SECOM Trust Systems
Subordinate Advanced CA
Certificate Policy

Version 1.08

October 23, 2024

SECOM Trust Systems Co., Ltd.

Version History		
Version Number	Date	Description
1.00	2020/06/15	Publication of the first version
1.01	2021/05/31	Modified the description for domain authentication Modified the certificate revocation reason Addition of the special requirements for key compromise
1.02	2021/06/15	Modified the certificate validity period of Certificate Subscriber Modified the certificate revocation reason
1.03	2021/11/30	Modified the description for domain authentication Revision of overall descriptions and style
1.04	2022/06/10	Revision of overall descriptions and style
1.05	2023/05/17	Update “2.3 Time or Frequency of Publication” Update “4.9.1 Circumstances for Certificate Revocation” Update “5.5.1 Types of Records Archived” Update “5.5.2 Retention Period for Archive” Update “5.5.3 Protection of Archive” Update “5.5.4 Archive Backup Procedures” Update “5.5.5 Requirements for Time-Stamping of Records” Update “5.5.6 Archive Collection System” Update “5.5.7 Procedures to Obtain and Verify Archive Information” Update “5.7.1 Incident and Compromise Handling Procedures” Update “5.7.2 Computing Resources, Software, and/or Data are Corrupted” Update “5.7.3 Entity Private Key Compromise Procedures” Update “5.7.4 Business Continuity Capabilities after a Disaster” Update “7.1 Certificate Profile” Update “7.2 CRL Profile" Update “7.2.2 Certificate Revocation Lists and CRL Entry Extensions”

1.06	2024/04/01	Update “1.1 Overview” Update “1.6 Definitions and Acronyms” Update “7.1 Certificate Profile” Update “7.1.3 Algorithm Object Identifier” Update “7.2 CRL Profile”
1.07	2024/08/21	Update the below: 1.3.1 CA 1.3.2 RA 1.3.3 Subscribers 1.3.4 Relying Party 1.6 Definitions and Acronyms 2.1 Repository 2.2 Publication of Certificate Information 4.1.2 Enrollment Process and Responsibilities 4.2.1 Performing Identification and Authentication Functions 4.9.1 Circumstances for Certificate Revocation 4.9.7 CRL Issuance Frequency 6.1.1 Key Pair Generation 7.1 Certificate Profile 7.2 CRL Profile 7.2.2 CRL Entry Extensions Delete the below: 4.2.4 CAA Records Processing
1.08	2024/10/23	Update the below: 1.5.2 Contact Information 1.6 Definitions and Acronyms 2.2 Publication of Certificate Information 3.2.2.4 Domain Authentication 3.2.2.9 Multi-Perspective Issuance Corroboration 3.2.6 Criteria for Interoperation 4.3.1.1 Manual authorization of certificate issuance for Root CAs 4.3.1.2 Linting of to-be-signed Certificate content 4.3.1.3 Linting of issued Certificates 4.9.11 Other Forms of Revocation Advertisements

		Available 6.2.1 Cryptographic Module Standards and Controls 6.2.7 Private Key Storage on Cryptographic Module 7.1.1 Version Number(s) 7.1.2 Certificate Extension 7.1.8 Policy Qualifier Syntax and Semantics 7.2.1 Version Number(s)

Table of Contents

1. Introduction

1.1 Overview

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

Unilateral cross-certificate by Security Communication RootCA3 or Security Communication ECC RootCA1 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, the Service Terms and the CPS, and agree to all three prior to getting the Certificates issued.
The CA shall comply with the latest versions of the standards set forth by the CA/Browser Forum and Application Software Supplier Standards published at https://www.cabforum.org/.

Table 1.1-1 List of Standards

Types of certificates issued by subordinate CAs	Standards to comply with
TLS Server Certificate	● Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates（hereinafter, Baseline Requirements） ● Apple Root Certificate Program ● Chrome Root Program Policy ● Microsoft Trusted Root Program ● Mozilla Root Store Policy

In the event of a conflict between this CP and the CPS, the order of precedence in shall be this CP, and the 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 "SECOM Trust Systems Subordinate Advanced CA Certificate Policy".
This CP is identified with the OID given in "Table 1.2-1 OID (This CP)"

Table 1.2-1 OID (This CP)

CP	OID
SECOM Trust Systems Subordinate Advanced CA (Superior CA: Security Communication RootCA3)	1.2.392.200091.100.999.11
SECOM Trust Systems Subordinate Advanced CA (Superior CA: Security Communication ECC RootCA)	1.2.392.200091.100.999.13

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

CA is an organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Root CAs and Subordinate CAs.

1.3.2 RA

Any Legal Entity that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the certificate application process or revocation process or both. When RA is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.

With the exception of this CP "3.2.2.4 Domain Authentication" and this CP "3.2.2.5 Authentication for an IP Address", the CA MAY delegate the performance of all, or any part, of this CP "3.2 Initial Identity Validation" requirements to a Delegated Third Party, provided that the process as a whole fulfills all of the requirements of this CP "3.2 Initial Identity Validation".

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

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

1.3.3 Subscribers

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

1.3.4 Relying Parties

Relying Party is 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.

1.3.5 Other Parties

Other Parties include auditors, and companies or organizations that have service

contracts with SECOM Trust Systems, and companies that perform system integration.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

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 shall not be used for purposes other than server authentication and data encryption in the communication routing.

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:

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

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

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

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

Business hours	24x7

1.5.3 Person Determining CP Suitability for the Policy

The Certification Services Improvement 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

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

1.6 Definitions and Acronyms

ADN（Authorization Domain Name）

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

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.

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

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

Key Pair

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

Linting

A process in which the content of digitally signed data such as a Precertificate [RFC 6962], Certificate, Certificate Revocation List, or OCSP response, or data-to-be-signed object (as described in RFC 5280, Section 4.1.1.1) is checked for conformance with the profiles and requirements defined in the Baseline Requirements.

Multi-Perspective Issuance Corroboration

A process by which the determinations made during domain validation and CAA checking by the Primary Network Perspectiveare corroborated by other Network Perspectives before Certificate issuance.

Network Perspective

Related to Multi-Perspective Issuance Corroboration. A system (e.g., a cloud-hosted server instance) or collection of network components (e.g., a VPN and corresponding infrastructure) for sending outbound Internet traffic associated with a domain control validation method and/or CAA check. The location of a Network Perspective is determined by the point where unencapsulated outbound Internet traffic is typically first handed off to the network infrastructure providing Internet connectivity to that perspective.

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.

Precertificate
A Precertificate is a signed data structure that can be submitted to a Certificate Transparency log, as defined by RFC 6962. A Precertificate is created after a CA has decided to issue a Certificate, but prior to the actual signing of the Certificate. The CA MAY construct and sign a Precertificate corresponding to the Certificate, for purposes of submitting to CT Logs. The CA MAY use the returned Signed Certificate Timestamps to then alter the Certificate's extensions field, adding a Signed Certificate Timestamp List, as defined in Section 7.1.2.11.3 of the Baseline Requirements and as permitted by the relevant profile, prior to signing the Certificate.

Primary Network Perspective
The Network Perspective used by the CA to make the determination of 1) the CA's authority to issue a Certificate for the requested domain(s) or IP address(es) and 2) the Applicant's authority and/or domain authorization or control of the requested domain(s) or IP address(es).

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.

Short-lived Subscriber Certificate

For Certificates issued on or after 15 March 2024 and prior to 15 March 2026, a Subscriber Certificate with a Validity Period less than or equal to 10 days (864,000 seconds). For Certificates issued on or after 15 March 2026, a Subscriber Certificate with a Validity Period less than or equal to 7 days (604,800 seconds).

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 SHALL make revocation information for Subordinate Certificates and Subscriber Certificates available in accordance with this CP.

2.2 Publication of Certificate Information

The CA SHALL publicly disclose its CP and/or CPS through an appropriate and readily accessible online means that is available on a 24x7 basis. The CA SHALL publicly disclose its CA business practices to the extent required by the CA's selected audit scheme (see this CP “8.4 Topics Covered by Assessment “).

The CP and/or CPS MUST be structured in accordance with RFC 3647 and MUST include all material required by RFC 3647.

The regulations that the CA complies with shall be described in "1.1 Overview."

The CA SHALL host test Web pages that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate.

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

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

2.3 Time or Frequency of Publication

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

2.4 Access Controls on 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. "Organization Name" (O) shall be the name of the relevant organization in the form of a legal person, corporation, or other form of a legal person. For a sole proprietor, the name shall be that of the individual proprietor.
3. [Organizational Unit Name (OU)] shall be an optional field. The OU field is used to distinguish departments (e.g., Human Resources, Marketing, or Development). However, that option shall be prohibited to use for the certificates to be issued after September 1, 2022.
4. 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.

3.1.2 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 Organization Name or 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

SECOM Trust Systems does not verify intellectual property rights for the names indicated in Certificate applications. Subscribers may not submit any registered trademark or other trademark-related names of a third party. SECOM Trust Systems will not arbitrate or engage itself in the resolution of any dispute between Subscribers and third parties over the registered trademark or any alike. SECOM Trust Systems reserves the right to 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

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

3.2.2.1 Identity

If the Subject Identity Information is to include the name or address of an organization, the CA SHALL verify the identity and address of the organization and that the address is the Applicant's address of existence or operation. The CA SHALL verify the identity and address of the Applicant using documentation provided by, or through communication with, at least one of the following:

1. A government agency in the jurisdiction of the Applicant's legal creation,

existence, or recognition;

2. A third party database that is periodically updated and considered a Reliable Data Source;
3. A site visit by the CA or a third party who is acting as an agent for the CA; or
4. An Attestation Letter.

The CA MAY use the same documentation or communication described in 1 through 4 above to verify both the Applicant's identity and address.

3.2.2.2 DBA/Tradename

If the Subject Identity Information is to include a DBA or tradename, the CA SHALL verify the Applicant's right to use the DBA/tradename using at least one of the following:

1. Documentation provided by, or communication with, a government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;
2. A Reliable Data Source;
3. Communication with a government agency responsible for the management of such DBAs or tradenames;
4. An Attestation Letter accompanied by documentary support; or
5. A utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that the CA determines to be reliable.

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 the CP, "Section 3.2.2.1 Identity".

3.2.2.4 Domain Authentication

Secom Trust Systems 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.
The 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).
The CA using this method MUST implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. To count as corroborating, a Network Perspective MUST observe the same challenge information (i.e. Random Value or Request Token) as the Primary Network Perspective.
(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.
The CA using this method MUST implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. To count as corroborating, a Network Perspective MUST observe the selected contact address used for domain validation observed by the Primary Network Perspective.
（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.
The CA using this method MUST implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. To count as corroborating, a Network Perspective MUST observe the selected contact address used for domain validation observed by the Primary Network Perspective.
（Baseline Requirement Section 3.2.2.4.14）

6. 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.
Except for Onion Domain Names, the CA using this method MUST implement MultiPerspective Issuance Corroboration as specified in Section 3.2.2.9. To count as corroborating, a Network Perspective MUST observe the same challenge information (i.e. Random Value or Request Token) as the Primary Network Perspective.
(Baseline Requirements Section 3.2.2.4.18)

7. Confirming the Applicant's control over a FQDN by validating domain control of the FQDN using the ACME HTTP Challenge method defined in Section 8.3 of RFC 8555.

   The CA MUST receive a successful HTTP response from the request (meaning a 2xx HTTP status code must be received).

   The token (as defined in RFC 8555, Section 8.3) MUST NOT be used for more than 30 days from its creation.

   If the CA follows redirects, the following apply:

   1. Redirects MUST be initiated at the HTTP protocol layer.
      For validations performed on or after July 1, 2021, redirects MUST be the result of a 301, 302, or 307 HTTP status code response, as defined in RFC 7231, Section 6.4, or a 308 HTTP status code response, as defined in RFC 7538, Section 3. Redirects MUST be to the final value of the Location HTTP response header, as defined in RFC 7231, Section 7.1.2.
   2. Redirects MUST be to resource URLs with either via the "http" or "https" scheme.
   3. Redirects MUST be to resource URLs accessed via Authorized Ports.

Except for Onion Domain Names, the CA MUST implement MultiPerspective Issuance Corroboration as specified in Section 3.2.2.9. To count as corroborating, a Network Perspective MUST observe the same challenge information (i.e. Random Value or Request Token) as the Primary Network Perspective.

(Baseline Requirements section 3.2.2.4.19 Agreed-Upon Change to Website – ACME)

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

The CA does not issue wildcard certificates.

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.

3.2.2.9 Multi-Perspective Issuance Corroboration

Multi-Perspective Issuance Corroboration attempts to corroborate the determinations (i.e., domain validation pass/fail, CAA permission/prohibition) made by the Primary Network Perspective from multiple remote Network Perspectives before Certificate issuance. This process can improve protection against equally-specific prefix Border Gateway Protocol (BGP) attacks or hijacks.

The CA MAY use either the same set, or different sets of Network Perspectives when performing Multi-Perspective Issuance Corroboration for the required 1) Domain Authorization or Control and 2) CAA Record checks.

The set of responses from the relied upon Network Perspectives MUST provide the CA

with the necessary information to allow it to affirmatively assess:

- the presence of the expected 1) Random Value, 2) Request Token, 3) Contact Address as specified in this CP "3.2.2.4 Domain Authentication".
- the CA's authority to issue to the requested domain(s), as specified in this CP "3.2.2.8 CAA Records"

This CP 3.2.2.4 ""Domain Authentication" describe the validation methods that require the use of Multi-Perspective Issuance Corroboration and how a Network Perspective can corroborate the outcomes determined by the Primary Network Perspective.

Results or information obtained from one Network Perspective MUST NOT be reused or cached when performing validation through subsequent Network Perspectives (e.g., different Network Perspectives cannot rely on a shared DNS cache to prevent an adversary with control of traffic from one Network Perspective from poisoning the DNS cache used by other Network Perspectives). The network infrastructure providing Internet connectivity to a Network Perspective MAY be administered by the same organization providing the computational services required to operate the Network Perspective. All communications between a remote Network Perspective and the CA MUST take place over an authenticated and encrypted channel relying on modern protocols (e.g., over HTTPS).

A Network Perspective MAY use a recursive DNS resolver that is NOT co-located with the Network Perspective. However, the DNS resolver used by the Network Perspective MUST fall within the same Regional Internet Registry service region as the Network Perspective relying upon it. Furthermore, for any pair of DNS resolvers used on a Multi-Perspective Issuance Corroboration attempt, the straight-line distance between the two States, Provinces, or Countries the DNS resolvers reside in MUST be at least 500 km. The location of a DNS resolver is determined by the point where unencapsulated outbound DNS queries are typically first handed off to the network infrastructure providing Internet connectivity to that DNS resolver.

The CA MAY immediately retry Multi-Perspective Issuance Corroboration using the same validation method or an alternative method (e.g., the CA can immediately retry validation using "Email to DNS TXT Contact" if "Agreed-Upon Change to Website -

ACME" does not corroborate the outcome of Multi-Perspective Issuance Corroboration). When retrying Multi-Perspective Issuance Corroboration, the CA MUST NOT rely on corroborations from previous attempts. There is no stipulation regarding the maximum number of validation attempts that may be performed in any period of time.

The "Quorum Requirements" Table describes quorum requirements related to MultiPerspective Issuance Corroboration. If the CA does NOT rely on the same set of Network Perspectives for both Domain Authorization or Control and CAA Record checks, the quorum requirements MUST be met for both sets of Network Perspectives (i.e.,the Domain Authorization or Control set and the CAA record check set). Network Perspectives are considered distinct when the straight-line distance between the two States, Provinces, or Countries they reside in is at least 500 km. Network Perspectives are considered "remote" when they are distinct from the Primary Network Perspective and the other Network Perspectives represented in a quorum.

The CA MAY reuse corroborating evidence for CAA record quorum compliance for a maximum of 398 days. After issuing a Certificate to a domain, remote Network Perspectives MAY omit retrieving and processing CAA records for the same domain or its subdomains in subsequent Certificate requests from the same Applicant for up to a maximum of 398 days.

Table 3.2.2.9-1 Quorum Requirements

# of Distinct Remote Network Perspectives Used	# of Allowed non-Corroborations
2-5	1
6+	2

Remote Network Perspectives performing Multi-Perspective Issuance Corroboration:

MUST:

● Network Hardening

・Rely upon networks (e.g., Internet Service Providers or Cloud Provider Networks) implementing measures to mitigate BGP routing incidents in the global Internet routing system for providing internet connectivity to the Network Perspective.

SHOULD:

● Facility & Service Provider Requirements

・Be hosted from an ISO/IEC 27001certified facility or equivalent security framework independently audited and certified or reported.

・Rely on services covered in one of the following reports: System and Organization Controls 2 (SOC 2), IASE 3000, ENISA 715, FedRAMP Moderate, C5:2020, CSA STAR CCM, or equivalent services framework independently audited and certified or reported.

● Vulnerability Detection and Patch Management

・Implement intrusion detection and prevention controls to protect against common network and system threats.

・ Document and follow a vulnerability correction process that addresses the identification, review, response, and remediation of vulnerabilities.

・Undergo or perform a Vulnerability Scan at least every three (3) months.

・Undergo a Penetration Test on at least an annual basis.

・Apply recommended security patches within six (6) months of the security patch's availability, unless the CA documents that the security patch would introduce additional vulnerabilities or instabilities that outweigh the benefits of applying the security patch.

● System Hardening

・Disable all accounts, applications, services, protocols, and ports that are not used.

・Implement multi-factor authentication for all user accounts.

● Network Hardening

・Configure each network boundary control (firewall, switch, router, gateway, or other network control device or system) with rules that support only the services, protocols, ports, and communications identified as necessary to its operations.

・Rely upon networks (e.g., Internet Service Providers) that:

1) use mechanisms based on Secure Inter-Domain Routing (RFC 6480), for example, BGP Prefix Origin Validation (RFC 6811),

2) make use of other non-RPKI route-leak prevention mechanisms (such as RFC 9234),

3) apply current best practices described in BCP 194.

While it is RECOMMENDED that under normal operating conditions Network Perspectives performing Multi-Perspective Issuance Corroboration forward all Internet traffic via a network or set of networks that filter RPKI-invalid BGP routes

as defined by RFC 6811, it is NOT REQUIRED.

Beyond the above considerations, computing systems performing Multi-Perspective Issuance Corroboration are considered outside of the audit scope described in “8 Compliance Audit and Other Assessments” of this CP.

If any of the above considerations are performed by a Delegated Third Party, the CA MAY obtain reasonable evidence from the Delegated Third Party to ascertain assurance that one or more of the above considerations are followed. As an exception to this CP “1.3.2 RA”, Delegated Third Parties are not required to be within the audit scope described in Section “8 Compliance Audit and Other Assessments” of this CP to satisfy the above considerations.

Phased Implementation Timeline

Effective September 15, 2024, the CA SHOULD implement Multi-Perspective Issuance Corroboration using at least two (2) remote Network Perspectives.
Effective March 15, 2025, the CA MUST implement Multi-Perspective Issuance Corroboration using at least two (2) remote Network Perspectives. The CA MAY proceed with certificate issuance if the number of remote Network Perspectives that do not corroborate the determinations made by the Primary Network Perspective (“non-corroborations”) is greater than allowed in the Quorum Requirements table.

Effective September 15, 2025, the CA MUST implement Multi-Perspective Issuance Corroboration using at least two (2) remote Network Perspectives. The CA MUST NOT proceed with certificate issuance if the number of non-corroborations is greater than allowed in the Quorum Requirements table.
Effective March 15, 2026, the CA MUST implement Multi-Perspective Issuance Corroboration using at least three (3) remote Network Perspectives. The CA MUST NOT proceed with certificate issuance if the number of non-corroborations is greater than allowed in the Quorum Requirements table and if the remote Network Perspectives that do corroborate the determinations made by the Primary Network Perspective do not fall within the service regions of at least two (2) distinct Regional Internet Registries.
Effective June 15, 2026, the CA MUST implement Multi-Perspective Issuance Corroboration using at least four (4) remote Network Perspectives. The CA MUST

NOT proceed with certificate issuance if the number of non-corroborations is greater than allowed in the Quorum Requirements table and if the remote Network Perspectives that do corroborate the determinations made by the Primary Network Perspective do not fall within the service regions of at least two (2) distinct Regional Internet Registries.
Effective December 15, 2026, the CA MUST implement Multi-Perspective Issuance Corroboration using at least five (5) remote Network Perspectives. The CA MUST NOT proceed with certificate issuance if the number of non-corroborations is greater than allowed in the Quorum Requirements table and if the remote Network Perspectives that do corroborate the determinations made by the Primary Network Perspective do not fall within the service regions of at least two (2) distinct Regional Internet Registries.

3.2.3 Authentication of Individual Identity

The CA does not issue certificates to individuals.

3.2.4 Non-Verified Subscriber Information

The CA confirms that the department name (Organizational Unit Name) is not misleading from the certificate issuance application documents and CSR information submitted by the subscriber. Otherwise, non-verified information is not included in certificates.

3.2.5 Validation of Authority

When an entity submits a Certificate-related application, legitimacy of authority for such request is authenticated by SECOM Trust Systems in accordance with "3.2.2 Authentication of Organization Identity" and "3.2.3 Authentication of Individual Identity" hereof.

*As used in this clause, "Subscriber" signifies a corporation, or any other organization that uses the hostname indicated as the Common Name populated in the Certificates as stipulated in "3.1.1 Types of Names" hereof.

3.2.6 Criteria for Interoperation

The CA SHALL disclose all Cross-Certified Subordinate CA Certificates that identify the CA as the Subject, provided that the CA arranged for or accepted the establishment of the trust relationship (i.e. the Cross-Certified Subordinate CA Certificate at issue).

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

Accepting a Revocation Request via a website accessible only by the Subscriber, SECOM Trust Systems identifies and authenticates the applicant Subscriber.

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 an employee of SECOM Trust Systems who has accepted the contents of this CP and other documents presented by this CA when applying for the issuance of a certificate.
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

Prior to the issuance of a Certificate, the CA SHALL obtain the following documentation from the Applicant:
1. A certificate request, which may be electronic; and
2. An executed Subscriber Agreement or Terms of Use, which may be electronic.
The CA SHOULD obtain any additional documentation the CA determines necessary to meet the Baseline Requirements.

Prior to the issuance of a Certificate, the CA SHALL obtain from the Applicant a certificate request in a form prescribed by the CA and that complies with the Baseline Requirements. One certificate request MAY suffice for multiple Certificates to be issued to the same Applicant, subject to the aging and updating requirement in this CP "4.2.1 Performing Identification and Authentication Functions", provided that each Certificate is supported by a valid, current certificate request signed by the appropriate Applicant Representative on behalf of the Applicant. The certificate request MAY be made, submitted and/or signed electronically.
The certificate request MUST contain a request from, or on behalf of, the Applicant for the issuance of a Certificate, and a certification by, or on behalf of, the Applicant that all of the information contained therein is correct.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Once accepted, the Certificate Application is authenticated by SECOM Trust Systems in accordance with this CP "3.2 Initial Identity Validation" 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 this CP "3.2 Initial Identity Validation" to verify certificate information, or may reuse previous validations themselves, provided that:

The CA obtained the data or document from a source specified under this CP "3.2 Initial Identity Validation" or completed the validation itself no more than 825 days prior to issuing the Certificate.

For validation of Domain Names according to this CP "3.2.2.4 Domain Authentication", any data, document, or completed validation used 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.

After the change to any validation method specified in the Baseline Requirements or EV Guidelines, a CA may continue to reuse validation data or documents collected prior to the change, or the validation itself, for the period stated in the Baseline Requirements Section 4.2.1 unless otherwise specifically provided in a ballot.

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 this CA, the value of "secomtrust.net" must be included in the property "issue" or “issuewild” of the CAA record.

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 shall not issue Certificates containing Internal Names or Reserved IP Addresses
SECOM Trust Systems issues a Certificate corresponding to any application that it approves following the review and authentication, subsequently notifying the relevant Subscriber of the completion thereof and the issuance of the Certificate. Should a Certificate Application be inadequate or deficient, SECOM Trust Systems shall notify the relevant Subscriber of the reason therefor and ask for re-submission of the documents and any other information required.

4.2.3 Time to Process Certificate Applications

SECOM Trust Systems promptly issues a Certificate corresponding to any approved Certificate Application.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

4.3.1.1 Manual authorization of certificate issuance for Root CAs

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.

4.3.1.2 Linting of to-be-signed Certificate content

Due to the complexity involved in implementing Certificate Profiles that conform to these Requirements, it is considered best practice for the CA to implement a Linting process to test the technical conformity of each to-be-signed artifact prior to signing it. When a Precertificate has undergone Linting, it is not necessary for the corresponding to-be-signed Certificate to also undergo Linting, provided that the CA has a technical control to verify that the to-be-signed Certificate corresponds to the to-be-signed Precertificate in the manner described by RFC 6962 (Certificate Transparency), Section 3.2. Effective 2024-09-15, the CA SHOULD implement such a Linting process. Effective 2025-03-15, the CA SHALL implement such a Linting process.
Methods used to produce a certificate containing the to-be-signed Certificate content include, but are not limited to:

1. Sign the tbsCertificate with a “dummy” Private Key whose Public Key component is not certified by a Certificate that chains to a publicly-trusted CA Certificate; or
2. Specify a static value for the signature field of the Certificate ASN.1 SEQUENCE.

The CA MAY implement their own certificate Linting tools, but the CA SHOULD use the Linting tools that have been widely adopted by the industry.
(see https://cabforum.org/resources/tools/)

The CA is encouraged to contribute to open-source Linting projects, such as by:
- creating new or improving existing lints,
- reporting potentially inaccurate linting results as bugs,
- notifying maintainers of Linting software of checks that are not covered by existing lints,
- updating documentation of existing lints, and
- generating test certificates for positive/negative tests of specific lints.

4.3.1.3 Linting of issued Certificates

The CA MAY use a Linting process to test each issued Certificate.

4.3.2 Notifications to Subscriber of Certificate Issuance

Secom Trust Systems will notify the Certificate Subscriber of the issuance by sending the certificate.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

When the Certificate is sent to the Subscriber, the acceptance thereof shall be deemed complete if no such claim by the Subscriber as wrong descriptions on the Certificate is made within a week from the delivery.

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

SECOM Trust Systems 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

No stipulation

4.6.2 Who May Request Renewal

No stipulation

4.6.3 Processing Certificate Renewal Requests

No stipulation

4.6.4 Notification of New Certificate Issuance to Subscriber

No stipulation

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

No stipulation

4.6.6 Publication of the Renewal Certificates by the CA

No stipulation

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation

4.7 Certificate 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

No stipulation

4.8.3 Processing Certificate Modification Requests

No stipulation

4.8.4 Notification of New Certificate Issuance to Subscriber

No stipulation

4.8.5 Conduct Constituting Acceptance of Modified Certificate

No stipulation

4.8.6 Publication of the Modified Certificates by the CA

No stipulation

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Certificate Revocation

The CA MAY support revocation of Short-lived Subscriber Certificates.

With the exception of Short-lived Subscriber Certificates, the CA shall revoke a Certificate within 24 hours and use the corresponding CRLReason (revocation reason) in this CP "7.2.2 Certificate Revocation Lists and CRL Entry Extensions" if one or more of the following occurs:

1. The Subscriber requests in writing, without specifying CRLreason, that the CA revoke the Certificate (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL);
2. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization (CRL Reason #9, privilegeWithdrawn);
3. The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise (CRL Reason #1, key Compromise);
4. The CA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate, including but not limited to those identified in (the Baseline Requirements Section 6.1.1.3(5), CPS 6.1.1 "Key Pair Generation") (CRL Reason #1, key Compromise);
5. The CA obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon (CRLReason #4, superseded);

With the exception of Short-lived Subscriber Certificates, the CA should revoke a certificate within 24 hours, must revoke a Certificate within 5 days and use the corresponding CRLReason if one or more of the following occurs:

6. The Certificate no longer complies with the requirements of Section "6.1.5 Key Sizes" and Section "6.1.6 Public Key Parameters Generation and Quality

Checking" of this CP (CRLReason #4, superseded) ;

7. The CA obtains evidence that the Certificate was misused (CRLReason #9, privilegeWithdrawn);
8. The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use (CRL Reason #9, privilegeWithdrawn);
9. The CA is made aware of any circumstance indicating that use of a Fully-Qualified 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) (CRLReason #5, cessationOfOperation);
10. The CA is made aware of a material change in the information contained in the Certificate (CRLReason #9, privilegeWithdrawn);
11. The CA is made aware that the Certificate was not issued in accordance with the Baseline Requirements or the CA's CP or CPS (CRLReason #4, superseded);
12. The CA determines or is made aware that any of the information appearing in the Certificate is inaccurate (CRLReason #9, privilegeWithdrawn);
13. The CA's right to issue Certificates under the Baseline Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL);
14. Revocation is required by the CA's CP and CPS for a reason that is not otherwise required to be specified by this section 4.9.1.1 (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL);
15. The CA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed (CRL Reason #1, key Compromise).

4.9.2 Who Can Request Revocation

A request for revocation of a Certificate may be made by the Certificate user corporation, an Authorized Person, as specified in the Client Organization-Based

Document Submission Criteria, of a non-user corporation, or an agent appointed by representatives of a corporation or other form of a legal person.
The Subscriber, RA, or Issuing CA can initiate revocation. Additionally, Subscribers, Relying Parties, Application Software Suppliers, and other third parties may submit Certificate Problem Reports informing the issuing CA of reasonable cause to revoke the certificate.

4.9.3 Procedure for Revocation Request

A Subscriber shall submit a Revocation Request by selecting the relevant Certificate information on the website accessible only by the Subscriber.

4.9.4 Revocation Request Grace Period

Should a Subscriber determine that a Private Key has or could have been compromised, the Subscriber 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

CRLs must be available via a publicly-accessible HTTP URL (i.e., “published”).

Within twenty-four (24) hours of issuing its first Certificate, the CA MUST generate and publish either: - a full and complete CRL; OR - partitioned (i.e., “sharded”) CRLs that, when aggregated, represent the equivalent of a full and complete CRL.

If the CA publishes a CRL, then the CA shall update and reissue CRLs at least once every seven days, and the value of the nextUpdate field MUST NOT be more than 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 8t 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 eight 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 allows the subscribers to use OCSP stapling in accordance with RFC4366 (Transport Layer Security (TLS) Extensions), RFC 5246 (The Transport Layer Security (TLS) Protocol Version 1.2), RFC 8446 (The Transport Layer Security (TLS) Protocol Version 1.3).

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 may end the certificate issuing service provided by the CA (hereinafter "The Service") by submitting a Certificate Revocation Request or naturally letting it expire.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

The CA does not Escrow Subscriber Private Keys.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5. Facility, Management, and Operational Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

Relevant provisions are stipulated in the CPS.

5.1.2 Physical Access

Relevant provisions are stipulated in the CPS.

5.1.3 Power and Air Conditioning

Relevant provisions are stipulated in the CPS.

5.1.4 Water Exposures

Relevant provisions are stipulated in the CPS.

5.1.5 Fire Prevention and Protection

Relevant provisions are stipulated in the CPS.

5.1.6 Media Storage

Relevant provisions are stipulated in the CPS.

5.1.7 Waste Disposal

Relevant provisions are stipulated in the CPS.

5.1.8 Off-Site Backup

Relevant provisions are stipulated in the CPS.

5.2 Procedural Controls

5.2.1 Trusted Roles

Relevant provisions are stipulated in the CPS.

5.2.2 Number of Persons Required per Task

Relevant provisions are stipulated in the CPS.

5.2.3 Identification and Authentication for Each Role

Relevant provisions are stipulated in the CPS.

5.2.4 Roles Requiring Separation of Duties

Relevant provisions are stipulated in the CPS.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

Relevant provisions are stipulated in the CPS.

5.3.2 Background Check Procedures

Relevant provisions are stipulated in the CPS.

5.3.3 Training Requirements

Relevant provisions are stipulated in the CPS.

5.3.4 Retraining Frequency and Requirements

Relevant provisions are stipulated in the CPS.

5.3.5 Job Rotation Frequency and Sequence

Relevant provisions are stipulated in the CPS.

5.3.6 Sanctions for Unauthorized Actions

Relevant provisions are stipulated in the CPS.

5.3.7 Independent Contractor Requirements

Relevant provisions are stipulated in the CPS.

5.3.8 Documentation Supplied to Personnel

Relevant provisions are stipulated in the CPS.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

Relevant provisions are stipulated in the CPS.

5.4.2 Frequency of Processing Audit Log

Relevant provisions are stipulated in the CPS.

5.4.3 Retention Period for Audit Log

Relevant provisions are stipulated in the CPS.

5.4.4 Protection of Audit Log

Relevant provisions are stipulated in the CPS.

5.4.5 Audit Log Backup Procedure

Relevant provisions are stipulated in the CPS.

5.4.6 Audit Log Collection System

Relevant provisions are stipulated in the CPS.

5.4.7 Notification to Event-Causing Subject

Relevant provisions are stipulated in the CPS.

5.4.8 Vulnerability Assessments

Relevant provisions are stipulated in the CPS.

5.5 Records Archival

5.5.1 Types of Records Archived

Relevant provisions are stipulated in the CPS.

5.5.2 Retention Period for Archive

Relevant provisions are stipulated in the CPS.

5.5.3 Protection of Archive

Relevant provisions are stipulated in the CPS.

5.5.4 Archive Backup Procedures

Relevant provisions are stipulated in the CPS.

5.5.5 Requirements for Time-Stamping of Records

Relevant provisions are stipulated in the CPS.

5.5.6 Archive Collection System

Relevant provisions are stipulated in the CPS.

5.5.7 Procedures to Obtain and Verify Archive Information

Relevant provisions are stipulated in the CPS.

5.6 Key Changeover

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

Relevant provisions are stipulated in the CPS.

5.7.2 Hardware, Software, and/or Data are Corrupted

Relevant provisions are stipulated in the CPS.

5.7.3 Entity Private Key Compromise Procedures

Relevant provisions are stipulated in the CPS.

5.7.4 Business Continuity Capabilities after a Disaster

Relevant provisions are stipulated in the CPS.

5.8 CA or RA Termination

In the event of termination of the CA by SECOM Trust Systems, the company shall so notify Subscribers and other affected participants, including Application Software Suppliers, 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

Relevant provisions are stipulated in the CPS.

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 ※ECC method is not set
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 the CPS "6.2.7 Private Key Storage on Cryptographic Module" 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 shall be protected by the cryptographic module that complies with the CPS "6.2.7 Private Key Storage on 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

This 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".

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

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

As defined in Section 7.1.2.9 of the Baseline Requirements, for Version, Serial Number, Signature, Issuer, Validity, Subject, SubjectPublicKeyInfo, and SignatureAlgorithm of the Precertificate of the TLS server certificate, the encoded values must be byte-for-byte identical to the TLS server certificate. The order, criticality, and encoded values of Extension fields other than "Extension for Certificate Transparency" must be byte-for-byte identical to the extensions field of the certificate. The Precertificate MUST contain the Precertificate Poison extension (OID: 1.3.6.1.4.1.11129.2.4.3). This extension MUST have an extnValue OCTET STRING which is exactly the hex-encoded bytes 0500, the encoded representation of the ASN.1 NULL value, as specified in RFC 6962, Section 3.1.

Table 7.1-1 Subordinate Advanced CA G2 Server Certificate Profile

Basic Fields		Settings	Critical
Version		Version 3	-
Serial Number		Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG	-
Signature Algorithm		One of the following: sha256WithRSAEncryption sha384WithRSAEncryption	-
Issuer	Country	C=JP	-
	Organization	O=SECOM Trust Systems CO.,LTD.	-
	Common Name	CN=Subordinate Advanced CA G2	-
Validity	NotBefore	A value within 48 hours before the certificate signing	-

	NotAfter	Specified in the CPS “6.3.2 Certificate Operational Periods and Key Pair Usage Periods”.	-
Subject	Country	C=JP (Fixed value)	-
	State Or Province	Required	-
	Locality	Required	-
	Organization	Required	-
	Organizational Unit	Prohibited.	-
	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. Includes fully qualified domain names verified 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	N

	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 PLabels or Non-Reserved LDH Labels.	
CertificatePolicies	[1]policyIdentifier OID=1.2.392.200091.100.999.11 policyQualifiers policyQualifierId=CPS qualifier= HTTP(S) URL for the repository of the CA [2]policyIdentifier= 2.23.140.1.2.2	N
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	Optional 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）	Optional SignedCertificateTimestampList	N

	value	

Table 7.1-2 Subordinate Advanced CA G2 OCSP Responder Certificate Profile

Basic Fields		Settings	Critical
Version		Version 3	-
Serial Number		Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG	-
Signature Algorithm		One of the following: sha256WithRSAEncryption sha384WithRSAEncryption	-
Issuer	Country	C=JP	-
	Organization	O=SECOM Trust Systems CO.,LTD.	-
	Common Name	CN=Subordinate Advanced CA G2	-
Validity	NotBefore	A value within 1 day before the certificate signing	-
	NotAfter	Specified in the CPS "6.3.2 Certificate Operational Periods and Key Pair Usage Periods".	-
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 or higher	-
Extension Fields		Settings	Critical
keyUsage		digitalSignature	Y
extendedKeyUsage		OCSPSigning	N
OCSP No Check		null	N
CertificatePolicies		Prohibited	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

Table 7.1-3 Subordinate Advanced ECC CA G2 Server Certificate Profile

Basic Fields		Settings	Critical
Version		Version 3	-
Serial Number		Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG	-
Signature Algorithm		ecdsa-with-SHA384	-
Issuer	Country	C=JP	-
	Organization	O=SECOM Trust Systems CO.,LTD.	-
	Common Name	CN=Subordinate Advanced ECC CA G2	-
Validity	NotBefore	A value within 48 hours before the certificate signing	-
	NotAfter	Specified in the CPS “6.3.2 Certificate Operational Periods and Key Pair Usage Periods”.	-
Subject	Country	C=JP (Fixed value)	-
	State Or Province	Required	-
	Locality	Required	-
	Organization	Required	-
	Organizational Unit	Prohibited	-
	Common Name	Server Name (Required)	-
Subject Public Key Info		Subject Public Key 256 bits or higher	-
Extension Fields		Settings	Critical
keyUsage		digitalSignature,	Y
extendedKeyUsage		serverAuth	N
Subject Altanative Name		dNSName = Server Name	N
CertificatePolicies		[1]policyIdentifier OID=1.2.392.200091.100.999.13 policyQualifiers policyQualifierId=CPS qualifier= HTTP(S) URL for the repository of the CA	N

	[2]policyIdentifier= 2.23.140.1.2.2	
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 of 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	Optional 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)	Optional SignedCertificateTimestampList value	N

Table 7.1-4 Subordinate Advanced ECC CA G2 OCSP Responder Certificate Profile

Basic Fields		Settings	Critical
Version		Version 3	-
Serial Number		Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG	-
Signature Algorithm		ecdsa-with-SHA384	-
Issuer	Country	C=JP	-
	Organization	O=SECOM Trust Systems CO.,LTD.	-
	Common Name	CN= Subordinate Advanced ECC CA G2	-
Validity	NotBefore	A value within 1 day before the certificate signing	-
	NotAfter	Specified in the CPS “6.3.2	-

		Certificate Operational Periods and Key Pair Usage Periods".	
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 256 bits	
Extension Fields		Settings	Critical
keyUsage		digitalSignature	Y
extendedKeyUsage		OCSPSigning	N
OCSP No Check		null	N
CertificatePolicies		Prohibited	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 shall use X.509 v3

7.1.2 Certificate Extension

Certificates issued by the CA use the RFC 5280 compliant certificate extension fields. The certificate profile described in "7.1 Certificate Profile" includes a certificate extension.

7.1.3 Algorithm Object Identifier

The algorithm OID used in this service is as follows:

Algorithm	Object Identifier
rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 11}
sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 12}
id-ecPublicKey	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) id-

	publicKeyType(2) 1 }
ecdsa-with-SHA384	{ iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2(3) 3 }

7.1.4 Name Format

This 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. CAs 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.

This 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

If the Subordinate CA Certificate includes the id-kp-serverAuth extended key usage, then the Subordinate CA Certificate MUST include the Name Constraints X.509v3 extension with constraints on dNSName, iPAddress and DirectoryName as follows:-

a. For each dNSName in permittedSubtrees, the CA MUST confirm that the Applicant has registered the dNSName or has been authorized by the domain registrant to act on the registrant's behalf in line with the verification practices of Baseline Requirements 3.2.2.4.

b. For each iPAddress range in permittedSubtrees, the CA MUST confirm that the Applicant has been assigned the iPAddress range or has been authorized by the

assigner to act on the assignee's behalf.

c. For each DirectoryName in permittedSubtrees the CA MUST confirm the Applicant's and/or Subsidiary's Organizational name and location such that end entity certificates issued from the subordinate CA Certificate will be in compliance with Baseline Requirements 7.1.2.4 and Baseline Requirements 7.1.2.5.

If the Subordinate CA Certificate is not allowed to issue certificates with an IPAddress, then the Subordinate CA Certificate MUST specify the entire IPv4 and IPv6 address ranges in excludedSubtrees. The Subordinate CA Certificate MUST include within excludedSubtrees an iPAddress GeneralName of 8 zero octets (covering the IPv4 address range of 0.0.0.0/0). The Subordinate CA Certificate MUST also include within excludedSubtrees an iPAddress GeneralName of 32 zero octets (covering the IPv6 address range of ::0/0). Otherwise, the Subordinate CA Certificate MUST include at least one iPAddress in permittedSubtrees.

If the Subordinate CA is not allowed to issue certificates with dNSNames, then the Subordinate CA Certificate MUST include a zero-length dNSName in excludedSubtrees. Otherwise, the Subordinate CA Certificate MUST include at least one dNSName in permittedSubtrees.

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 CAs as an optional means of asserting that a Certificate complies with Baseline Requirements.

【For OV certificate】

{joint-iso-itu-t (2) international-organizations (23) ca-browser-forum (140) certificate-policies (1) baseline-requirements (2) organization-validated (2)} (2.23.140.1.2.2)

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 MAY be 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 7.2-1 Subordinate Advanced CA G2 CRL Profile

Basic Fields		Settings	Critical
Version		Version 2	-
Signature Algorithm		One of the following: sha256WithRSAEncryption sha384WithRSAEncryption	-
Issuer	Country	C=JP	-
	Organization	O= SECOM Trust Systems CO.,LTD.	-
	Common Name	CN=Subordinate Advanced CA G2	-
This Update		Issued date and time of CRL	-
Next Update		Date and time when the next CRL will be issued. Up to 10 days after thisUpdate.	-
Revoked Certificates	Serial Number	Byte-for-bite identical value to the serialNumber included in the revoked certificate	-
	Revocation Date	Usually, the date and time the revocation occurred.	-
	Reason Code	Value specified in "7.2.2 CRL Entry Extensions"	-
Extension Fields		Settings	Critical
CRL Number		CRL Number	N
Authority Key Identifier		SHA-1 hash value of Authority Public Key (160 bits)	N

Table 7.2-2 Subordinate Advanced ECC CA G2 CRL Profile

Basic Fields		Settings	Critical
Version		Version 2	-
Signature Algorithm		ecdsa-with-SHA384	-
Issuer	Country	C=JP	-

	Organization	O= SECOM Trust Systems CO.,LTD.	-
	Common Name	CN=Subordinate Advanced ECC CA G2	-
This Update		Issued date and time of CRL	-
Next Update		Date and time when the next CRL will be issued. Up to 10 days after thisUpdate	-
Revoked Certificates	Serial Number	Byte-for-bite identical value to the serialNumber included in the revoked certificate	-
	Revocation Date	Usually, the date and time the revocation occurred.	-
	Reason Code	Value specified in "7.2.2 CRL Entry Extensions"	-
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 shall use X.509 v2 CRLs as specified in RFC 5280.

7.2.2 CRL Entry Extensions

Table 7.2-2-1 CRL Extensions

Extension	Presence	Critical	Description
authorityKeyIdentifier	Required	N	-
CRLNumber	Required	N	Contains an INTEGER (number) greater than or equal to 0 and less than 2^{159}.
IssuingDistributionPoint	*	Y	This extension is not recommended for full and complete CRLs. Full and complete CRLs are used in the CA

Any other extension	Not Recommended	-	-

Table 7.2-2-2 Revoked Certificates Component

Component	Presence	Description
serialNumber	Required	Byte-for-byte identical to the serialNumber contained in the revoked certificate.
revocationDate	Required	Nomally the date and time revocation occurred. See below this table for circumstances where backdating is permitted.
crlEntryExtensions	*	For requirements, see "Table 7.2-2-3 crlEntryExtensions Component."

The CA SHOULD update the revocation date in a CRL entry when it is determined that the private key of the Certificate was compromised prior to the revocation date that is indicated in the CRL entry for that Certificate. Backdating the revocationDate field is an exception to best practice described in RFC 5280 (Section 5.3.2); however, the Baseline Requirements specify the use of the revocationDate field to support TLS implementations that process the revocationDate field as the date when the Certificate is first considered to be compromised.

Table 7.2-2-3　crlEntryExtensions Component

CRL Entry Extension	Presence	Description
reasonCode	*	When present（OID 2.5.29.21）, not be marked critical and indicate the most appropriate reason for revocation of the Certificate.　However, be omitted if the CRL entry is for a Certificate not technically capable of causing issuance and either 1) the CRL entry is for Subscriber Certificate subject to the Requirements revoked prior to July 15, 2023 or 2) the reason for revocation (i.e.,reasonCode) is unspecified. See the table of “CRLReasons” for the requirements.
Any other value	Not Recommended	-

Table 7.2-2-4 CRLReasons

RFC 5280 reasonCode	RFC 5280 reasonCode value	Description
unspecified	0	Represented by the omission of a reasonCode. However, be omitted if the CRL entry is for a Subscriber Certificate subject to the Baseline Requirements revoked prior to July 15, 2023.
keyCompromise	1	Indicate that it is known or suspected that the Subscriber's Private Key has been compromised.
affiliationChanged	3	Indicate that the Subject's name or other Subject's Identity Information in the Certificate has changed, but there is no cause to suspect that the Certificate's Private Key has been compromised.
superseded	4	Indicate that the Subscriber has requested a new Certificate, the CA has reasonable evidence that the validation of domain authorization or control for any FDQN or IP address in the Certificate should not be relied upon, or the CA has revoked the Certificate for compliance reasons such as the Certificate does not comply with the Baseline Requirements or the CA's CP or CPS.
cessationOfOperation	5	Indicates that the website with the Certificate is shut down prior to the expiration of the Certificate, or if the Subscriber no longer owns or controls the Domain Name in the Certificate prior to the expiration of the Certificate.
certificateHold	6	MUST NOT be included if the CRL entry is for: 1) a Certificate subject to the Baseline Requirements, 2) a Certificate not subject to the Baseline Requirements and was either: A) issued on-or-after 2020-09-30 or B) has a notBefore on-or-after 2020-09-30.

privilegeWithdrawn	9	Indicates that there has been a subscriber-side infraction that has not resulted in keyCompromise, such as the Certificate Subscriber provided misleading information in their Certificate Request or has not upheld their material obligations under the Subscriber Agreement or Terms of Use.

The Subscriber Agreement, or an online resource referenced therein, must inform Subscribers about the revocation reason options listed above and provide explanation about when to choose each option. Tools that the CA provides to the Subscriber must allow for these options to be easily specified when the Subscriber requests revocation of their Certificate, with the default value being that no revocation reason is provided (i.e. the default corresponds to the CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL).

The privilegeWithdrawn reasonCode should not be made available to the Subscriber as a revocation reason option, because the use of this reasonCode is determined by the CA and not the Subscriber.
When the CA obtains verifiable evidence of Key Compromise for a Certificate whose CRL entry does not contain a reasonCode extension or has a reasonCode extension with a non-keyCompromise reason, the CA should update the CRL entry to enter keyCompromise as the CRLReason in the reasonCode extension.

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

SECOM Trust Systems performs compliance audits at least once a year 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.

8.3 Assessor's Relationship to Assessed Entity

Auditors shall be in a position independent of the work of the audited department, except for matters related to auditing. In conducting the audit, the audited department shall cooperate with the audit.

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

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

8.6 Communication of Results

Audit reports are reported to the Certification Services Improvement Committee. Audit reports are retained and managed to allow access only by the authorized parties.

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

Certificates issued or renewed by this CA shall be free of charge.

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

Certificates issued or renewed by this CA shall be free of charge.

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 the 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 this CA, make sure that the certificate can be signed and verified by this 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

SECOM Trust Systems 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

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

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

9.9 Indemnities

SECOM Trust Systems shall compensate a Subscriber for the damages incurred thereby for reasons attributable to a Certificate in an amount not to exceed the contract fees received and equal to the fees for the remaining months of the contract period (period of less than one month is rounded off) and shall not be liable in any other way.

9.10 Term and Termination

9.10.1 Term

This CP goes into effect upon approval by the Certification Services Improvement Committee.
This CP will not be invalidated under any circumstances prior to the termination stipulated in "9.10.2 Termination" hereof.

9.10.2 Termination

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

9.10.3 Effect of Termination and Survival

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

9.11 Individual Notices and Communications with Participants

SECOM Trust Systems provides the necessary notices 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 SECOM Trust Systems as appropriate and goes into effect upon approval by its Certification Services Improvement Committee.

9.12.2 Notification Method and Timing

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

9.12.3 Circumstances under Which OID Must Be Changed

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 SECOM Trust Systems for the resolution of a dispute relating to a Certificate issued by the CA, said party shall notify SECOM Trust Systems to this effect in advance. As regards the location for arbitration and court proceedings, a dispute settlement institution located within Tokyo shall have exclusive jurisdiction.

9.14 Governing Law

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

9.15 Compliance with Applicable Law

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

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

SECOM Trust Systems comprehensively stipulates the obligations of Subscribers and Relying Parties and other relevant matters in this CP, 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.
This 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 this CA, SECOM Trust Systems may suspend this CA until the situation stops.

9.17 Other Provisions

No stipulation