

This CP is maintained and administered by SECOM Trust Systems.

1.5.2 Contact Information

Contact information for this CP is as follows:

SECOM Trust Systems Co., Ltd.
E-mail address: ca-support@secom.co.jp

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.

1.5.3 Person Determining CP Suitability for the Policy

The Certification Services Improvement Committee determines the suitability of the contents of this CP.

1.5.4 Approval Procedure

This CP is prepared and revised by SECOM Trust Systems and goes into effect upon approval by the Certification Services Improvement Committee.

1.6 Definitions and Acronyms

A～Z

AATL（Adobe Approved Trust List）
A program that allows to create digital signatures that are trusted whenever the signed document is opened in Adobe® Acrobat® or Acrobat® Reader® software.

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

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

Baseline Requirements
A document issued by the CA/Browser Forum that integrates a set of fundamental requirements for Certificate issuance/administration.

CA（Certification Authority）
An entity that mainly issues, renews and revokes Certificates, generates and protects CA Private Keys, and registers Subscribers.

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

Certification Service Improvement Committee

A decision-making organization that manages this CP, considers changes, and determines the operational policy for this service.

Code signing

This refers to embedding digital signature data indicating the creator or issuer in a created program file or the like (hereinafter referred to as "code").
By verifying this digital signature, the code user can obtain information such as the creator, issuer, and expiration date of the code, and can confirm that the code has not been tampered with by a third party.

CP（Certificate Policy）

A document that sets forth provisions pertaining to Certificates issued by a CA, including Certificate types, usage and application procedure.

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 on Certificates which were revoked prior to their expiration due to reasons such as changes to the information provided in the Certificates and loss of the relevant Private Key.

Cross Certificate

A certificate that is used to establish a trust relationship between two Root CAs.

Digital Certificate

Digital data certifying that a public key is owned by the party specified, validity of which is certified by the digital signature of the relevant CA affixed thereto.

Enterprise RA

An employee or agent of an organization unaffiliated with the CA who authorizes issuance of Certificates to that organization.

Escrow

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

FIPS140-2

The security certification standards developed by the U.S. NIST (National Institute of Standards and Technology) for cryptographic modules, defining four security levels, the lowest 1 through the highest 4.

HSM（Hardware Security Module）

A tamper-resistant cryptographic module used to ensure the security mainly in generation, storage and usage of private keys.

Key Pair

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

LRA Operating Standards

A document that describes the standards to be followed by the LRA for the organization, operations, facilities, and audits when performing LRA operations.

Mailbox Address

Also Email Address. From RFC 5321: “A character string that identifies a user to whom mail will be sent or a location into which mail will be deposited.”

Mailbox Field

Include the subject's email address in rfc822Name in the subjectAltName extension of the S/MIME certificate.

Mailbox - Validated

One of the validation method for S/MIME certificates.
Subject is limited to (optional) subject:emailAddress and/or subject:serialNumber attributes.

OCSP（Online Certificate Status Protocol）

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

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.

PKI（Public Key Infrastructure）

An infrastructure for use of the encryption technology known as the public key cryptosystem to realize such security technologies as digital signature, encryption and certification.

Private Key

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

Public Key

A key of a Key Pair used in the Public Key cryptosystem. A Public Key corresponds to the Private Key and is published 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, requests Certificate issuance to CAs.

Repository

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

RFC3647（Request For Comments 3647）

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

RSA

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

S/MIME

Abbreviation for Secure MIME (Multipurpose Internet Mail Extensions).
A standard for digital signatures and encryption using public key cryptography in email.
In the case of digital signature, the sender's private key is used to sign the message, and the receiver verifies the signature with the sender's public key.
In the case of encryption, the recipient's public key is used to encrypt and the recipient's private key is used to decrypt.

Time-Stamp

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

WebTrust Principles and Criteria for Certification Authority（WebTrust for CA）

Standards of internal control and a certification framework based thereon maintained by CPA Canada regarding the reliability of CAs, the security of electronic commerce transactions, and other relevant matters.

WebTrust Principles and Criteria for Certification Authorities - Code Signing Baseline Requirements （WebTrust for CA - Code Signing Baseline Requirements）

Auditing standard maintained by CPA Canada for the examination and certification of certificate authorities when issuing code signing certificates.

WebTrust Principles and Criteria for Certification Authorities – S/MIME（WebTrust for CAs - S/MIME）

Auditing standard maintained by CPA Canada for the examination and certification of certificate authorities when issuing S/MIME certificates.

X.500

A series of computer network standards regarding the decentralized directory service.

2. Publication and Repository Responsibilities

2.1 Repository

SECOM Trust Systems maintains and manages a Repository in order to allow Subscribers and Relying Parties to access CRL, this CP and CPS information 24x7. It also manages the OCSP responder so that Subscribers and Relying Parties can use online certificate status information 24x7. However, the Repository and the OCSP responder may not be available temporarily at times due to maintenance or for any other reason.

2.2 Publication of Certificate Information

SECOM Trust Systems stores the following information in the Repository to allow the online access thereto by Subscribers:

- CRL
- The CA Subordinate Certificates
- The latest versions of this CP and the CPS
- Other information pertaining to Certificates issued by the CA

SECOM Trust Systems will also make the Certificate status available online to Subscribers and Relying Parties for browsing on the OCSP responder.

2.3 Time or Frequency of Publication

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

2.4 Access Controls on 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

The certificate issued by the CA meets the requirements of the X.509 standard, RFC5280 standard and Baseline Requirements, and the distinguished name assigned to the certificate holder is set according to the X.500 distinguished name format.

3.1.2 Need for Names to Be Meaningful

The Distinguished Name used for the certificate issued by this CA shall be used to identify the Subscriber and shall be meaningful.

3.1.3 Anonymity or Pseudonymity of Subscribers

Anonymous or pseudonym registration is not performed for the organization name and common name of the certificate issued by the CA. In each certificate policy not defined in Baseline Requirements (Code Signing), a number or a character string for managing a certificate may be registered.

3.1.4 Rules for Interpreting Various Name Forms

Rules concerning the interpretation of various name forms are governed by the X.500 Series DN rules.

3.1.5 Uniqueness of Names

In the CA, the issued certificate guarantees that the certificate owner can be uniquely identified by the information contained in the Distinguished Name of the Subject. The serial number of the certificate shall be the serial number including random numbers generated by CSPRNG. Serial numbers assigned in the CA are unique.

3.1.6 Recognition, Authentication, and Roles of Trademarks

SECOM Trust Systems will confirm, as necessary, whether it has intellectual property rights for the name indicated in the certificate application. Subscribers must not apply for a registered trademark or related name of a third party to the CA. SECOM Trust Systems will not arbitrate or engage itself in the resolution of any dispute between Subscribers and third parties over the registered trademark or any alike. SECOM Trust Systems reserves the right to revoke an issued Certificate due to the dispute.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

SECOM Trust Systems verifies the signature of the certificate issuance request in the certificate application procedure, and confirms that it is signed with the private key corresponding to the public key included in the certificate issuance request. Alternatively, by generating a private key within the CA and securely distributing the private key to the subscribers, the fact that the subscribers has the private key corresponding to the certificate can be proved.

3.2.2 Authentication of Organization Identity

SECOM Trust Systems authenticates the identity of LRA or corporations, and organizations based on official documents issued by national or local governments, investigations conducted, or databases owned by third parties that SECOM Trust Systems trusts, or through other means deemed equally trustworthy by the Certification Services Improvement Committee.
In the case of certification using public documents issued by the national or local governments, a seal certificate (within three months from the date of issuance) or equivalent documents must be submitted.

Documents to be submitted to SECOM Trust Systems at the time of LRA or organization/corporation screening are as follows:

- Documents that report information on LRA or organizations, corporations, etc.
- Other documents required by SECOM Trust Systems at the time of screening

As a result of the examination, If SECOM Trust Systems determines that it is non-conforming, the submitted official documents will be returned or destroyed. If SECOM Trust Systems has received the application form, SECOM shall destroy it.

［S/MIME Certificate］

When issuing an S/MIME on or before August 31, 2023, the CA authenticates that it controls the email account associated with the email address registered in the certificate, or that it is authorized by the email account owner to apply on behalf of, by using the methods described below. The random value described in this section shall consist of a random number of 112 bits or more generated by the CA, and shall be effective for the use of response confirmation for 30 days from the generation.

1. The CA will refer to the registration person（Registrant）information registered in the WHOIS Registry Service in the domain under @ included in the e-mail address, and confirm that the applicant owns the domain (the applicant and the domain owner are the same organization). If the CA confirms that the domain is owned by a third-party organization, it makes sure the account is approved for use, for that the owner of the domain will submit a "domain name use consent form" stamped by the owner organization.

2. The CA confirms that the owner of the e-mail account approves the use of the account by sending a random value by e-mail to the domain contact registered in the WHOIS Registry Service and receiving an acknowledgment containing the random value.

3. Local parts should be 'admin', 'administrator', 'webmaster', 'hostmaster', or ‘postmaster', and by sending a random value to the email address created in the domain below @ included in the email address and receiving the acknowledgment containing the random value, so that CA makes sure that the owner of the email account approves the use of the account.

4. The CA confirms the control of the email account by verifying that the request token or random value is included in the contents of the file. By accessing via the approved port, the CA confirms that a random value is displayed under the "http (or https): // [domains under @ included in the email address] /.well-known/pki-validation" directory, and it receives a successful HTTP or HTTPS response from the request.

5. The CA confirms the control of the email account by verifying that there is a random value or application token in either the DNS CNAME, TXT or CAA record of any of the domains under @ contained in the email address (including the one having a prefix of label with an underscore character at the beginning).

When the CA issues an S/MIME certificate that complies with the Baseline Requirements (S/MIME) on or after September 1, 2023, the CA SHALL verify that Applicant controls the email accounts associated with all Mailbox Fields referenced in the Certificate or has been authorized by the account holder to act on the account holder’s behalf. The CA SHALL NOT delegate the verification of mailbox authorization

or control.
The CA's CP and/or CPS SHALL specify the procedures that the CA employs to perform this verification. The CA SHALL maintain a record of which validation method, including the relevant version number from the Baseline Requirements or S/MIME Baseline Requirements, was used to validate every domain or email address in issued Certificates.

1. The CA MAY confirm the Applicant, such as an Enterprise RA, has been authorized by the email account holder to act on the account holder's behalf by verifying the entity's control over the domain portion of the Mailbox Address to be used in the Certificate. The CA SHALL use only the approved methods in Section 3.2.2.4 of the Baseline Requirements to perform this verification. The term Applicant includes the Applicant's Parent Company, Subsidiary Company, or Affiliate. (Baseline Requirements (S/MIME) 3.2.2.1 Validating authority over mailbox via domain)

2. The CA MAY confirm the Applicant's control over each Mailbox Field to be included in a Certificate by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. Control over each Mailbox Address SHALL be confirmed using a unique Random Value. The Random Value SHALL be sent only to the email address being validated and SHALL not be shared in any other way. The Random Value SHALL be unique in each email. The Random Value SHALL remain valid for use in a confirming response for no more than 24 hours from its creation. (Baseline Requirements (S/MIME) 3.2.2.2 Validating control over mailbox via email)

3. The CA MAY confirm the Applicant's control over each Mailbox Field to be included in the Certificate, by confirming control of the SMTP FQDN to which a message delivered to the Mailbox Address should be directed. The SMTP FQDN SHALL be identified using the address resolution algorithm defined in RFC 5321 Section 5.1 which determines which SMTP FQDNs are authoritative for a given Mailbox Address. If more than one SMTP FQDN has been discovered, the CA SHALL verify control of an SMTP FQDN following the selection process at RFC 5321 Section 5.1. Aliases in MX record RDATA SHALL NOT be used for this validation method. (Baseline Requirements (S/MIME) 3.2.2.3 Validating applicant as operator of associated mail server(s))

3.2.3 Authentication of Applicant and Individual Identity

SECOM Trust Systems authenticates the identity of applicants or individuals based on official documents issued by national or local governments, investigations conducted, or databases owned by third parties that SECOM Trust Systems trusts, or through other means deemed equally trustworthy by the Certification Services Improvement Committee.

Upon issuance of a certificate for a client certificate and a data signing certificate, an examination of an applicant and a subscriber may be performed by terms and conditions separately stipulated by SECOM, or a method determined by the LRA based on the SECOM Passport for PublicID LRA Operational Standards (hereinafter, "LRA Operational Standards")

The following methods shall be used to issue certificates for the AATL Document Signing Certificate.

To authenticate an individual belonging to an organization, the CA shall confirm the existence of the representative or a person delegated by the representative. To authenticate official positions in the civil service, the CA shall confirm the existence of the representative or a person delegated by the representative. The representative or a person authorized by the representative shall be the one who verified the identity of the individual face-to-face and confirmed a match.

The individual identity shall be authenticated through one of the following methods:

1. Confirm the Applicant's seal impression included with any application received in writing;
2. Verify the Applicant's identity using official documents;
3. Performing a postal challenge/response to the Applicant using an address obtained from a reliable third party;
4. Performing a telephone challenge/response to the Applicant using a telephone number from a reliable third party;
5. Performing an email challenge/response to the Applicant using an email address from a reliable third party.

Information used for examination can be reused within the period prescribed by the CA.

3.2.4 Non-Verified Subscriber Information

SECOM Trust Systems verifies all information specified in BR such as the trade name, name, and location of the certificate subscriber included in the certificate's

distinguished name. In addition, in providing the service, there is a case where it is requested to provide information necessary for office procedures such as billing information.

3.2.5 Validation of Authority

The legitimacy of authority for the applicant is authenticated in accordance with "3.2.2 Authentication of Organization Identity" and "3.2.3 Authentication of applicant and certificate subscriber" hereof.

3.2.6 Criteria for Interoperation

The CA SHALL disclose all Cross Certificates that identify the CA as the Subject, provided that the CA arranged for or accepted the establishment of the trust relationship.

3.2.7 Reliability of verification sources

Before relying on a source of verification data to validate Certificate Requests, the CA SHALL verify its suitability as a Reliable Data Source.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

Shall be in the same manner as set forth in "3.2.3 Authentication of Applicant and Individual Identity" and "3.2.5 Validation of Authority".

3.3.2 Identification and Authentication for Re-Key after Revocation

Shall be in the same manner as set forth in "3.2.3 Authentication of Applicant and Individual Identity" and "3.2.5 Validation of Authority".

3.4 Identification and Authentication for Revocation Requests

Shall be in the same manner as set forth in "3.2.3 Authentication of Applicant and Individual Identity" and "3.2.5 Validation of Authority".

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who May Submit a Certificate Application

An application for the CA can be made by an LRA, corporation, or organization that has been certified by SECOM Trust Systems based on "3.2.2 Authentication of Organization Identity".
Applications for LRA can be made by persons specified by LRA based on the LRA operational standards.

4.1.2 Enrollment Process and Responsibilities

In submitting a Certificate Application, a Subscriber or an Applicant to perform the application procedure shall agree to the provisions of this CP, and the CPS before proceeding with the application, as well as certify that the information submitted is accurate.

[S/MIME Certificate]
Prior to the issuance of a S/MIME Certificate, the CA SHALL obtain the following documentation from the Applicant:

1. A Certificate Request; and
2. An executed Subscriber Agreement and/or Terms of Use.

The Certificate Request and Subscriber Agreement or Terms of Use SHALL be in a form prescribed by the CA and SHALL comply with the Baseline Requirements including Section "9.6.3 Applicant and Subscriber Representations and Warranties" of this CP. The CA SHOULD obtain any additional documentation the CA determines necessary to fulfil the Baseline Requirements.
The Certificate Request SHALL contain a request from, or on behalf of, the Applicant for the issuance of a Certificate, and a certification by, or on behalf of, the Applicant that all of the information contained therein is correct.
One Certificate Request MAY suffice for multiple Certificates to be issued to the same Applicant, subject to the validation reuse periods described in Section "4.2.1 Performing Identification and Authentication Functions" of this CP, provided that each Certificate is supported by a valid, current Certificate Request signed by the appropriate Applicant Representative on behalf of the Applicant.

The CA may rely on a previously verified Certificate Request to issue a replacement Certificate if:

1. The previous Certificate being referenced was not revoked;
2. The expiration date of the replacement Certificate is the same as the previous Certificate being referenced; and
3. The Subject Information of the Certificate is the same as the previous Certificate being referenced.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

SECOM Trust Systems performs identity verification and authentication of the LRA or the corporation, organization in accordance with "3.2 Initial Identification and Authentication". In applying for a certificate accepted from the LRA, the certificate presented by the LRA is verified and authenticated for the identity of the LRA.
The LRA performs identity verification and authentication based on the LRA operational standards in the manner determined by the LRA.

[S/MIME Certificate]
Applicant information SHALL include at least one Mailbox Field to be included in the Certificate's subjectAltName extension.
The CA MAY reuse completed validations and/or supporting evidence performed in accordance with Section "3.2 Initial Identity Validation" of this CP within the following limits:
Validation of mailbox authorization or control:
Completed validation of the control of a mail server in accordance with "Baseline Requirements (S/MIME) 3.2.2.1 Validating authority over mailbox via domain" or "Baseline Requirements (S/MIME) 3.2.2.3 Validating applicant as operator of associated mail server(s)" SHALL be obtained no more than 398 days prior to issuing the Certificate.
In the event of changes to the Baseline Requirements specified in "Baseline Requirements (S/MIME) 3.2.2.1 Validating authority over mailbox via domain", a CA MAY continue to reuse completed validations and/or supporting evidence for the period stated in this section.
Completed validation of control of a mailbox in accordance with "Baseline Requirements (S/MIME) 3.2.2.2 Validating control over mailbox via email" SHALL be

obtained no more than 30 days prior to issuing the Certificate.

[AATL Document Signing Certificate]
The CA MAY reuse completed validations and/or supporting evidence performed in accordance with Section "3.2 Initial Identity Validation" of this CP within the following limits:
The validation SHALL be obtained no more than 825 days prior to issuing the Certificate.

[Microsoft Document Signing Certificate]
The CA MAY reuse completed validations and/or supporting evidence performed in accordance with Section "3.2 Initial Identity Validation" of this CP within the following limits:
The validation SHALL be obtained no more than 825 days prior to issuing the Certificate.

4.2.2 Approval or Rejection of Certificate Applications

The CA or LRA issues a certificate for the application that has been approved as a result of the review. In addition, it shall be possible to reject a certificate application for which the examination of all items is not completed successfully, and reject any certificate that includes the following reasons:

- Certificate of the applicant or the subscriber that was previously rejected or previously violated the terms of the agreement
- Suspected or concerned about phishing, malware, or other fraudulent use

4.2.3 Time to Process Certificate Applications

After accepting the certificate application, the CA shall immediately enable the LRA, the certificate subscriber or the applicant to obtain the certificate.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

The CA issues a certificate signed using the CA's private key based on the application information.
Subordinate CA certificate issuance by the Root CA shall require an individual authorized by the CA (i.e. the CA system operator, system officer, or PKI

administrator) to deliberately issue a direct command in order for the Root CA to perform a certificate signing operation.
When issuing certificates for Code Signing Certificate Policy, the CA confirms whether the format conforms to Baseline Requirements for some items of the certificate to be issued by the pre-certificate linting function, and refuses to issue if it does not meet the requirements.
The CA enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.
The backdating of a certificate's notBefore date to avoid a deadline, prohibition or code-enforced restriction is not used by the CA.

4.3.2 Notifications to Subscriber of Certificate Issuance

After the issuance of the certificate for the received application is completed, the CA distributes the issued certificate online or offline to the LRA, the certificate subscriber, or the applicant. When the CA generates the private key of the certificate subscriber, the private key and PIN will be sent separately by mail, e-mail, hand exchange, etc.
Notification of certificate issuance is made by distributing the certificate.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

If the CA receives a report for receipt from the LRA or the Subscriber, or if no objection is made within 14 days of the CA's distribution of the Certificate, consider that the LRA or Subscriber has received the certificate.

4.4.2 Publication of the Certificate by the CA

The CA does not publish Subscriber Certificates.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

The CA will not send a notice of Certificate issuance to entities other than the person in charge, who was registered at the time of the Certificate Application submission.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

The use of the private key and certificate of the Subscribers shall be in accordance

with “1.4.1 Appropriate Certificate Uses” and the terms and conditions. The Subscribers shall use the certificate and the corresponding private key for the purpose described in "1.4.1 Appropriate Certificate Uses" and the terms and conditions.

4.5.2 Relying Party Public Key and Certificate Usage

Relying Parties can use the public key and certificate of the Subscribers to verify the authenticity of the certificate issued by the CA. Relying Parties must understands and accepts the contents of this CP and CPS before using the CA's certificate.

4.6 Certificate Renewal

The CA recommends generating a new Key Pair when Subscribers renew a Certificate.

4.6.1 Circumstances for Certificate Renewal

No stipulation

4.6.2 Who May Request Renewal

No stipulation

4.6.3 Processing Certificate Renewal Requests

No stipulation

4.6.4 Notification of New Certificate Issuance to Subscriber

No stipulation

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

No stipulation

4.6.6 Publication of the Renewal Certificates by the CA

No stipulation

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation

4.7 Certificate renewal with Re-Key

4.7.1 Circumstances for Certificate Re-Key

Renewal of a certificate with a key is performed when the validity period of the certificate expires or when the certificate is revoked due to compromise of the key.

4.7.2 Who May Request Certification of a New Public Key

Shall be same as “4.1.1 Who May Submit a Certificate Application”.

4.7.3 Processing Certificate Re-Keying Requests

Shall be same as “4.3.1 CA Actions during Certificate Issuance”.

4.7.4 Notification of New Certificate Issuance to Subscriber

Shall be same as “4.3.2 Notifications to Subscriber of Certificate Issuance”.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

Shall be same as “4.4.1 Conduct Constituting Certificate Acceptance”.

4.7.6 Publication of the Re-Keyed Certificate by the CA

Shall be same as “4.4.2 Publication of the Certificate by the CA”.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Shall be same as “4.4.3 Notification of Certificate Issuance by the CA to Other Entities”

4.8 Certificate Modification

If there is any change in the information on the certificate, Subscribers must promptly apply for the change. The procedure for the change shall be the same as that for the first issue. After the certificate is changed, the certificate before the change shall be revoked immediately.

4.8.1 Circumstances for Certificate Modification

No stipulation

4.8.2 Who May Request Certificate Modification

Shall be same as “4.1.1 Who May Submit a Certificate Application”.

4.8.3 Processing Certificate Modification Requests

Shall be same as “4.3.1 CA Actions during Certificate Issuance”. The revocation of the certificate before the change shall be the same as in “4.9.3 Procedure for Revocation Request”.

4.8.4 Notification of New Certificate Issuance to Subscriber

Shall be same as “4.3.2 Notifications to Subscriber of Certificate Issuance”.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Shall be same as “4.4.1 Conduct Constituting Certificate Acceptance”.

4.8.6 Publication of the Modified Certificates by the CA

Shall be same as “4.4.2 Publication of the Certificate by the CA”.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Certificate Revocation

A Subscriber must promptly request the CA to revoke a Certificate in the event of any of the following:

- There has been a change in information populated in the Certificate;
- The Private Key has or may have been compromised for any reason, including the theft, loss, unauthorized disclosure or unauthorized use thereof;
- The Certificate is incorrectly populated or not being used for authorized purposes;
- The use of the Certificate is being terminated.

SECOM Trust Systems may revoke the Subscriber Certificate at its discretion in the event of any of the following:

- The Subscriber is not performing the obligations thereof set forth in this CP, the CPS, relevant agreements or laws;
- When it has been determined that the Subscriber has been refused to issue a certificate or has been revoked to breach of contract or other reasons;
- When it is determined that the private key of the Subscriber and the CA has been

compromised or may be compromised;

- It is recognized that the Certificate is not issued in compliance with this CP or CPS;
- It is recognized that the certificate was used for a purpose other than the proper use described in this CP, or was used for a purpose other than that indicated in the contract with SECOM Trust Systems, or the certificate was misused in other ways;
- The CA receives notice or otherwise becomes aware of any circumstance indicating that use of the email address in the certificate is no longer legally permitted;
- When it is recognized that a change in the information contained in the certificate;
- When it is recognized that the certificate of the Subscriber has been illegally accessed;
- When it is recognized that the suspicious code was signed using a certificate;
- When the S/MIME certificate is issued in violation of the current version of the Mozilla Root Store Policy or Apple Root Certificate Program;
- SECOM Trust Systems recognizes any other situation deemed to necessitate revocation.

[Code Signing Certificate]
The CA SHALL revoke a Certificate within 24 hours if one or more of the following occurs:

1. The Subscriber requests in writing that the CA revoke the Certificate;
2. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization;
3. The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise;
4. The CA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate;
5. The CA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, or if there is clear evidence that the specific method used to generate the Private Key was flawed;
6. The CA has reasonable assurance that a Certificate was used to sign Suspect Code.

The CA SHOULD revoke a certificate within 24 hours and SHALL revoke a Certificate

within 5 days if one or more of the following occurs:

7. The Certificate no longer complies with the Baseline Requirements (Code Signing) Section 6.1.5 and Section 6.1.6;
8. The CA obtains evidence that the Certificate was misused;
9. The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;
10. The CA is made aware of a material change in the information contained in the Certificate;
11. The CA is made aware that the Certificate was not issued in accordance with the Baseline Requirements (Code Signing) or the CA's Certificate Policy or Certification Practice Statement;
12. The CA determines or is made aware that any of the information appearing in the Certificate is inaccurate;
13. The CA's right to issue Certificates under the Baseline Requirements (Code Signing) expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository;
14. Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement.

The CA MAY delay revocation based on a request from Application Software Suppliers where immediate revocation has a potentially large negative impact to the ecosystem.

[S/MIME Certificate]

The CA SHALL revoke a Certificate within 24 hours if one or more of the following occurs:

1. The Subscriber requests in writing that the CA revoke the Certificate;
2. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization (CRLReason #9, privilegeWithdrawn);
3. The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise (CRLReason #1, keyCompromise);
4. The CA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys) (CRLReason #1, keyCompromise);
5. The CA obtains evidence that the validation of domain authorization or mailbox

control for any email address in the Certificate should not be relied upon (CRLReason #4, superseded).

The CA SHOULD revoke a certificate within 24 hours and SHALL revoke a Certificate within 5 days if one or more of the following occurs:

1. The Certificate no longer complies with the requirements of Section "6.1.5 Key Sizes" and Section "6.1.6 Public Key Parameters Generation and Quality Checking" of this CP (CRLReason #4, superseded);
2. The CA obtains evidence that the Certificate was misused (CRLReason #9, privilegeWithdrawn);
3. The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use (CRLReason #9, privilegeWithdrawn);
4. The CA is made aware of any circumstance indicating that use of an email address or Fully-Qualified Domain Name in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked the right to use an email address or Domain Name, a relevant licensing or services agreement between the Subscriber has terminated, or the account holder has failed to maintain the active status of the email address or Domain Name) (CRLReason #5, cessationOfOperation);
5. The CA is made aware of a material change in the information contained in the Certificate (CRLReason #9, privilegeWithdrawn);
6. The CA is made aware that the Certificate was not issued in accordance with the Baseline Requirements (S/MIME) or the CA's CP and/or CPS (CRLReason #4, superseded) ;
7. The CA determines or is made aware that any of the information appearing in the Certificate is inaccurate (CRLReason #9, privilegeWithdrawn);
8. The CA's right to issue Certificates under the Baseline Requirements (S/MIME) expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL);
9. Revocation is required by the CA's CP and/or CPS (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL);
10. The CA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed (CRLReason #1, keyCompromise.

4.9.2 Who Can Request Revocation

Shall be same as “4.1.1 Who May Submit a Certificate Application”.

[Code Signing Certificate]

The CA MUST provide Anti-Malware Organizations, Subscribers, Relying Parties, Application Software Suppliers, and other third parties with clear instructions on how they can report suspected private key compromise, Certificate misuse, Certificates used to sign Suspect Code, Takeover Attacks, or other types of possible fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates. The CA MUST publicly disclose the instructions on its website.

[S/MIME Certificate]

The Subscriber, RA, or Issuing CA can initiate revocation. Additionally, Subscribers, Relying Parties, Application Software Suppliers, and other third parties MAY submit Certificate Problem Reports informing the issuing CA of reasonable cause to revoke a certificate.

4.9.3 Procedure for Revocation Request

A Subscriber submits a revocation request for the Subscriber certificate to the CA according to the prescribed procedure. For the certificates requested and issued by the LRA, a revocation request for a Subscriber certificate shall be made by the method determined by the LRA based on the LRA operational standards. LRA accesses the site provided by SECOM using the LRA certificate, and applies for revocation of the Subscriber certificate to the CA.

The CA SHALL maintain a continuous 24x7 ability to accept and respond to revocation requests and Certificate Problem Reports.

4.9.4 Revocation Request Grace Period

The Subscriber must apply for revocation immediately after the cause of the certificate revocation.

The LRA must apply for revocation to the CA immediately after receiving the application from the Subscriber.

4.9.5 Time within Which CA Shall Process the Revocation Request

Upon receipt of a valid Revocation Request, the CA will promptly process the request

and reflect the relevant Certificate information in the CRL.

[Code Signing Certificate]
The CA MUST maintain a continuous 24x7 ability to communicate with Anti-Malware Organizations, Application Software Suppliers, and law enforcement agencies and respond to high-priority Certificate Problem Reports, such as reports requesting revocation of Certificates used to sign malicious code, fraud, or other illegal conduct.
The CA MUST acknowledge receipt of plausible notices about Suspect Code signed with a certificate issued by the CA or a Subordinate CA.
The CA MUST begin investigating Certificate Problem Reports within twenty-four hours of receipt, and decide whether revocation or other appropriate action is warranted based on at least the following criteria:

1. The nature of the alleged problem (adware, spyware, malware, software bug, etc.),
2. The number of Certificate Problem Reports received about a particular Certificate or Subscriber,
3. The entity making the report (for example, a notification from an Anti-Malware Organization or law enforcement agency carries more weight than an anonymous complaint), and
4. Relevant legislation.

When revoking a Certificate, the CA SHOULD work with the Subscriber to estimate a date of when the revocation should occur in order to mitigate the impact of revocation on validly signed Code. For key compromise events, this date SHOULD be the earliest date of suspected compromise.

[S/MIME Certificate]
Within 24 hours after receiving a Certificate Problem Report, the CA SHALL investigate the facts and circumstances related to a Certificate Problem Report and provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report.
After reviewing the facts and circumstances, the CA SHALL work with the Subscriber and any entity reporting the Certificate Problem Report or other revocation-related notice to establish whether or not the Certificate will be revoked, and if so, a date on which the CA will revoke the certificate. The period from receipt of the Certificate Problem Report or revocation-related notice to published revocation SHALL NOT exceed the time frame set forth in Section 4.9.1.1. The date selected by the CA SHOULD consider the following criteria:

1. The nature of the alleged problem (scope, context, severity, magnitude, risk of harm);
2. The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties);
3. The number of Certificate Problem Reports received about a particular Certificate or Subscriber;
4. The entity making the complaint (for example, a complaint from a law enforcement official should be addressed with higher priority); and
5. Relevant legislation.

4.9.6 Revocation Checking Requests

In the certificate issued by the CA, describe the URL where the CRL is stored. For certificates issued by the code signing certificate policy, the URL of the OCSP responder is also described. Relying Parties must authenticate the validity of a Subscriber Certificate. The validity of a Certificate may be verified by using the CRL posted on the Repository site or the OCSP responder.

4.9.7 CRL Issuance Frequency

If the CA publishes a CRL, then the CA SHALL update and reissue CRLs at least once every seven days, and the value of the nextUpdate field MUST NOT be more than ten days beyond the value of the thisUpdate field.

4.9.8 Maximum Latency for CRLs

The CRLs issued by the CA will be reflected onto the Repository within a reasonable time.

4.9.9 On-Line Revocation/Status Checking Availability

For the Code Signing Certificate and the S/MIME Certificate, online certificate status information is provided through the OCSP responder. Policies other than the code signing certificate policy are provided as needed.

OCSP responses SHALL conform to RFC6960 and/or RFC5019. OCSP responses SHALL either:

1. Be signed by the CA that issued the Certificates whose revocation status is being checked, or
2. Be signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked.

In the latter case, the OCSP signing Certificate MUST contain an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960.

4.9.10 On-Line Revocation/Status Checking Requirements

Relying Parties must authenticate the validity of Subscriber Certificates. If not using the CRL posted on the Repository to check for the Revocation registration of a Certificate, the Relying Parties must confirm the Certificate status available through the OCSP responder.

OCSP responders operated by the CA SHALL support the HTTP GETmethod, as described in RFC 6960 and/or RFC 5019.

The validity interval of an OCSP response is the difference in time between the thisUpdate and nextUpdate field, inclusive. For purposes of computing differences, a difference of 3,600 seconds shall be equal to one hour, and a difference of 86,400 seconds shall be equal to one day, ignoring leap-seconds.

For the status of Subscriber Certificates:

1. OCSP responses MUST have a validity interval greater than or equal to eight hours;
2. OCSP responses MUST have a validity interval less than or equal to ten days;
3. For OCSP responses with validity intervals less than sixteen hours, then the CA SHALL update the information provided via an Online Certificate Status Protocol prior to one-half of the validity period before the nextUpdate.
4. For OCSP responses with validity intervals greater than or equal to sixteen hours, then the CA SHALL update the information provided via an Online Certificate Status Protocol at least eight hours prior to the nextUpdate, and no later than four days after the thisUpdate.

For the status of Subordinate CA Certificates:

The CA SHALL update information provided via an Online Certificate Status Protocol

i. at least every twelve months; and

ii. within 24 hours after revoking a Subordinate CA Certificate.

If the OCSP responder receives a request for the status of a certificate serial number that is "unused", then the responder SHOULD NOT respond with a "good" status. If the OCSP responder is for a CA that is not Technically Constrained in line with Section “7.1.5 Name Constraints” of this CP, the responder MUST NOT respond with a "good" status for such requests.

The CA SHOULD monitor the OCSP responder for requests for "unused" serial

numbers as part of its security response procedures.
A certificate serial number within an OCSP request is "assigned" if a Certificate with that serial number has been issued by the Issuing CA, using any current or previous key associated with that CA subject; or "unused" in other case.

4.9.11 Other Forms of Revocation Advertisements Available
If the certificate is for a high traffic FQDN, the CA can distribute this OCSP response using stapling in accordance with RFC4366, RFC 5246, RFC 8446. In this case, the CA ensures that the subscriber "staples" the OCSP response of the certificate within the TLS handshake.
The CA shall enforce this requirement for the subscriber by responding to the service usage rules, the contract with the subscriber, etc., or a technical review by the CA.

4.9.12 Special Requirements Regarding Key Compromise
Refer to “4.9.1. Circumstances for Certificate Revocation”.

4.9.13 Circumstances for Suspension Who Can Request Suspension
The suspension of the certificate can be performed at the discretion of the certificate subscriber. Suspension of a certificate shall be performed at the responsibility of the Subscriber. When a certificate is suspended, an application for revocation of the certificate must be made.

4.9.14 Who Can Request Suspension
The suspension of the certificate shall be performed by the Subscriber.

4.9.15 Procedure for Suspension Request
Access the website notified in advance from the CA, and apply for suspension using the login password separately notified.

4.9.16 Limits on Suspension Period
Not applicable.

4.10 Certificate Status Services

4.10.1 Operational Characteristics
The revocation information of the CRL or OCSP responder shall be confirmed until the

expiration date written on the revoked certificate. For the certificates issued by the code signing certificate policy, revocation information shall be confirmed for at least 10 years after the expiration date.

4.10.2 Service Availability

The CA SHALL operate and maintain its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

The CA SHALL maintain an online 24x7 Repository that application software can use to automatically check the current status of all unexpired Certificates issued by the CA.

The CA SHALL maintain a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint.

4.10.3 Optional Features

No stipulation

4.11 End of Subscription (Registry)

When terminating the use of this service, the LRA or the Subscriber must apply for revocation of the issued certificate.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

The CA does not Escrow Subscriber Private Keys.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5. Facility, Management, and Operational Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

Relevant provisions are stipulated in the CPS.

5.1.2 Physical Access

Relevant provisions are stipulated in the CPS.

5.1.3 Power and Air Conditioning

Relevant provisions are stipulated in the CPS.

5.1.4 Water Exposures

Relevant provisions are stipulated in the CPS.

5.1.5 Fire Prevention and Protection

Relevant provisions are stipulated in the CPS.

5.1.6 Media Storage

Relevant provisions are stipulated in the CPS.

5.1.7 Waste Disposal

Relevant provisions are stipulated in the CPS.

5.1.8 Off-Site Backup

Relevant provisions are stipulated in the CPS.

5.2 Procedural Controls

5.2.1 Trusted Roles

Relevant provisions are stipulated in the CPS.

5.2.2 Number of Persons Required per Task

Relevant provisions are stipulated in the CPS.

5.2.3 Identification and Authentication for Each Role

Relevant provisions are stipulated in the CPS.

5.2.4 Roles Requiring Separation of Duties

Relevant provisions are stipulated in the CPS.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

Relevant provisions are stipulated in the CPS.

5.3.2 Background Check Procedures

Relevant provisions are stipulated in the CPS.

5.3.3 Training Requirements

Relevant provisions are stipulated in the CPS.

5.3.4 Retraining Frequency and Requirements

Relevant provisions are stipulated in the CPS.

5.3.5 Job Rotation Frequency and Sequence

Relevant provisions are stipulated in the CPS.

5.3.6 Sanctions for Unauthorized Actions

Relevant provisions are stipulated in the CPS.

5.3.7 Independent Contractor Requirements

Relevant provisions are stipulated in the CPS.

5.3.8 Documentation Supplied to Personnel

Relevant provisions are stipulated in the CPS.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

Relevant provisions are stipulated in the CPS.

5.4.2 Frequency of Processing Audit Log

Relevant provisions are stipulated in the CPS.

5.4.3 Retention Period for Audit Log

Relevant provisions are stipulated in the CPS.

5.4.4 Protection of Audit Log

Relevant provisions are stipulated in the CPS.

5.4.5 Audit Log Backup Procedure

Relevant provisions are stipulated in the CPS.

5.4.6 Audit Log Collection System

Relevant provisions are stipulated in the CPS.

5.4.7 Notification to Event-Causing Subject

Relevant provisions are stipulated in the CPS.

5.4.8 Vulnerability Assessments

Relevant provisions are stipulated in the CPS.

5.5 Records Archival

5.5.1 Types of Records Archived

Relevant provisions are stipulated in the CPS.

5.5.2 Retention Period for Archive

Relevant provisions are stipulated in the CPS.

5.5.3 Protection of Archive

Relevant provisions are stipulated in the CPS.

5.5.4 Archive Backup Procedures

Relevant provisions are stipulated in the CPS.

5.5.5 Requirements for Time-Stamping of Records

Relevant provisions are stipulated in the CPS.

5.5.6 Archive Collection System

Relevant provisions are stipulated in the CPS.

5.5.7 Procedures to Obtain and Verify Archive Information

Relevant provisions are stipulated in the CPS.

5.6 Key Changeover

Before the remaining validity period of a Certificate corresponding to the CA Private Key becomes shorter than the maximum validity period of the Certificate issued to a Subscriber, a new Private Key is generated in its stead and a new Certificate is issued. Once a new Private Key is generated, Certificates and CRLs are issued using the new Private Key.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

Relevant provisions are stipulated in the CPS.

5.7.2 Procedure when Hardware, Software, and/or Data are Corrupted

Relevant provisions are stipulated in the CPS.

5.7.3 Entity Private Key Compromise Procedures

Relevant provisions are stipulated in the CPS.

5.7.4 Business Continuity Capabilities after a Disaster

Relevant provisions are stipulated in the CPS.

5.8 CA or RA Termination

In the event of termination of the CA by SECOM Trust Systems, the company shall so notify LRA, the service contractor and other affected participants, including Application Software Suppliers. All Certificates issued by the CA are revoked prior to the termination thereof.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The certification infrastructure system generates a CA key pair on a hardware security module (hereinafter, "HSM") compliant with level 3 of FIPS140-2.
The Key Pair generation operation is jointly performed by at least two authorized individuals.
The key pair of the Subscriber shall be generated within the terminal or HSM used by the Subscriber or in the CA facility.
Subscriber's key pair for AATL Document Signing Certificate shall be generated on a cryptographic hardware device within the HSM used by the Subscriber or in the CA facility.

6.1.2 Private Key Delivery to Subscriber

The CA sent a PIN for using the private key and a private key by different routes. Or, exchange the PIN and private key in person.

[S/MIME Certificate]
Parties other than the Subscriber SHALL NOT archive the Subscriber Private Key without authorization by the Subscriber.
If the CA or any of its designated RAs become aware that a Subscriber's Private Key has been communicated to a person or organization not authorized by the Subscriber, then the CA SHALL revoke all Certificates that include the Public Key corresponding to the communicated Private Key.
If the CA or a Delegated Third Party generates the Private Key on behalf of the Subscriber where the Private Keys will be transported to the Subscriber, then the entity generating the Private Key SHALL either transport the Private Key in hardware with an activation method that is equivalent to 128 bits of encryption or encrypt the Private Key with at least 128 bits of encryption strength. Example methods include using a 128-bit AES key to wrap the private key or storing the key in a PKCS 12 file encrypted with a randomly generated password of more than 16 characters containing uppercase letters, lowercase letters, numbers, and symbols for transport. The CA or Delegated Third Party SHALL NOT store Subscriber Private

Keys in clear text.
The material used to activate/protect the Private Key (e.g., a password used to secure a PKCS 12 file) must be delivered to the Subscriber securely and separately from the container holding the Private Key.

6.1.3 Public Key Delivery to Certificate Issuer
A Subscriber Public Key may be delivered online to the CA, the communication routing of which is encrypted by SSL/TLS.

6.1.4 CA Public Key Delivery to Relying Parties
Relying Parties may obtain the CA Public Keys by accessing the CA Repository.

6.1.5 Key Sizes
Relevant provisions are stipulated in the CPS.

6.1.6 Public Key Parameters Generation and Quality Checking
Relevant provisions are stipulated in the CPS.

6.1.7 Key Usage Purposes
"keyCertSign" and "cRLSign" bits shall be specified to the [keyUsage] of the CA Certificate.
One of digitalSignature, nonRepudiation, keyEncipherment, and dataEncipherment is set in the KeyUsage of the certificate of the Subscriber issued by the CA, and the settable combination is appropriately limited for each use of the certificate.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls
The generation, storage and signing operations of the CA Private Keys are performed using an FIPS140-2 Level 3 conformant HSM.
Certificates of the AATL Document Signing Certificate shall have one of the following accreditations:

1. FIPS 140-2 Level 2; or
2. Common Criteria (ISO 15408 & ISO 18045) - Protection Profiles CEN prEN 14169 (all parts applicable to the device type) or standards such as CEN EN 419 241 series or equivalent, for remotely managed devices; or

3. by an EU Member State as a Qualified Signature Creation Device (QSCD) after 1 July 2016, or that was recognized as a Secure Signature Creation Device (SSCD) by an EU Member State designated body before 1 July 2016.

6.2.2 Private Key Multi-Person Control

Activation, deactivation, backup and other operations relating to CA Private Keys are jointly performed by at least two authorized individuals in a secure environment.
No stipulation for Subscriber Private Keys.

6.2.3 Private Key Escrow

The CA does not Escrow the CA Private Keys.
The CA does not Escrow Subscriber Private Keys.

6.2.4 Private Key Backup

Backup of Private Keys of the CA is jointly performed by at least two authorized individuals and is stored in a secure room as encrypted.
No stipulation for Subscriber Private Keys.

6.2.5 Private Key Archive

The CA does not archive CA Private Keys.
No stipulation for Subscriber Private Keys.

6.2.6 Private Key Transfer into or from a Cryptographic Module

The transfer of Private Keys of the CA into and from an HSM is performed in a secure room while encrypted.
No stipulation for Subscriber Private Keys.

6.2.7 Private Key Storage on Cryptographic Module

The CA's private keys shall be protected within systems or devices validated to meet at least FIPS 140 Level 3 or Common Criteria Protection Profile or Security Target, EAL 4 or higher. This includes protecting private keys and other assets from the known threats.
Timestamp Authority for Code Signing purpose shall use processes of at least FIPS 140-2 Level 3, Common Criteria EAL 4+ (ALC_FLR.2) or better to protect private keys.
The CA MUST protect its signing operations in accordance with the CA/Browser Forum's Network Security Guidelines.

Effective June 1, 2023, Subscriber Private Keys for Code Signing Certificates SHALL be protected per the following requirements. The CA MUST obtain a contractual representation from the Subscriber that the Subscriber will use one of the following options to generate and protect their Code Signing Certificate Private Keys in a Hardware Crypto Module with a unit design form factor certified as conforming to at least FIPS 140-2 Level 2 or Common Criteria EAL 4+:

(1) Subscriber uses a Hardware Crypto Module meeting the specified requirement.

(2) Subscriber uses a cloud-base key generation and protection solution with the following requirements:

a Key creation, storage, and usage of Private Key must remain within the security boundaries of the cloud solution's Hardware Crypto Module that conforms to the specified requirements;

b Subscription at the level that manages the Private Key must be configured to log all access, operations, and configuration changes on the resources securing the Private Key.

(3) Subscriber uses a Signing Service which meets the Baseline Requirements (Code Signing) of Section 6.2.7.3.

Effective June 1, 2023, for Code Signing Certificates, CAs SHALL ensure that the Subscriber's Private Key is generated, stored, and used in a suitable Hardware Crypto Module that meets or exceeds the requirements specified in Section 6.2.7.4.1. One of the following methods MUST be employed to satisfy this requirement:

1. The CA ships a suitable Hardware Crypto Module, with one or more pre-generated Key Pairs that the CA has generated using the Hardware Crypto Module;
2. The Subscriber counter-signs certificate requests that can be verified by using a manufacturer's certificate, commonly known as key attestation, indicating that the Private Key was generated in a non-exportable way using a suitable Hardware Crypto Module;
3. The Subscriber uses a CA prescribed crypto library and a suitable Hardware Crypto Module combination for the Key Pair generation and storage;
4. The Subscriber provides an internal or external IT audit indicating that it is only using a suitable Hardware Crypto Module to generate Key Pairs to be associated with Code Signing Certificates;
5. The Subscriber provides a suitable report from the cloud-based key protection solution subscription and resources configuration protecting the Private Key in a suitable Hardware Crypto Module;

6. The CA relies on a report provided by the Applicant that is signed by an auditor who is approved by the CA and who has IT and security training or is a CISA witnesses the Key Pair creation in a suitable Hardware Crypto Module solution including a cloud-based key generation and protection solution;
7. The Subscriber provides an agreement that they use a Signing Service meeting the Baseline Requirements (Code Signing) of Section 6.2.7.3;

For AATL Document Signing Certificate, if it is confirmed that the CA has generated a private key within the HSM used by the Subscriber, in the certificate application procedure, the CA verify the signature of the certificate issuance request and confirm that it is signed with the private key corresponding to the public key included in the certificate issuance request. Alternatively, the CA generates a private key on a cryptographic hardware device and securely distributes the private key to the Subscriber, so that the CA proves the Subscriber owns the private key corresponding to the applicable certificate.

No stipulation for Subscriber's private keys other than Code Signing Certificates and AATL Document Signing Certificates.

6.2.8 Method of Activating Private Key

The CA Private Keys are jointly activated by at least two authorized individuals in a secure room. No stipulation for Subscriber Private Keys.

6.2.9 Method of Deactivating Private Key

CA Private Keys are jointly deactivated by at least two authorized individuals in a secure room.
No stipulation for Subscriber Private Keys.

6.2.10 Method of Destroying Private Key

The CA Private Keys 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.
No stipulation for Subscriber Private Keys.

6.2.11 Cryptographic Module Rating

Shall be same 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

Archives of the CA's public key and the Subscriber's public key are included in this CP "5.5.1 Types of Records Archived".
No stipulation for Subscriber Private Keys.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

Relevant provisions are stipulated in the CPS.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Relevant provisions are stipulated in the CPS.

6.4.2 Activation Data Protection

Relevant provisions are stipulated in the CPS.

6.4.3 Other Aspects of Activation Data

No stipulation

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

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

6.5.2 Computer Security Rating

Relevant provisions are stipulated in the CPS.

6.6 Life-Cycle Security Controls

6.6.1 System Development Controls

Relevant provisions are stipulated in the CPS.

6.6.2 Security Management Controls

Relevant provisions are stipulated in the CPS.

6.6.3 Life-Cycle Security Controls

Relevant provisions are stipulated in the CPS.

6.7 Network Security Controls

Relevant provisions are stipulated in the CPS.

6.8 Time-Stamping

Relevant provisions are stipulated in the CPS.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

The CA SHALL meet the technical requirements set forth in Section "2.2 Publication of Information", Section "6.1.5 Key Sizes", and Section "6.1.6 Public Key Parameters Generation and Quality Checking" of this CP.

The CA SHALL generate non-sequential Certificate serial numbers greater than zero (0) and less than 2^159 containing at least 64 bits of output from a CSPRNG.

Certificates issued by the CA conform to RFC5280, the profile of which are indicated in the tables below.

Table 7.1-1 Subscriber Certificate (SHA256: Certificate Policy for Clients, Certificate Policy for Data Signing) Profile

Basic Fields		Settings	critical
Version		Version 3	-
serialNumber		e.g.) 123456789abcdef0	-
signatureAlgorithm		sha256WithRSAEncryption	-
issuer	countryName	JP	-
	organizationName	Set the CA's Organization	
	organizationalUnitName	The CA's Organizational Unit can be set	
	commonName	Set the CA's Common Name	
validity	notBefore	A value within 48 hours before the certificate signing	-
	notAfter	Stipulated in the CPS "6.3.2 Certificate Operational Periods and Key Pair Usage Periods"	
subject	countryName	JP	-
	stateOrProvinceName	State or Province Name 【Optional】	
	localityName	Locality Name 【Optional】	
	organizationName	Organization Name	
	organizationalUnitName	Organizational Unit 【Optional】	
	commonName	Subscriber Name	

	serialNumber	Serial Number【Optional】	
subjectPublicKeyInfo		Subject's RSA Public Key Data (At least 2048 bit)	–

Extension Fields（x.509 v3）	Settings	critical
authorityKeyIdentifier	Authority Public Key Identifier （160-bit SHA-1 hash value of Authority Public key）	N
subjectKeyIdentifier	Subject Public Key Identifier （160-bit SHA-1 hash value of the Subject Public key）	N
keyUsage	The following can be set: digitalSignature (Digital Signature) Non Repudiation (Non Repudiation) keyEncipherment (Key Encipherment) dataEncipherment (Data Encipherment)	Y
certificatePolicies	The following can be set: Policy: 1.2.392.200091.100.381.4 Policy: 1.2.392.200091.100.381.5 CPS: Repository URL	N
subjectAltName	The following can be set: OtherName: UPN="User Principal Name " OtherName: "OID"=" Any character string " Rfc822Name: " Mail address" (Can be set up to 2023/08/31)	N
extKeyUsage	The following can be set: id-kp-clientAuth (Client Authentication) id-kp-emailProtection (E-mail Protection) (Can be set up to 2023/08/31) SmartCard Logon (Smart Card Logon) Adobe Authentic Documents Trust =1.2.840.113583.1.1.5 Microsoft Signer of documents =1.3.6.1.4.1.311.10.3.12 ＊When SmartCard Logon is selected, also select id-kp-clientAuth	N

crlDistributionPoints	HTTP URL of the CA's CRL service ldap://repo1.secomtrust.net/"IssuerDN"?certificateRevocationList ＊ldap is set as required	N
authorityInformationAccess	accessMethod ocsp (1.3.6.1.5.5.7.48.1) accessLocation OCSP Responder URL accessMethod caIssuers (1.3.6.1.5.5.7.48.2) accessLocation URL of the Subordinate CA Certificate ＊Set as needed	N
Netscape Certificate Type	The following can be set: SSL Client S/MIME Client (Can be set up to 2023/08/31)	N

Table 7.1-2 Subscriber Certificate (SHA256：Certificate Policy for Code Signing)
Profile (Not be issued after May 1, 2024)

Basic Fields		Settings	critical
version		Version 3	-
serialNumber		e.g.) 123456789abcdef0	-
signatureAlgorithm		sha256WithRSAEncryption	-
issuer	countryName	JP	-
	organizationName	Set the CA's Organization	
	commonName	Set the CA's Common Name	
validity	notBefore	A value within 48 hours before the certificate signing	-
	notAfter	Stipulated in the CPS "6.3.2 Certificate Operational Periods and Key Pair Usage Periods"	
subject	countryName	JP	-
	stateOrProvinceName	stateOrProvinceName	

	localityName	localityName	
	organizationName	Organization Name	
	organizationalUnitName	Organizational Unit 【Optional】	
	commonName	Subscriber Name	
subjectPublicKeyInfo		Subject's RSA Public Key Data （3072bit or 4096bit）	-

Extension Fields（x.509 v3）	Settings	critical
authorityKeyIdentifier	Authority Public Key Identifier （160-bit SHA-1 hash value of Authority Public key）	N
subjectKeyIdentifier	Subject Public Key Identifier （160-bit SHA-1 hash value of the Subject Public key）	N
keyUsage	digitalSignature	Y
certificatePolicies	Policy: 1.2.392.200091.100.381.8 CPS: Repository URL Policy: 2.23.140.1.4.1（Certificate Policy for Code Signing）	N
subjectAltName	Not used	N
extKeyUsage	id-kp-codeSigning	N
crlDistributionPoints	HTTP URL of the CA's CRL service	N
authorityInformationAccess	accessMethod ocsp (1.3.6.1.5.5.7.48.1) accessLocation OCSP Responder URL accessMethod caIssuers (1.3.6.1.5.5.7.48.2) accessLocation URL of the Subordinate CA Certificate	N

Table 7.1-3 Subscriber Certificate (Certificate Policy for AATL Document Signing) Profile

Basic Fields		Settings	critical
version		Version 3	-
serialNumber		e.g.) 123456789abcdef0	-
signatureAlgorithm		Set one of the following : sha256WithRSAEncryption sha384WithRSAEncryption	-
issuer	countryName	JP	-
	organizationName	SECOM Trust Systems Co., Ltd.	
	commonName	Set the CA's Common Name	
	organizationIdentifier(2.5.4.97)	NTRJP-4011001040781 (NTRJP-Corporation Number of the CA)	
validity	notBefore	A value within 48 hours before the certificate signing	-
	notAfter	Stipulated in the CPS "6.3.2 Certificate Operational Periods and Key Pair Usage Periods"	
subject	countryName	JP	-
	stateOrProvinceName	State or Province Name【Optional】	
	localityName	Locality Name 【Optional】	
	organizationName	Organization Name【Do not set for individual use 】	
	organizationalUnitName	Organizational Unit 【Optional】	
	commonName	Subscriber Name	
	serialNumber	Serial number 【Optional】	
	organizationIdentifier(2.5.4.97)	NTRJP - Organization Corporate Number 【Optional】	
subjectPublicKeyInfo		Subject's RSA Public Key Data (At least 2048 bit)	–

Extension Fields（x.509 v3）	Settings	critical
authorityKeyIdentifier	Authority Public Key Identifier （160-bit SHA-1 hash value of Authority Public key）	N
subjectKeyIdentifier	Subject Public Key Identifier （160-bit SHA-1 hash value of the Subject Public key）	N
keyUsage	digitalSignature (Digital Signature) Non Repudiation (Non Repudiation)	Y
certificatePolicies	Policy: 1.2.392.200091.100.382.1 CPS: Repository URL	N
subjectAltName	Not used	N
extKeyUsage	Adobe Authentic Documents Trust =1.2.840.113583.1.1.5	N
crlDistributionPoints	HTTP URL of the CA's CRL service	N
authorityInformationAccess	accessMethod ocsp (1.3.6.1.5.5.7.48.1) accessLocation OCSP Responder URL accessMethod caIssuers (1.3.6.1.5.5.7.48.2) accessLocation URL of the Subordinate CA Certificate	N

Table 7.1-4 Subscriber Certificate(Certificate Policy for S/MIME) Profile

Basic Fields		Settings	critical
version		Version 3	–
serialNumber		e.g.) 123456789abcdef0	–
signatureAlgorithm		Set one of the following : sha256WithRSAEncryption sha384WithRSAEncryption	–
issuer	countryName	JP	–
	organizationName	Set the CA's Organization	
	commonName	Set the CA's Common Name	
validity	notBefore	A value within 48 hours before the certificate signing	–

	notAfter	Stipulated in the CPS "6.3.2 Certificate Operational Periods and Key Pair Usage Periods"	
subject	commonName	Mail address	–
subjectPublicKeyInfo		Subject's RSA Public Key Data (At least 2048 bit)	–

Extension Fields (x.509 v3)	Settings	critical
authorityKeyIdentifier	Authority Public Key Identifier (160-bit SHA-1 hash value of Authority Public key)	N
subjectKeyIdentifier	Subject Public Key Identifier (160-bit SHA-1 hash value of the Subject Public key)	N
keyUsage	digitalSignature (Digital Signature) keyEncipherment (Key Encipherment)	Y
certificatePolicies	CA/Browser Forum Reserved Certificate Policy Identifier (Recommended to set first) Policy: 1.2.392.200091.100.383.1 【Optional】 CPS: Repository URL 【Optional】	N
subjectAltName	Rfc822Name: " Mail address"	N
extKeyUsage	id-kp-emailProtection (E-mail Protection)	N
crlDistributionPoints	HTTP URL of the CA's CRL service	N
authorityInformationAccess	accessMethod ocsp (1.3.6.1.5.5.7.48.1) accessLocation URL of the OCSPResponder accessMethod caIssuers (1.3.6.1.5.5.7.48.2) accessLocation URL of the Subordinate CA Certificate	N

※ Items described as 【can be arbitrarily specified】 are items whose setting can be changed for each certificate application.

※ Items described as [options] are items for which the setting can be changed for each LRA. However, it can be set only in the combinations determined by SECOM Trust Systems. And when issuing a certificate including a code signing certificate policy, registration shall be in accordance with Baseline Requirements (Code Signing).

7.1.1 Version Number(s)

This CA applies version 3.

7.1.2 Certificate Extension

Certificates issued by this CA use certificate extension fields.

7.1.3 Algorithm Object Identifier

The algorithm OID used in the CA is as follows:

Algorithm	Object Identifier
rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 11}
sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 12}

7.1.4 Name Format

The CA uses Distinguished Name defined in RFC5280.

For every valid Certification Path as defined by RFC 5280, Section 6), for each Certificate in the Certification Path, the encoded content of the Issuer Distinguished Name field of a Certificate SHALL be byte-for-byte identical with the encoded form of the Subject Distinguished Name field of the Issuing CA certificate.

By issuing the Certificate, the CA represents that it followed the procedure set forth in its CP and/or CPS to verify that, as of the Certificate's issuance date, all of the Distinguished Name was accurate.

7.1.5 Name Constraints

Set in the CA if necessary.

7.1.6 Certificate Policy Object Identifier

The OID described in "1.2 Document Name and Identification" shall be applied to the object identifier of the certificate issued by the CA.

The following Certificate Policy identifiers are reserved for use by the CA as an optional means of assertaing that a Certificate complies with the Baseline Requirements:

【Code Signing Certificate】

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) code-signing-requirements(4) code signing(1)} (2.23.140.1.4.1)

【S/MIME Certificate（Mailbox-validated StrictProfile)】

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) mailbox-validated (1) strict (3)} (2.23.140.1.5.1.3)

7.1.7 Use of Policy Constraint Extensions

Not set.

7.1.8 Policy Qualifier Syntax and Semantics

For the policy qualifier, the URI of the Web page that publishes this CP and CPS is stored.

7.1.9 How to interpret Critical Certificate Policy Extensions

Not set.

7.2 CRL Profile

Table 7.2-1 CRL (SHA256: Certificate Policy for Clients,
Certificate Policy for Data Signing, Certificate Policy for Code Signing) Profile

Basic Fields		Settings	critical
version		Version 2	–
signatureAlgorithm		sha256WithRSAEncryption	–
issuer	countryName	JP	–
	organizationName	Set the CA's organization	
	organizationalUnitName	The CA's Organizational Unit can be set	
	commonName	Set the Common Name of the CA	
thisUpdate		CRL issued date and time	–
nextUpdate		Date and time when the next CRL will be issued.Up to 10 days after thisUpdate.	
revoked Certificates	serialNumber	e.g.) 123456789abcdef0	–
	revocationDate	e.g.) 2016/09/01 12:00:00 GMT	
	crlEntryExtensions reasonCode	Values specified in "7.2.2 Certificate Revocation Lists and CRL Entry Extensions"	

Extension Fields	Settings	
CRLNumber	e.g.) 1 (Integer value indicating the order in which CRLs are issued)	N
authorityKeyIdentifier	Authority Public Key Identifier (SHA-1 hash value of the Public Key)	N

Table 7.2-2 CRL (AATL Document Signing Certificate) Profile

Basic Fields		Settings	critical
version		Version 2	–
signatureAlgorithm		Set one of the following: sha256WithRSAEncryption sha384WithRSAEncryption	–
issuer	countryName	JP	–
	organizationName	SECOM Trust Systems Co., Ltd.	
	commonName	Set the Common Name of the CA	
	organizationIdentifier(2.5.4.97)	NTRJP-4011001040781 (NTRJP-Corporation Number of the CA)	
thisUpdate		CRL issued date and time	–
nextUpdate		Date and time when the next CRL will be issued. Up to 10 days after thisUpdate.	
revoked Certificates	serialNumber	e.g.) 123456789abcdef0	–
	revocationDate	e.g.) 2023/02/16 00:00:00 GMT	
	crlEntryExtensions reasonCode	Values specified in "7.2.2 Certificate Revocation Lists and CRL Entry Extensions"	

Extension Fields	Settings	
CRLNumber	e.g.) 1 （Integer value indicating the order in which CRLs are issued）	N
authorityKeyIdentifier	Authority Public Key Identifier （SHA-1 hash value of the Public Key）	N

Table 7.2-3 CRL (S/MIME Certificate) Profile

Basic Fields		Settings	critical
version		Version 2	-
signatureAlgorithm		Set one of the following: sha256WithRSAEncryption sha384WithRSAEncryption	-
isuer	countryName	JP	-
	organizationName	Set the CA's organization	
	commonName	Set the CA's Common Name	
thisUpdate		CRL issued date and time	-
nextUpdate		Date and time when the next CRL will be issued. Up to 10 days after thisUpdate	
revoked Certificates	serialNumber	e.g.) 123456789abcdef0	-
	revocationDate	e.g.) 2023/04/30 00:00:00 GMT	
	crlEntryExtensions reasonCode	Values specified in "7.2.2 Certificate Revocation Lists and CRL Entry Extensions"	

Extension Fields	Settings	
CRLNumber	e.g.) 1 (Integer value indicating the order in which CRLs are issued)	N
authorityKeyIdentifier	Authority Public Key Identifier (SHA-1 hash value of the Public Key)	N

7.2.1 Version Number(s)

This CA applies CRL version 2.

7.2.2 Certificate Revocation Lists and CRL Entry Extensions

reasonCode (OID 2.5.29.21) extensions Must not be marked critical.

If the CRL entry is for a Root CA or Subordinate CA Certificate (including Cross CA Certificate), this CRL entry extension is present.

certificateHold (6) as CRLreason should not be used with Root CA or Subordinate CA Certificates.
If the CRL entry is for a Certificate not technically capable of causing issuance, this CRL entry extension should be present, but can be omitted according to the following requirements:
CRLReason shall not be unspecified (0).
If the reason for revocation is unspecified, the CA will omit the reasonCode entry extension.
certificateHold (6) as the CRLreason for the certificate is not included in the CRL entry.
If the reasonCode CRL entry extension is present, CRLReason indicates the most appropriate reason for certificate revocation, as defined by "4.9.1 Circumstances for Certificate Revocation" in this CP.

7.3 OCSP Profile

Table 7.3-1 OCSP profile (SHA256: Certificate Policy for Client, Certificate Policy for Data Signing, Certificate Policy for Code Signing)

Basic Fields		Settings	critical
version		Version 3	-
serialNumber		e.g.) 123456789abcdef0	-
signatureAlgorithm		sha256WithRSAEncryption	-
issuer	countryName	JP	-
	organizationName	Set the CA's Organization	
	organizationalUnitName	The CA's Organizational Unit can be set	
	commonName	Set the CA's Common Name	
validity	notBefore	A value within 1 day before the certificate signing	-
	notAfter	Stipulated in the CPS "6.3.2 Certificate Operational Periods and Key Pair Usage Periods"	-
subject	countryName	JP	-
	organizationName	Set the CA's Organization	-
	organizationalUnitNam	The CA's Organizational Unit can be set	-
	commonName	OCSP Responder Name	-
subjectPublicKeyInfo		Subject Public Key Data	-

Extension Fields	Settings	
keyUsage	digitalSignature	Y
extKeyUsage	id-kp-OCSPSigning	N
id-pkix-ocsp-nocheck	null	N
certificatePolicies	Not set.	N
authorityKeyIdentifier	SHA-1 hash value of Authority public key (160 bits)	N
subjectKeyIdentifier	SHA-1 hash value of Subject Public Key (160 bits)	N

Table 7.3-2 OCSP Profile (Certificate Policy for AATL Document Signing)

Basic Fields		Settings	critical
version		Version 3	-
serialNumber		e.g.) 123456789abcdef0	-
signatureAlgorithm		Set one of the following: sha256WithRSAEncryption sha384WithRSAEncryption	-
issuer	countryName	JP	-
	organizationName	SECOM Trust Systems Co., Ltd.	
	commonName	Set the CA's Common Name	
	organizationIdentifier(2.5.4.97)	NTRJP-4011001040781 (NTRJP-Corporation Number of the CA)	
validity	notBefore	A value within 1 day before the certificate signing	-
	notAfter	CPS "6.3.2 Certificate Operational Periods and Key Pair Usage Periods"	-
subject	countryName	JP	-
	organizationName	Set the CA's Organization	-
	organizationalUnitName	Not set.	-
	commonName	OCSP Responder Name	-
Subject Public Key Info		Subject Public Key Data	-

Extension Fields	Settings	
keyUsage	digitalSignature	Y
extKeyUsage	id-kp-OCSPSigning	N
id-pkix-ocsp-nocheck	null	N

certificatePolicies	Not set.	N
authorityKeyIdentifier	SHA-1 hash value of Authority public key (160 bits)	N
subjectKeyIdentifier	SHA-1 hash value of Subject Public Key (160 bits)	N

Table 7.3-3 OCSP Profile (S/MIME Certificate)

Basic Fields		Settings	critical
version		Version 3	-
serialNumber		e.g.) 123456789abcdef0	-
signatureAlgorithm		Set one of the following: sha256WithRSAEncryption sha384WithRSAEncryption	-
issuer	countryName	JP	-
	organizationName	Set the CA's Organization	
	commonName	Set the CA's Common Name	
validity	notBefore	A value within 1 day before the certificate signing	-
	notAfter	CPS "6.3.2 Certificate Operational Periods and Key Pair Usage Periods"	-
subject	countryName	JP	-
	organizationName	Set the CA's Organization	-
	organizationalUnitName	Not set.	-
	commonName	OCSP Responder Name	-
subjectPublicKeyInfo		Subject Public Key Data	-

Extension Fields	Settings	
keyUsage	digitalSignature	Y
extKeyUsage	id-kp-OCSPSigning	N
id-pkix-ocsp-nocheck	null	N
certificatePolicies	Not set.	
authorityKeyIdentifier	SHA-1 hash value of Authority public key (160 bits)	N
subjectKeyIdentifier	SHA-1 hash value of Subject Public Key (160 bits)	N

7.3.1 Version Number(s)

The CA uses OCSP Version 1.

7.3.2 OCSP Extensions

Use the OCSP extended field issued by the CA.

8. Compliance Audit and Other Assessments

8.1 Frequency and Circumstances of Assessment

Relevant provisions are stipulated in the CPS.

8.2 Identity/Qualifications of Assessor

Relevant provisions are stipulated in the CPS.

8.3 Assessor's Relationship to Assessed Entity

Relevant provisions are stipulated in the CPS.

8.4 Topics Covered by Assessment

Relevant provisions are stipulated in the CPS..

8.5 Actions Taken as a Result of Deficiency

Relevant provisions are stipulated in the CPS.

8.6 Communication of Results

Relevant provisions are stipulated in the CPS.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Fees for Issuing or Renewing Certificates

Stipulated separately in contracts.

9.1.2 Certificate Access Fee

No stipulation.

9.1.3 Expiration or Access Fee for Status Information

No stipulation.

9.1.4 Fees for Other Services

No stipulation.

9.1.5 Refund Policy

Stipulated separately in contracts.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

SECOM Trust Systems shall maintain a sufficient financial base for the operation and maintenance of the CA.

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

Relevant provisions are stipulated in the CPS.

9.3.2 Information Not Within the Scope of Confidential Information

Relevant provisions are stipulated in the CPS.

9.3.3 Responsibility to Protect Confidential Information

Relevant provisions are stipulated in the CPS.

9.4 Privacy of Personal Information

9.4.1 Personal Information Protection Plan

Relevant provisions are stipulated in the CPS.

9.4.2 Information Treated as Personal Information

Relevant provisions are stipulated in the CPS.

9.4.3 Information that is not considered Personal Information

Relevant provisions are stipulated in the CPS.

9.4.4 Responsibility for protecting Personal Information

Relevant provisions are stipulated in the CPS.

9.4.5 Notice and Consent regarding use of Personal Information

Relevant provisions are stipulated in the CPS.

9.4.6 Disclosure of Information in accordance with Judicial or Administrative Procedures

Relevant provisions are stipulated in the CPS.

9.4.7 Other Information Disclosure Conditions

Relevant provisions are stipulated in the CPS.

9.5 Intellectual Property Rights

The following copyrighted materials are the property of SECOM Trust Systems.

- This CP : Property of SECOM Trust Systems (including copyright)
- CPS : Property of SECOM Trust Systems (including copyright)
- CRL : Property of SECOM Trust Systems

This CP, may be reproduced provided that the original document is properly referenced.

9.6 Representations and Warranties

9.6.1 CA Representation and Warranties

SECOM Trust Systems shall comply with the contents stipulated in this CP and the CPS, provide certification services including assessment of Subscribers, registration, issuance and revocation of certificate, so that we ensure the reliability of certification services including the reliability of CA private keys.
Except for the warranties set forth in this CP and the CPS, SECOM Trust Systems shall make no warranties, express, implied, or otherwise.

By issuing a Certificate, the CA makes the certificate warranties listed herein to the following Certificate Beneficiaries:

1. The Subscriber that is a party to the Subscriber Agreement or Terms of Use for the Certificate;
2. All Application Software Suppliers with whom the Root CA has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Supplier; and
3. All Relying Parties who reasonably rely on a Valid Certificate. The CA represents and warrants to the Certificate Beneficiaries that, during the period when the Certificate is valid, the CA has complied with the Baseline Requirements and its Certificate Policy and/or Certification Practice Statement in issuing and managing the Certificate.

The Certificate Warranties specifically include, but are not limited to, the following:

1. Compliance.
   For Code Signing Certificates, The CA and any Signing Service each represents that it has complied with the Baseline Requirements (Code Signing) and the applicable Certificate Policy and Certification Practice Statement in issuing each Code Signing Certificate and operating its PKI or Signing Service.
2. Identity of Subscriber
   For Code Signing Certificates, at the time of issuance, the CA or Signing Service

represents that it (i) operated a procedure for verifying the identity of the Subscriber that at least meets the requirements in Section 3.2 of the Baseline Requirements (Code Signing), (ii) followed the procedure when issuing or managing the Certificate, and (iii) accurately described the same procedure in the CA's Certificate Policy or Certification Practice Statement.

For S/MIME Certificates, if the Certificate contains Subject Identity Information, the CA represents that it (i) operated a procedure for verifying the identity of the Subscriber that meets the requirements in Section 3.2 and 7.1.4.2.2 of the Baseline Requirements (S/MIME), (ii) followed the procedure when issuing or managing the Certificate, and (iii) accurately described the same procedure in the CA's Certificate Policy or Certification Practice Statement.

3. Right to Use Mailbox Address

   For S/MIME Certificates, at the time of issuance, the CA:

   (i) implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the Mailbox Addresses listed in the Certificate's subject field and subjectAltName extension (or was delegated such right or control by someone who had such right to use or control);

   (ii) followed the procedure when issuing the Certificate; and

   (iii) accurately described the procedure in the CA's CP and/or CPS;

4. Authorization for Certificate

   At the time of issuance, the CA represents that it (i) operated a procedure for verifying that the Applicant authorized the issuance of the Certificate, (ii) followed the procedure, and (iii) accurately described the same procedure in the CA's Certificate Policy or Certification Practice Statement.

5. Accuracy of Information

   At the time of issuance, the CA represents that it (i) operated a procedure for verifying that all of the information contained in the Certificate (with the exception of the subject:organizationalUnitName attribute for Code Signing Certificates, with the exception of the subject:serualNumber attribute for S/MIME Certificates) was true and accurate, (ii) followed the procedure, and (iii) accurately described the same procedure in the CA's Certificate Policy or Certification Practice Statement.

6. Key Protection

   For Code Signing Certificates, the CA represents that it provided the Subscriber at the time of issuance with documentation on how to securely store and prevent

the misuse of Private Keys associated with Code Signing Certificates, or in the case of a Signing Service, securely stored and prevented the misuse of Private Keys associated with Code Signing Certificates

7. Subscriber Agreement
   The CA and Signing Service represent that the CA or Signing Service entered into a legally valid and enforceable Subscriber Agreement with the Applicant that satisfies the Baseline Requirements or, if they are affiliated, the Applicant Representative has acknowledged and accepted the Terms of Use.
8. Status
   The CA represents that the CA maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates.
9. Revocation
   CA will revoke the Certificate for any of the reasons specified in the Baseline Requirements.

The Root CA SHALL be responsible for the performance and warranties of the Subordinate CA, for the Subordinate CA's compliance with the Baseline Requirements, and for all liabilities and indemnification obligations of the Subordinate CA under the Baseline Requirements, as if the Root CA were the Subordinate CA issuing the Certificates.

9.6.2 RA Representations and Warranties

SECOM Trust Systems bears the obligation to perform the following in the execution of its duties as an RA:

- Installation and operation of registration terminals in a secure environment;
- Appropriate examination such as confirmation of the existence of the application from the LRA and corporations and organizations.

And LRA bears the obligation to perform the following in the execution of its duties as LRA:

- Installation and operation of registration terminals in a secure environment;
- Appropriate examination such as confirmation of the existence of the application from the Applicants and Subscribers.
- Accurate and prompt application for certificate issuance/revocation to the CA.

9.6.3 Applicant and Subscriber Representations and Warranties

The CA SHALL require, as part of the Subscriber Agreement or Terms of Use, that the Applicant make the commitments and warranties in this section for the benefit of the CA and the Certificate Beneficiaries.

Prior to the issuance of a Certificate, the CA SHALL obtain, for the express benefit of the CA and the Certificate Beneficiaries, either:

1. The Applicant's agreement to the Subscriber Agreement with the CA, or
2. The Applicant's acknowledgement of the Terms of Use.

The CA SHALL implement a process to ensure that each Subscriber Agreement or Terms of Use is legally enforceable against the Applicant. In either case, the Agreement MUST apply to the Certificate to be issued pursuant to the certificate request. The CA MAY use an electronic or "click-through" Agreement provided that the CA has determined that such agreements are legally enforceable. A separate Agreement MAY be used for each certificate request, or a single Agreement MAY be used to cover multiple future certificate requests and the resulting Certificates, so long as each Certificate that the CA issues to the Applicant is clearly covered by that Subscriber Agreement or Terms of Use.

The Subscriber Agreement or Terms of Use MUST contain provisions imposing on the Applicant itself (or made by the Applicant on behalf of its principal or agent under a subcontractor or hosting service relationship) the following obligations and warranties:

1. Accuracy of Information:
   An obligation and warranty to provide accurate and complete information at all times to the CA, both in the certificate request and as otherwise requested by the CA in connection with the issuance of the Certificate(s) to be supplied by the CA.
2. Protection of Private Key:
   An obligation and warranty by the Subscriber to take all reasonable measures to assure control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token). For Code Signing Certificates, the CA MUST provide the Subscriber with documentation on how to protect a Private Key. The CA MAY provide this documentation as a white paper or as part of the Subscriber Agreement. The Subscriber MUST represent that it will generate and operate any device storing

private keys in a secure manner, as described in a document of code signing best practices, which the CA MUST provide to the Subscriber during the ordering process. The CA MUST obligate the Subscriber to use passwords that are randomly generated with at least 16 characters containing uppercase letters, lowercase letters, numbers, and symbols to transport private keys.

3. Private Key Reuse:
   For Code Signing Certificates, the CA shall not apply for a Code Signing Certificate if the Public Key in the Certificate is or will be used with a non-Code Signing Certificate.
4. Use of Certificate:
   For Code Signing Certificates, the CA shall use the Certificate and associated Private Key only for authorized and legal purposes, including not using the Certificate to sign Suspect Code and to use the Certificate and Private Key solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use.
   For S/MIME Certificate, the CA shall use the Certificate only on MailBox Addresses listed in the Certificate, and to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use.
5. Compliance with Industry Standards:
   An acknowledgment and acceptance that the CA may modify the Subscriber Agreement or Terms of Use when necessary to comply with the Baseline Requirements.
6. Prevention of Misuse:
   To provide adequate network and other security controls to protect against misuse of the Private Key and that the CA will revoke the Certificate without requiring prior notification if there is unauthorized access to the Private Keys.
7. Acceptance of Certificate:
   Not to use the Certificate until after the Applicant, or an agent of Applicant, has reviewed and verified the Certificate contents for accuracy.
8. Reporting and Revocation:
   To promptly cease using a Certificate and its associated Private Key and promptly request that the CA revoke the Certificate if the Subscriber believes that (a) any information in the Certificate is, or becomes, incorrect or inaccurate, (b) the Private Key associated with the Public Key contained in the Certificate was misused or compromised, or (c) there is evidence that the Certificate was used to sign Suspect

Code (for Code Signing Certificates).

9. Sharing of Information:
   An acknowledgment and acceptance that, if: (a) the Certificate or the Applicant is identified as a source of Suspect Code, (b) the authority to request the Certificate cannot be verified, or (c) the Certificate is revoked for reasons other than Subscriber request (e.g. as a result of private key compromise, discovery of malware, etc.), then the CA is authorized to share information about the Applicant, signed application, Certificate, and surrounding circumstances with other CAs or industry groups, including the CA/Browser Forum.
10. Termination of Use of Certificate
    To promptly cease using the Private Key corresponding to the Public Key listed in a Certificate upon expiration or revocation of the Certificate.
11. Responsiveness:
    An obligation to respond to the CA's instructions concerning Key Compromise or Certificate misuse within a specified time period.
12. Acknowledgment and Acceptance:
    An acknowledgement and acceptance that the CA is entitled to revoke the certificate immediately if the Applicant were to violate the Terms of Use or the Subscriber Agreement.

9.6.4 Relying Party Representations and Warranties

Relying Parties shall bear the obligations to the following:

- Authenticate the validity of the CA Certificate;
- Authenticate the validity of the Subscriber Certificate by checking the validity period thereof to ensure that it has not expired and that it is not registered as a revoked Certificate in the CRL or on the OCSP responder; and
- Determine whether or not to trust the Subscriber information on their own responsibilities.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimer of Warranties

SECOM Trust Systems is not liable for any direct, special, incidental or consequential damages arising in connection with the warranties stipulated in "9.6.1CA Representations and Warranties" and "9.6.2 RA Representations and Warranties"

hereof, or for lost earnings, loss of data, or any other indirect or consequential damages.

9.8 Limitations of Liability

SECOM Trust Systems is not liable for the provisions of "9.6.1 CA Representations and Warranties" and "9.6.2 RA Representations and Warranties" hereof in any of the following cases:

- Any damage arising from unlawful conduct, unauthorized use, negligence or any other cause not attributable to SECOM Trust Systems;
- Any damage attributable to the failure of a Subscriber to perform its obligations;
- Any damage attributable to LRA or a Subscriber system;
- Damages attributable to a hardware or software defect or malfunction or any other behavior of LRA or the Subscriber system;
- Damages caused by information published in a Certificate, a CRL or on the OCSP Responder due to the reasons not attributable to SECOM Trust Systems;
- Any damage incurred in an outage of the normal communication due to reasons not attributable to SECOM Trust Systems;
- Any damage arising in connection with the use of a Certificate, including transaction debts;
- Damages attributable to improvement, beyond expectations at this point in time, in hardware or software type of cryptographic algorithm decoding skills; and
- Any damage attributable to the suspension of the CA's operations due to force majeure, including, but not limited to, natural disasters, earthquakes, volcanic eruptions, fires, tsunami, floods, lightning strikes, wars, civil commotion and terrorism.

9.9 Indemnities

Indemnities for certificates issued by the CA will be stipulated separately.

9.10 Term and Termination

9.10.1 Term

This CP goes into effect upon approval by the Certification Services Improvement Committee.

This CP will not be invalidated under any circumstances prior to the termination stipulated in "9.10.2 Termination" hereof.

9.10.2 Termination

This CP loses effect as of the termination hereof by SECOM Trust Systems with the exception of the provisions stipulated in "9.10.3 Effect of Termination and Survival".

9.10.3 Effect of Termination and Survival

When the Subscriber terminates the use of the certificate, the contract between SECOM Trust Systems and the contractor is terminated, and even if the services provided by SECOM Trust Systems are terminated, the provisions that should be maintained due to the nature, shall apply to the Subscriber, the Relaying Party, the contractor of SECOM Trust Systems, and SECOM Trust Systems regardless of the reason.

9.11 Individual Notices and Communications with Participants

SECOM Trust Systems provides the necessary notices to LRA, Subscribers and Relying Parties through its website, e-mail or in other written forms.

9.12 Amendments

9.12.1 Procedure for Amendment

This CP shall be revised by SECOM Trust Systems as appropriate at its discretion, and goes into effect upon approval by its Certification Services Improvement Committee.

9.12.2 Notification Method and Timing

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

9.12.3 Circumstances under Which OID Must Be Changed

Change the OID if the Certification Service Improvement Committee determines that it is necessary.

9.13 Dispute Resolution Procedures

A party seeking to file a lawsuit, request arbitration or take any other legal action against SECOM Trust Systems for the resolution of a dispute relating to a Certificate issued by the CA, said party shall notify SECOM Trust Systems to this effect in

advance. As regards the location for arbitration and court proceedings, a dispute settlement institution located within Tokyo shall have exclusive jurisdiction.

9.14 Governing Law

The laws of Japan will apply to any dispute concerning the interpretation or validity of this CP and the CPS, as well as the use of the Certificates.

9.15 Compliance with Applicable Law

The CA shall handle cryptographic hardware and software in compliance with relevant export regulations of Japan.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

SECOM Trust Systems comprehensively stipulates the obligations of Subscribers and Relying Parties and other relevant matters in this CP and the CPS, for provision of the services. Any agreement otherwise, whether oral or written, shall have no effect.

9.16.2 Assignment

When assigning the services to a third party, Secom Trust Systems may assign its responsibilities and other obligations specified in this CP and the CPS.

9.16.3 Severability

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

Disputes regarding this service shall be governed by the Tokyo District Court, and Secom Trust Systems may seek compensation and attorney's fees from the parties for any dispute arising from the contractual provisions of each prescribed document, damages, losses and costs related to the parties' actions.

9.16.5 Irresistible Force

Secom Trust Systems shall not be liable for any damages caused by natural disasters, earthquakes, eruptions, fires, tsunamis, floods, lightning strikes, disturbances, terrorism, or any other force majeure, whether or not foreseeable. If it becomes impossible to provide the CA, we may suspend the CA until the situation ceases.

9.17 Other Provisions

No stipulation