Domain Validation Certificate Policy

Version 1.19

December 8, 2022

SECOM Trust Systems Co., Ltd.

Version History		
Version Number	Date	Description
1.00	2018/07/24	Publication of the first version
1.10	2018/10/12	Modified the contents of the profile
1.11	2019/05/24	Revision of the overall descriptions and style Deleted IP address for domain authentication
1.12	2020/03/30	Revision of chapters, and Addition of some "No stipulation" contents
1.13	2020/09/01	Changed Certificate validity period from 825 days to 398 days
1.14	2020/09/29	Modified Reason code in CRL profile
1.15	2021/05/31	Modified the description for Domain Authentication Modified Certificate Revocation Reason Addition of special requirements for Key Compromise
1.16	2021/06/15	Revision of the descriptions and style Modified Certificate Revocation Reason
1.17	2021/11/30	Modified the description for Domain Authentication Revision of the overall descriptions and style
1.18	2022/06/10	Revision of the overall descriptions and style
1.19	2022/12/08	“7.1 Certificate Profile” Modified “ Table 7.1-1 Server Certificate Profile”

Table of Contents

1. Introduction

1.1 Overview

Domain Validation Certificate Policy (hereinafter, "this CP") defines the policy on certificates issued by SC Domain Validation 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 subscriber 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").

Unilateral cross-certificate by Security Communication RootCA2 has been issued to the CA. Certificates issued by the CA are used for server authentication and data encryption in the communication routing.

A party seeking to obtain Certificates from the CA must examine its usage purposes against this CP and the CPS, and agree to both prior to getting the Certificates issued. The CA conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates of the CA/Browser Forum (hereinafter, "Baseline Requirements") disclosed at https://www.cabforum.org/.

The certificate issued by the CA is provided by a service operated by the certificate administrator (hereinafter referred to as "Certification Service"), and the contract between the two companies shall be stipulated in the PB-SSL/TLS certificate issuance service terms (hereinafter referred to as "Service Terms").
In the event of a conflict between this CP, Service Terms and the CPS, the order of precedence in shall be Service Terms, this CP and the CPS. In addition, if there is a separate contract, etc. between SECOM Trust Systems and an organization that has a contractual relationship, the document such as the contract will take precedence over Service Terms, this CP, and CPS. In the event of any inconsistency between this CP and the Baseline Requirements, the Baseline Requirements take precedence over this CP.

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.

1.2 Document Name and Identification

The official name of this CP is "Domain Validation Certificate Policy ".

This CP is identified with the Object IDentifier (hereinafter, "OID") given in "Table 1.2-1 OID (This CP)"

Table 1.2-1 OID (This CP)

CP	OID
SC Domain Validation CA1	1.2.392.200091.110.213.1
SC Domain Validation CA2	1.2.392.200091.110.213.2
SC Domain Validation CA3	1.2.392.200091.110.213.3

The OID of the CPS associated with this CP is given in Table 1.2-2 OID (CPS)

Table 1.2-2 OID (CPS)

CPS	OID
SECOM Digital Certification Infrastructure Certification Practice Statement	1.2.392.200091.100.401.1

1.3 PKI Participants

1.3.1 CA

A CA mainly issues or revokes Certificates, publishes CRLs (Certificate Revocation Lists), provides information on Certificate status using the OCSP (Online Certificate Status Protocol). The operating body of the CAs on the Digital Certification Infrastructure is SECOM Trust Systems.

1.3.2 RA

RA refers to the entity that registers the information necessary for issuing a certificate and requests the CA to issue a certificate.

Upon receiving a certificate application, RA examines the contents, issue a certificate, registers for revocation and also approves or rejects the issuance of the certificate, and approves the request for revocation.

1.3.3 Administrator

The administrator shall refer to both the subscriber who uses the certificate issued by the CA and the certificate administrator who has contracted with the CA to issue the certificate.

1.3.4 Subscribers

Subscribers shall be an individual, corporation, or other organization that receives a certificate issued by the CA and uses the issued certificate.

1.3.5 Certificate Administrator

The certificate administrator is an organization that has a contractual relationship with the CA, and is a business operator that operates the authentication service and provides the issued certificate to the Subscriber.
All requirements and terms and conditions of this CP shall be complied with and shall be accepted and implemented with respect to the operational and technical implementations instructed by the CA.

1.3.6 Relying Parties

Relying Parties signify individuals, corporations or any other organizations that authenticate the identity of Subscribers and the validity of Public Keys. They also signify individuals, corporations or any other organizations that trust and use this CP and CPS for the purpose of conducting encrypted communication with web servers owned by Subscribers using said Public Keys.

1.3.7 Other Parties

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

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

Certificates issued by the CA may be used for server authentication and data encryption in the communication routing.

1.4.2 Prohibited Certificate Uses

Certificates issued by the CA may not be used for purposes other than server authentication and data encryption in the communication routing.
The CA doesn't permit certificate issuance unless it has confirmed from the domain name registrant verified in accordance with this CP "3.2.2.4 Domain Authentication" that he/she has the right to use the domain.

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

Inquiries concerning this CP should be directed to:

	CA Support Center, SECOM Trust Systems Co., Ltd.
Address:	8-10-16 Shimorenjaku, Mitaka-shi, Tokyo 181-8528
E-mail address:	ca-support@secom.co.jp
Website:	https://www.secomtrust.net/

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 (hereinafter, "this Committee") determines the suitability of the contents of this CP. This CP shall be reviewed and revised at least annually.

1.5.4 Approval Procedure

The CP goes into effect upon approval by this Committee of the CA.

1.6 Definitions and Acronyms

Application Software Supplier

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

Archive

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

ADN（Authorization Domain Name）

Domain name used to obtain authentication for certificate issuance for a particular FQDN

Attestation Letter

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

Audit Log

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

Baseline Requirements

A document issued by the CA/Browser Forum (available at cabforum.org.) 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. This CP also includes the Issuing Authority (IA).

CAA (Certificate Authority Authorization)

A function to prevent false issuance of Certificates by an unintended CA, by including the CA information for the domain ownership/control rights to grant the Certificate issuance for the specific domain, in the DNS record.

CA/Browser Forum

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

CP (Certificate Policy)

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

CT (Certificate Transparency)

Certificate Transparency, stipulated in RFC 6962, is an open framework for monitoring/auditing the records of the issued Certificates by registering and publishing them on the log servers.

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.

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.

INAN (Internet Assigned Numbers Authority)
The organization that globally manages information related to the Internet, such as IP addresses and port numbers.

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

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 of a Key Pair that is possessed by the holder of the corresponding public key.

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

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

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

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

RFC3647 (Request for Comments 3647)
A document defining the framework for CP and CPS published by the IETF (The Internet Engineering Task Force), an industry group which establishes technical standards for the Internet.

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

SHA-1 (Secure Hash Algorithm 1)
A hash function used in digital signing. A hash function is a computation technique for generating a fixed-length string from a given text. The hash length is 160 bits.
The algorithm works to detect any alterations in the original message during the transmission by comparing the hash values transmitted and received.

SHA-256 (Secure Hash Algorithm 256)
A hash function used in digital signing. The hash length is 256 bits.
The algorithm works to detect any alterations in the original message during the transmission by comparing the hash values transmitted and received.

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

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 for CA - SSL Baseline with Network Security
Audit standards maintained by CPA Canada defining the rules for the

reviews/authentications by the CAs for issuance of SSL Certificates and on the Certificates themselves.

WHOIS

Information obtained directly from a domain name registrar or registry operator via a protocol defined in RFC3912, a registry data access protocol defined in RFC7482, or an HTTPS website.

X.500

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

2. Publication and Repository Responsibilities

2.1 Repository

The CA maintains and manages a Repository in order to allow Subscribers and Relying Parties to access CRL information 24x7. Further, it manages an OCSP responder to allow Subscribers and Relying Parties to check online the status of Certificates 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

The CA stores this CP and CPS in the Repository to allow the online access thereto by Subscribers and Relying Parties:

2.3 Time or Frequency of Publication

This CP and the CPS are published in the Repository as revised. A CRL containing information of revocation processed conforming to this CP is published in the Repository as issued. Certificates with expired validity period shall be removed from the CRL.

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.
The following information shall be included in a Certificate issued by the CA:

1. [Country Name (C)] shall be JP.
2. The "Common Name" (CN) is the main domain name and shall be the domain name existing in the Subject Alternative Name. All domain names are added to Subject Alternative Name.
3. If the dNSName entry value in the Subject Alternative Name extension area contains international characters other than ASCII strings, puny-code converted version of the string is used.

3.1.2 Need for Names to Be Meaningful

The Common Name used in a Certificate issued by the CA shall be meaningful when the hostname used in the web server DNS for which the relevant Subscriber plans to install the Certificate is assigned.

3.1.3 Anonymity or Pseudonymity of Subscribers

An anonymous or pseudonymous name may not be registered as the Common Name in the Certificate issued by the CA.

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

The CAs does not verify intellectual property rights for the names indicated in Certificate applications. Subscribers may not submit the CA any registered trademark or other trademark-related names of a third party. The CA will not arbitrate or engage itself in the resolution of any dispute between Subscribers and third parties over the registered trademark or any alike. The CA reserves the right to reject a Subscriber Certificate Application or revoke an issued Certificate due to the dispute.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

A Subscriber proves possession of the relevant Private Key in accordance with the following method.

The signature on the relevant Certificate Signing Request (hereinafter, "CSR") is authenticated to prove that said CSR is signed with the Private Key corresponding to the Public Key.

3.2.2 Authentication of Organization Identity

The CA does not authenticate the Organization Identity.

3.2.2.1 Identity

The CA does not issue a certificate containing the name or address of the organization in the Subject Identity Information.

3.2.2.2 DBA/Tradename

The CA does not issue a certificate containing DBA/Tradename in the Subject Identity Information.

3.2.2.3 Verification of Country

If the countryName field is present in the subject Distinguished Name of the certificate, then the CA SHALL verify the country associated with the Subject using one of the following:

- information provided by the Domain Name Registrar; or
- a method identified in this CP, “Section 3.2.2.1 Identity”.

3.2.2.4 Domain Authentication

The CA will authenticate the domain using the following Baseline Requirements-compliant method to verify that the certificate subscriber has the right to use the domain name. 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 valid for the use of response confirmation for 30 days from the generation.
In the CA, when making a WHOIS inquiry, the IP address of the contacted WHOIS server is checked by "<Top Level Domain>.whois-servers.net" on the DNS server, and the inquiry is made to that WHOIS server first. WHOIS responses are not cached and are referenced with each inquiry.
WHOIS obtains the information from domain name registrars or registry operators via the HTTPS website or the protocol defined in RFC3912.
This CA doesn't issue certificates if "RFC 7686 - The ".onion" Special-Use Domain Name" is included in the certificates.

1. Prove the applicant's authority over the FQDN by sending a random value by email, fax, SMS or postal mail to a domain contact registered with the WHOIS Registry Service and receiving an acknowledgment containing the random value. Random values are sent to an email address, fax number, SMS number or resident address that is recognized as a domain contact. The management of multiple authentication domain names can be checked by email, fax, SMS or postal mail.
(Baseline Requirements Section 3.2.2.4.2).

2.The local part is 'admin',' administrator',' webmaster',' hostmaster', or 'postmaster' and the following "@" demonstrates control of the requested FQDN by sending a random value to the email address created as the authentication domain name and receiving an acknowledgment containing the random value. The authentication domain name under "@" used in the e-mail address should be the domain name included in the FQDN for which the certificate is issued, and if the authentication domain is the same, multiple FQDNs can be also checked by e-mail.
(Baseline Requirements Section 3.2.2.4.4)

3. Prove the applicant's authority over the FQDN by verifying that there is a random value or application token in either the DNS CNAME, TXT or CAA record of either the FQDN for which the certificate is issued or the authentication domain name (includes each prefixed with a label that begins with an underscore character).
(Baseline Requirement Section 3.2.2.4.7)

4, Prove the applicant's authority over the FQDN by sending a random value via email to the Email contact in the DNS CAA record of the authentication domain name and receiving an acknowledgment containing the random value. If the email contacts are the same, the multiple FQDNs can also be checked by email. Relevant CAA resource records should be verified using the search algorithm defined in Section 3 of RFC 8659.
（Baseline Requirement Section 3.2.2.4.13）

5. Prove the applicant's authority over the FQDN by sending a random value via email to the Email contact in the DNS TXT record of the authentication domain name and receiving an acknowledgment containing the random value. If the email contacts are the same, the multiple FQDNs can also be checked by email.
（Baseline Requirement Section 3.2.2.4.14）

6. Prove the applicant's authority over the FQDN by calling the domain contact phone number and getting a response to permission to use the authenticated domain name. In addition, when the telephone number of the domain contact is the same in a plurality of authentication domain names, the authority can be proved for a plurality of FQDNs by presenting each authentication domain name and obtaining a response of permission to use.
（Baseline Requirement Section 3.2.2.4.15）

7. Prove the applicant's authority over the FQDN by calling the phone number of the phone contact on the DNS TXT record and getting a response to authorize the use of the authentication domain name. In addition, when the telephone number of the domain contact is the same in a plurality of authentication domain names, the authority can be proved for a plurality of FQDNs by presenting each authentication domain name and obtaining a response of permission to use.
（Baseline Requirement Section 3.2.2.4.16）

8. Prove the applicant's authority over the FQDN by calling the phone number of the phone contact in the DNSCAA record and getting a response to authorize the use of the authentication domain name. In addition, when the telephone number of the telephone contact is the same in a plurality of authentication domain names, the authority can be proved for the plurality of FQDNs by presenting each FQDN and

obtaining a response of permission to use.
（Baseline Requirement Section 3.2.2.4.17）

9. Confirm the applicant's control over the FQDN by verifying that the request token or random value is included in the contents of the file. The CA accesses via an approved port, and confirms that Random value is placed under the "http (or https): // [FQDN to be issued certificate] /.well-known/pki-validation" directory, and that it receives a normal HTTP or HTTPS response sent from the request.
For Certificates issued on or after 2021-12-01, the CA MUST NOT issue Certificates for other FQDNs that end with all the labels of the validated FQDN unless the CA performs a separate validation for that FQDN using an authorized method. This method is NOT used for validating Wildcard Domain Names.
(Baseline Requirements Section 3.2.2.4.18)

3.2.2.5 Authentication for an IP Address
The CA does not issue a certificate by authenticating the IP address.

3.2.2.6 Wildcard Domain Validation
Before issuing a Wildcard Certificate, the CA MUST establish documented procedure that determines if the FQDN portion of any Wildcard Domain Name in the Certificate is “registry-controlled” label or is a “public suffix”.
If the FQDN portion of any Wildcard Domain Name is “registry-controlled” or is a “public suffix”, CAs MUST refuse issuance unless the Applicant proves its rightful control of the entire Domain Namespace.
Determination of what is “registry-controlled” versus the registerable portion of a Country Code Top-Level Domain Namespace is referred to the Public Suffix List (PSL), and to retrieve a fresh copy regularly. If using the PSL, the CA SHOULD consult the “ICANN DOMAINS” section only, not the “PRIVATE DOMAINS” section.

3.2.2.7 Data Source Accuracy
Prior to using any data source as a Reliable Data Source, the CA evaluates the source for its reliability, accuracy, and resistance to alteration or falsification. The CA should consider the following during its evaluation:
1. The age of the information provided,
2. The frequency of updates to the information source,
3. The data provider and purpose of the data collection,

4. The public accessibility of the data availability, and
5. The relative difficulty in falsifying or altering the data.

3.2.2.8 CAA Records

As part of the issuance process, the CA must check for CAA records and follow the processing instructions found, for each dNSName in the subjectAltName extension of the certificate to be issued, as specified in RFC 8659. If the CA issues, they MUST do so within the TTL of the CAA record, or 8 hours, whichever is greater.

When processing CAA records, the CA MUST process the issue, issuewild, and iodef property tags as specified in RFC 8659, although they are not required to act on the contents of the iodef property tag.

Additional property tags may be supported, but must not conflict with or supersede the mandatory property tags set out in Baseline Requirements. The CA must respect the critical flag and not issue a certificate if they encounter an unrecognized property tag with this flag set.

The CA is permitted to treat a record lookup failure as permission to issue if:

- the failure is outside the CA's infrastructure; and
- the lookup has been retried at least once; and
- the domain's zone does not have a DNSSEC validation chain to the ICANN root.

The CA shall log any actions taken as part of its processing practices.

3.2.3 Authentication of Individual Identity

The CA does not authenticate the identity of individual.

The Certificate Administrator authenticate the identity of the person who applies for the certificate or his / her agent, and confirms the intention of the application.

3.2.4 Non-Verified Subscriber Information

Information of non-verified Subscriber information is not included in the certificate issued by the CA.

3.2.5 Validation of Authority

The CA authenticates that the Subscriber has been granted the usage right by the administrator of the domain name described in the certificate.

3.2.6 Criteria for Interoperation

Unilateral cross-certificate by Security Communication RootCA2 has been issued to

the CA.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

Subscribers shall be identified and authenticated for Re-Keying in the same manner as set forth in this CP "3.2 Initial Identity Validation" hereof.

3.3.2 Identification and Authentication for Re-Key after Revocation

A routine Re-Key after Revocation is not supported. The (Re-Keying) application for a Certificate shall be treated as a new submission, and the applicant Subscriber shall be identified and authenticated in the same manner as set forth in this CP "3.2 Initial Identity Validation" hereof.

3.4 Identification and Authentication for Revocation Requests

The CA authenticates the identity at the time of application for certificate revocation by accepting the revocation request from the Subscriber or the applicant according to the prescribed procedure, or receiving the presentation of information that only the CA and the Subscriber can know by other communication means.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who May Submit a Certificate Application

A person who may submit a certificate application shall be individuals, corporations, other organizations that use certificates, and agents delegated by certificate subscribers (hereinafter referred to as "Applicant").

In accordance with the CP, “Section 5.5.2, Retention Period for Archive”, the CA SHALL maintain an internal database of all previously revoked Certificates and previously rejected certificate requests due to suspected phishing or other fraudulent usage or concerns. The CA SHALL use this information to identify subsequent suspicious certificate requests.

4.1.2 Enrollment Process and Responsibilities

When applying for the issuance of a certificate, the Certificate Subscriber and Applicant shall apply after accepting the contents of this CP and the CPS, as well as certify that the information submitted is accurate.

4.2 Certificate Application Processing

The Certificate Subscriber or Applicant applies for the certificate using the certificate issuance service provided by the Certificate Administrator.

4.2.1 Performing Identification and Authentication Functions

The CA will examine the application information based on the information described in this CP "3.2 Initial Identification and Authentication" hereof.

The certificate request may include all factual information about the Applicant to be included in the Certificate, and such additional information as is necessary for the CA to obtain from the Applicant in order to comply with Baseline Requirements and the CA’s Certificate Policy and/or Certification Practice Statement. In cases where the certificate request does not contain all the necessary information about the Applicant, the CA shall obtain the remaining information from the Applicant or, having obtained it from a reliable, independent, third-party data source, confirm it with the Applicant. The CA shall establish and follow a documented procedure for verifying all data requested for inclusion in the Certificate by the Applicant.

Applicant information include, but not be limited to, at least one Fully-Qualified

Domain Name to be included in the Certificate's Subject Alternative Name extension.
In this CP "6.3.2 Certificate Operational Periods and Key Pair Usage Periods", the expiration date of the subscriber certificate is limited.
The CA may use the documents and data provided in Section 3.2 to verify certificate information, or may reuse previous validations themselves, provided that:
The CA obtained the data or document from a source specified under Section "3.2 Initial Identity Validation" or completed the validation itself no more than 825 days prior to issuing the Certificate.
Effective 2021-10-01, for validation of Domain Names according to Section "3.2.2.4 Domain Authentication", any reused data, document, or completed validation must be obtained no more than 398 days prior to issuing the Certificate.
In no case may a prior validation be reused if any data or document used in the prior validation was obtained more than the maximum time permitted for reuse of the data or document prior to issuing the Certificate.
The CA shall develop, maintain, and implement documented procedures that identify and require additional verification activity for High Risk Certificate Requests prior to the Certificate's approval, as reasonably necessary to ensure that such requests are properly verified under Baseline Requirements.
If a Delegated Third Party fulfills any of the CA's obligations under this section, the CA shall verify that the process used by the Delegated Third Party to identify and further verify High Risk Certificate Requests provides at least the same level of assurance as the CA's own processes.

4.2.2 Approval or Rejection of Certificate Applications

The CA issues a Certificate corresponding to any application that it approves, notifying the relevant Subscriber of the completion thereof and the issuance of the Certificate
In addition, it shall be possible to reject the application for a certificate in which the examination of all items is not completed adequately, and the one including the following reasons shall be rejected.

- Certificate of Applicant or Subscriber who was previously rejected or previously violated the terms of the contract
- Have an internal server name or reserved IP address in the Subject Alternative Name extension field or "common name" field

Should a Certificate Application be inadequate or deficient, the CA shall notify the relevant Applicant or Subscriber directly or through the Delegated Third Party of the reason therefor and ask for re-submission of the documents.

4.2.3 Time to Process Certificate Applications

The CA promptly issues a Certificate corresponding to any approved Certificate Application.

4.2.4 CAA Records Processing

The CA checks the CAA record at the time of reviewing the application information.
The Certificate Subscribers who want to grant the authority to issue certificates to the FQDN must include the value of "secomtrust.net" in the property "issue" or “issuewild” of the CAA record for each DNS zone.
If there is already a CAA entry in each DNS zone of the Certificate Subscriber and a certificate is required to be issued by the CA, the value of "secomtrust.net" must be included in the property "issue" or “issuewild” of the CAA record.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

Upon completion of the review and authentication of a Certificate Application, the CA issues the corresponding Certificate and the Certificate Administrator makes it available for download via a website accessible only by the Subscriber or send the Certificate to the Subscriber by email or post mail.
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.
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 enforces 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

The Certificate Administrator shall notify the Subscriber of the issuance via the homepage that only the Subscriber can access, or by sending the Certificate by email

or postal mail.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

When the Subscriber downloaded the Certificate, or when the certificate sent by the Subscriber is introduced to the server by other methods, the acceptance thereof shall be deemed complete.

4.4.2 Publication of the Certificate by the CA

The CA certificate of the CA will be published in the repository. The CA can publish the certificate of the certificate subscriber by registering it in the CT (Certificate Transparency) log.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

The CA and Certificate Administrator 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

Subscribers shall use Private Keys and Certificates for the server authentication and data encryption in the communication routing. Subscribers shall use the relevant Certificates and corresponding Private Keys only for the purposes approved by the CA and for no other purpose.

4.5.2 Relying Party Public Key and Certificate Usage

Relying Parties shall acknowledge and agree to the provisions of this CP and the CPS before using the CA Certificates.
Relying Parties may use the CA Certificates for assessment of Subscriber Certificates.

4.6 Certificate Renewal

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

4.6.1 Circumstances for Certificate Renewal

Certificate renewal without key renewal is performed when the validity period of the certificate expires.

4.6.2 Who May Request Renewal

The provisions of this CP "4.1.1 Who May Submit a Certificate Application" hereof shall apply.

4.6.3 Processing Certificate Renewal Requests

The provisions of this CP "4.3.1 CA Actions during Certificate Issuance" hereof shall apply.

4.6.4 Notification of New Certificate Issuance to Subscriber

The provisions of this CP “4.3.2 Notifications to Subscriber of Certificate Issuance" hereof shall apply.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

The provisions of this CP "4.4.1 Conduct Constituting Certificate Acceptance" hereof shall apply.

4.6.6 Publication of the Renewal Certificates by the CA

The provisions of CP "4.4.2 Publication of the Certificate by the CA" hereof shall apply.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

The provisions of this CP “4.4.3 Notification of Certificate Issuance by the CA to Other Entities" hereof shall apply.

4.7 Certificate Re-Key

4.7.1 Circumstances for Certificate Re-Key

A Certificate is Re-Keyed when the validity period of the Certificate is about to expire or when the Certificate is revoked due to the key compromise.

4.7.2 Who May Request Certification of a New Public Key

The provisions of this CP "4.1.1 Who Can Submit a Certificate Application" hereof shall apply.

4.7.3 Processing Certificate Re-Keying Requests

The provisions of this CP "4.3.1 CA Actions during Certificate Issuance" hereof shall apply.

4.7.4 Notification of New Certificate Issuance to Subscriber

The provisions of this CP "4.3.2 Notifications to Subscriber of Certificate Issuance" hereof shall apply.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

The provisions of this CP "4.4.1 Conduct Constituting Certificate Acceptance" hereof shall apply.

4.7.6 Publication of the Re-Keyed Certificate by the CA

The provisions of this CP "4.4.2 Publication of the Certificate by the CA" hereof shall apply.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

The provisions of this CP "4.4.3 Notification of Certificate Issuance by the CA to Other Entities" hereof shall apply.

4.8 Certificate Modification

Should modification be required in any information registered in a Certificate, the CA shall revoke the relevant Certificate and issue a new Certificate.

4.8.1 Circumstances for Certificate Modification

No stipulation

4.8.2 Who May Request Certificate Modification

The provisions of this CP "4.1.1 Who May Submit a Certificate Application" hereof shall apply.

4.8.3 Processing Certificate Modification Requests

The provisions of this CP "4.3.1 CA Actions during Certificate Issuance" hereof shall apply.

4.8.4 Notification of New Certificate Issuance to Subscriber

The provisions of this CP "4.3.2 Notifications to Subscriber of Certificate Issuance" hereof shall apply.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

The provisions of this CP "4.4.1 Conduct Constituting Certificate Acceptance" hereof shall apply.

4.8.6 Publication of the Modified Certificates by the CA

The provisions of this CP "4.4.2 Publication of the Certificate by the CA" hereof shall apply.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

The provisions of this CP "4.4.3 Notification of Certificate Issuance by the CA to Other Entities" hereof shall apply.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Certificate Revocation

A Subscriber must promptly request the Certificate Administrator 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; or
- The use of the Certificate is being terminated.

The CA shall be able to revoke the certificate of the Certificate Subscriber at the discretion of the CA in the event of the following reasons:

- The Subscriber is not performing the obligations thereof under this CP, the CPS, relevant agreements or laws;
- The CA determined that the Certificate Subscriber and the CA Private Key has or could have been compromised;
- The CA determines or is made aware that any of the information appearing in the Certificate contains inappropriate strings or symbols, which are inaccurate or misleading;
- It is recognized that the Certificate is not issued in compliance with Baseline

Requirements, this CP or CPS;

- The Secret Key of the Subscriber and CA is compromised, and the reasonable evidence is found, which shows that the key isn't complying with the algorithm type and the requirement for the key size as standard, or the certificate is abused by some other way;
- It is recognized that the certificate has been refused or revoked by the SECOM Trust Systems due to breach of contract or other reasons.
- The CA is made aware of any circumstance indicating that use of a Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
- The contract terms of the contract between the Certificate Administrator and the CA are no longer satisfied;
- The CA recognizes any other situation deemed to necessitate revocation.

If one or more of the following events occur, the CA performs revocation processing within 24 hours:

- If the Certificate Subscriber requests the CA to revoke the certificate in writing;
- If the Certificate Subscriber notifies the CA that the original certificate request was not approved and that the approval is not permitted retroactively;
- If the CA obtains the evidence that the private key corresponding to the public key in the Certificate Subscriber's certificate has been compromised;
- If the CA recognizes the proven or demonstrated method that can easily calculate the Subscriber's private key (Debian weak keys, etc. See https: //wiki.debian.org/SSLkeys) based on the public key of the certificate; or
- If the CA obtains the unreliable evidence of domain authentication approval in the certificate or management of fully qualified domain names.

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

- If the certificate no longer complies with the requirements of the CP, "section 6.1.5 Key Sizes "and "6.1.6 Public Key Parameters Generation and Quality Checking";
- If the CA obtains the evidence of unauthorized use of the certificate;

- If the CA finds out that the Certificate Subscriber has violated one or more of the service contracts or material obligations under the Service Term;
- If the CA finds out the situation indicating that the use of a fully qualified domain name or IP address in a certificate is no longer legally permitted (For example, a domain name whose rights to the domain name registrant to use the domain name have been revoked by a court or arbitrator, and the associated license or service agreement between the domain name registrant and the applicant has been terminated. The registrant neglected to update the domain name, etc.);
- The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
- If the CA becomes aware of any material changes to the information contained in the certificate;
- If the CA finds out that the certificate was not issued in accordance with Baseline Requirements or this CP or CPS and determines that it needs to be revoked;
- If the CA determines or finds out that the information described on the certificate is inaccurate;
- If the CA's right to issue a certificate under Baseline Requirements has been expired, revoked, or suspended (Except for the case that the CA has made arrangements to continue maintaining the CRL /OCSP repository);
- If the revocation is required by the CP or CPS; or
- If the CA recognizes that there is clear evidence of a proven method to compromise the private key of the Certificate Subscriber or that particular method used to generate the private key is flawed.

In the following cases, revocation processing may be carried out within a commercially reasonable period.

- Certificate revocation due to the change in the information described in the certificate for the Subscriber's reasons
- Certificate revocation due to suspension of use of certificate due to the Subscriber's reasons such as service termination or the site closure
- Certificate revocation due to the late payment or delinquency from the Subscribers
- Revocation of the original certificate when the certificate is reissued due to the Subscriber's reasons such as server replacement
- Certificate revocation due to the termination of contract with Secom Trust Systems

- Certificate revocation due to the bankruptcy or company closure

4.9.2 Who Can Request Revocation

A request for revocation of a Certificate shall be made by the Certificate Subscriber or the Applicant. If the CA determines that the CP/CPS "4.9.1 Circumstances for Certificate Revocation" applies, the CA may be the Applicant. RA, or the CA can initiate revocation. Additionally, Subscribers, Relying Parties, Application Software Suppliers, and other third parties may submit Certificate Problem Reports informing the CA of reasonable cause to revoke the certificate.

4.9.3 Procedure for Revocation Request

A Subscriber or Applicant shall notify the CA by using the application provided by the CA or the Certificate Administrator and performing the prescribed procedures.
The CA confirms the information received by the prescribed procedure and revokes the certificate.

4.9.4 Revocation Request Grace Period

Should a Subscriber or an Applicant determine that a Private Key has or could have been compromised, they must promptly make a revocation request.

4.9.5 Time within Which CA Shall Process the Revocation Request

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 which the CA will revoke the certificate. The period from receipt of the Certificate Problem Report or revocation-related notice to published revocation MUST NOT exceed the time frame set forth in the CP, “Section 4.9.1. Circumstances for Certificate Revocation”.
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

If the CA receives an application for revocation with a specified date, it shall revoke on the specified date.

4.9.6 Revocation Checking Requirements for Relying Parties

The URLs of the CRL storage destination and the OCSP responder are indicated on the Certificates issued by the CA. CRLs and the OCSP responder may be accessed using a commonly available Web Interface. CRLs do not contain expired Certificate information.

Relying Parties must authenticate the validity of a Subscriber's 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 7 days, and the value of the nextUpdate field MUST NOT be more than 10 days beyond the value of the thisUpdate field.

4.9.8 Maximum Latency for CRLs

The CRLs issued by the CA are immediately reflected onto the Repository.

4.9.9 On-Line Revocation/Status Checking Availability

OCSP responses MUST conform to RFC6960 and/or RFC5019. OCSP responses MUST 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. When 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 GET method, 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 8 hours;
2. OCSP responses MUST have a validity interval less than or equal to 10 days;
3. For OCSP responses with validity intervals less than 16 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 16 hours, then the CA shall update the information provided via an Online Certificate Status Protocol at least 8 hours prior to the nextUpdate, and no later than 4 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 12 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 this CP "7.1.5 Name Constraints", 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.
The OCSP responder MAY provide definitive responses about "reserved" certificate serial numbers, as if there was a corresponding Certificate that matches the Precertificate [RFC6962].
A certificate serial number within an OCSP request is one of the following 3 options:

1. "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

2. "reserved" if a Precertificate [RFC6962] with that serial number has been issued by
   a. the Issuing CA; or
   b. a Precertificate Signing Certificate [RFC6962] associated with the Issuing CA; or
3. "unused" if neither of the previous conditions are met.

4.9.11 Other Forms of Revocation Advertisements Available

The CA can distribute OCSP responses using stapling in accordance with RFC4366 RFC 5246, RFC 8446. In this case, the CA ensures that the subscriber includes the OCSP response of the certificate in the TLS process. The CA will comply with this requirement for the subscriber after the Service Terms or the contract with the subscriber, or after the technical confirmation by the CA and the approval of the service manager.

4.9.12 Special Requirements Regarding Key Compromise

The Relying Party shall demonstrate key compromise in the following methods:

- Submitting the private key itself, or the data containing the private key and how to extract the private key from the data
- Submitting the CSR that includes data such as distinguished names that are recognized as compromised and that can verify the signature
- Submitting the challenge response specified by the CA that can be verified by public key, and the private key signature for public key
- Providing the vulnerabilities that can be verified for compromise and the sources of referenced security incidents

The CA will notify the Certificate Subscriber that the private key may have been compromised if they learn that the private key of the Certificate Subscriber may have been compromised.

If the CA determines that the private key has been compromised or is likely to be compromised, the CP "4.9.1 Circumstances for Certificate Revocation" shall be dealt with.

4.9.13 Circumstances for Suspension

The CA will not suspend Certificates.

4.9.14 Who Can Request Suspension
Not applicable.

4.9.15 Procedure for Suspension Request
Not applicable.

4.9.16 Limits on Suspension Period
Not applicable.

4.10 Certificate Status Services

4.10.1 Operational Characteristics
Certificate status is available to Subscribers and Relying Party for confirmation through the OCSP responder.
The CA MUST NOT remove revocation entries in CRL or OCSP responses until after the Expiry Date of the revoked Certificate.

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 10 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)
Subscribers shall submit a Certificate Revocation Request when ending the certificate use. It will also end if they do not apply for the renewal of the certificate and the

validity period of the corresponding certificate has expired.

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

The CA stores the following information in addition to the CA-related system logs specified in "5.4.1 Types of Events Recorded" in the CPS, as Archive:

- Certificates and CRLs issued;
- processing history relating to CRL issuance;
- the CPS;
- Documents governing the CA business practices, developed in compliance with the CPS;
- documents associated with agreements of subcontracting if the certification services are outsourced;
- records of audit results and the audit reports;

- OCSP responder access log;
- application documentary submissions from Subscribers.

5.5.2 Retention Period for Archive

The CA retains its Archive for a minimum of seven (7) years.

5.5.3 Protection of Archive

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

5.5.4 Archive Backup Procedures

The Archive is backed up whenever a change is made in such critical data pertaining to the CA-related systems as Certificate issuance/revocation or CRL issuance.

5.5.5 Requirements for Time-Stamping of Records

The CA uses the NTP (Network Time Protocol) to time synchronize systems related to the CA and Time-Stamps critical information recorded therein.

5.5.6 Archive Collection System

The Archive collection system is included as a function of the systems related to the CA.

5.5.7 Procedures to Obtain and Verify Archive Information

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

5.6 Key Changeover

Renewal of Key-Pairs or Certificates of the CA, as a general rule, shall be made before their remaining validity periods become shorter than the maximum validity periods of the Certificates issued to Subscribers. When the remaining validity period of the CA becomes shorter than the maximum validity periods of the Certificates issued to Subscribers, the validity periods of the Certificates issued thereto shall be so changed to be within the validity period of the CA.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

The CA establishes measures against incidents and compromises, including the following, to ensure the prompt recovery of the CA-related systems and relevant operations thereafter:

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

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

In the event of damage to any hardware, software or data of a CA-related system, The CA promptly engages in the system recovery efforts using the relevant hardware, software or data that it retains as backup.

5.7.3 Entity Private Key Compromise Procedures

Should it be determined that the Private Keys of the CA using the CA-related system have been or may be compromised or should a disaster or any other unexpected incidents result in a situation that may lead to interruptions or suspensions of the operation of the CA-related system, the CA follows the predetermined plans and procedures to notify affected parties, including Application Software Suppliers, and to securely resume the operation.

5.7.4 Business Continuity Capabilities after a Disaster

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

5.8 CA or RA Termination

In the event of termination of the CA, it shall so notify Subscribers and other affected participants, including Application Software Suppliers through the Certificate Administrator, three (3) months prior to the termination. 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

In the certification infrastructure system, CA Key Pairs are generated on an FIPS140-2 Level 3 conformant cryptographic module. The Key Pair generation operation is jointly performed by at least two authorized individuals.
Subscriber Key Pairs are generated by Subscriber.

6.1.2 Private Key Delivery to Subscriber

The CA does not deliver Private Keys to Subscribers.

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 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

Usage Purposes of the CA and the Certificates issued by the CA shall be as follows:

Table 6.1-1 Key Usage Purposes

	The CA	The Certificates issued by the CA
digital Signature	-	yes
nonRepudiation	-	-
keyEncipherment	-	yes
dataEncipherment	-	-

keyAgreement	-	-
keyCertSign	yes	-
cRLSign	yes	-
encipherOnly	-	-
decipherOnly	-	-

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 cryptographic module.
No stipulation for Subscriber Private Keys.

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.
Activation, deactivation, backup and other operations relating to Subscriber Private Keys must be performed securely under the control of the relevant Subscribers.

6.2.3 Private Key Escrow

The CA does not Escrow 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.
The backup of Subscriber Private Keys must be securely stored under the control of the relevant Subscribers.

6.2.5 Private Key Archival

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

The transfer of Private Keys of the CA into and from a cryptographic module is performed in a secure room while encrypted.

No stipulation for Subscriber Private Keys.

6.2.7 Private Key Storage on Cryptographic Module

Private Keys of the CA operated on the Digital Certification Infrastructure are stored within the cryptographic module.

No stipulation for Subscriber Private Keys.

6.2.8 Method of Activating Private Key

The CA Private Key is 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

The CA Private Key is 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

Private Keys of the CA 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

The quality standards to be applied to the cryptographic modules used by the CA are as specified in "6.2.1 Cryptographic Module Standards and Controls" hereof.

No stipulation for Subscriber Private Keys.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The provisions for CA Public Keys are stipulated in "6.2.1 Cryptographic Module Standards and Controls" of the CPS.

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

Relevant provisions are stipulated in the CPS.

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 Technical 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 the CP, “Section 2.2 Publication of Information”, “Section 6.1.5 Key Sizes”, and “Section 6.1.6 Public Key Parameters Generation and Quality Checking”.

The CA SHALL generate non-sequential Certificate serial numbers greater than zero (0) 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 Server Certificate Profile

Basic Fields		Settings	critical
Version		Version 3	-
Serial Number		e.g.) 0123456789	-
Signature Algorithm		sha256 With RSA Encryption	-
Issuer	Country	C=JP	-
	Organization	O=SECOM Trust Systems CO.,LTD.	-
	Common Name	CN= Set the common name of each certificate authority	-
Validity	NotBefore	e.g.) 2018/3/1 00:00:00 GMT	-
	NotAfter	e.g.) 2019/3/1 00:00:00 GMT	-
Subject	Country	No description	-
	State Or Province	No description	-
	Locality	No description	-
	Organization	No description	-
	Organizational Unit	No description	-
	Common Name	Required Only one entry must be included, which is one of the values included in the Subject Alternative Name extension of the certificate. The value must be encoded as a character-for-character copy of the dNSName entry value from the Subject Alternative Name extension. Specifically, the FQDN part of all	-

		domain labels in a fully qualified domain name must be encoded as LDH labels, and P labels must not be converted to Unicode representation. Must not contain a reserved IP address or internal name.	
Subject Public Key Info		Subject Public Key 2048 bits	-
Extension Fields		Settings	critical
keyUsage		digitalSignature, keyEncipherment	y
extendedKeyUsage		serverAuth	n
Subject Altanative Name		Required Includes at least one dNSName. dNSName: The entry includes fully qualified domain names verified by the CA according to this CP "3.2.2.4 Domain Authentication ". The entry cannot include an internal name. The FQDN portion of the fully qualified domain name contained in the entry must be composed entirely of LDH Labels joined together by a U+002E FULL STOP (".") character. The zero-length Domain Label representing the root zone of the Internet Domain Name System must not be included. Effective 2021-10-01, the Fully-Qualified Domain Name must consist solely of Domain Labels that are P-Labels or Non-Reserved LDH Labels.	n
CertificatePolicies		[1]policyIdentifier OID= Set [1.2-1 OID] of this CP policyQualifiers policyQualifierId=CPS qualifier= HTTP(S) URL for the	n

	Repository of the CA [2]policyIdentifier= 2.23.140.1.2.1	
CRL Distribution Points	HTTP URL for the CRL service of the CA	n
Authority Information Access	accessMethod ocsp (1.3.6.1.5.5.7.48.1) accessLocation HTTP URL for OCSP responder CA Issuers (1.3.6.1.5.5.7.48.2) accessLocation HTTP URL for the CA Certificate * Set CA Issuers as needed	n
Authority Key Identifier	SHA-1 hash value of Authority Public Key (160 bits)	n
Subject Key Identifier	SHA-1 hash value of the Subject Public Key (160 bits)	n
Certificate Transparency Extension （1.3.6.1.4.1.11129.2.4.2）	SignedCertificateTimestampList value	n

Table 7.1-2 OCSP Responder Certificate Profile

Basic Fields		Settings	critical
Version		Version 3	-
Serial Number		e.g.) 0123456789	-
Signature Algorithm		sha256 With RSA Encryption	-
Issuer	Country	C=JP	-
	Organization	O=SECOM Trust Systems CO.,LTD.	-
	Common Name	CN=Set the common name of each certificate authority	-
Validity	NotBefore	e.g.) 2018/03/01 00:00:00 GMT	-
	NotAfter	e.g.) 2018/07/01 00:00:00 GMT	-
Subject	Country	C=JP (Fixed value)	-
	Organization	SECOM Trust Systems CO., LTD. (Fixed value)	-
	Common Name	OCSP Responder name (Required)	-
Subject Public Key Info		Subject Public Key 2048 bits	-

Extension Fields	Settings	critical
keyUsage	digitalSignature	y
extendedKeyUsage	OCSPSigning	n
OCSP No Check	null	n
CertificatePolicies	policyIdentifier OID = Set [1.2-1 OID] of this CP policyQualifiers policyQualifierId=CPS qualifiier= HTTP(S) URL for the Repository of the CA	n
Authority Key Identifier	SHA-1 hash value of authority Public Key (160 bits)	n
Subject Key Identifier	SHA-1 hash value of the subject Public Key (160 bits)	n

7.1.1 Version Number(s)

The CA applies version 3.

7.1.2 Certificate Extension

Certificates issued by the CA use certificate extension fields.

7.1.3 Algorithm Object Identifier

The algorithm OID used in this service is as follows:

Algorithm	Object Identifier
sha256 With RSA Encryption	1.2.840.113549.1.1.11
RSA Encryption	1.2.840.113549.1.1.1

7.1.4 Name Format

The CA uses the Distinguished Name specified 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 Certificate Policy and/or Certification Practice Statement to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate. The CA SHALL

NOT include a Domain Name in a Subject attribute except as specified in Baseline Requirements Section 3.2.2.4.
Distinguished Names MUST NOT contain only metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.
The CA will not issue a certificate with a Subject Alternative Name extension or "common name" field that contains a reserved IP address or internal name.
If the "common name" value is a fully qualified domain name or a wildcard domain name, the "common name" value is encoded as a character-for-character copy of the dNSName entry value in the Subject Alternative Name extension. Specifically, all Domain Labels in the FQDN part of a fully qualified domain name or wildcard domain name are encoded as LDH Labels, and P-Labels does not convert to Unicode.

7.1.5 Name Constraints
Not set in this CA.

7.1.6 Certificate Policy Object Identifier
The OID of the certificate issued by the CA is as described in this CP "1.2 Document Name and Identification".
The following Certificate Policy identifiers are reserved for use by the CA as an optional means of assertaing that a Certificate complies with Baseline Requirements.
{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) domain-validated(1)} (2.23.140.1.2.1)

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
CRLs issued by the CA conform to RFC5280, the profile of which are indicated in the

tables below.

Table 7.2 CRL Profile

Basic Fields		Settings	critical
Version		Version 2	-
Signature Algorithm		SHA256 with RSAEncryption	-
Issuer	Country	C=JP	-
	Organization	O= SECOM Trust Systems CO.,LTD.	-
	Common Name	CN= Set the common name of each Certificate Authority	-
This Update		e.g.) 2018/3/1 00:00:00 GMT	-
Next Update		e.g.) 2018/3/5 00:00:00 GMT	-
Revoked Certificates	Serial Number	e.g.) 0123456789	-
	Revocation Date	e.g.) 2018/3/1 00:00:00 GMT	-
	Reason Code	e.g.) cessation of operation (Revocation reason) ＊ Setting is optional	-
Extension Fields		Settings	critical
CRL Number		CRL number	n
Authority Key Identifier		SHA-1 hash value of authority Public Key (160 bits)	n

7.2.1 Version Number(s)

The CA applies CRL version 2.

7.2.2 CRL Entry Extensions

Use the CRL extension field issued by the CA.

reasonCode (OID 2.5.29.21)

Effective 2020-09-30, all of the following requirements MUST be met:

If present, this extension MUST NOT be marked critical.

If a CRL entry is for a Root CA or Subordinate CA Certificate, including Cross Certificates, this CRL entry extension MUST be present.

If a CRL entry is not for CA, but for the Subscriber Certificate, this CRL entry extension SHOULD be present, but MAY be omitted, subject to the following requirements.

The CRLReason indicated MUST NOT be unspecified (0). If the reason for revocation is unspecified, CAs MUST omit reasonCode entry extension, if allowed by the previous

requirements. If a CRL entry is for a Certificate not subject to these Requirements and was either issued on-or-after 2020-09-30 or has a notBefore on-or-after 2020-09-30, the CRLReason MUST NOT be certificateHold (6). If a CRL entry is for a Certificate subject to Baseline Requirements, the CRLReason MUST NOT be certificateHold (6). If a reasonCode CRL entry extension is present, the CRLReason MUST indicate the most appropriate reason for revocation of the certificate, as defined by the CA within its CP/CPS.
In the CA, the following reasonCode shall be used.

keyCompromise (1)
affiliationChanged (3)
superseded (4)
cessationOfOperation (5)
privilegeWithdrawn (9)

7.3 OCSP Profile

The CA operates the OCSP responder in compliance with RFC5019 and 6960.
Effective 2020-09-30, if an OCSP response is for a Root CA or Subordinate CA Certificate, including Cross Certificates, and that certificate has been revoked, then the revocationReason field within the RevokedInfo of the CertStatus MUST be present.
Effective 2020-09-30, the CRLReason indicated MUST contain a value permitted for CRLs, as specified in the CP “Section 7.2.2 CRL Entry Extensions”.

7.3.1 Version Number(s)

The CA uses OCSP Version 1.

7.3.2 OCSP Extensions

Refer to this CP “7.1 Certificate Profile”.
The singleExtensions of an OCSP response MUST NOT contain the reasonCode (OID 2.5.29.21) CRL entry extension.

8. Compliance Audit and Other Assessments

The CA performs audits from time to time to examine if the operation thereof is in compliance with this CP and the CPS. Provisions for the compliance verification audits thereof are set forth in this CP and the CPS.

8.1 Frequency and Circumstances of Assessment

The CA performs compliance audits periodically to examine if the operation of the services is in compliance with this CP and the CPS.

8.2 Identity/Qualifications of Assessor

The compliance audits of the CA shall be performed by auditors with solid proficiency in the CA operations. The audit of the WebTrust-certified CA shall be performed by an auditing firm.

8.3 Assessor's Relationship to Assessed Entity

Auditors to be appointed shall be those who have no special interests in the CA.

8.4 Topics Covered by Assessment

Audits are performed with respect to business activities for operation of the CA.
Audits may also be performed, conforming to the standards for CA set forth in WebTrust for CA and WebTrust for CA - SSL Baseline with Network Security.

8.5 Actions Taken as a Result of Deficiency

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

8.6 Communication of Results

Audit reports are reported to this Committee. Audit reports are retained and managed to allow access only by the authorized parties.
Verification reports based on WebTrust for CA and WebTrust for CA - SSL Baseline with Network Security are made available on a specific website conforming to the rules of WebTrust for CA and WebTrust for CA - SSL Baseline with Network Security.

8.7 Self-Audits

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 resources 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 Information Disclosure 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

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

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

Secom Trust Systems provides authentication services including subscriber examination, certificate registration, issuance, and revocation in compliance with the contents stipulated in this CP and CPS, and ensure the reliability of authentication work, including the reliability of CA private keys.
Except for the warranties set forth in this CP and CPS, SECOM Trust Systems makes no warranties, explicitly or implied, or in any other way.

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 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. Right to Use Domain Name or IP Address: That, 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 Domain Name(s) and IP address(es) listed in the Certificate's subject field and subjectAltName extension (or, only in the case of Domain Names, 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 Certificate Policy and/or Certification Practice Statement;
2. Authorization for Certificate: That, at the time of issuance, the CA
   i. implemented a procedure for verifying that the Subject authorized the issuance

of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject;

ii. followed the procedure when issuing the Certificate; and

iii. accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;

3. Accuracy of Information: That, at the time of issuance, the CA

i. implemented a procedure for verifying the accuracy of all of the information contained in the Certificate (with the exception of the subject:organizationalUnitName attribute);

ii. followed the procedure when issuing the Certificate; and

iii. accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;

4. No Misleading Information: That, at the time of issuance, the CA

i. implemented a procedure for reducing the likelihood that the information contained in the Certificate's subject:organizationalUnitName attribute would be misleading;

ii. followed the procedure when issuing the Certificate; and

iii. accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;

5. Identity of Applicant: That, if the Certificate contains Subject Identity Information, the CA

i. implemented a procedure to verify the identity of the Applicant in accordance with Baseline Requirements Section 3.2 and Section 7.1.4.2.2;

ii. followed the procedure when issuing the Certificate; and

iii. accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;

6. Subscriber Agreement: That, if the CA and Subscriber are not Affiliated, the Subscriber and CA are parties to a legally valid and enforceable Subscriber Agreement that satisfies Baseline Requirements, or, if the CA and Subscriber are the same entity or are Affiliated, the Applicant Representative acknowledged the Terms of Use;

7. Status: That the CA maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates; and

8. Revocation: That the CA will revoke the Certificate for any of the reasons specified in Baseline Requirements.

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

9.6.2 RA Representations and Warranties

Same as this CP "9.6.1 CA Representation and Warranties".

9.6.3 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 Applicant 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);
3. Acceptance of Certificate: An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy;
4. Use of Certificate: For TLS server certificate, an obligation and warranty to install the Certificate only on servers that are accessible at the subjectAltName(s) 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. Reporting and Revocation: An obligation and warranty to:
   a. promptly request revocation of the Certificate, and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate, and
   b. promptly request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate.
6. Termination of Use of Certificate: An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise.
7. Responsiveness: An obligation to respond to the CA's instructions concerning Key Compromise or Certificate misuse within a specified time period.
8. Acknowledgment and Acceptance: An acknowledgment and acceptance that the CA is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber Agreement or Terms of Use or if revocation is required by the CA's CP, CPS, or Baseline Requirements.

9.6.4 Relying Party Representations and Warranties

The Relying Party of the services of this CA has the following obligations:

. ・ Trust the certificate issued by this CA and use the certificate only for the purposes specified by this CA in this CP and CPS.
・ When trying to trust a certificate, make sure that the certificate has not been revoked by the CRL or OCSP responder in the repository.
・ When trying to trust a certificate, check the validity period of the certificate and confirm that it is within the validity period.

- When trying to trust a certificate issued by the CA, make sure that the certificate can be signed and verified by the CA's certificate.
- Agree to be responsible as a Relying Party as specified in this CP and CPS when trying to trust and use the CA's certificate.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimer of Warranties

The CA is not liable for any direct, special, incidental or consequential damages arising in connection with the warranties stipulated in "9.6.1 CA 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

In this CP, the CA shall not be liable for in the following cases.

- any damage arising from unlawful conduct, unauthorized use, negligence or any other cause not attributable to the CA;
- all liability in any case if the confirmed information error is the result of the Applicant's fraud or willful misconduct.
- any damage attributable to the failure of a Subscriber to perform its obligations;
- any damage attributable to the system of the Certificate Administrator and Subscriber;
- damages attributable to the defect or malfunction or any other behavior for the environment of the Certificate Administrator and Subscriber (hardware or software);
- damages caused by information published in a Certificate, a CRL or on the OCSP responder due to the reasons not attributable to the CA;
- any damage incurred in an outage of the normal communication due to reasons not attributable to the CA;
- any damage arising in connection with the use of a Certificate, including transaction debts;
- any damage caused by the Certificate Administrator’s failure to fulfill its service provision obligations, such as the termination of service provision by them;
- 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

Compensation for the certificate issued by the CA shall be stipulated separately.

9.10 Term and Termination

9.10.1 Term

This CP goes into effect upon approval by this Committee.

9.10.2 Termination

This CP loses effect as of the termination hereof by the CA.

9.10.3 Effect of Termination and Survival

Even in the event of termination of the use of a Certificate by a Subscriber or the termination of a service provided by the Certificate Administrator, or the CA closes its business, provisions that should remain in effect, due to the nature thereof, shall survive any such termination, regardless of the reasons therefor, and remain in full force and effect with respect to any Subscriber, the Certificate Administrator and the CA..

9.11 Individual Notices and Communications with Participants

The CA provides the necessary notices to the Certificate Administrator, then the Certificate Administrator provides the necessary notice to 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 the CA as appropriate and goes into effect upon approval by this 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

OID shall be changed 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 the CA for the resolution of a dispute relating to a Certificate issued by the CA, said party shall notify the CA 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, the Service Terms and 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, the Service Terms and CPS.

9.16.3 Severability

Even if any provision of this CP, the Service Terms and 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 a CA operates or issues certificates, a 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 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 Baseline Requirements and the Law simultaneously. An appropriate change in practice, modification to the CA's CPS and a notice to the CA/Browser Forum, as outlined above, MUST be made within 90 days.

9.16.4 Enforcement

Disputes regarding this service shall be governed by the Tokyo District Court, and SECOM Trust Systems may request the parties for compensation and attorney's fees for disputes arising from the contractual provisions of the respective regulatory documents, 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, SECOM Trust Systems may suspend the CA until the situation stops.

9.17 Other Provisions

No stipulation