SECOM TLS Server Certificate Policy

Version 1.00

April 1, 2024

SECOM Trust Systems Co., Ltd.

Revision History		
Version Number	Date	Description
1.00	2024/04/01	Publication of the first version

Table of Contents

1. Introduction

1.1 Overview

This CP shall indicate the purpose of use, scope of application, and user procedures for TLS server certificates operated by Secom Trust Systems Co., Ltd. (hereinafter, "SECOM Trust Systems "), and stipulate policies concerning the certificates. Various procedures regarding the operation and maintenance of the CA are stipulated in the SECOM Digital Certification Infrastructure Certification Practice Statement (hereinafter, "CPS").

A party seeking to obtain Certificates from the Subordinate CA (hereinafter, "the CA ") that complies with "Security Communication RootCA Subordinate CA Certificate Policy" must examine its usage purposes against this CP and the CPS, and agree to them 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 Standard List

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

The CA may outsource the part of the certification work to an external business operator that complies with Baseline Requirements (hereinafter, "Delegated Third Party"), and

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

This CP shall be revised as necessary in order to reflect any technical or operational developments or improvements pertaining to the CA.
This CP conforms to the RFC3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" advocated by the IETF as a CA practice framework”.

1.2 Document Name and Identification

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 TLS OV CP	1.2.392.200091.100.752.1
SECOM TLS DV CP	1.2.392.200091.100.752.2
SECOM Passport for Web EV CA CP	1.2.392.200091.100.721.1

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

Table 1.2-2 OID（CPS）

CPS	OID
SECOM Digital Certification Infrastructure Certification Practice Statement	1.2.392.200091.100.401.1

1.3 PKI Participants

1.3.1 CA

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

1.3.2 RA

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

Upon receiving a certificate application, RA examines the contents, issue a certificate, confirms the existence of the certificate subscriber who applies for revocation, and approves or rejects the issuance of the certificate, and approves the request for revocation.

Delegated Third Party can perform the business except "3.2.2.4 Domain Authentication" of this CP.

1.3.3 Subscribers

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

1.3.4 Relying Party

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

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

The certificates issued by the CA are intended for establishing Web-based data communication conduits via the TLS protocols and for verifying the authenticity of executable code.

The primary purposes of an EV Certificate are to:

1. Identify the legal entity that controls a Web site:
   Provide a reasonable assurance to the user of an Internet browser that the Web site the user is accessing is controlled by a specific legal entity identified in the EV Certificate by name, address of Place of Business, Jurisdiction of Incorporation or Registration and Registration Number or other disambiguating information;
2. Enable encrypted communications with a Web site:
   Facilitate the exchange of encryption keys in order to enable the encrypted communication of information over the Internet between the user of an Internet browser and a Web site.

The secondary purposes of an EV Certificate are to help establish the legitimacy of a business claiming to operate a Web site or distribute executable code, and to provide a vehicle that can be used to assist in addressing problems related to phishing, malware, and other forms of online identity fraud. By providing more reliable third-party verified identity and address information regarding the business, EV Certificates may help to:

1. Make it more difficult to mount phishing and other online identity fraud attacks using Certificates;
2. Assist companies that may be the target of phishing attacks or online identity fraud by providing them with a tool to better identify themselves to users;
3. Assist law enforcement organizations in their investigations of phishing and other online identity fraud, including where appropriate, contacting, investigating, or taking legal action against the Subject.

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.
The CA does not permit the issuance of certificates unless it is confirmed from the domain owner verified in accordance with this CP "3.2.2.4 Domain Authentication" that the domain owner has the right to use the domain.

EV Certificates focus only on the identity of the Subject named in the Certificate, and not on the behavior of the Subject. As such, an EV Certificate is not intended to provide any assurances, or otherwise represent or warrant:

1. That the Subject named in the EV Certificate is actively engaged in doing business;
2. That the Subject named in the EV Certificate complies with applicable laws;
3. That the Subject named in the EV Certificate is trustworthy, honest, or reputable in its business dealings;
4. That it is “safe” to do business with the Subject named in the EV Certificate.

1.5 Policy Administration

1.5.1 Organization Administering the Document

This CP is maintained and administered by SECOM Trust Systems.

1.5.2 Contact Information

Inquiries concerning this CP should be directed to:

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

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

1.5.3 Person Determining CP Suitability for the Policy

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

1.5.4 Approval Procedure

This CP goes into effect upon approval by this Committee for the CA.

1.6 Definitions and Acronyms

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

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

ADN（Authorization Domain Name）
Domain name used to obtain authentication for certificate issuance for a particular FQDN

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

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

Baseline Requirements
A document issued by the CA/Browser Forum (available at cabforum.org.) that integrates a set of fundamental requirements for Certificate issuance/administration.

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

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

CA/Browser Forum

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

CP (Certificate Policy)

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

CPS (Certification Practices Statement)

A document that sets forth provisions pertaining to the practices of CAs, including procedures for the CA operations and the security standards.

CRL (Certificate Revocation List)

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

CSPRNG（Cryptographically Secure Pseudo Random Number Generator）

A random number generator intended for use in cryptographic system.

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.

EV Processes

The keys, software, processes, and procedures by which the CA verifies Certificate Data under this Guideline, issues EV Certificates, maintains a Repository, and revokes EV

Certificates.

FIPS140-2

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

HSM (Hardware Security Module)

The hardware that works as a protecting safe to store private keys used for encryption and digital signing. An HSM computes encryption and digital signing as well as generates private keys and random digits.

INAN (Internet Assigned Numbers Authority)

The organization that globally manages information related to the Internet, such as IP addresses and port numbers.

Key Pair

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

OCSP (Online Certificate Status Protocol)

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

OID (Object Identifier)

A unique numeric identifier registered by the international registration authority, in a framework to maintain and administer the uniqueness of the mutual connectivity, services and other aspects of the networks.

PKI (Public Key Infrastructure)

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

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.

Private Key

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

Public Key

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

RA (Registration Authority)

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

Relying Party

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

Repository

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

RFC3647 (Request for Comments 3647)

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

RSA

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

SHA-1 (Secure Hash Algorithm 1)

A hash function used in digital signing. A hash function is a computation technique for generating a fixed-length string from a given text. The hash length is 160 bits.

The algorithm works to detect any alterations in the original message during the transmission by comparing the hash values transmitted and received.

SHA-256 (Secure Hash Algorithm 256)

A hash function used in digital signing. The hash length is 256 bits.

The algorithm works to detect any alterations in the original message during the transmission by comparing the hash values transmitted and received.

Time-Stamp

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

WebTrust for CA

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

WebTrust for CA- Extended Validation SSL

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

WebTrust for CA - SSL Baseline with Network Security

Audit standards maintained by CPA Canada defining the rules for the reviews/authentications by the CAs for issuance of SSL Certificates and on the Certificates themselves.

WHOIS

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

X.500

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

2. Publication and Repository Responsibilities

2.1 Repository

The CA maintains and manages a Repository in order to allow Subscribers and Relying Parties to access CRL information 24x7. Further, it manages an OCSP responder to allow Subscribers and Relying Parties to check online the status of Certificates 24x7. However, the Repository and the OCSP responder may not be available temporarily at times due to maintenance or for any other reason.

2.2 Publication of Certificate Information

The CA stores the following information in the Repository to allow the online access thereto by Subscribers and Relying Parties:

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

Additionally, Subscribers and Relying Parties can refer the certificate status information by online of the OCSP responder by the CA. The CA also hosts the test Web pages that allow vendors to perform verifications, as part of the publication.

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. 「countryName（Country Name）」（C） shall be JP, the two-letter ISO 3166-1 country code abbreviation for Japan.(For OV certificates and EV certificates)
2. "organizationName (Organization Name)" (O) shall be the name of a corporation, company, or other legal entity and sole proprietorship. "stateOrProvinceName (State or Province Name)" (ST) and "localityName (Locality Name)" (L) include the organization's local information (For OV certificates and EV certificates)

   The following notation shall be used in accordance with Appendix D-1 of the EV Guidelines.

   A. The Revised Hepburn method of Romanization, as well as Kunrei-shiki and Nihon-shiki methods described in ISO 3602, are acceptable for Japanese Romanizations.

   B. The CA MAY verify the Romanized transliteration, language translation (e.g. English name), or other recognized Roman-letter substitute of the Applicant's formal legal name with either a QIIS, Verified Legal Opinion, or Verified Accountant Letter.

   C. The CA MAY use the Financial Services Agency to verify a Romanized, translated, or other recognized Roman-letter substitute name. When used, the CA MUST verify that the translated English is recorded in the audited Financial Statements.

   D. When relying on Articles of Incorporation to verify a Romanized, translated, or other recognized Roman-letter substitute name, the Articles of Incorporation MUST be accompanied either: by a document, signed with the original Japanese Corporate Stamp, that proves that the Articles of Incorporation are authentic and current, or by a Verified Legal Opinion or a Verified Accountant Letter. The CA MUST verify the authenticity of the Corporate Stamp.

3. [Common Name (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. (For DV certificates, OV certificates and EV certificates)
4. If the dNSName entry value in the Subject Alternative Name extension area contains international characters other than ASCII strings, puny-code converted version of the string is used. (For DV certificates, OV certificates and EV certificates)

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 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

The CA guarantees that the issued certificate can uniquely identify the owner of the certificate by the information contained in the identification name of the Subject. The serial number of the certificate shall be the serial number including the random number generated by CSPRNG. The serial number assigned in the CA is unique.

3.1.6 Recognition, Authentication, and Roles of Trademarks

The CA 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. The CA will not arbitrate or engage itself in the resolution of any dispute between Subscribers and third parties over the registered trademark or any alike. The CA reserves the right to reject a Subscriber Certificate Application or revoke an issued Certificate due to the dispute.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

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

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

3.2.2 Authentication of Organization Identity

If the Applicant requests a Certificate that will contain Subject Identity Information comprised only of the countryName field, then the CA SHALL verify the country associated with the Subject using a verification process meeting the requirements of this CP "3.2.2.3 Verification of Country" and that is described in the CA's CP and CPS. If the Applicant requests a Certificate that will contain the countryName field and other Subject Identity Information, then the CA SHALL verify the identity of the Applicant, and the authenticity of the Applicant Representative's certificate request using a verification process meeting the requirements of this CP "3.2.2.1 Identity" and that is described in the CA's CP and CPS. The CA SHALL inspect any document relied upon under this Section for alteration or falsification.

The verification source used when issuing EV Certificates shall be disclosed at the URL below.
https://www.secomtrust.net/service/pfw/apply/ev/list.html

【EV Certificate】

For EV Certificates, to verify the Applicant's legal existence and identity, the CA MUST do the following.

Private Organization Subjects

A. Legal Existence: Verify that the Applicant is a legally recognized entity, in existence and validly formed (e.g., incorporated) with the Incorporating or Registration Agency in the Applicant's Jurisdiction of Incorporation or Registration, and not designated on the records of the Incorporating or Registration Agency by labels such as "inactive", "invalid", "not current", or the equivalent.

B. Organization Name: Verify that the Applicant's formal legal name as recorded with the Incorporating or Registration Agency in the Applicant's Jurisdiction of Incorporation or Registration matches the Applicant's name in the EV Certificate Request.

C. Registration Number: Obtain the specific Registration Number assigned to the Applicant by the Incorporating or Registration Agency in the Applicant's Jurisdiction of Incorporation or Registration. Where the Incorporating or Registration Agency does not assign a Registration Number, the CA SHALL obtain the Applicant's date of Incorporation or Registration.

D. Registered Agent: Obtain the identity and address of the Applicant's Registered Agent or Registered Office (as applicable in the Applicant's Jurisdiction of Incorporation or Registration).

Government Entity Subjects

A. Legal Existence: Verify that the Applicant is a legally recognized Government Entity, in existence in the political subdivision in which such Government Entity operates.

B. Entity Name: Verify that the Applicant's formal legal name matches the Applicant's name in the EV Certificate Request.

C. Registration Number: The CA MUST attempt to obtain the Applicant's date of incorporation, registration, or formation, or the identifier for the legislative act that created the Government Entity. In circumstances where this information is not available, the CA MUST enter appropriate language to indicate that the Subject is a Government Entity.

Business Entity Subjects

A. Legal Existence: Verify that the Applicant is engaged in business under the name submitted by the Applicant in the Application.

B. Organization Name: Verify that the Applicant's formal legal name as recognized by the Registration Agency in the Applicant's Jurisdiction of Registration matches the Applicant's name in the EV Certificate Request.

C. Registration Number: Attempt to obtain the specific unique Registration Number assigned to the Applicant by the Registration Agency in the Applicant's Jurisdiction of Registration. Where the Registration Agency does not assign a Registration Number, the CA SHALL obtain the Applicant's date of Registration.

D. Principal Individual: Verify the identity of the identified Principal Individual.

Non-Commercial Entity Subjects (International Organizations)

A. Legal Existence: Verify that the Applicant is a legally recognized International Organization Entity.

B. Entity Name: Verify that the Applicant's formal legal name matches the Applicant's name in the EV Certificate Request.

C. Registration Number: The CA MUST attempt to obtain the Applicant's date of formation, or the identifier for the legislative act that created the International Organization Entity. In circumstances where this information is not available, the CA MUST enter appropriate language to indicate that the Subject is an International Organization Entity.

If, in addition to the Applicant's formal legal name, as recorded with the applicable Incorporating Agency or Registration Agency in the Applicant's Jurisdiction of Incorporation or Registration, the Applicant's identity, as asserted in the EV Certificate, is to contain any assumed name under which the Applicant conducts business, the CA MUST verify that:

i. the Applicant has registered its use of the assumed name with the appropriate government agency for such filings in the jurisdiction of its Place of Business (as verified in accordance with EV Guidelines),

ii. That such filing continues to be valid.

To verify the Applicant's physical existence and business presence, the CA MUST verify that the physical address provided by the Applicant is an address where the Applicant or a Parent/Subsidiary Company conducts business operations, and is the address of the Applicant's Place of Business.

A. Place of Business in the Country of Incorporation or Registration

ｉ. For Applicants whose Place of Business is in the same country as the Applicant's Jurisdiction of Incorporation or Registration and whose Place of Business is NOT the same as that indicated in the relevant Qualified Government Information Source (hereinafter, QGIS) to verify legal existence:

1. For Applicants listed at the same Place of Business address in the current version of either at least one QGIS (other than that used to verify legal existence), QIIS, the CA MUST confirm that the Applicant's address, as listed in the EV Certificate Request, is a valid business address for the Applicant or

a Parent/Subsidiary Company by reference to such QGIS, QIIS, and MAY rely on the Applicant's representation that such address is its Place of Business;

2. For Applicants who are not listed at the same Place of Business address in the current version of either at least one QIIS, the CA MUST confirm that the address provided by the Applicant in the EV Certificate Request is the Applicant's or a Parent/Subsidiary Company's business address, by obtaining documentation of a site visit to the business address, which MUST be performed by a reliable individual or firm. The documentation of the site visit MUST:
   a. Verify that the Applicant's business is located at the exact address stated in the EV Certificate Request (e.g., via permanent signage, employee confirmation, etc.),
   b. Identify the type of facility (e.g., office in a commercial building, private residence, storefront, etc.) and whether it appears to be a permanent business location,
   c. Indicate whether there is a permanent sign (that cannot be moved) that identifies the Applicant,
   d. Indicate whether there is evidence that the Applicant is conducting ongoing business activities at the site (not that it is just, for example, a mail drop, P.O. box, etc.)
   e. Include one or more photos of
      i. the exterior of the site (showing signage indicating the Applicant's name, if present, and showing the street address if possible),
      ii. the interior reception area or workspace.

ii. For all Applicants, the CA MAY alternatively rely on a Verified Professional Letter that indicates the address of the Applicant's or a Parent/Subsidiary Company's Place of Business and that business operations are conducted there.

iii. For Government Entity Applicants, the CA MAY rely on the address contained in the records of the QGIS in the Applicant's jurisdiction.

iv. For Applicants whose Place of Business is in the same country as the Applicant's Jurisdiction of Incorporation or Registration and where the QGIS used in to verify legal existence contains a business address for the Applicant, the CA MAY rely on the address in the QGIS to confirm the Applicant's or a Parent/Subsidiary Company's address as listed in the EV Certificate Request.

B. Place of Business not in the Country of Incorporation or Registration: The CA MUST rely on a Verified Professional Letter that indicates the address of the Applicant's Place of Business and that business operations are conducted there.

To assist in communicating with the Applicant and confirming that the Applicant is aware of and approves issuance, the CA MUST verify a telephone number, fax number, email address, or postal delivery address as a Verified Method of Communication with the Applicant.

To verify a Verified Method of Communication with the Applicant, the CA MUST:

A. Verify that the Verified Method of Communication belongs to the Applicant, or a Parent/Subsidiary or Affiliate of the Applicant, by matching it with one of the Applicant's Parent/Subsidiary or Affiliate's Places of Business in:

i. records provided by the applicable phone company;
ii. QGIS or QIIS
iii. a Verified Professional Letter

B. Confirm the Verified Method of Communication by using it to obtain an affirmative response sufficient to enable a reasonable person to conclude that the Applicant, or a Parent/Subsidiary or Affiliate of Applicant, can be contacted reliably by using the Verified Method of Communication.

The CA MUST verify that the Applicant has the ability to engage in business by verifying the Applicant's, or Affiliate/Parent/Subsidiary Company's, operational existence. The CA MAY rely on its verification of a Government Entity's legal existence under the EV Guidelines Section 11.2 as verification of a Government Entity's operational existence.

To verify the Applicant's ability to engage in business, the CA MUST verify the operational existence of the Applicant, or it's Affiliate/Parent/Subsidiary Company, by:

1. Verifying that the Applicant, Affiliate, Parent Company, or Subsidiary Company has been in existence for at least three years, as indicated by the records of an Incorporating Agency or Registration Agency;
2. Verifying that the Applicant, Affiliate, Parent Company, or Subsidiary Company is listed in either a current QIIS or QTIS;
3. Verifying that the Applicant, Affiliate, Parent Company, or Subsidiary Company has an active current Demand Deposit Account with a Regulated Financial Institution by receiving authenticated documentation of the Applicant's,

Affiliate's, Parent Company's, or Subsidiary Company's Demand Deposit Account directly from a Regulated Financial Institution;

4. Relying on a Verified Professional Letter to the effect that the Applicant has an active current Demand Deposit Account with a Regulated Financial Institution.

For each Fully-Qualified Domain Name listed in a Certificate which is not an Onion Domain Name, the CA SHALL confirm that, as of the date the Certificate was issued, the Applicant either is the Domain Name Registrant or has control over the FQDN using a procedure specified in Section 3.2.2.4 of the Baseline Requirements.

EV Certificates MAY include Domain Names containing mixed character sets only in compliance with the rules set forth by the domain registrar. The CA MUST visually compare any Domain Names with mixed character sets with known high risk domains. If a similarity is found, then the EV Certificate Request MUST be flagged as High Risk. The CA must perform reasonably appropriate additional authentication and verification to be certain beyond reasonable doubt that the Applicant and the target in question are the same organization.

For both the Contract Signer and the Certificate Approver, the CA MUST verify the following.

1. Name, Title and Agency:

The CA MUST verify the name and title of the Contract Signer and the Certificate Approver, as applicable. The CA MUST also verify that the Contract Signer and the Certificate Approver are agents representing the Applicant.

2. Signing Authority of Contract Signer:

The CA MUST verify that the Contract Signer is authorized by the Applicant to enter into the Subscriber Agreement (and any other relevant contractual obligations) on behalf of the Applicant, including a contract that designates one or more Certificate Approvers on behalf of the Applicant.

3. EV Authority of Certificate Approver:

The CA MUST verify, through a source other than the Certificate Approver him- or herself, that the Certificate Approver is expressly authorized by the Applicant to do the following, as of the date of the EV Certificate Request:

A. Submit, and, if applicable, authorize a Certificate Requester to submit, the EV Certificate Request on behalf of the Applicant;

B. Provide, and, if applicable, authorize a Certificate Requester to provide, the information requested from the Applicant by the CA for issuance of the EV

Certificate;

C. Approve EV Certificate Requests submitted by a Certificate Requester.

Where the CA and Applicant contemplate the submission of multiple future EV Certificate Requests, then, after the CA:

1. Has verified the name and title of the Contract Signer and that he/she is an employee or agent of the Applicant;
2. Has verified the Signing Authority of such Contract Signer in accordance with one of the procedures in the EV Guidelines, Section 11.8.3.

The CA and the Applicant MAY enter into a written agreement, signed by the Contract Signer on behalf of the Applicant, whereby, for a specified term, the Applicant expressly authorizes one or more Certificate Approver(s) designated in such agreement to exercise EV Authority with respect to each future EV Certificate Request submitted on behalf of the Applicant and properly authenticated as originating with, or otherwise being approved by, such Certificate Approver(s).

Such an agreement MUST provide that the Applicant shall be obligated under the Subscriber Agreement for all EV Certificates issued at the request of, or approved by, such Certificate Approver(s) until such EV Authority is revoked, and MUST include mutually agreed-upon provisions for:

i. authenticating the Certificate Approver when EV Certificate Requests are approved,
ii. periodic re-confirmation of the EV Authority of the Certificate Approver,
iii. secure procedures by which the Applicant can notify the CA that the EV Authority of any such Certificate Approver is revoked,
iv. such other appropriate precautions as are reasonably necessary.

Both the Subscriber Agreement and each non-pre-authorized EV Certificate Request MUST be signed. The Subscriber Agreement MUST be signed by an authorized Contract Signer. The EV Certificate Request MUST be signed by the Certificate Requester submitting the document, unless the Certificate Request has been pre-authorized in line with the EV Guidelines, Section 11.8.4. If the Certificate Requester is not also an authorized Certificate Approver, then an authorized Certificate Approver MUST independently approve the EV Certificate Request. In all cases, applicable signatures MUST be a legally valid and contain an enforceable seal or handwritten signature (for a paper Subscriber Agreement and/or EV Certificate Request), or a legally valid and enforceable electronic signature (for an electronic Subscriber Agreement and/or EV Certificate Request), that binds the Applicant to the terms of each respective document.

In cases where an EV Certificate Request is submitted by a Certificate Requester, before the CA issues the requested EV Certificate, the CA MUST verify that an authorized Certificate Approver reviewed and approved the EV Certificate Request.
Acceptable methods of verifying the Certificate Approver's approval of an EV Certificate Request include:

1. Contacting the Certificate Approver using a Verified Method of Communication for the Applicant and obtaining oral or written confirmation that the Certificate Approver has reviewed and approved the EV Certificate Request;
2. Notifying the Certificate Approver that one or more new EV Certificate Requests are available for review and approval at a designated access-controlled and secure Web site, followed by a login by, and an indication of approval from, the Certificate Approver in the manner required by the Web site;
3. Verifying the signature of the Certificate Approver on the EV Certificate Request.

The CA MUST verify whether the Applicant, the Contract Signer, the Certificate Approver, the Applicant's Jurisdiction of Incorporation, Registration, or Place of Business:

A. Is identified on any government denied list, list of prohibited persons, or other list that prohibits doing business with such organization or person under the laws of the country of the CA's jurisdiction(s) of operation;

B. Has its Jurisdiction of Incorporation, Registration, or Place of Business in any country with which the laws of the CA's jurisdiction prohibit doing business.

The CA MUST NOT issue any EV Certificate to the Applicant if either the Applicant, the Contract Signer, or Certificate Approver or if the Applicant's Jurisdiction of Incorporation or Registration or Place of Business is on any such list.

Final Cross-Correlation and Due Diligence

1. The results of the verification processes and procedures outlined in these Guidelines are intended to be viewed both individually and as a group.
   Thus, after all of the verification processes and procedures are completed, the CA MUST have a person who is not responsible for the collection of information review all of the information and documentation assembled in support of the EV Certificate application and look for discrepancies or other details requiring further explanation.

2. The CA MUST obtain and document further explanation or clarification from the Applicant, Certificate Approver, Certificate Requester, Qualified Independent Information Sources, and/or other sources of information, as necessary, to resolve those discrepancies or details that require further explanation.

3. The CA MUST refrain from issuing an EV Certificate until the entire corpus of information and documentation assembled in support of the EV Certificate Request is such that issuance of the EV Certificate will not communicate factual information that the CA knows, or the exercise of due diligence should discover from the assembled information and documentation, to be inaccurate,. If satisfactory explanation and/or additional documentation are not received within a reasonable time, the CA MUST decline the EV Certificate Request and SHOULD notify the Applicant accordingly.

4. In the case where some or all of the documentation used to support the application is in a language other than the CA's normal operating language, the CA or its Affiliate MUST perform the requirements of this Final Cross-Correlation and Due Diligence section using employees under its control and having appropriate training, experience, and judgment in confirming organizational identification and authorization and fulfilling all qualification requirements contained in the EV Guidelines, Section 1.4.1. When employees under the control of the CA do not possess the language skills necessary to perform the Final Cross-Correlation and Due Diligence a CA MAY:
   A. Rely on language translations of the relevant portions of the documentation, provided that the translations are received from a Translator;
   B. When the CA has utilized the services of an RA, the CA MAY rely on the language skills of the RA to perform the Final Cross-Correlation and Due Diligence, provided that the RA complies with the EV Guidelines, Section 11.13, Subsections (1), (2) and (3). Notwithstanding the foregoing, prior to issuing the EV Certificate, the CA MUST review the work completed by the RA and determine that all requirements have been met;
   C. When the CA has utilized the services of an RA, the CA MAY rely on the RA to perform the Final Cross-Correlation and Due Diligence, provided that the RA complies with this section and is subjected to the Audit Requirements of the EV Guidelines, Section 17.5 and Section 17.6.

In the case of EV Certificates to be issued in compliance with the requirements of the EV Guidelines, Section 14.2, the Enterprise RA MAY perform the requirements of this

Final Cross-Correlation and Due Diligence section.

Roles requiring separation of duties

1. The CA MUST enforce rigorous control procedures for the separation of validation duties to ensure that no one person can single-handedly validate and authorize the issuance of an EV Certificate. The Final Cross-Correlation and Due Diligence steps, as outlined in the EV Guidelines, Section 11.13, MAY be performed by one of the persons. For example, one Validation Specialist MAY review and verify all the Applicant information and a second Validation Specialist MAY approve issuance of the EV Certificate.

2. Such controls MUST be auditable.

Securitiy for data

As specified in Section 5 of the Baseline Requirements. In addition, systems used to process and approve EV Certificate Requests MUST require actions by at least two trusted persons before creating an EV Certificate.

In consistent with this CP "5.5.2 Retention Period for Archive", the CA shall maintain an internal database containing all previously revoked Certificates and previously rejected Certificate Requests due to suspicion or concern of phishing or other fraudulent use. The CA shall use this information to identify future suspicious certificate requests.

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;
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;
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;
・a method identified in this 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.

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.

   The Random Value SHALL be unique in each email, fax, SMS, or postal mail. The CA MAY resend the email, fax, SMS, or postal mail in its entirety, including re-use of the Random Value, provided that the communication's entire contents and recipient(s) remain unchanged.

   The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation.

   (Baseline Requirements Section 3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact).

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.

   The Random Value SHALL be unique in each email.

   The CA MAY resend the email in its entirety, including re-use of the Random Value, provided that the communication's entire contents and recipient(s) remain unchanged.

   The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation.

   (Baseline Requirements Section 3.2.2.4.4 Constructed Email to Domain Contact)

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 Random Value SHALL be valid for 30 days, and SHALL not use the Random Value after the time frame permitted for reuse of validated information relevant to the Certificate if the Applicant submitted the Certificate request,
(Baseline Requirement Section 3.2.2.4.7 DNS Change)

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.
The relevant CAA Resource Record Set MUST be found using the search algorithm defined in RFC 8659, Section 3. The Random Value SHALL be unique in each email. The CA MAY resend the email in its entirety, including re-use of the Random Value, provided that the communication's entire contents and recipient(s) remain unchanged. The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation.
（Baseline Requirement Section 3.2.2.4.13 Email to DNS CAA Contact ）

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 Random Value SHALL be unique in each email. The CA MAY resend the email in its entirety, including re-use of the Random Value, provided that the communication's entire contents and recipient(s) remain unchanged. The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation.
(Baseline Requirement Section 3.2.2.4.14 Email to DNS TXT Contact)

6. Prove the applicant's authority over the FQDN by calling the domain contact phone number and getting a response to permission to use the authenticated domain name. In addition, when the telephone number of the domain contact is the same in a plurality of authentication domain names, the authority can be proved for a plurality of FQDNs by presenting each authentication domain name and obtaining a response of permission to use.
The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation.

(Baseline Requirement Section 3.2.2.4.15 Phone Contact with Domain Contact)

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

   The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation.

   (Baseline Requirement Section 3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact)

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

   The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation.

   (Baseline Requirement Section 3.2.2.4.17 Phone Contact with DNS CAA Phone Contact)

9. Confirm the applicant's control over the FQDN by verifying that the request token or random value is included in the contents of the file. The CA accesses via an approved port, and confirms that Random value is placed under the "http (or https): // [FQDN to be issued certificate] /.well-known/pki-validation" directory, and that it receives a normal HTTP or HTTPS response sent from the request.

   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.

   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 3xx301, 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 the "http" or "https" scheme.
3. Redirects MUST be to resource URLs accessed via Authorized Ports.

If a Random Value is used, then:

1. The CA MUST provide a Random Value unique to the certificate request.
2. The Random Value MUST remain valid for use in a confirming response for no more than 30 days from its creation.

（Baseline Requirements section 3.2.2.4.18 Agreed-Upon Change to Website v2）

3.2.2.5 Authentication for an IP Address

The CA does not issue a certificate by authenticating the IP address.

3.2.2.6 Wildcard Domain Validation

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

When issuing an EV certificate, A Qualified Independent Information Source (QIIS) is a regularly-updated and publicly available database that is generally recognized as a dependable source for certain information. A database qualifies as a QIIS if the CA determines that:

1. Industries other than the certificate industry rely on the database for accurate location, contact, or other information;
2. The database provider updates its data on at least an annual basis.

The CA SHALL use a documented process to check the accuracy of the database and ensure its data is acceptable, including reviewing the database provider's terms of use. The CA SHALL NOT use any data in a QIIS that the CA knows is

i. self-reported.
ii. not verified by the QIIS as accurate.

Databases in which the CA or its owners or affiliated companies maintain a controlling interest, or in which any Registration Authorities or subcontractors to whom the CA has outsourced any portion of the vetting process (or their owners or affiliated companies) maintain any ownership or beneficial interest, do not qualify as a QIIS.

A Qualified Government Information Source (QGIS) is a regularly-updated and current, publicly available, database designed for the purpose of accurately providing the information for which it is consulted, and which is generally recognized as a dependable source of such information provided that it is maintained by a Government Entity, the reporting of data is required by law, and false or misleading reporting is punishable with criminal or civil penalties. Nothing in these Guidelines shall prohibit the use of third-party vendors to obtain the information from the Government Entity provided that the third party obtains the information directly from the Government Entity.

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

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

3.2.3 Authentication of Individual Identity

The CA does not issue Individual Valididate certificates (IV certificates) that comply with the following certificate policy identifiers.

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) individual-validated(3)} (2.23.140.1.2.3)

3.2.4 Non-Verified Subscriber Information

The information about non-verified certificate subscribers will not be included in the certificates issued by the CA.

3.2.5 Validation of Authority

If the Applicant for a Certificate containing Subject Identity Information is an organization, the CA SHALL use a Reliable Method of Communication to verify the authenticity of the Applicant Representative’s certificate request.

The CA MAY use the sources listed in this CP, “Section 3.2.2.1 Identity” to verify the Reliable Method of Communication. Provided that the CA uses a Reliable Method of Communication, the CA MAY establish the authenticity of the certificate request directly with the Applicant Representative or with an authoritative source within the Applicant’s organization, such as the Applicant’s main business offices, corporate offices, human resource offices, information technology offices, or other department that the CA deems appropriate.

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 the revocation request from the Subscriber or the applicant according to the prescribed procedure, the CA identifies and authenticates the 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 individuals, corporations, other organizations that use certificates, and agents delegated by certificate subscribers (hereinafter referred to as "Applicant").

In accordance with this 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.

For EV Certificate, to verify the Applicant's legal existence and identity, the CA MUST do the following.

Private Organization Subjects

A. Legal Existence: Verify that the Applicant is a legally recognized entity, in existence and validly formed (e.g., incorporated) with the Incorporating or Registration Agency in the Applicant's Jurisdiction of Incorporation or Registration, and not designated on the records of the Incorporating or Registration Agency by labels such as "inactive", "invalid", "not current", or the equivalent.

B. Organization Name: Verify that the Applicant's formal legal name as recorded with the Incorporating or Registration Agency in the Applicant's Jurisdiction of Incorporation or Registration matches the Applicant's name in the EV Certificate Request.

C. Registration Number: Obtain the specific Registration Number assigned to the Applicant by the Incorporating or Registration Agency in the Applicant's Jurisdiction of Incorporation or Registration. Where the Incorporating or Registration Agency does not assign a Registration Number, the CA SHALL obtain the Applicant's date of Incorporation or Registration.

D. Registered Agent: Obtain the identity and address of the Applicant's Registered Agent or Registered Office (as applicable in the Applicant's Jurisdiction of Incorporation or Registration).

Government Entity Subjects

A. Legal Existence: Verify that the Applicant is a legally recognized Government Entity, in existence in the political subdivision in which such Government Entity operates.

B. Entity Name: Verify that the Applicant's formal legal name matches the Applicant's name in the EV Certificate Request.

C. Registration Number: The CA MUST attempt to obtain the Applicant's date of incorporation, registration, or formation, or the identifier for the legislative act that created the Government Entity. In circumstances where this information is not available, the CA MUST enter appropriate language to indicate that the Subject is a Government Entity.

Business Entity Subjects

A. Legal Existence: Verify that the Applicant is engaged in business under the name submitted by the Applicant in the Application.

B. Organization Name: Verify that the Applicant's formal legal name as recognized by the Registration Agency in the Applicant's Jurisdiction of Registration matches the Applicant's name in the EV Certificate Request.

C. Registration Number: Attempt to obtain the specific unique Registration Number assigned to the Applicant by the Registration Agency in the Applicant's Jurisdiction of Registration. Where the Registration Agency does not assign a Registration Number, the CA SHALL obtain the Applicant's date of Registration.

D. Principal Individual: Verify the identity of the identified Principal Individual.

Non-Commercial Entity Subjects (International Organizations)

A. Legal Existence: Verify that the Applicant is a legally recognized International Organization Entity.

B. Entity Name: Verify that the Applicant's formal legal name matches the Applicant's name in the EV Certificate Request.

C. Registration Number: The CA MUST attempt to obtain the Applicant's date of formation, or the identifier for the legislative act that created the International Organization Entity. In circumstances where this information is not available, the CA MUST enter appropriate language to indicate that the Subject is an International Organization Entity.

Specifically, register the following values.

If the subscriber is as follows, the CA will set the serialNumber as follows:

Registered corporation : Company corporation number or corporate number
Central ministries and national agencies : Corporate number or or establishment date
Local governments and their institutions : Corporate number or or establishment date
National and public universities and high school institutions : Corporate number or or establishment date

If the corporate number and establishment date cannot be confirmed by the CA, enter the following text in serialNumber.

Central ministries and national agencies : Government
Local governments and their institutions : Local Government
National and public universities and high school institutions : Public School

If the subscriber is as follows, the CA will set the business Category as follows.

Registered corporation : Private Organization
Central ministries and national agencies : Government Entity
Local governments and their institutions : Government Entity
National and public universities and high school institutions : Government Entity

4.1.2 Enrollment Process and Responsibilities

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

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Once accepted, the Certificate Application is authenticated by the CA in accordance with this CP "3.2 Initial Identification and Authentication" hereof.

The certificate request may include all factual information about the Applicant to be included in the Certificate, and such additional information as is necessary for the CA to obtain from the Applicant in order to comply with Baseline Requirements and the

CA's Certificate Policy and/or Certification Practice Statement. In cases where the certificate request does not contain all the necessary information about the Applicant, the CA shall obtain the remaining information from the Applicant or, having obtained it from a reliable, independent, third-party data source, confirm it with the Applicant. The CA shall establish and follow a documented procedure for verifying all data requested for inclusion in the Certificate by the Applicant.

Applicant information include, but not be limited to, at least one Fully-Qualified Domain Name to be included in the Certificate's Subject Alternative Name extension.

In the CPS "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, Section "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, Section "3.2 Initial Identity Validation" or completed the validation itself no more than 825 days prior to issuing the Certificate.

Effective 2021-10-01, for validation of Domain Names according to this CP, Section "3.2.2.4 Domain Authentication", any reused data, document, or completed validation must be obtained no more than 398 days prior to issuing the Certificate.

In no case may a prior validation be reused if any data or document used in the prior validation was obtained more than the maximum time permitted for reuse of the data or document prior to issuing the Certificate.

The CA shall develop, maintain, and implement documented procedures that identify and require additional verification activity for High Risk Certificate Requests prior to the Certificate's approval, as reasonably necessary to ensure that such requests are properly verified under Baseline Requirements.

If a Delegated Third Party fulfills any of the CA's obligations under this section, the CA shall verify that the process used by the Delegated Third Party to identify and further verify High Risk Certificate Requests provides at least the same level of assurance as the CA's own processes.

The validity period of EV certificate verified data is as follows:

1. Except for reissuance of an EV Certificate under the EV Guidelines, Section 11.14.2 and except when permitted otherwise in the EV Guidelines, Section 11.14.1, the age of all data used to support issuance of an EV Certificate (before revalidation is required) SHALL NOT exceed the following limits:

A. Legal existence and identity - 398 days
B. Assumed name - 398 days
C. Address of Place of Business - 398 days
D. Verified Method of Communication - 398 days
E. Operational existence - 398 days
F. Domain Name - 398 days
G. Name, Title, Agency, and Authority - 398 days, unless a contract between the CA and the Applicant specifies a different term, in which case, the term specified in such contract controls. For example, the contract MAY include the perpetual assignment of EV roles until revoked by the Applicant or CA, or until the contract expires or is terminated.

2. The 398-day period set forth above SHALL begin to run on the date the information was collected by the CA.
3. The CA MAY reuse a previously submitted EV Certificate Request, Subscriber Agreement, or Terms of Use, including use of a single EV Certificate Request in support of multiple EV Certificates containing the same Subject to the extent permitted under the EV Guideline, Section 11.9 and the EV Guideline, Section 11.10.
4. The CA MUST repeat the verification process required in the EV Guidelines for any information obtained outside the time limits specified above except when permitted otherwise under the EV Guideline, Section 11.14.1.

The following Applicant roles are required for the issuance of an EV Certificate.

1. Certificate Requester:

   The EV Certificate Request MUST be submitted by an authorized Certificate Requester. A Certificate Requester is a natural person who is either the Applicant, employed by the Applicant, an authorized agent who has express authority to represent the Applicant, or a third party (such as an ISP or hosting company) that completes and submits an EV Certificate Request on behalf of the Applicant.

2. Certificate Approver:

   The EV Certificate Request MUST be approved by an authorized Certificate Approver. A Certificate Approver is a natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant to

   i. act as a Certificate Requester and to authorize other employees or third parties to act as a Certificate Requester, and

ii.to approve EV Certificate Requests submitted by other Certificate Requesters.

3. Contract Signer:

A Subscriber Agreement applicable to the requested EV Certificate MUST be signed by an authorized Contract Signer. A Contract Signer is a natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant, and who has authority on behalf of the Applicant to sign Subscriber Agreements.

4. Applicant Representative:

In the case where the CA and the Subscriber are affiliated, Terms of Use applicable to the requested EV Certificate MUST be acknowledged and agreed to by an authorized Applicant Representative. An Applicant Representative is a natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant, and who has authority on behalf of the Applicant to acknowledge and agree to the Terms of Use.

The Applicant MAY authorize one individual to occupy two or more of these roles. The Applicant MAY authorize more than one individual to occupy any of these roles.

4.2.2 Approval or Rejection of Certificate Applications

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

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

The CA shall notify the Applicant or the Subscriber of the content of the deficiency and the resubmission of documents, etc., either directly or through Delegated Third Party.

4.2.3 Time to Process Certificate Application

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

4.2.4 CAA Records Processing

The CA checks the CAA record at the time of reviewing the application information. The Certificate Subscribers who want to grant the authority to issue certificates to the FQDN must include the value of "secomtrust.net" in the property "issue" or “issuewild” of the CAA record for each DNS zone.

If there is already a CAA entry in each DNS zone of the Certificate Subscriber and a certificate is required to be issued by this CA, the value of "secomtrust.net" must be included in the property "issue" or “issuewild” of the CAA record.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

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

Certificate issuance by the Root CA SHALL require an individual authorized by the CA (i.e. the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command in order for the Root CA to perform a certificate signing operation.

The CA confirms whether the format conforms to Baseline Requirements for some items of the certificate to be issued by the pre-certificate linting function, and refuses to issue if it does not meet the requirements.

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

The backdating of a certificate's notBefore date to avoid a deadline, prohibition or code-enforced restriction is not used by the CA.

4.3.2 Notifications to Subscriber of Certificate Issuance

The CA will notify the Certificate Subscriber of the issuance via the website that only the Certificate Subscriber can access, or by e-mail.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

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

4.4.2 Publication of the Certificate by the CA

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

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

The CA 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

Certificates shall be used in accordance with this CP, Service Terms and CPS.
Subscriber shall protect the Private Key from unauthorized use or disclosure by third parties and shall use the Private Key only for its intended purpose in accordance with "9.6.3 Subscriber Representations and Warranties".

4.5.2 Relying Party Public Key and Certificate Usage

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

4.6 Certificate Renewal

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

4.6.1 Circumstances for Certificate Renewal

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

4.6.2 Who May Request Renewal

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

4.6.3 Processing Certificate Renewal Requests

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

4.6.4 Notification of New Certificate Issuance to Subscriber

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

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

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

4.6.6 Publication of the Renewal Certificates by the CA

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

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

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

4.7 Certificate Re-Key

4.7.1 Circumstances for Certificate Re-Key

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

4.7.2 Who May Request Certification of a New Public Key

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

4.7.3 Processing Certificate Re-Keying Requests

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

4.7.4 Notification of New Certificate Issuance to Subscriber

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

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

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

4.7.6 Publication of the Re-Keyed Certificate by the CA

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

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

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

4.8 Certificate Modification

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

4.8.1 Circumstances for Certificate Modification

No stipulation

4.8.2 Who May Request Certificate Modification

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

4.8.3 Processing Certificate Modification Requests

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

4.8.4 Notification of New Certificate Issuance to Subscriber

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

4.8.5 Conduct Constituting Acceptance of Modified Certificate

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

4.8.6 Publication of the Modified Certificates by the CA

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

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

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

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Certificate Revocation

The CA shall revoke a Certificate within 24 hours and use the corresponding CRLReason (revocation reason) in “7.2.2 Certificate Revocation Lists and CRL Entry Extensions” of this CP 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 (such as a Debian weak key, see https://wiki.debian.org/SSLkeys) (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);

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 that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name (CRLReason #9, privilegeWithdrawn);
11. The CA is made aware of a material change in the information contained in the Certificate (CRLReason #9, privilegeWithdrawn);
12. The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement (CRLReason #4, superseded);
13. The CA determines or is made aware that any of the information appearing in the Certificate is inaccurate (CRLReason #9, privilegeWithdrawn);
14. The CA's right to issue Certificates under these 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);
15. Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement 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);
16. The CA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, or if there is clear evidence that the specific method used to generate the Private Key was flawed (CRLReason #1,

keyCompromise).

4.9.2 Who Can Request Revocation

A request for revocation of a Certificate shall be made by the Certificate Subscriber or the Applicant. If the CA determines that the CP/CPS "4.9.1 Circumstances for Certificate Revocation" applies, the CA may be the Applicant.

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 or Applicant shall notify the CA by using the application provided by the CA or the Delegated third Party and performing the prescribed procedures.

The CA confirms the information received by the prescribed procedure and revokes the certificate.

4.9.4 Revocation Request Grace Period

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

4.9.5 Time within Which CA Shall Process the Revocation Request

The CA will promptly process the revocation of the certificate after receiving a valid revocation application, and reflect the certificate information in the CRL.

Within 24 hours after receiving a Certificate Problem Report, the CA SHALL investigate the facts and circumstances related to a Certificate Problem Report and provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report.

After reviewing the facts and circumstances, the CA SHALL work with the Subscriber and any entity reporting the Certificate Problem Report or other revocation-related notice to establish whether or not the certificate will be revoked, and if so, a date which the CA will revoke the certificate. The period from receipt of the Certificate Problem Report or revocation-related notice to published revocation MUST NOT exceed the time frame set forth in the CP, “Section 4.9.1. Circumstances for Certificate Revocation”.

The date selected by the CA SHOULD consider the following criteria:

1. The nature of the alleged problem (scope, context, severity, magnitude, risk of

harm);

2. The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties);
3. The number of Certificate Problem Reports received about a particular Certificate or Subscriber;
4. The entity making the complaint

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

4.9.6 Revocation Checking Requirements for Relying Parties

The URLs of the CRL storage destination and the OCSP responder are indicated on the Certificates issued by the CA.

CRLs and the OCSP responder may be accessed using a commonly available Web Interface. CRLs do not contain expired Certificate information.

Relying Parties must authenticate the validity of a Subscriber's Certificate. The validity of a Certificate may be verified by using the CRL posted on the Repository site or the OCSP responder.

4.9.7 CRL Issuance Frequency

If the CA publishes a CRL, then the CA shall update and reissue CRLs at least once every 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 will be reflected onto the repository within a reasonable time.

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

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

4.9.10 On-Line Revocation/Status Checking Requirements

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

OCSP responders operated by the CA shall support the HTTP GET method, as described in RFC 6960 and/or RFC 5019.

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

For the status of Subscriber Certificates:

1. OCSP responses MUST have a validity interval greater than or equal to 8 hours;
2. OCSP responses MUST have a validity interval less than or equal to 10 days;
3. For OCSP responses with validity intervals less than sixteen hours, then the CA shall update the information provided via an Online Certificate Status Protocol prior to one-half of the validity period before the nextUpdate.
4. For OCSP responses with validity intervals greater than or equal to 16 hours, then the CA shall update the information provided via an Online Certificate Status Protocol at least 8 hours prior to the nextUpdate, and no later than 4 days after the thisUpdate.

For the status of Subordinate CA Certificates:

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

i. at least every 12 months; and

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

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

The CA SHOULD monitor the OCSP responder for requests for "unused" serial numbers as part of its security response procedures.

The OCSP responder MAY provide definitive responses about "reserved" certificate serial numbers, as if there was a corresponding Certificate that matches the

Precertificate [RFC6962].

A certificate serial number within an OCSP request is one of the following 3 options:

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

4.9.11 Other Forms of Revocation Advertisements Available

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

4.9.12 Special Requirements Regarding Key Compromise

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

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

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

If the CA determines that the private key has been compromised or is likely to be compromised, this 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 for confirmation through the OCSP responder. The CA MUST NOT remove revocation entries in CRL or OCSP responses until after the Expiry Date of the revoked Certificate.

4.10.2 Service Availability

The CA SHALL operate and maintain its CRL and OCSP capability with resources sufficient to provide a response time of 10 seconds or less under normal operating conditions.

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

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

4.10.3 Optional Features

No stipulation

4.11 End of Subscription (Registry)

Subscribers shall submit a Certificate Revocation Request when ending the certificate use. It will also end if they do not apply for the renewal of the certificate and the validity period of the corresponding certificate has expired.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

The CA does not Escrow Subscriber Private Keys.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5. Facility, Management, and Operational Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

Relevant provisions are stipulated in the CPS.

5.1.2 Physical Access

Relevant provisions are stipulated in the CPS.

5.1.3 Power and Air Conditioning

Relevant provisions are stipulated in the CPS.

5.1.4 Water Exposures

Relevant provisions are stipulated in the CPS.

5.1.5 Fire Prevention and Protection

Relevant provisions are stipulated in the CPS.

5.1.6 Media Storage

Relevant provisions are stipulated in the CPS.

5.1.7 Waste Disposal

Relevant provisions are stipulated in the CPS.

5.1.8 Off-Site Backup

Relevant provisions are stipulated in the CPS.

5.2 Procedural Controls

5.2.1 Trusted Roles

Relevant provisions are stipulated in the CPS.

5.2.2 Number of Persons Required per Task

Relevant provisions are stipulated in the CPS.

5.2.3 Identification and Authentication for Each Role

Relevant provisions are stipulated in the CPS.

5.2.4 Roles Requiring Separation of Duties

Relevant provisions are stipulated in the CPS.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

Relevant provisions are stipulated in the CPS.

5.3.2 Background Check Procedures

Relevant provisions are stipulated in the CPS.

5.3.3 Training Requirements

Relevant provisions are stipulated in the CPS.

5.3.4 Retraining Frequency and Requirements

Relevant provisions are stipulated in the CPS.

5.3.5 Job Rotation Frequency and Sequence

Relevant provisions are stipulated in the CPS.

5.3.6 Sanctions for Unauthorized Actions

Relevant provisions are stipulated in the CPS.

5.3.7 Independent Contractor Requirements

Relevant provisions are stipulated in the CPS.

5.3.8 Documentation Supplied to Personnel

Relevant provisions are stipulated in the CPS.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

Relevant provisions are stipulated in the CPS.

5.4.2 Frequency of Processing Audit Log

Relevant provisions are stipulated in the CPS.

5.4.3 Retention Period for Audit Log

Relevant provisions are stipulated in the CPS.

5.4.4 Protection of Audit Log

Relevant provisions are stipulated in the CPS.

5.4.5 Audit Log Backup Procedure

Relevant provisions are stipulated in the CPS.

5.4.6 Audit Log Collection System

Relevant provisions are stipulated in the CPS.

5.4.7 Notification to Event-Causing Subject

Relevant provisions are stipulated in the CPS.

5.4.8 Vulnerability Assessments

Relevant provisions are stipulated in the CPS.

5.5 Records Archival

5.5.1 Types of Records Archived

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. After the new key pair is generated, the certificate and CRL are issued using the new key pair.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

Relevant provisions are stipulated in the CPS.

5.7.2 Computing Resources, 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, it shall so notify Subscribers and other affected participants, including Application Software Suppliers through the Delegated Third Party, three (3) months prior to the termination.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

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

Subscriber Key Pairs are generated by Subscriber.

6.1.2 Private Key Delivery to Subscriber

The CA does not deliver Private Keys to Subscribers.

6.1.3 Public Key Delivery to Certificate Issuer

A Subscriber Public Key may be delivered online to the CA, the communication routing of which is encrypted by 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 （Optional if the public key of the end entity certificate is RSA, prohibited if it is ECDSA）

dataEncipherment	—	—
keyAgreement	—	—
keyCertSign	yes	—
cRLSign	yes	—
encipherOnly	—	—
decipherOnly	—	—

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The generation, storage and signing operations of the CA Private Keys are performed using an FIPS140-2 Level 3 conformant cryptographic module. No stipulation for Subscriber Private Keys.

6.2.2 Private Key Multi-Person Control

Activation, deactivation, backup and other operations relating to CA Private Keys are jointly performed by at least two authorized individuals in a secure environment. Activation, deactivation, backup and other operations relating to Subscriber Private Keys must be performed securely under the control of the relevant Subscribers.

6.2.3 Private Key Escrow

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

6.2.4 Private Key Backup

Backup of Private Keys of the CA is jointly performed by at least two authorized individuals and is stored in a secure room as encrypted.
The backup of Subscriber Private Keys must be securely stored under the control of the relevant Subscribers.

6.2.5 Private Key Archival

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

6.2.6 Private Key Transfer into or from a Cryptographic

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

6.2.7 Private Key Storage on Cryptographic Module

Private Keys of the CA operated on the Digital Certification Infrastructure are stored within the cryptographic module. No stipulation for Subscriber Private Keys.

6.2.8 Method of Activating Private Key

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

6.2.9 Method of Deactivating Private Key

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

6.2.10 Method of Destroying Private Key

Private Keys of the CA are jointly destroyed by at least two authorized individuals by means of complete initialization or physical destruction. The Private Key backups are also destroyed in the same manner. No stipulation for Subscriber Private Keys.

6.2.11 Cryptographic Module Rating

The quality standards to be applied to the cryptographic modules used by the CA are as specified in this CP, "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 the CA Public Keys are stipulated in "6.2.1 Cryptographic Module Standards and Controls" of the CPS. No stipulation for Subscriber Private Keys.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

Relevant provisions are stipulated in the CPS.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Relevant provisions are stipulated in the CPS.

6.4.2 Activation Data Protection

Relevant provisions are stipulated in the CPS.

6.4.3 Other Aspects of Activation Data

Relevant provisions are stipulated in the CPS.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

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

6.5.2 Computer Security Rating

Relevant provisions are stipulated in the CPS.

6.6 Life-Cycle Technical Controls

6.6.1 System Development Controls

Relevant provisions are stipulated in the CPS.

6.6.2 Security Management Controls

Relevant provisions are stipulated in the CPS.

6.6.3 Life-Cycle Security Controls

Relevant provisions are stipulated in the CPS.

6.7 Network Security Controls

Relevant provisions are stipulated in the CPS.

6.8 Time-Stamping

Relevant provisions are stipulated in the CPS.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

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

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 TLS Server Certificate Profile

Basic Fields		Settings	critical
version		Version 3	-
serialNumber		non - sequential Certificate serial numbers greater than zero (0) and less than 2^159 containing at least 64 bits of output from a CSPRNG	-
signatureAlgorithm		One of the following: sha256WithRSAEncryption sha384WithRSAEncryption ecdsa-with-SHA384	-
issuer	countryName	JP	-
	organizationName	Organization name of the CA	-
	commonName	Common name of the CA	-

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	countryName	JP（OV Certificate & EV Certificate）	-
	stateOrProvinceName	Required （OV Certificate & EV Certificate）	-
	localityName	Required （OV Certificate & EV Certificate）	-
	organizationName	Required （OV Certificate & EV Certificate）	-
	organizationalUnitName	Prohibited	-
	jurisdictionCountryName	Required（EV Certificate） JP	
	serialNumber	Required（EV Certificate）	
	businessCategory	Required（EV Certificate）	
	commonName	Optional. 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.	-
subjectPublicKeyInfo		One of the following: RSA2048 bits,3072 bits, 4096 bits,	-

	ECDSA384 bits (secp384r1) , 256 bits (secp256r1)	
Extension Fields	Settings	critical
keyUsage	digitalSignature, (keyEncipherment) * If subjectPublicKeyInfo is RSA, keyEncipherment is optional. For ECDSA, keyEncipherment is prohibited.	y
extKeyUsage	id-kp-serverAuth, id-kp-clientAuth * id-kp-clientAuth is optional.	n
subjectAltName	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 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. The FQDN part of a fully Fully-Qualified Domain Name must consist solely of Domain Labels that are P-Labels or Non-Reserved LDH Labels.	n
certificatePolicies	policyIdentifier ● [1]policyIdentifier=CABF Reserved Certificate Policy Identifier (CABF Reserved Certificate Policy Identifier,	n

	recommended to list Reserved Certificate Policy Identifier as the first value） ● [2]policyIdentifier OID= Set [1.2-1 OID] of this CP（Optional for DV and OV Certificates, required for EV Certificates） policyQualifiers ● policyQualifierID=id-qt-cps ● qualifiier= Repository of the CA HTTP(S) URL（Optional） * policyQualifier is deprecated for DV and OV certificates, and required for EV certificates.	
crlDistributionPoints	HTTP URL for the CRL service of the CA * Optional if id-ad-ocsp accessMethod is present in the Authority Information Access extension.	n
authorityInformationAccess	accessMethod id-ad-ocsp（1.3.6.1.5.5.7.48.1） accessLocation HTTP URL of OCSP responder id-ad-caIssuers (1.3.6.1.5.5.7.48.2) accessLocation HTTP URL of the CA certificate	n
authorityKeyIdentifier	SHA-1 hash value of Authority Public Key (160 bits)	n
subjectKeyIdentifier	Optional SHA-1 hash value of the Subject Public Key (160 bits)	n
Signed Certificate Timestamp List（1.3.6.1.4.1.11129.2.4.2）	Optional Value of SignedCertificateTimestampList	n

Table 7.1-2 OCSP Responder Certificate Profile

Basic Fields		Settings	critical
version		Version 3	-
serialNumber		non - sequential Certificate serial numbers greater than zero (0) and less than 2^159 containing at least 64 bits of output from a CSPRNG	-
signatureAlgorithm		One of the following: sha256WithRSAEncryption sha384WithRSAEncryption ecdsa-with-SHA384	-
issuer	countryName	JP	-
	organizationName	Organization name of the CA	-
	commonName	Common name of the CA	-
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	countryName	JP	-
	organizationName	Organization name of the CA	-
	commonName	OCSP responder name	-
subjectPublicKeyInfo		One of the following: RSA2048 bits, 3072 bits, 4096 bits, ECDSA384 bits (secp384r1), 256 bits (secp256r1)	-
Extension Fields		Settings	critical
keyUsage		digitalSignature	y
extKeyUsage		id-kp-OCSPSigning	n
id-pkix-ocsp-nocheck		NULL	n
certificatePolicies		Prohibited	n
authorityKeyIdentifier		SHA-1 hash value of the Authority Public Key (160 bits)	n

subjectKeyIdentifier	SHA-1 hash value of the Subject Public Key (160 bits)	n

7.1.1 Version Number(s)

The CA applies version 3

7.1.2 Certificate Extension

Certificates issued by the CA use certificate extension fields. 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

The CA uses the Distinguished Name specified in RFC5280.

For every valid Certification Path (as defined by RFC 5280, Section 6):

For each Certificate in the Certification Path, the encoded content of the Issuer Distinguished Name field of a Certificate SHALL be byte-for-byte identical with the encoded form of the Subject Distinguished Name field of the Issuing CA certificate

By issuing the Certificate, the CA represents that it followed the procedure set forth in its Certificate Policy and/or Certification Practice Statement to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate. 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.
The CA will not issue a certificate with a Subject Alternative Name extension or "common name" field that contains a reserved IP address or internal name.
If the "common name" value is a fully qualified domain name or a wildcard domain name, the "common name" value is encoded as a character-for-character copy of the dNSName entry value in the Subject Alternative Name extension. Specifically, all Domain Labels in the FQDN part of a fully qualified domain name or wildcard domain name are encoded as LDH Labels, and P-Labels does not convert to Unicode.

7.1.5 Name Constraints

Not set in the CA.

7.1.6 Certificate Policy Object Identifier

The OID of the certificate issued by the CA is as described in this CP "1.2 Document Name and Identification".
The following Certificate Policy identifiers are reserved for use by CAs as an optional means of assertaing that a Certificate complies with Baseline Requirements.

CABF Reserved Certificate Policy Identifier （CABF reserved Certificate Policy Identifier ）

(1) {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) domain-validated(1)} (2.23.140.1.2.1)
(2) {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)
(3) {joint - iso - itu - t(2) international - organizations(23) ca - browser - forum(140) certificate - policies(1) ev-guidelines(1)} (2.23.140.1.1)

7.1.7 Use of Policy Constraint Extensions

Not set.

7.1.8 Policy Qualifier Syntax and Semantics

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

7.1.9 How to interpret Critical Certificate Policy Extensions

Not set.

7.2 CRL Profile

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

Table 7.2-1 CRL Profile

Basic Fields		Settings	critical
version		Version 2	-
signatureAlgorithm		One of the following: sha256WithRSAEncryption sha384WithRSAEncryption ecdsa-with-SHA384	-
issuer	countryName	JP	-
	organizationName	Organization name of the CA	-
	commonName	Common name of the CA	-
thisUpdate		Issued date and time of CRL	-
nextUpdate		Date and time when the next CRL will be issued. Up to 10 days after thisUpdate.	-
revokedCertificates	serialNumber	Byte-for-bite identical value to the serialNumber included in the revoked certificate	-
	revocationDate	Usually, the date and time the revocation occurred.	-
	crlEntryExtensions reasonCode	Value specified in "7.2.2 CRL Entry Extensions"	-
Extension Fields		Settings	critical
CRLNumber		CRL Number	n
authorityKeyIdentifier		SHA-1 hash value of Authority Public Key (160 bits)	n

7.2.1 Version Number(s)

The CA applies CRL version 2.

7.2.2 CRL Entry Extensions

Use the CRL extension field issued by the CA.

reasonCode (OID 2.5.29.21)

If present, this extension MUST NOT be marked critical.

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

If a CRL entry is for a Subscriber Certificate, this CRL entry extension SHOULD be present, but MAY be omitted, subject to the following requirements.

The CRLReason indicated MUST NOT be unspecified (0). If the reason for revocation is unspecified, CAs MUST omit reasonCode entry extension, if allowed by the previous requirements. If a CRL entry is for a Certificate not subject to Baseline Requirements and was either issued on-or-after 2020-09-30 or has a notBefore on-or-after 2020-09-30, the CRLReason MUST NOT be certificateHold (6). If a CRL entry is for a Certificate subject to Baseline Requirements, the CRLReason MUST NOT be certificateHold (6).

If a reasonCode CRL entry extension is present, the CRLReason MUST indicate the most appropriate reason for revocation of the certificate, as defined by the CA within its CP/CPS.

CRLReason must be included in the reasonCode extension of the CRL entry corresponding to a Subscriber Certificate that is revoked on-or-after July 15, 2023, unless the CRLReason is “unspecified (0)”. Revocation reason code entries for Subscriber Certificates revoked prior to July 15, 2023, do not need to be added or changed.

One of the following CRLReasons may be present in the CRL reasonCode extension for Subscriber Certifificates:

1. keyCompromise (RFC 5280 CRLReason #1): Indicates that it is known or suspected that the Subscriber’s Private Key has been compromised;
2. affiliationChanged (RFC 5280 CRLReason #3): Indicates that the Subject’s name or other Subject Identity Information in the Certificate has changed, but there is no cause to suspect that the Certificate’s Private Key has been compromised;
3. superseded (RFC 5280 CRLReason #4): Indicates that the Certificate is being replaced because: the Subscriber has requested a new Certificate, the CA has reasonable 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, 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;
4. cessationOfOperation (RFC 5280 CRLReason #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;

5. privilegeWithdrawn (RFC 5280 CRLReason #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. Additionally, 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.

Note: Backdating the revocationDate field is an exception to best practice described in RFC 5280 (section 5.3.2); however, these 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.

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

Relevant provisions are stipulated in the CPS.

8.1 Frequency and Circumstances of Assessment

Relevant provisions are stipulated in the CPS.

8.2 Identity/Qualifications of Assessor

Relevant provisions are stipulated in the CPS.

8.3 Assessor's Relationship to Assessed Entity

Relevant provisions are stipulated in the CPS.

8.4 Topics Covered by Assessment

The CA SHALL undergo an audit as appropriate in accordance with the WebTrust Standards below:

- WebTrust for CAs
- WebTrust for CAs SSL Baseline with Network Security
- WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL
- WebTrust Principles and Criteria for Certification Authorities - Network Security

8.5 Actions Taken as a Result of Deficiency

Relevant provisions are stipulated in the CPS.

8.6 Communication of Results

Relevant provisions are stipulated in the CPS.

8.7 Self-Audits

Relevant provisions are stipulated in the CPS.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Fees for Issuing or Renewing Certificates

Stipulated separately in contracts.

9.1.2 Certificate Access Fee

No stipulation.

9.1.3 Expiration or Access Fee for Status Information

No stipulation.

9.1.4 Fees for Other Services

No stipulation.

9.1.5 Refund Policy

Stipulated separately in contracts.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

The CA shall maintain a sufficient financial resources for the operation and maintenance.

The CA SHALL maintain the following insurance related to their respective performance and obligations the EV Guidelines:

A. Commercial General Liability insurance (occurrence form) with policy limits of at least two million US dollars in coverage;

B. Professional Liability/Errors and Omissions insurance, with policy limits of at least five million US dollars in coverage, and including coverage for:

i. claims for damages arising out of an act, error, or omission, unintentional breach of contract, or neglect in issuing or maintaining EV Certificates,

ii. claims for damages arising out of infringement of the proprietary rights of any third party (excluding copyright, and trademark infringement), and invasion of privacy and advertising injury.

Such insurance must be with a company rated no less than A- as to Policy Holder's Rating in the current edition of Best's Insurance Guide (or with an association of companies each of the members of which are so rated).
The CA MAY self-insure for liabilities that arise from such party's performance and obligations under these Guidelines provided that it has at least five hundred million US dollars in liquid assets based on audited financial statements in the past twelve months, and a quick ratio (ratio of liquid assets to current liabilities) of not less than 1.0.

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

This CP includes copyright and is the property of SECOM Trust Systems.
This CP may be reproduced provided that the original document is properly referenced.
It is published under the Creative Commons license Attribution-NoDerivatives (CC-BY-ND) 4.0.

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

9.6 Representations and Warranties

9.6.1 CA 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;

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;
   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;
   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;
   ii. followed the procedure when issuing the Certificate;
   iii. accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;
4. 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. 2;
   ii. followed the procedure when issuing the Certificate;
   iii. accurately described the procedure in the CA's Certificate Policy and/or

Certification Practice Statement;

5. 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;
6. 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
7. 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,
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,
   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 the CA has the following obligations:

- Trust the certificate issued by the 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 the CA's certificate.
- Agree to be responsible as a Relying Party as specified in this CP and CPS when trying to trust and use the CA's certificate.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimer of Warranties

The CA is not liable for any direct, special, incidental or consequential damages arising in connection with the warranties stipulated in this CP, "9.6.1 CA Representations and Warranties" and "9.6.2 RA Representations and Warranties" hereof, or for lost earnings, loss of data, or any other indirect or consequential damages.

9.8 Limitations of Liability

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

- any damage arising from unlawful conduct, unauthorized use, negligence or any other cause not attributable to the CA;
- all liability in any case if the confirmed information error is the result of the applicant's fraud or willful misconduct.
- any damage attributable to the failure of a Subscriber to perform its obligations;
- any damage attributable to 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 the CA;
- any damage incurred in an outage of the normal communication due to reasons not

attributable to the CA;

- any damage arising in connection with the use of a Certificate, including transaction debts;
- any damage caused by the Delegated Third Party's failure to fulfill its service provision obligations, such as the termination of service provision by them;
- any damages attributable to improvement, beyond expectations at this point in time, in hardware or software type of cryptographic algorithm decoding skills;
- any damage attributable to the suspension of the CA's operations due to force majeure, including, but not limited to, natural disasters, earthquakes, volcanic eruptions, fires, tsunami, floods, lightning strikes, wars, civil commotion and terrorism.

9.9 Indemnities

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

9.10 Term and Termination

9.10.1 Term

This CP goes into effect upon approval by this Committee.

9.10.2 Termination

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

9.10.3 Effect of Termination and Survival

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

9.11 Individual Notices and Communications with Participants

The CA provides the necessary notices to the Delegated Third Party, then the Delegated Third Party provides the necessary notice to Subscribers and Relying Parties through its website, e-mail or in other written forms.

9.12 Amendments

9.12.1 Procedure for Amendment

This CP shall be revised by the CA as appropriate and goes into effect upon approval by this Committee.

9.12.2 Notification Method and Timing

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

9.12.3 Circumstances under Which OID Must Be Changed

OID shall be changed if the Certification Service Improvement Committee determines that it is necessary.

9.13 Dispute Resolution Procedures

A party seeking to file a lawsuit, request arbitration or take any other legal action against the CA for the resolution of a dispute relating to a Certificate issued by the CA, said party shall notify the CA to this effect in advance. As regards the location for arbitration and court proceedings, a dispute settlement institution located within Tokyo shall have exclusive jurisdiction.

9.14 Governing Law

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

9.15 Compliance with Applicable Law

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

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

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

9.16.2 Assignment

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

9.16.3 Severability

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

In the event of a conflict between Baseline Requirements and a law, regulation or government order (hereinafter 'Law') of any jurisdiction in which a CA operates or issues certificates, a CA MAY modify any conflicting Baseline Requirement to the minimum extent necessary to make the requirement valid and legal in the jurisdiction. This applies only to operations or certificate issuances that are subject to that Law. In such event, the CA SHALL immediately (and prior to issuing a certificate under the modified requirement) include in Section 9.16.3 of the CA's CPS a detailed reference to the Law requiring a modification of Baseline Requirements under this section, and the specific modification to Baseline Requirements implemented by the CA.

The CA MUST also (prior to issuing a certificate under the modified requirement) notify the CA/Browser Forum of the relevant information newly added to its CPS by sending a message to questions@cabforum.org and receiving confirmation that it has been posted to the Public Mailing List and is indexed in the Public Mail Archives available at https://cabforum.org/pipermail/public/ (or such other email addresses and links as the Forum may designate), so that the CA/Browser Forum may consider possible revisions to Baseline Requirements accordingly.

Any modification to CA practice enabled under this section MUST be discontinued if and when the Law no longer applies, or Baseline Requirements are modified to make it possible to comply with both Baseline Requirements and the Law simultaneously. An appropriate change in practice, modification to the CA's CPS and a notice to the CA/Browser Forum, as outlined above, MUST be made within 90 days.

9.16.4 Enforcement

Disputes regarding this service shall be governed by the Tokyo District Court, and SECOM Trust Systems may request the parties for compensation and attorney's fees for disputes arising from the contractual provisions of the respective regulatory documents, damages, losses and costs related to the parties' actions.

9.16.5 Irresistible Force

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

9.17 Other Provisions

No stipulation