

Security Communication RootCA Subordinate CA Certificate Policy

**January 16, 2023
Version 6.00**

SECOM Trust Systems Co., Ltd.

Security Communication RootCA
Subordinate CA Certificate Policy Ver.6.00

Version History		
Version Number	Date	Description
V1.00	2003.09.29	Publication of the first version
V2.00	2004.11.08	Major version upgrade Separation of the Security Communication RootCA1 Certificate Policy (CP)/Certification Practice Statement (CPS) document into the independent CP and CPS documents, with new publication of the Security Communication RootCA1 CP Revision of the descriptions
V3.00	2006.05.22	"SECOM TrustNet" was renamed to "SECOM Trust Systems" after the merger. "SECOM TrustNet Security Policy Committee" was renamed as "Certification Services Improvement Committee."
V4.00	2009.05.29	Major version upgrade Renaming of "Security Communication RootCA1 CP" to "Security Communication RootCA CP" and addition of the CA Private Key "Security Communication RootCA2"
V4.10	2012.02.15	Addition of "4.6 Certificate Renewal" procedure
V4.20	2012.11.09	Amendment associated with commencement of the OSCP server operations
V4.30	2015.03.20	Addition of the signature algorithm used Revision of the descriptions
V5.00	2016.06.01	Major version upgrade Addition of the CA Private Key "Security Communication RootCA3" Addition of the CA Private Key "Security Communication ECC RootCA1"
V5.10	2017.05.23	Overall revision of the descriptions and styles
V5.11	2018.11.28	Overall revision of the descriptions and styles
V5.12	2019.03.12	Revision of 7.1.2 and 7.1.5
V5.13	2019.05.24	Overall revision of the descriptions and styles
V5.14	2019.09.25	Addition of OID for EV certificate use
V5.15	2020.03.30	Revised chapters and added some "No Stipulation" content
V5.16	2020/09/29	Revised CRL basic area Revised HTTPS notation for lower CA certificate extension certificatePolicies

Security Communication RootCA
Subordinate CA Certificate Policy Ver.6.00

V5.17	2021/05/31	Modification of certificate revocation reasons Addition of special requirements for key compromise
V5.18	2021/11/30	Addition of profile of RootCA certificate Overall revision of the descriptions and styles
V5.19	2022/06/10	Overall revision of the descriptions and styles
V5.20	2022/12/08	"7.1.2 Certificate Extension" Modification of "Table 7.1-2-8 Security Communication ECC RootCA1 Subordinate CA Certificate Extension"
V6.00	2023/01/16	Major version upgrade Addition of the CA Private Key "SECOM TLS RSA Root CA 2023" Addition of the CA Private Key "SECOM RSA Root CA 2023" Addition of the CA Private Key "SECOM Document Signing RSA Root CA 2023"

Table of Contents

1. Introduction.....	1
1.1 Overview	1
1.2 Document Name and Identification.....	1
1.3 PKI Participants.....	2
1.3.1 Certification Authorities	2
1.3.2 Registration Authorities.....	2
1.3.3 Subscribers.....	3
1.3.4 Relying Parties	3
1.3.5 Other Participants.....	3
1.4 Certificate Usage.....	3
1.4.1 Appropriate Certificate Uses	3
1.4.2 Prohibited Certificate Uses.....	3
1.5 Policy Administration	3
1.5.1 Organization Administering the Document	3
1.5.2 Contact Information	4
1.5.3 Person Determining CP Suitability for the Policy	4
1.5.4 Approval Procedure	4
1.6 Definitions and Acronyms.....	4
2. Publication and Repository Responsibilities.....	9
2.1 Repository	9
2.2 Publication of Certificate Information.....	9
2.3 Time or Frequency of Publication	9
2.4 Access Controls on Repositories	9
3. Identification and Authentication.....	10
3.1 Naming.....	10
3.1.1 Types of Names	10
3.1.2 Need for Names to Be Meaningful	10
3.1.3 Anonymity or Pseudonymity of Subscribers.....	10
3.1.4 Rules for Interpreting Various Name Forms.....	10
3.1.5 Uniqueness of Names	10
3.1.6 Recognition, Authentication, and Roles of Trademarks	10
3.2 Initial Identity Validation.....	10
3.2.1 Method to Prove Possession of Private Key.....	10
3.2.2 Authentication of Organization Identity.....	11
3.2.2.1 Identity	11
3.2.2.2 DBA/Tradename.....	11
3.2.2.3 Verification of Country	12
3.2.3 Authentication of Individual Identity	12

3.2.4 Non-Verified Subscriber Information.....	12
3.2.5 Validation of Authority.....	12
3.2.6 Criteria for Interoperation.....	12
3.3 Identification and Authentication for Re-Key Requests.....	12
3.3.1 Identification and Authentication for Routine Re-Key.....	13
3.3.2 Identification and Authentication for Re-Key after Revocation.....	13
3.4 Identification and Authentication for Revocation Requests	13
4. Certificate Life-Cycle Operational Requirements	14
4.1 Certificate Application	14
4.1.1 Who Can Submit a Certificate Application.....	14
4.1.2 Enrollment Process and Responsibilities.....	14
4.2 Certificate Application Processing	14
4.2.1 Performing Identification and Authentication Functions	14
4.2.2 Approval or Rejection of Certificate Applications	15
4.2.3 Time to Process Certificate Applications	15
4.3 Certificate Issuance.....	15
4.3.1 CAActions during Certificate Issuance	15
4.3.2 Notifications to Subscriber of Certificate Issuance.....	15
4.4 Certificate Acceptance.....	16
4.4.1 Conduct Constituting Certificate Acceptance.....	16
4.4.2 Publication of the Certificate by the CA	16
4.4.3 Notification of Certificate Issuance by the CA to Other Entities.....	16
4.5 Key Pair and Certificate Usage.....	16
4.5.1 Subscriber Private Key and Certificate Usage.....	16
4.5.2 Relying Party Public Key and Certificate Usage	16
4.6 Certificate Renewal.....	16
4.6.1 Circumstances for Certificate Renewal	16
4.6.2 Who May Request Renewal	16
4.6.3 Processing Certificate Renewal Requests.....	17
4.6.4 Notification of New Certificate Issuance to Subscriber.....	17
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate.....	17
4.6.6 Publication of the Renewal Certificates by the CA.....	17
4.6.7 Notification of Certificate Issuance by the CA to Other Entities.....	17
4.7 Certificate Re-Key	17
4.7.1 Circumstances for Certificate Re-Key.....	17
4.7.2 Who May Request Certification of a New Public Key.....	17
4.7.3 Processing Certificate Re-Keying Requests.....	17
4.7.4 Notification of New Certificate Issuance to Subscriber.....	17
4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate	17
4.7.6 Publication of the Re-Keyed Certificate by the CA.....	17

4.7.7 Notification of Certificate Issuance by the CA to Other Entities.....	18
4.8 Certificate Modification	18
4.8.1 Circumstances for Certificate Modification	18
4.8.2 Who May Request Certificate Modification.....	18
4.8.3 Processing Certificate Modification Requests	18
4.8.4 Notification of New Certificate Issuance to Subscriber.....	18
4.8.5 Conduct Constituting Acceptance of Modified Certificate.....	18
4.8.6 Publication of the Modified Certificate by the CA	18
4.8.7 Notification of Certificate Issuance by the CA to Other Entities.....	18
4.9 Certificate Revocation and Suspension	18
4.9.1 Circumstances for Certificate Revocation	18
4.9.2 Who Can Request Revocation.....	21
4.9.3 Procedure for Revocation Request.....	21
4.9.4 Revocation Request Grace Period.....	21
4.9.5 Time within Which CA Shall Process the Revocation Request.....	21
4.9.6 Revocation Checking Requirements for Relying Parties.....	22
4.9.7 CRL Issuance Frequency	22
4.9.8 Maximum Latency for CRLs.....	22
4.9.9 On-Line Revocation/Status Checking Availability	22
4.9.10 On-Line Revocation/Status Checking Requirements.....	23
4.9.11 Other Forms of Revocation Advertisements Available.....	24
4.9.12 Special Requirements Regarding Key Compromise	24
4.9.13 Circumstances for Suspension.....	25
4.9.14 Who Can Request Suspension	25
4.9.15 Procedure for Suspension Request.....	25
4.9.16 Limits on Suspension Period	25
4.10 Certificate Status Services	25
4.10.1 Operational Characteristics.....	25
4.10.2 Service Availability	25
4.10.3 Optional Features.....	25
4.11 End of Subscription (Registry)	25
4.12 Key Escrow and Recovery.....	26
4.12.1 Key Escrow and Recovery Policy and Practices	26
4.12.2 Session Key Encapsulation and Recovery Policy and Practices	26
5. Facility, Management, and Operational Controls	27
5.1 Physical Controls.....	27
5.1.1 Site Location and Construction	27
5.1.2 Physical Access	27
5.1.3 Power and Air Conditioning.....	27
5.1.4 Water Exposures.....	27

5.1.5 Fire Prevention and Protection	27
5.1.6 Media Storage	27
5.1.7 Waste Disposal.....	27
5.1.8 Off-Site Backup.....	27
5.2 Procedural Controls	27
5.2.1 Trusted Roles	27
5.2.2 Number of Persons Required per Task	27
5.2.3 Identification and Authentication for Each Role.....	27
5.2.4 Roles Requiring Separation of Duties.....	28
5.3 Personnel Controls	28
5.3.1 Qualifications, Experience, and Clearance Requirements	28
5.3.2 Background Check Procedures	28
5.3.3 Training Requirements	28
5.3.4 Retraining Frequency and Requirements	28
5.3.5 Job Rotation Frequency and Sequence	28
5.3.6 Sanctions for Unauthorized Actions.....	28
5.3.7 Independent Contractor Requirement.....	28
5.3.8 Documentation Supplied to Personnel.....	28
5.4 Audit Logging Procedures.....	28
5.4.1Types of Events Recorded	28
5.4.2 Frequency of Processing Audit Log	28
5.4.3 Retention Period for Audit Log.....	28
5.4.4 Protection of Audit Log.....	29
5.4.5 Audit Log Backup Procedure	29
5.4.6 Audit Log Collection System.....	29
5.4.7 Notification to Event-Causing Subject.....	29
5.4.8 Vulnerability Assessments.....	29
5.5 Records Archival.....	29
5.5.1 Types of Records Archived	29
5.5.2 Retention Period for Archive.....	29
5.5.3 Protection of Archive	29
5.5.4 Archive Backup Procedures	29
5.5.5 Requirements for Time-Stamping of Records.....	29
5.5.6 Archive Collection System	29
5.5.7 Procedures to Obtain and Verify Archive Information	29
5.6 Key Changeover	30
5.7 Compromise and Disaster Recovery	30
5.7.1 Incident and Compromise Handling Procedures	30
5.7.2 Hardware, Software, and/or Data are Corrupted	30
5.7.3 Entity Private Key Compromise Procedures.....	30

5.7.4 Business Continuity Capabilities after a Disaster	30
5.8 CA or RA Termination.....	30
6. Technical Security Controls	31
6.1 Key Pair Generation and Installation	31
6.1.1 Key Pair Generation.....	31
6.1.2 Private Key Delivery to Subscriber	31
6.1.3 Public Key Delivery to Certificate Issuer	31
6.1.4 CA Public Key Delivery to Relying Parties.....	31
6.1.5 Key Sizes	31
6.1.6 Public Key Parameters Generation and Quality Checking.....	31
6.1.7 Key Usage Purposes	31
6.2 Private Key Protection and Cryptographic Module Engineering Controls	31
6.2.1 Cryptographic Module Standards and Controls	31
6.2.2 Private Key Multi-Person Control.....	31
6.2.3 Private Key Escrow	31
6.2.4 Private Key Backup.....	31
6.2.5 Private Key Archive.....	31
6.2.6 Private Key Transfer into or from a Cryptographic Module	32
6.2.7 Private Key Storage on Cryptographic Module.....	32
6.2.8 Method of Activating Private Key	32
6.2.9 Method of Deactivating Private Key	32
6.2.10 Method of Destroying Private Key	32
6.2.11 Cryptographic Module Rating.....	32
6.3 Other Aspects of Key Pair Management	32
6.3.1 Public Key Archival	32
6.3.2 Certificate Operational Periods and Key Pair Usage Periods	32
6.4 Activation Data.....	32
6.4.1 Activation Data Generation and Installation.....	32
6.4.2 Activation Data Protection.....	32
6.4.3 Other Aspects of Activation Data	32
6.5 Computer Security Controls.....	33
6.5.1 Specific Computer Security Technical Requirements	33
6.5.2 Computer Security Rating	33
6.6 Life-Cycle Technical Controls	33
6.6.1 System Development Controls.....	33
6.6.2 Security Management Controls.....	33
6.6.3 Life-Cycle Security Controls	33
6.7 Network Security Controls	33
6.8 Time-Stamping	33
7. Certificate, CRL, and OCSP Profiles.....	34

7.1 Certificate Profile	34
7.1.1 Version Number(s)	42
7.1.2 Certificate Extensions	42
7.1.3 Algorithm Object Identifiers	56
7.1.5 Name Constraints	58
7.1.6 Certificate Policy Object Identifier	59
7.1.7 Usage of Policy Constraints Extension	60
7.1.8 Policy Qualifiers Syntax and Semantics	60
7.1.9 Processing Semantics for the Critical Certificate Policies Extension	60
7.2 CRL Profile	61
7.2.1 Version Number(s)	61
7.2.2 CRL and CRL Entry Extensions	61
7.3 OCSP Profile	62
7.3.1 Version Number(s)	62
7.3.2 OCSP Extensions	62
8 Compliance Audit and Other Assessments	63
8.1 Frequency and Circumstances of Assessment	63
8.2 Identity/Qualifications of Assessor	63
8.3 Assessor's Relationship to Assessed Entity	63
8.4 Topics Covered by Assessment	63
8.5 Actions Taken as a Result of Deficiency	63
8.6 Communication of Results	63
8.7 Self-Audit	63
9. Other Business and Legal Matters	64
9.1 Fees	64
9.1.1 Certificate Issuance or Renewal Fees	64
9.1.2 Certificate Access Fees	64
9.1.3 Revocation or Status Information Access Fees	64
9.1.4 Fees for Other Services	64
9.1.5 Refund Policy	64
9.2 Financial Responsibility	64
9.2.1 Insurance Coverage	64
9.2.2 Other Assets	64
9.2.3 Insurance or Warranty Coverage for End-Entities	64
9.3 Confidentiality of Business Information	64
9.3.1 Scope of Confidential Information	64
9.3.2 Information Not Within the Scope of Confidential Information	65
9.3.3 Responsibility to Protect Confidential Information	65
9.4 Privacy of Personal Information	65
9.4.1 Personal Information Protection Plan	65

9.4.2 Information Treated as Personal Information.....	65
9.4.3 Information that is not considered Personal Information.....	66
9.4.4 Responsibility for protecting Personal Information.....	66
9.4.5 Notice and Consent regarding use of Personal Information	66
9.4.6 Disclosure of Information with Judicial or Administrative Procedures	66
9.4.7 Other Information Disclosure Conditions	66
9.5 Intellectual Property Rights.....	66
9.6 Representations and Warranties	67
9.6.1 CA Representations and Warranties.....	67
9.6.2 RA Representations and Warranties.....	69
9.6.3 Subscriber Representations and Warranties.....	69
9.6.4 Relying Party Representations and Warranties	71
9.6.5 Representations and Warranties of Other Participants	71
9.7 Disclaimers of Warranties	71
9.8 Limitations of Liability	71
9.9 Indemnities.....	72
9.10 Term and Termination	72
9.10.1 Term.....	72
9.10.2 Termination.....	72
9.10.3 Effect of Termination and Survival.....	72
9.11 Individual Notices and Communications with Participants	72
9.12 Amendments	73
9.12.1 Procedure for Amendment	73
9.12.2 Notification Mechanism and Period.....	73
9.12.3 Circumstances under Which OID Must Be Changed	73
9.13 Dispute Resolution Provisions	73
9.14 Governing Law	73
9.15 Compliance with Applicable Law	74
9.16 Miscellaneous Provisions.....	74
9.16.1 Entire Agreement	74
9.16.2 Assignment.....	74
9.16.3 Severability	74
9.16.4 Enforcement.....	75
9.16.5 Force Majeure	75
9.17 Other Provisions.....	75

1. Introduction

1.1 Overview

Security Communication RootCA Subordinate CA Certificate Policy (hereinafter, "this CP") is a document that defines operational policies for the subordinate CA certificates (hereinafter, "Certificates") issued by Security Communication RootCA1, Security Communication RootCA2, Security Communication RootCA3, Security Communication ECC RootCA1, SECOM TLS RSA Root CA 2023, SECOM RSA Root CA 2023 as well as SECOM Document Signing RSA Root CA 2023 (hereinafter collectively, "the CAs") that are all operated by SECOM Trust Systems Co., Ltd. (hereinafter, "SECOM"), by specifying the purpose of use, the scope of application and the user procedures for the Certificates. Various procedures regarding the operation and maintenance of the CAs are stipulated in the Security Communication RootCA Certification Practice Statement (hereinafter, "CPS").

SECOM provides the certification services as the CAs, including the CA key administration as well as issuance/revocation of Certificates (hereinafter, "the Services"). The Certificates issued by the CAs prove and certify the unique correspondence between the subjects of the issuance and their public keys.

The CAs conform to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, Guidelines for the Issuance and Management of Extended Validation Certificates, Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates (hereinafter, Baseline Requirements) defined by CA/Browser Forum provisions disclosed at <https://www.cabforum.org/>.

Any provisions in this CP inconsistent with the CPS shall prevail and any provisions in a separate agreement or the like between the subscribers and SECOM inconsistent with this CP or the CPS shall prevail. In the event of any inconsistency between this CP and Baseline Requirements, Baseline Requirements take precedence over this CP.

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

This CPS conforms to the RFC3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" advocated by the IETF as a CA practice framework.

1.2 Document Name and Identification

The official name of this CP is "Security Communication RootCA Subordinate CA Certificate Policy". SECOM, which is the provider and operational body of the Services,

uses the Object Identifier (hereinafter, "OID") assigned by ISO, given in the Table "1.2-1 OID (SECOM)" below.

Table 1.2-1 OID (SECOM)

Name of organization	OID
SECOM Trust Systems Co., Ltd.	1.2.392.200091

This CP is identified with the Object Identifier (hereinafter, "OID") given in "Table 1.2-2 OID (This CP)"

Table 1.2-2 OID (This CP)

CP	OID
Security Communication RootCA1	1.2.392.200091.100.901.1
Security Communication RootCA2	1.2.392.200091.100.901.4
Security Communication RootCA3	1.2.392.200091.100.901.6
Security Communication ECC RootCA1	1.2.392.200091.100.902.1
SECOM TLS RSA Root CA 2023	1.2.392.200091.100.901.8
SECOM RSA Root CA 2023	1.2.392.200091.100.901.9
SECOM Document Signing RSA Root CA 2023	1.2.392.200091.100.901.10

The OID of the CPS associated with this CP is given in Table 1.2-3 OID (The CPS)

Table 1.2-3 OID (The CPS)

CPS	OID
Security Communication RootCA Certification Practice Statement	1.2.392.200091.100.901.3

1.3 PKI Participants

1.3.1 Certification Authorities

A CA mainly issues or revokes Certificates, publishes CRLs (Certificate Revocation Lists), and stores and provides information on Certificate status using the OCSP responder.

CA is defined in this CP "1.6 Definitions and Acronyms".

1.3.2 Registration Authorities

An RA mainly performs identification, authentication, as well as assessment of the

operation rules of the subscriber organizations or institutions when such a Certificate request as issuance or revocation is submitted.

1.3.3 Subscribers

Subscribers are organizations or institutions that generate Key Pairs in their own rights, to which Certificates are issued by the CAs. They are qualified as Subscribers upon accepting the issued Certificates after submitting the Certificate applications to the CAs. Subscribers must assess this CP and the CPS in light of their usage purposes, and agree thereto.

1.3.4 Relying Parties

Relying Parties are the entities that authenticate the validity of Certificates issued by the CAs. Relying Parties are assumed to be performing the authentication and placing trust upon confirming and agreeing to the contents of this CP and the CPS in light of the Relying Parties' own purposes of use.

Relying parties and application software suppliers are defined in this CP "1.6 Definitions and Acronyms".

1.3.5 Other Participants

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 CAs are the Certification Authorities functioning as top of the Subordinate CAs and issue Subordinate CA Certificates as Subscriber Certificates. Relying Parties that trust and use the Certificates may authenticate the reliability of such Certificates using the CA public key Certificates.

1.4.2 Prohibited Certificate Uses

Certificates issued by the CAs may not be used for purposes other than those set forth in this CP.

1.5 Policy Administration

1.5.1 Organization Administering the Document

This CP is maintained and administered by SECOM.

1.5.2 Contact Information

Inquiries concerning this CP should be directed to:

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

The Subscribers, Relying Parties, Application Software Suppliers, and other third parties can report suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates.

The CAs revoke certificates when it is determined that it needs to be revoked.

1.5.3 Person Determining CP Suitability for the Policy

Suitability of this CP as the CAs' practice policy is determined by SECOM's Certification Services Improvement Committee.

This CP will be reviewed and revised at least annually.

1.5.4 Approval Procedure

This CP shall be published in the repository as developed and revised under approval of the SECOM Certification Services Improvement Committee.

1.6 Definitions and Acronyms

Application Software Supplier

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

Attestation Letter

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

Audit Log

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

Baseline Requirements

A document in which the CA/Browser Forum sets out the basic requirements for

issuing and managing certificates.

CA

CA stands for Certification Authority, an entity that mainly issues, renews and revokes Certificates, generates and protects CA Private Keys, and registers Subscribers.

CA/Browser Forum

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

Certificate

The word "Certificate" is simply used to indicate a digital certificate in this CP which is the electronic data certifying that a public key is owned by the party specified therein. The validity of a Certificate is certified by the digital signature of the relevant CA affixed thereto.

Certification Services Improvement Committee

The decision making body for the operational policy of the Services, including administration of this CP and modification reviews.

CP

CP stands for Certificate Policy, a document that sets forth the policy regarding the Certificates.

CPS

CPS stands for Certification Practice Statement, which sets forth provisions to be followed in providing and subscribing to the Services, including applications of digital Certificates, application reviews, and issuance/revocation/storage/publication of Certificates by the CAs.

CRL

CRL stands for Certificate Revocation List, which records the list of Certificates revoked by the CAs.

CSR

CSR stands for Certificate Signing Request, a data file on which the digital certificate issuance is based. A CSR contains the public key of the entity requesting the Certificate signing, to which the issuer's digital signature is affixed upon the issuance thereof.

Digital Signature/Signing

A digital data to prove that a specific individual is the author of a specific digital documentation. It is a signature representing that the reliability of the information contained in such documentation is certified by the author.

Escrow

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

Key Pair

A Key Pair consists of a private key and a public key in the public key cryptosystem.

Major Version Number

A number to be given to a revision of this CP (e.g., the underlined digit [1] of Version 1.02) whose magnitude of the amendment(s) thereof is considered to have an obvious impact on the use of the Certificates and the CRLs by Subscribers and Relying Parties.

Minor Version Number

A number to be given to a revision of this CP (e.g., the underlined digit [02] of Version 1.02) whose magnitude of the amendment(s) thereof is considered to have no or less impact on the use of the Certificates and the CRLs by Subscribers and Relying Parties.

OCSP (Online Certificate Status Protocol)

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

OID

OID stands for Object IDentifier. OIDs are registered in the registration institutions (ISO and ITU) as globally unique IDs. The IDs registered as OIDs are used for such parameters as algorithms used in the PKI, types (attributes like [Country name]) of the names (subject) to be included in the digital Certificates.

PKI (Public Key Infrastructure)

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

Private Key

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

Public Key

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

RA

RA stands for Registration Authority, an entity that conducts qualifications (identification and authentication) among the CA operations in the Services.

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

The storage for such data as Certificates issued by the CAs. The Repository is a mechanism to allow access by the users or applications to the Certificates from any point in the network. CRLs as well as this CP are also stored in the Repository.

RFC3647 (Request for Comments 3647)

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

Root CA

The Root CA described in this CP is an institute owned and run by SECOM as a Root CA that issues the subordinate CA Certificates and functions as top of the subordinate CAs.

RSA

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

SHA-1 (Secure Hash Algorithm 1)

A hash function used in digital 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-2

A Secure Hash Algorithm family function used in digital signing and the improved

version of SHA-1. The size of the SHA-256 and SHA-384 described in this CP are respectively 256 and 384 bits. The algorithm works to detect any alterations in the original message during the transmission by comparing the hash values transmitted and received.

Subordinate CA

A CA trusted and signed by the CAs.

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.

X.500

X.500 is a series of directory standards that was developed by ITU-T in order to provide a range of services from the name and address lookup to the query by attribute value. The X.500 Distinguished Names (DN) will be used for the names of the X.509 Issuers and Subjects.

X.509

The Certificate and CRL formats set forth by X.509 ITU-T. With [X.509 v3 (Version 3)], extension fields were additionally defined for storage of optional data.

2. Publication and Repository Responsibilities

2.1 Repository

Stipulated in the CPS.

2.2 Publication of Certificate Information

Stipulated in the CPS.

2.3 Time or Frequency of Publication

Stipulated in the CPS.

2.4 Access Controls on Repositories

Stipulated in the CPS.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

The certificate issued by the CAs 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 and this CP "7.1.4 Name Forms"

3.1.2 Need for Names to Be Meaningful

The Distinguished Names assigned to Subscribers shall be meaningful, and the Subjects' names specified in Certificates shall have association with the organizations or the institutions to an appropriate extent. Subscribers shall not submit Certificate applications with third parties' trademarks or associated names to the CAs.

3.1.3 Anonymity or Pseudonymity of Subscribers

No anonym nor pseudonym shall be used as Subject names specified in Certificates.

3.1.4 Rules for Interpreting Various Name Forms

DNs are interpreted as defined in the CP "3.1.1 Types of Names" and "3.1.2 Need for Names to Be Meaningful" hereof.

3.1.5 Uniqueness of Names

The CAs ensure that the owner of the certificate can be uniquely identified by the issued certificate, based on the information contained in the Subject's Distinguished Name (DN).

3.1.6 Recognition, Authentication, and Roles of Trademarks

Rights to use the trademarks shall be reserved by the trademark owners. The CAs may, as necessary, require the trademark owners to present such official documentation as the submission for the trademark.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The signature on the relevant CSR made by a Subscriber is authenticated to prove that such CSR is signed with the Private Key corresponding to the Public Key contained therein. In addition, the fingerprint of the CSR is inspected to identify the Public Key owner.

3.2.2 Authentication of Organization Identity

The applicant shall provide the CAs with the following information in submitting a Certificate Application:

- Certificate Application Form;
- Records or information to prove the (legal) existence of the organization or institution;
- CSR; and
- Other documentation required by SECOM.

The CAs use the provided information to make sure that there is no inaccuracy or missing information in the application.

3.2.2.1 Identity

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

1. A government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;
2. A third party database that is periodically updated and considered a Reliable Data Source;
3. A site visit by the CA or a third party who is acting as an agent for the CA; or
4. An Attestation Letter.

The CAs 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 CAs shall verify the Applicant's right to use the DBA/tradename using at least one of the following:

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

3.2.2.3 Verification of Country

If the subject:countryName field is present, then the CAs shall verify the country associated with the Subject using one of the following:

- Information provided by the Domain Name Registrar; or
- A method identified in this CP "3.2.2.1 Identity".

3.2.3 Authentication of Individual Identity

The CAs will not issue Certificates to individuals.

3.2.4 Non-Verified Subscriber Information

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

3.2.5 Validation of Authority

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

The CAs may use the sources listed in "3.2.2.1 Identity" to verify the Reliable Method of Communication. Provided that the CAs use a Reliable Method of Communication, the CAs 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 CAs deem appropriate.

In addition, the CAs shall establish a process that allows an Applicant to specify the individuals who may request Certificates. If an Applicant specifies, in writing, the individuals who may request a Certificate, then the CAs shall NOT accept any certificate requests that are outside this specification. The CAs shall provide an Applicant with a list of its authorized certificate requesters upon the Applicant's verified written request.

3.2.6 Criteria for Interoperation

The CAs issue a unilateral cross-certificate to the CAs identified and authenticated by this CAs based on this CP.

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

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

The procedure set forth in this CP "3.2 Initial Identity Validation" hereof shall be followed.

3.3.2 Identification and Authentication for Re-Key after Revocation

The procedure set forth in this CP "3.2 Initial Identity Validation" hereof shall be followed.

3.4 Identification and Authentication for Revocation Requests

When a Certificate revocation request is accepted, legitimacy of the request is authenticated by the CAs based on the submitted Subscriber information.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

A Certificate Application can be submitted by representatives, employees or agents of the applicant organizations or institutions.

In accordance with this CP "5.5.2 Retention Period for Archive", the CAs 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 CAs shall use this information to identify subsequent suspicious certificate requests.

4.1.2 Enrollment Process and Responsibilities

Prior to the issuance of a Certificate, the CAs shall obtain the following documentation from the Applicant:

1. A certificate request, which may be electronic; and
2. An executed Subscriber Agreement or Terms of Use, which may be electronic.

The CAs should obtain any additional documentation the CAs determine necessary to meet these Requirements.

Prior to the issuance of a Certificate, the CAs shall obtain from the Applicant a certificate request in a form prescribed by the CAs and that complies with these Requirements. One certificate request may suffice for multiple Certificates to be issued to the same Applicant, subject to the aging and updating requirement of this CP "4.2.1 Performing Identification and Authentication Functions", provided that each Certificate is supported by a valid, current certificate request signed by the appropriate Applicant Representative on behalf of the Applicant. The certificate request may be made, submitted and/or signed electronically.

The certificate request must contain a request from, or on behalf of, the Applicant for the issuance of a Certificate, and a certification by, or on behalf of, the Applicant that all of the information contained therein is correct.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Accepting the applications by the Subscribers, the documentary submissions as well as the CSR are authenticated by the CAs in accordance with "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 CAs

to obtain from the Applicant in order to comply with these 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 CAs 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 CAs shall establish and follow a documented procedure for verifying all data requested for inclusion in the Certificate by the Applicant.

The CAs and subordinate CAs 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 these Requirements.

4.2.2 Approval or Rejection of Certificate Applications

The CAs decide approval or rejection of the Certificate Applications according to the prescribed authentication procedure for the Subscribers' submissions, and notify the Subscribers of the results thereof.

4.2.3 Time to Process Certificate Applications

The CAs promptly issue Certificates once the CSRs submitted by the Subscribers are approved.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

The CAs issue Certificates containing the CA Private Key signature for the Public Key of the CSR submitted by the Subscriber conforming to "7.1 Certificate Profile" hereof.

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

This 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 CAs.

4.3.2 Notifications to Subscriber of Certificate Issuance

After completing the issuance of Certificates for approved Certificate Applications, the CAs store the issued Certificates on external memory media, seal them together with the receipts, and then personally deliver or just send them to the Subscribers.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Subscribers must send the receipts to the CAs upon confirming how the Certificate is populated and no deficiency therein, while the CAs assume the Certificate Acceptance is complete upon receiving such receipts. Subscribers must promptly notify the CAs if any deficiency is found in how the Certificate is populated. Any claims thereon must be made within fourteen (14) days of the date the Certificate is sent.

4.4.2 Publication of the Certificate by the CA

The CA certificate of this CAs will be published in the repository. The Subordinate CA may publish the certificates of the Certificate Subscribers by registering them in the CT (Certificate Transparency) log.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

The CAs will not issue Certificates to individuals.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

The usage of Certificates issued by the CAs and Private Keys possessed by Subscribers is restricted to those specified for the services and products provided by the Subscribers of the CAs having contractual relationship with SECOM. Certificates issued by the CAs shall not be used otherwise.

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 and authenticating the Certificates issued by the CAs.

4.6 Certificate Renewal

4.6.1 Circumstances for Certificate Renewal

Certificate Renewal means to issue a new Certificate for continuous use of the Certificate with the same DN and without renewal of the Key Pair.

A Certificate may be renewed when it is about to expire and if the cryptographic algorithm used for the Key is confirmed by SECOM to be secure as of the renewal.

4.6.2 Who May Request Renewal

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

4.6.3 Processing Certificate Renewal Requests

The provisions of "4.2 Certificate Application Processing" hereof shall apply.

4.6.4 Notification of New Certificate Issuance to Subscriber

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

4.6.6 Publication of the Renewal Certificates by the CA

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

4.7.3 Processing Certificate Re-Keying Requests

The provisions of "4.2 Certificate Application Processing" hereof shall apply.

4.7.4 Notification of New Certificate Issuance to Subscriber

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

4.8 Certificate Modification

4.8.1 Circumstances for Certificate Modification

If any of the descriptions in a Certificate has to be modified, the Subscriber must promptly submit a Certificate Modification application. The procedure for reissuing a certificate due to a change is performed according to the procedure at the time of initial issuance. The certificate before the change will be revoked at the discretion of the CAs.

4.8.2 Who May Request Certificate Modification

The provisions of "4.9.2 Who Can Request Revocation" and "4.1.1 Who Can Submit a Certificate Application" hereof shall apply.

4.8.3 Processing Certificate Modification Requests

The provisions of "4.9.3 Procedure for Revocation Request" and "4.2 Certificate Application Processing" hereof shall apply.

4.8.4 Notification of New Certificate Issuance to Subscriber

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

4.8.5 Conduct Constituting Acceptance of Modified Certificate

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

4.8.6 Publication of the Modified Certificate by the CA

The provisions of "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 "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

Subscribers may request a Certificate Revocation based on their own decisions,

provided that they must always request the revocation to the CAs in any of the following cases:

- There has been a change in information populated in the Certificate;
- The Private Key has or may have been compromised or no longer reliable for any reason, including the theft, loss, unauthorized disclosure or unauthorized use thereof;
- The Private Key has or may have been compromised to have lost the privacy or confidentiality;
- The Certificate is incorrectly populated or not being used for authorized purposes; or
- The use of the Certificate is being terminated.

The CAs may revoke the Certificate with or without the Subscriber's revocation request when the CAs are aware of the following situations:

- The Subscriber is not performing the obligations thereof under this CP, the CPS, relevant agreements or laws;
- SECOM terminates the Services;
- The CA determined that the Subscriber's and the CA's Private Key have or could have been compromised; or
- The CAs recognize any other situation deemed to necessitate revocation.

The Subordinate CA shall revoke the Subscriber Certificate issued under Baseline Requirements within 24 hours if one or more of the following occurs:

1. The Subscriber requests in writing that the subordinate CA revoke the Subscriber Certificate;
2. The Subscriber notifies the Subordinate CA that the original certificate request was not authorized and does not retroactively grant authorization;
3. The Subordinate CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise;
4. The Subordinate 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>);
5. The Subordinate 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.

The Subordinate CA should revoke a Subscriber Certificate issued under Baseline Requirements within 24 hours and must revoke them within 5 days if one or more of the following occurs:

1. The certificate no longer complies with the requirements of this CP "6.1.5 Key Sizes" and this CP "6.1.6 Public Key Parameters Generation and Quality

Checking";

2. The Subordinate CA obtains evidence that the Certificate was misused;
3. The Subordinate CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;
4. The Subordinate CA is made aware of any circumstance indicating that the use of a Fully Qualified Domain Name or IP address in the Subscriber 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);
5. The CAs made aware that a Wildcard Certificate has been used to authenticate a fraudulent misleading subordinate Fully Qualified Domain Name;
6. The Subordinate CA is made aware of a material change in the information contained in the Subscriber Certificate;
7. The Subordinate CA is made aware that the Certificate was not issued in accordance with Baseline Requirements or the Subordinate CA's CP or CPS;
8. The Subordinate CA determines or is made aware that any of the information appearing in the Subscriber Certificate is inaccurate;
9. The Subordinate CA's right to issue a Subscriber Certificate under Baseline Requirements expires, or is revoked, or terminated, unless the Subordinate CA has made arrangements to continue maintaining the CRL/OCSP repository;
10. Revocation is required by this CP or CPS of the Subordinate CA; or
11. The Subordinate 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.

The CAs shall revoke a Subordinate CA Certificate issued under Baseline Requirements within 7 days if one or more of the following occurs:

1. The Subordinate CA requests revocation in writing;
2. The Subordinate CA notifies the Issuing CA that the original certificate request was not authorized and does not retroactively grant authorization;
3. The Issuing CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of this CP "6.1.5 Key Sizes" and the requirements of this CP "6.1.6 Public Key Parameters Generation and Quality Checking" ;
4. The Issuing CA obtains evidence that the Certificate was misused;
5. The Issuing CA is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with Baseline Requirements or

applicable CP or CPS;

6. The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
7. The Issuing CA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
8. The Issuing CA's or Subordinate CA's right to issue Certificates under Baseline Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository; or
9. Revocation is required by the Issuing CA's Certificate Policy and/or Certification Practice Statement.

4.9.2 Who Can Request Revocation

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

Certificate Revocation Request shall be submitted by sending (post-mailing) the information required for the revocation to the CAs. However, e-mail submission is allowed in an emergency or when the said submission option is not available.

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

The CAs shall provide Subscribers, Relying Parties, Application Software Suppliers, and other third parties with clear instructions for reporting suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates. The CAs shall publicly disclose the instructions through a readily accessible online means and this CP "1.5.2 Contact Information".

4.9.4 Revocation Request Grace Period

Revocation Requests due to other than Private Key compromise shall be submitted to the CAs five (5) operational days prior to the desired revocation date. However, should a Subscriber determine that a Private Key has or could have been compromised, the Subscriber must promptly make a revocation request after identifying the compromise.

4.9.5 Time within Which CA Shall Process the Revocation Request

Within 24 hours after receiving a Certificate Problem Report, the CAs 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 CAs 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 CAs 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 this CP, Section 4.9.1. "Circumstances for Certificate Revocation". The date selected by the CAs 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 CAs receive an application for revocation with a specified revocation date, it will revoke on the specified date.

4.9.6 Revocation Checking Requirements for Relying Parties

Before placing trust and using a Certificate issued by the CAs, Relying Parties must confirm that the Certificate has not been revoked by checking the CRLs or the OCSP server.

4.9.7 CRL Issuance Frequency

The CAs shall update and reissue CRLs at least

- i. once every twelve months and
- ii. within 24 hours after revoking a Subordinate CA Certificate.

The value of the nextUpdate field must not be more than twelve months beyond the value of the thisUpdate field.

4.9.8 Maximum Latency for CRLs

A new CRL is promptly issued upon issuance or revocation of a Certificate and is published in the Repository.

4.9.9 On-Line Revocation/Status Checking Availability

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

1. Be signed by the CAs that issued the Certificates whose revocation status is being checked, or

2. Be signed by an OCSRP Responder whose Certificate is signed by the CAs that issued the Certificate whose revocation status is being checked.

In the latter case, the OCSRP 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

Before placing trust and using a Certificate issued by the CAs, Relying Parties must confirm the validity of the Certificate. If registered revocation is not confirmed with the CRL in the Repository, the Certificate Status provided through the OCSRP server shall be checked.

OCSRP responders operated by the CAs shall support the HTTP GETmethod, as described in RFC 6960 and/or RFC 5019.

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

For the status of Subordinate CA Certificates:

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

- i. at least every twelve months; and
- ii. within 24 hours after revoking a Subordinate CA Certificate.

If the OCSRP 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 OCSRP 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 CAs should monitor the OCSRP 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 three options:

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

4.9.11 Other Forms of Revocation Advertisements Available

The CAs can distribute OCSP responses using stapling in accordance with RFC 4366, RFC 5246, and RFC 8446.

In this case, the CAs ensure that the subscriber includes the OCSP response of the certificate in the TLS process. The CAs will comply with this requirement for the subscriber after the service usage rules or the contract with the subscriber, or after the technical confirmation by the CAs 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 CAs 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 CAs will notify the Subscriber that the private key may have been compromised if they learn that the private key of the Subscriber may have been compromised, If the CAs 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 CAs will not suspend Certificates.

4.9.14 Who Can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

Certificate status is available to Subscribers and Relying Parties for confirmation through the OCSP server.

Revocation entries on a CRL or OCSP Response must not be removed until after the Expiry Date of the revoked Certificate

4.10.2 Service Availability

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

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

The CAs 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)

In terminating subscription of the Services, Subscribers are required to proceed with the service subscription termination procedure set forth in the relevant agreement therefor or the like.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

The CAs will not Escrow the CA 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

Stipulated in the CPS.

5.1.2 Physical Access

Stipulated in the CPS.

5.1.3 Power and Air Conditioning

Stipulated in the CPS.

5.1.4 Water Exposures

Stipulated in the CPS.

5.1.5 Fire Prevention and Protection

Stipulated in the CPS.

5.1.6 Media Storage

Stipulated in the CPS.

5.1.7 Waste Disposal

Stipulated in the CPS.

5.1.8 Off-Site Backup

Stipulated in the CPS.

5.2 Procedural Controls

5.2.1 Trusted Roles

Stipulated in the CPS.

5.2.2 Number of Persons Required per Task

Stipulated in the CPS.

5.2.3 Identification and Authentication for Each Role

Stipulated in the CPS.

5.2.4 Roles Requiring Separation of Duties

Stipulated in the CPS.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

Stipulated in the CPS.

5.3.2 Background Check Procedures

Stipulated in the CPS.

5.3.3 Training Requirements

Stipulated in the CPS.

5.3.4 Retraining Frequency and Requirements

Stipulated in the CPS.

5.3.5 Job Rotation Frequency and Sequence

Stipulated in the CPS.

5.3.6 Sanctions for Unauthorized Actions

Stipulated in the CPS.

5.3.7 Independent Contractor Requirement

Stipulated in the CPS.

5.3.8 Documentation Supplied to Personnel

Stipulated in the CPS.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

Stipulated in the CPS.

5.4.2 Frequency of Processing Audit Log

Stipulated in the CPS.

5.4.3 Retention Period for Audit Log

Stipulated in the CPS.

5.4.4 Protection of Audit Log

Stipulated in the CPS.

5.4.5 Audit Log Backup Procedure

Stipulated in the CPS.

5.4.6 Audit Log Collection System

Stipulated in the CPS.

5.4.7 Notification to Event-Causing Subject

Stipulated in the CPS.

5.4.8 Vulnerability Assessments

Stipulated in the CPS.

5.5 Records Archival

5.5.1 Types of Records Archived

Stipulated in the CPS.

5.5.2 Retention Period for Archive

Stipulated in the CPS.

5.5.3 Protection of Archive

Stipulated in the CPS.

5.5.4 Archive Backup Procedures

Stipulated in the CPS.

5.5.5 Requirements for Time-Stamping of Records

Stipulated in the CPS.

5.5.6 Archive Collection System

Stipulated in the CPS.

5.5.7 Procedures to Obtain and Verify Archive Information

Stipulated in the CPS.

5.6 Key Changeover

Stipulated in the CPS.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

Stipulated in the CPS.

5.7.2 Hardware, Software, and/or Data are Corrupted

Stipulated in the CPS.

5.7.3 Entity Private Key Compromise Procedures

Stipulated in the CPS.

5.7.4 Business Continuity Capabilities after a Disaster

Stipulated in the CPS.

5.8 CA or RA Termination

Stipulated in the CPS.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Stipulated in the CPS.

6.1.2 Private Key Delivery to Subscriber

Stipulated in the CPS.

6.1.3 Public Key Delivery to Certificate Issuer

Stipulated in the CPS.

6.1.4 CA Public Key Delivery to Relying Parties

Stipulated in the CPS.

6.1.5 Key Sizes

Stipulated in the CPS.

6.1.6 Public Key Parameters Generation and Quality Checking

Stipulated in the CPS.

6.1.7 Key Usage Purposes

Stipulated in the CPS.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

Stipulated in the CPS.

6.2.2 Private Key Multi-Person Control

Stipulated in the CPS.

6.2.3 Private Key Escrow

Stipulated in the CPS.

6.2.4 Private Key Backup

Stipulated in the CPS.

6.2.5 Private Key Archive

Stipulated in the CPS.

6.2.6 Private Key Transfer into or from a Cryptographic Module

Stipulated in the CPS.

6.2.7 Private Key Storage on Cryptographic Module

Stipulated in the CPS.

6.2.8 Method of Activating Private Key

Stipulated in the CPS.

6.2.9 Method of Deactivating Private Key

Stipulated in the CPS.

6.2.10 Method of Destroying Private Key

Stipulated in the CPS.

6.2.11 Cryptographic Module Rating

Stipulated in the CPS.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Stipulated in the CPS.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

Stipulated in the CPS.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Stipulated in the CPS.

6.4.2 Activation Data Protection

Stipulated in the CPS.

6.4.3 Other Aspects of Activation Data

Stipulated in the CPS.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

Stipulated in the CPS.

6.5.2 Computer Security Rating

Stipulated in the CPS.

6.6 Life-Cycle Technical Controls

6.6.1 System Development Controls

Stipulated in the CPS.

6.6.2 Security Management Controls

Stipulated in the CPS.

6.6.3 Life-Cycle Security Controls

Stipulated in the CPS.

6.7 Network Security Controls

Stipulated in the CPS.

6.8 Time-Stamping

Stipulated in the CPS.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

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

When the CAs issue a CA certificate of a subordinate CA or when a subscriber certificate is issued by a subordinate CA, the CAs shall generate non-sequential Certificate serial numbers greater than zero (0) containing at least 64 bits of output from a CSPRNG.

Certificates issued by the CAs are generated in the X.509 Certificate Format, using the fields as follows.

Table 7.1-1 Basic Certificate Fields for Security Communication RootCA1
and Subordinate CAs

Field	Description
Version (Version number)	Version: 3 (0x2)
SerialNumber (Serial number)	For Root CA 0 For Subordinate CA Unique numbers across the CAs
Signature Algorithm (Digital Signature algorithm identifier)	sha1WithRSAEncryption
Issuer (Name of the issuer)	C = JP, O = SECOM Trust.net, OU = Security Communication RootCA1
Validity (Validity period)	For Root CA From: Sep 30 04:20:49 2003 GMT To: Sep 30 04:20:49 2023 GMT For Subordinate CA From: Certificate issued date To: Set as stipulated in "CPS 6.3.2 Certificate Operational Periods and Key Pair Usage Periods"
Subject (Subordinate CA Subscriber's name)	For Root CA C = JP, O = SECOM Trust.net, OU = Security Communication RootCA1 For Subordinate CA Set the Subordinate CA Subscriber information
SubjectPublicKeyInfo (Public key information of Subordinate CA Subscriber)	For Root CA Public Key Algorithm: rsaEncryption Public-Key: 2048 bit

Security Communication RootCA
Subordinate CA Certificate Policy Ver.6.00

Field	Description
	For Subordinate CA The Public Key algorithm identifier and the Public Key data of the Subordinate CA Subscriber
Extensions (Extension fields)	See "7.1.2 Certificate Extensions" hereof.

Table 7.1-2 Basic Certificate Fields for Security Communication RootCA2
and Subordinate CAs

Field	Description
Version (Version number)	Version: 3 (0x2)
SerialNumber (Serial number)	For Root CA 0 For Subordinate CA Unique numbers across the CAs
Signature Algorithm (Digital Signature algorithm identifier)	sha256WithRSAEncryption
Issuer (Name of the issuer)	C = JP, O = SECOM Trust Systems CO.,LTD., OU = Security Communication RootCA2
Validity (Validity period)	For Root CA From: May 29 05:00:39 2009 GMT To: May 29 05:00:39 2029 GMT For Subordinate CA From: Certificate issued date To: Set as stipulated in "CPS 6.3.2 Certificate Operational Periods and Key Pair Usage Periods"
Subject (Subordinate CA Subscriber's name)	For Root CA C = JP, O = SECOM Trust Systems CO.,LTD., OU = Security Communication RootCA2 For Subordinate CA Set the Subordinate CA Subscriber information
SubjectPublicKeyInfo (Public key information of Subordinate CA Subscriber)	For Root CA Public Key Algorithm: rsaEncryption Public-Key: 2048 bit For Subordinate CA The Public Key algorithm identifier and the Public Key data of the Subordinate CA Subscriber
Extensions (Extension fields)	See "7.1.2 Certificate Extensions" hereof.

Table 7.1-3 Basic Certificate Fields for Security Communication RootCA3
and Subordinate CAs

Field	Description
Version (Version number)	Version: 3 (0x2)
SerialNumber (Serial number)	For Root CA e1:7c:37:40:fd:1b:fe:67 For Subordinate CA Unique numbers across the CAs
Signature Algorithm (Digital Signature algorithm identifier)	sha384WithRSAEncryption
Issuer (Name of the issuer)	C = JP, O = SECOM Trust Systems CO.,LTD., CN = Security Communication RootCA3
Validity (Validity period)	For Root CA From: Jun 16 06:17:16 2016 GMT To: Jan 18 06:17:16 2038 GMT For Subordinate CA From: Certificate issued date To: Set as stipulated in "CPS 6.3.2 Certificate Operational Periods and Key Pair Usage Periods"
Subject (Subordinate CA Subscriber's name)	For Root CA C = JP, O = SECOM Trust Systems CO.,LTD., CN = Security Communication RootCA3 For Subordinate CA Set the Subordinate CA Subscriber information
SubjectPublicKeyInfo (Public key information of Subordinate CA Subscriber)	For Root CA Public Key Algorithm: rsaEncryption Public-Key: 4096 bit For Subordinate CA The Public Key algorithm identifier and the Public Key data of the Subordinate CA Subscriber
Extensions (Extension fields)	See "7.1.2 Certificate Extensions" hereof.

Table 7.1-4 Basic Certificate Fields for Security Communication ECC RootCA1
and Subordinate CAs

Field	Description
Version (Version number)	Version: 3 (0x2)
SerialNumber (Serial number)	For Root CA d6:5d:9b:b3:78:81:2e:eb For Subordinate CA Unique numbers across the CAs
Signature Algorithm (Digital Signature algorithm identifier)	ecdsa-with-SHA384
Issuer (Name of the issuer)	C = JP, O = SECOM Trust Systems CO.,LTD., CN = Security Communication ECC Root CA1
Validity (Validity period)	For Root CA From: Jun 16 05:15:28 2016 GMT To: Jan 18 05:15:28 2038 GMT For Subordinate CA From: Certificate issued date To: Set as stipulated in "CPS 6.3.2 Certificate Operational Periods and Key Pair Usage Periods"
Subject (Subordinate CA Subscriber's name)	For Root CA C = JP, O = SECOM Trust Systems CO.,LTD., CN = Security Communication ECC Root CA1 For Subordinate CA Set the Subordinate CA Subscriber information
SubjectPublicKeyInfo (Public key information of Subordinate CA Subscriber)	For Root CA Public Key Algorithm: id-ecPublicKey Public-Key: 384 bit For Subordinate CA The Public Key algorithm identifier and the Public Key data of the Subordinate CA Subscriber
Extensions (Extension fields)	See "7.1.2 Certificate Extensions" hereof.

Table 7.1-5 Basic Certificate Fields for SECOM TLS RSA RootCA 2023
and Subordinate CAs

Field	Description
Version (Version number)	Version: 3 (0x2)
SerialNumber (Serial number)	For Root CA TBD For Subordinate CA Unique numbers across the CAs
Signature Algorithm (Digital Signature algorithm identifier)	sha384WithRSAEncryption
Issuer (Name of the issuer)	C = JP, O = SECOM Trust Systems Co., Ltd., CN = SECOM TLS RSA Root CA 2023
Validity (Validity period)	For Root CA From: TBD To: TBD For Subordinate CA From: Certificate issued date To: Set as stipulated in "CPS 6.3.2 Certificate Operational Periods and Key Pair Usage Periods"
Subject (Subordinate CA Subscriber's name)	For Root CA C = JP, O = SECOM Trust Systems Co., Ltd., CN = SECOM TLS RSA Root CA 2023 For Subordinate CA Set the Subordinate CA Subscriber information
SubjectPublicKeyInfo (Public key information of Subordinate CA Subscriber)	For Root CA Public Key Algorithm: rsaEncryption Public-Key: 4096 bit For Subordinate CA The Public Key algorithm identifier and the Public Key data of the Subordinate CA Subscriber
Extensions (Extension fields)	See "7.1.2 Certificate Extensions" hereof.

Table 7.1-6 Basic Certificate Fields for SECOM RSA Root CA 2023
and Subordinate CAs

Field	Description
Version (Version number)	Version: 3 (0x2)
SerialNumber (Serial number)	For Root CA TBD For Subordinate CA Unique numbers across the CAs
Signature Algorithm (Digital Signature algorithm identifier)	sha384WithRSAEncryption
Issuer (Name of the issuer)	C = JP, O = SECOM Trust Systems Co., Ltd., CN = SECOM RSA Root CA 2023
Validity (Validity period)	For Root CA From: TBD To: TBD For Subordinate CA From: Certificate issued date To: Set as stipulated in "CPS 6.3.2 Certificate Operational Periods and Key Pair Usage Periods"
Subject (Subordinate CA Subscriber's name)	For Root CA C = JP, O = SECOM Trust Systems Co., Ltd., CN = SECOM RSA Root CA 2023 For Subordinate CA Set the Subordinate CA Subscriber information
SubjectPublicKeyInfo (Public key information of Subordinate CA Subscriber)	For Root CA Public Key Algorithm: rsaEncryption Public-Key: 4096 bit For Subordinate CA The Public Key algorithm identifier and the Public Key data of the Subordinate CA Subscriber
Extensions (Extension fields)	See "7.1.2 Certificate Extensions" hereof.

Table 7.1-7 Basic Certificate Fields for SECOM Document Signing RSA Root CA
2023 and Subordinate CAs

Field	Description
Version (Version number)	Version: 3 (0x2)
SerialNumber (Serial number)	For Root CA TBD For Subordinate CA Unique numbers across the CAs
Signature Algorithm (Digital Signature algorithm identifier)	sha384WithRSAEncryption
Issuer (Name of the issuer)	C = JP, O = SECOM Trust Systems Co., Ltd., CN = SECOM Document Signing RSA Root CA 2023, OrganizationIdentifier (2.5.4.97) = NTRJP-4011001040781
Validity (Validity period)	For Root CA From: TBD To: TBD For Subordinate CA From: Certificate issued date To: Set as stipulated in "CPS 6.3.2 Certificate Operational Periods and Key Pair Usage Periods"
Subject (Subordinate CA Subscriber's name)	For Root CA C = JP, O = SECOM Trust Systems Co., Ltd., CN = SECOM Document Signing RSA Root CA 2023, OrganizationIdentifier (2.5.4.97) = NTRJP-4011001040781 For Subordinate CA Set the Subordinate CA Subscriber information
SubjectPublicKeyInfo (Public key information of Subordinate CA Subscriber)	For Root CA Public Key Algorithm: rsaEncryption Public-Key: 4096 bit For Subordinate CA The Public Key algorithm identifier and the Public Key data of the Subordinate CA Subscriber
Extensions (Extension fields)	See "7.1.2 Certificate Extensions" hereof.

7.1.1 Version Number(s)

The X.509 Format version number of Certificates issued by the CAs is Version3.

7.1.2 Certificate Extensions

Certificates issued by the CAs use the X.509 Certificate Extension fields specified in Tables "7.1-2 Security Communication RootCA1 Subordinate CA Certificate

Table 7.1.2-1 Root CA Common Certificate Extension

フィールド	Description
authorityKeyIdentifier (2.5.29.35)	Not exist
subjectKeyIdentifier (2.5.29.14)	A 160-bit SHA-1 hash for Root CA Public Key
keyUsage (2.5.29.15)	Set to Critical keyCertSign,cRLSign Set digitalSignature if the RootCA private key is used to sign the OCSP response
extendedKeyUsage (2.5.29.37)	Not exist
certificatePolicies (2.5.29.32)	Not exist
basicConstraints (2.5.29.19)	Set to Critical Subject Type=CA pathLenConstraints does not exist

Table 7.1.2-2 Security Communication RootCA1 Subordinate CA Certificate Extensions

Field	Description
authorityKeyIdentifier (2.5.29.35)	A 160-bit SHA-1 hash for CA Public Key
subjectKeyIdentifier (2.5.29.14)	A 160-bit SHA-1 hash for Subscriber Public Key
keyUsage (2.5.29.15)	Set to Critical keyCertSign, cRLSign (Usage purpose of Subscriber Public Key)
extendedKeyUsage (2.5.29.37)	Be sure to set it after January 1, 2019, but do not set anyExtendedKeyUsage. Do not set id-kp-serverAuth and id-kp-emailProtection at the same time. For cross certificates, set as necessary.
certificatePolicies (2.5.29.32)	certPolicyId=[1.2.392.200091.100.901.1] or [any Policy] policyQualifierID=id-qt-cps any Policy qualifier=CPS=http(s)://repository.secomtrust.net/SC-Root1/ *() is optional
basicConstraints (2.5.29.19)	Set to Critical Subject Type=CA pathLenConstraints (To be specified as necessary)
cRLDistributionPoints (2.5.29.31)	URI:http://repository.secomtrust.net/SC-Root1/ SCRoot1CRL.crl (CRL distribution location in the directory)
Authority Information Access(1.3.6.1.5.5.7.1.1)	accessMethod OCSP (1.3.6.1.5.5.7.48.1) accessLocation URI:http://scrootca1.ocsp.secomtrust.net accessMethod CA Issuers (1.3.6.1.5.5.7.48.2) accessLocation http://repository.secomtrust.net/SC-Root1/SCRoot1ca.cer * Set OCSP and CA Issuers as necessary

Table 7.1.2-3 Security Communication RootCA1 OCSP Responder Certificate
Extensions

Field	Description
authorityKeyIdentifier (2.5.29.35)	A 160-bit SHA-1 hash for CA Public Key
subjectKeyIdentifier (2.5.29.14)	A 160-bit SHA-1 hash for Subscriber Public Key
keyUsage (2.5.29.15)	digitalSignature (Usage purpose of Subscriber Public Key)
extendedKeyUsage (2.5.29.37)	OCSPSigning
OCSP No Check (1.3.6.1.5.5.7.48.1.5)	null
certificatePolicies (2.5.29.32)	certPolicyId=1.2.392.200091.100.901.1 policyQualifierID=id-qt-cps qualifier=CPS=http(s)://repository.secomtrust.net/SC-Root1/ *() is optional

Table 7.1.2-4 Security Communication RootCA2 Subordinate CA Certificate
Extensions

Field	Description
authorityKeyIdentifier (2.5.29.35)	A 160-bit SHA-1 hash for CA Public Key
subjectKeyIdentifier (2.5.29.14)	A 160-bit SHA-1 hash for Subscriber Public Key
keyUsage (2.5.29.15)	Set to Critical keyCertSign, cRLSign (Usage purpose of Subscriber Public Key)
extendedKeyUsage (2.5.29.37)	Be sure to set it after January 1, 2019, but do not set anyExtendedKeyUsage. Do not set id-kp-serverAuth and id-kp-emailProtection at the same time. id-kp-codeSigning is set independently. For cross certificates, set as necessary.
certificatePolicies (2.5.29.32)	certPolicyId=[1.2.392.200091.100.901.4], CA/Browser Forum Reserved Certificate Policy Identifier, [1.2.392.200091.100.721.1] or [any Policy]*1 policyQualifierID=id-qt-cps qualifier=CPS=http(s)://repository.secomtrust.net/SC-Root2/ *() is optional
basicConstraints (2.5.29.19)	Set to Critical Subject Type=CA pathLenConstraints (To be specified by the CAs as necessary)
Name Constraints (2.5.29.30)	Should be set to Critical (Set when extendedKeyUsage limits the issue destination with id-kp-serverAuth or id-kp-emailProtection)
cRLDistributionPoints (2.5.29.31)	URI:http://repository.secomtrust.net/SC-Root2/ SCRoot2CRL.crl (CRL distribution location in the directory)
Authority Information Access(1.3.6.1.5.5.7.1.1)	accessMethod OCSP (1.3.6.1.5.5.7.48.1) accessLocation URI:http://scrootca2.ocsp.secomtrust.net accessMethod CA Issuers (1.3.6.1.5.5.7.48.2) accessLocation http://repository.secomtrust.net/SC-Root2/SCRoot2ca.cer * Set OCSP and CA Issuers as necessary

*1 When issuing an EV certificate, an OID (1.2.392.200091.100.721.1) or any Policy for the EV certificate may be set.

Table 7.1.2-5 Security Communication RootCA2 OCSP Responder Certificate
Extensions

Field	Description
authorityKeyIdentifier (2.5.29.35)	A 160-bit SHA-1 hash for CA Public Key
subjectKeyIdentifier (2.5.29.14)	A 160-bit SHA-1 hash for Subscriber Public Key
keyUsage (2.5.29.15)	digitalSignature (Usage purpose of Subscriber Public Key)
extendedKeyUsage (2.5.29.37)	OCSPSigning
OCSP No Check (1.3.6.1.5.5.7.48.1.5)	null
certificatePolicies (2.5.29.32)	certPolicyId=1.2.392.200091.100.901.4 policyQualifierID=id-qt-cps qualifier=CPS=http(s)://repository.secomtrust.net/SC-Root2/ *() is optional

Table 7.1.2-6 Security Communication RootCA3 Subordinate CA Certificate Extensions

Field	Description
authorityKeyIdentifier (2.5.29.35)	A 160-bit SHA-1 hash for CA Public Key
subjectKeyIdentifier (2.5.29.14)	A 160-bit SHA-1 hash for Subscriber Public Key
keyUsage (2.5.29.15)	Set to Critical keyCertSign, cRLSign (Usage purpose of Subscriber Public Key)
extendedKeyUsage (2.5.29.37)	Be sure to set it after January 1, 2019, but do not set anyExtendedKeyUsage. Do not set id-kp-serverAuth and id-kp-emailProtection at the same time. id-kp-codeSigning is set independently. For cross certificates, set as necessary.
certificatePolicies (2.5.29.32)	certPolicyId=[1.2.392.200091.100.901.6], CA/Browser Forum Reserved Certificate Policy Identifier, [1.2.392.200091.100.721.1] or [any Policy]*1 policyQualifierID=id-qt-cps qualifier=CPS=http(s)://repository.secomtrust.net/SC-Root3/ *() is optional
basicConstraints (2.5.29.19)	Set to Critical Subject Type=CA pathLenConstraints (To be specified by the CAs as necessary)
Name Constraints (2.5.29.30)	Should be set to Critical (Set when extendedKeyUsage limits the issue destination with id-kp-serverAuth or id-kp-emailProtection)
cRLDistributionPoints (2.5.29.31)	URI:http://repository.secomtrust.net/SC-Root3/ SCRoot3CRL.crl (CRL distribution location in the directory)
Authority Information Access(1.3.6.1.5.5.7.1.1)	accessMethod OCSP (1.3.6.1.5.5.7.48.1) accessLocation URI:http://scrootca3.ocsp.secomtrust.net accessMethod CA Issuers (1.3.6.1.5.5.7.48.2) accessLocation http://repository.secomtrust.net/SC-Root3/SCRoot3ca.cer * Set OCSP and CA Issuers as necessary

*1 When issuing an EV certificate, an OID (1.2.392.200091.100.721.1) or any Policy for the EV certificate may be set.

Table 7.1.2-7 Security Communication RootCA3 OCSP Responder Certificate
Extensions

Field	Description
authorityKeyIdentifier (2.5.29.35)	A 160-bit SHA-1 hash for CA Public Key
subjectKeyIdentifier (2.5.29.14)	A 160-bit SHA-1 hash for Subscriber Public Key
keyUsage (2.5.29.15)	digitalSignature (Usage purpose of Subscriber Public Key)
extendedKeyUsage (2.5.29.37)	OCSPSigning
OCSP No Check (1.3.6.1.5.5.7.48.1.5)	null
certificatePolicies (2.5.29.32)	certPolicyId=1.2.392.200091.100.901.6 policyQualifierID=id-qt-cps qualifier=CPS=http(s)://repository.secomtrust.net/SC-Root3/ *() is optional

Table 7.1.2-8 Security Communication ECC RootCA1 Subordinate CA Certificate
Extensions

Field	Description
authorityKeyIdentifier (2.5.29.35)	A 160-bit SHA-1 hash for CA Public Key
subjectKeyIdentifier (2.5.29.14)	A 160-bit SHA-1 hash for Subscriber Public Key
keyUsage (2.5.29.15)	Set to Critical keyCertSign, cRLSign (Usage purpose of Subscriber Public Key)
extendedKeyUsage (2.5.29.37)	Set one of the following: (1) id-kp-serverAuth (2) id-kp-serverAuth and id-kp-clientAuth For cross certificates, set as necessary.
certificatePolicies (2.5.29.32)	certPolicyId=[1.2.392.200091.100.902.1], CA/Browser Forum Reserved Certificate Policy Identifier, [1.2.392.200091.100.721.1] or [any Policy]*1 policyQualifierID=id-qt-cps qualifier=CPS=http(s://repository.secomtrust.net/SC-ECC-Root1/) *() is optional
basicConstraints (2.5.29.19)	Set to Critical Subject Type=CA pathLenConstraints (To be specified as necessary)
Name Constraints (2.5.29.30)	Should be set to Critical (Set when extendedKeyUsage limits the issue destination with id-kp-serverAuth or id-kp-emailProtection)
cRLDistributionPoints (2.5.29.31)	URI:http://repository.secomtrust.net/SC-ECC-Root1/ SCECCRoot1CRL.crl (CRL distribution location in the directory)
Authority Information Access(1.3.6.1.5.5.7.1.1)	accessMethod OCSP (1.3.6.1.5.5.7.48.1) accessLocation URI:http://sceccrootca1.ocsp.secomtrust.net accessMethod CA Issuers (1.3.6.1.5.5.7.48.2) accessLocation http://repository.secomtrust.net/SC-ECC-Root1/SCECCRoot1ca.cer * Set OCSP and CA Issuers as necessary

*1 When issuing an EV certificate, an OID (1.2.392.200091.100.721.1) or any Policy for the EV certificate may be set.

Table 7.1.2-9 Security Communication ECC RootCA1 OCSP Responder Certificate
Extensions

Field	Description
authorityKeyIdentifier (2.5.29.35)	A 160-bit SHA-1 hash for CA Public Key
subjectKeyIdentifier (2.5.29.14)	A 160-bit SHA-1 hash for Subscriber Public Key
keyUsage (2.5.29.15)	digitalSignature (Usage purpose of Subscriber Public Key)
extendedKeyUsage (2.5.29.37)	OCSPSigning
OCSP No Check (1.3.6.1.5.5.7.48.1.5)	null
certificatePolicies (2.5.29.32)	certPolicyId=1.2.392.200091.100.902.1 policyQualifierID=id-qt-cps qualifier=CPS=http(s)://repository.secomtrust.net/SC-ECC-Root1/ *() is optional

Table 7.1.2-10 SECOM TLS RSA Root CA 2023 Subordinate CA Certificate Extensions

Field	Description
authorityKeyIdentifier (2.5.29.35)	A 160-bit SHA-1 hash for CA Public Key
subjectKeyIdentifier (2.5.29.14)	A 160-bit SHA-1 hash for Subscriber Public Key
keyUsage (2.5.29.15)	Set to Critical keyCertSign,cRLSign (Usage purpose of Subscriber Public Key)
extendedKeyUsage (2.5.29.37)	Set one of the following: (1) id-kp-serverAuth (2) id-kp-serverAuth and id-kp-clientAuth For cross-certificate, set as required.
certificatePolicies (2.5.29.32)	certPolicyId=1.2.392.200091.100.901.8, the CA/Browser Forum reserved certificate policy identifier, 1.2.392.200091.100.721.1 or any Policy *1 policyQualifierID=id-qt-cps qualifier=CPS=http://repo1.secomtrust.net/root/tlsrsa/
basicConstraints (2.5.29.19)	Set to Critical Subject Type=CA pathLenConstraints (set as required)
Name Constraints (2.5.29.30)	Should be set to Critical (Set when extendedKeyUsage limits the issuer with id-kp-serverAuth or id-kp-emailProtection)
cRLDistributionPoints (2.5.29.31)	URI: http://repo1.secomtrust.net/root/tlsrsa/tlsrsarootca2023.crl (CRL distribution location on directory)
Authority Information Access(1.3.6.1.5.5.7.1.1)	accessMethod OCSP (1.3.6.1.5.5.7.48.1) accessLocation URI: http://tlsrsarootca2023.ocsp.secom-cert.jp accessMethod CA Issuers (1.3.6.1.5.5.7.48.2) accessLocation http://repo2.secomtrust.net/root/tlsrsa/tlsrsarootca2023.cer * Set OCSP and CA Issuers as needed

* 1 When issuing an EV certificate, OID for EV certificate (1.2.392.200091.100.721.1) or any Policy may be set.

Table 7.1.2-11 SECOM TLS RSA Root CA 2023 OCSP Responder Certificate
Extensions

Field	Description
authorityKeyIdentifier (2.5.29.35)	A 160-bit SHA-1 hash for CA Public Key
subjectKeyIdentifier (2.5.29.14)	A 160-bit SHA-1 hash for Subscriber Public Key
keyUsage (2.5.29.15)	digitalSignature (Usage purpose of Subscriber Public Key)
extendedKeyUsage (2.5.29.37)	OCSPSigning
OCSP No Check (1.3.6.1.5.5.7.48.1.5)	null
certificatePolicies (2.5.29.32)	certPolicyId=1.2.392.200091.100.901.8 policyQualifierID=id-qt-cps qualifier=CPS=http://repo1.secomtrust.net/root/tlsrsa/

Table 7.1.2-12 SECOM RSA Root CA 2023 Subordinate CA Certificate Extensions

Field	Description
authorityKeyIdentifier (2.5.29.35)	A 160-bit SHA-1 hash for CA Public Key
subjectKeyIdentifier (2.5.29.14)	A 160-bit SHA-1 hash for Subscriber Public Key
keyUsage (2.5.29.15)	Set to Critical keyCertSign,cRLSign (Usage purpose of Subscriber Public Key)
extendedKeyUsage (2.5.29.37)	Not set anyExtendedKeyUsage. Not set id-kp-serverAuth id-kp-emailProtection, id-kp-timeStamping and id-kp-codeSigning are set independently. For cross-certificate, set as required.
certificatePolicies (2.5.29.32)	certPolicyId=1.2.392.200091.100.901.9, the CA/Browser Forum reserved certificate policy identifier, or any Policy policyQualifierID=id-qt-cps qualifier=CPS=http://repo1.secomtrust.net/root/rsa/
basicConstraints (2.5.29.19)	Set to Critical Subject Type=CA pathLenConstraints (set as required)
Name Constraints (2.5.29.30)	Should be set to Critical (Set when extendedKeyUsage limits the issuer with id-kp-emailProtection)
cRLDistributionPoints (2.5.29.31)	URI: http://repo1.secomtrust.net/root/rsa/rsarootca2023.crl (CRL distribution location on directory)
Authority Information Access(1.3.6.1.5.5.7.1.1)	accessMethod OCSP (1.3.6.1.5.5.7.48.1) accessLocation URI: http://rsarootca2023.ocsp.secom-cert.jp accessMethod CA Issuers (1.3.6.1.5.5.7.48.2) accessLocation http://repo2.secomtrust.net/root/rsa/rsarootca2023.cer * Set OCSP and CA Issuers as needed

Table 7.1.2-13 SECOM RSA Root CA 2023 OCSP Responder Certificate Extensions

Field	Description
authorityKeyIdentifier (2.5.29.35)	A 160-bit SHA-1 hash for CA Public Key
subjectKeyIdentifier (2.5.29.14)	A 160-bit SHA-1 hash for Subscriber Public Key
keyUsage (2.5.29.15)	digitalSignature (Usage purpose of Subscriber Public Key)
extendedKeyUsage (2.5.29.37)	OCSPSigning
OCSP No Check (1.3.6.1.5.5.7.48.1.5)	null
certificatePolicies (2.5.29.32)	certPolicyId=1.2.392.200091.100.901.9 policyQualifierID=id-qt-cps qualifier=CPS=http://repo1.secomtrust.net/root/rsa/

Table 7.1.2-14 SECOM Document Signing RSA Root CA 2023 Subordinate CA
Certificate Extensions

Field	Description
authorityKeyIdentifier (2.5.29.35)	A 160-bit SHA-1 hash for CA Public Key
subjectKeyIdentifier (2.5.29.14)	A 160-bit SHA-1 hash for Subscriber Public Key
keyUsage (2.5.29.15)	Set to Critical keyCertSign,cRLSign (Usage purpose of Subscriber Public Key)
extendedKeyUsage (2.5.29.37)	Not set anyExtendedKeyUsage. Set Adobe Authentic Documents Trust (1.2.840.113583.1.1.5) or id-kp-timeStamping For cross-certificate, set as required.
certificatePolicies (2.5.29.32)	certPolicyId=1.2.392.200091.100.901.10, or any Policy policyQualifierID=id-qt-cps qualifier=CPS=http://repo1.secomtrust.net/root/docrsa/
basicConstraints (2.5.29.19)	Set to Critical Subject Type=CA pathLenConstraints (set as required)
Name Constraints (2.5.29.30)	Not exist
cRLDistributionPoints (2.5.29.31)	URI: http://repo1.secomtrust.net/root/docrsa/docrsarootca2023.crl (CRL distribution location on directory)
Authority Information Access(1.3.6.1.5.5.7.1.1)	accessMethod OCSP (1.3.6.1.5.5.7.48.1) accessLocation URI: http://docrsarootca2023.ocsp.secom-cert.jp accessMethod CA Issuers (1.3.6.1.5.5.7.48.2) accessLocation http://repo2.secomtrust.net/root/docrsa/docrsarootca2023.cer * Set OCSP and CA Issuers as needed

Table 7.1.2-15 SECOM Document Signing RSA Root CA 2023 OCSP Responder
Certificate Extensions

Field	Description
authorityKeyIdentifier (2.5.29.35)	A 160-bit SHA-1 hash for CA Public Key
subjectKeyIdentifier (2.5.29.14)	A 160-bit SHA-1 hash for Subscriber Public Key
keyUsage (2.5.29.15)	digitalSignature (Usage purpose of Subscriber Public Key)
extendedKeyUsage (2.5.29.37)	OCSPSigning
OCSP No Check (1.3.6.1.5.5.7.48.1.5)	null
certificatePolicies (2.5.29.32)	certPolicyId=1.2.392.200091.100.901.10 policyQualifierID=id-qt-cps qualifier=CPS=http://repo1.secomtrust.net/root/docrsa/

7.1.3 Algorithm Object Identifiers

The Algorithm OIDs used in the Services are as follows:

Subordinate CAs that comply with Baseline Requirements do not use "Security Communication RootCA1" as their RootCA and don't use "sha1 With RSA Encryption" as their algorithm.

Table 7.1-3-1 Security Communication RootCA1 Algorithm OIDs

Algorithm	OID
sha1 With RSA Encryption	1.2.840.113549.1.1.5
sha256 With RSA Encryption	1.2.840.113549.1.1.11
RSA Encryption	1.2.840.113549.1.1.1

Table 7.1-3-2 Security Communication RootCA2 Algorithm OIDs

Algorithm	OID
sha256 With RSA Encryption	1.2.840.113549.1.1.11
RSA Encryption	1.2.840.113549.1.1.1

Table 7.1-3-3 Security Communication RootCA3 Algorithm OIDs

Algorithm	OID
sha384 With RSA Encryption	1.2.840.113549.1.1.12
RSA Encryption	1.2.840.113549.1.1.1

Table 7.1-3-4 Security Communication ECC RootCA1 Algorithm OIDs

Algorithm	OID
ecdsa-with-SHA384	1.2.840.10045.4.3.3
ecPublicKey	1.2.840.10045.2.1
secp384r1	1.3.132.0.34

Table 7.1-3-5 SECOM TLS RSA Root CA 2023 Algorithm OIDs

Algorithm	OID
sha384 With RSA Encryption	1.2.840.113549.1.1.12
RSA Encryption	1.2.840.113549.1.1.1

Table 7.1-3-6 SECOM RSA Root CA 2023 Algorithm OIDs

Algorithm	OID
sha384 With RSA Encryption	1.2.840.113549.1.1.12
RSA Encryption	1.2.840.113549.1.1.1

Table 7.1-3-7 SECOM Document Signing RSA Root CA 2023 Algorithm OIDs

Algorithm	OID
sha384 With RSA Encryption	1.2.840.113549.1.1.12
RSA Encryption	1.2.840.113549.1.1.1

7.1.4 Name Forms

The CAs use the distinguished name specified in RFC5280.

The following requirements should be met by all newly-issued Subordinate CA Certificates that are not used to issue TLS certificates, and must be met for all other Certificates, regardless of whether the Certificate is a CA Certificate or a Subscriber Certificate.

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.
- For each CA Certificate in the Certification Path, the encoded content of the Subject Distinguished Name field of a Certificate shall be byte-for-byte identical among all Certificates whose Subject Distinguished Names can be compared as equal according to RFC 5280, Section 7.1, and including expired and revoked Certificates.

The CAs and the Subscribers are uniquely identified by the DN's defined conforming to the X.500 Distinguished Name. Valid characters are specified in Table "7.1-4-1 Valid Characters".

Table 7.1-4-1 Valid Characters

Alphabets	Numbers	Symbols
[A] through [Z], [a] through [z]	[0] through [9]	[-], [], and [blank]

7.1.5 Name Constraints

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

- a. For each dNSName in permittedSubtrees, the CAs must confirm that the Applicant has registered the dNSName or has been authorized by the domain registrant to act on the registrant's behalf in line with the verification practices of Baseline Requirements, Section 3.2.2.4.
- b. For each iPAddress range in permittedSubtrees, the CAs must confirm that the Applicant has been assigned the iPAddress range or has been authorized by the assigner to act on the assignee's behalf.
- c. For each DirectoryName in permittedSubtrees the CAs must confirm the Applicant's and/or Subsidiary's Organizational name and location such that end entity certificates issued from the subordinate CA Certificate will be in compliance with Baseline Requirements 7.1.2.4 and Baseline Requirements 7.1.2.5.

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

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

If the Subordinate CA Certificate includes the id-kp-emailProtection extended key usage, then the Subordinate CA Certificate must include Name Constraints X.509v3 extension area with constraints on rfc822Name, and at least one name in the permittedSubtrees is contained, and each such name shall be verified for ownership according to the validation procedure in Baseline Requirements 3.2.2.4.

7.1.6 Certificate Policy Object Identifier

Policy OID of the Certificates issued by the CAs are as indicated in the Table "1.2-2 OID (This CP)".

The following Certificate Policy identifiers are reserved for use by the CAs or subordinate CAs as an optional means of ascertaining that a Certificate complies with Baseline Requirements.

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

{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)

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140)
certificate-policies(1) ev-guidelines(1)} (2.23.140.1.1)

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140)
certificate-policies(1) code-signing-requirements(3)} (2.23.140.1.3)

7.1.7 Usage of Policy Constraints Extension

No stipulation

7.1.8 Policy Qualifiers Syntax and Semantics

Policy Qualifiers store the URL of the web pages on which this CP and the CPS are published.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation

7.2 CRL Profile

CRLs issued by the CAs are generated in the X.509 CRL Format, using the fields specified in Table 7.2-1 Basic CRL Profile Fields.

Table 7.2-1 Basic CRL Profile Fields

Field	Description
Version (Version number)	Version: 2 (0x1)
Signature (Digital Signature algorithm identifier)	Identifier of the Digital Signature algorithm used by the CAs *1
Issuer (Name of the issuer)	Information about the issuer (specified by the CAs)
ThisUpdate (Date of update)	Date of CRL issuance
NextUpdate (Date of next update)	Date of next CRL update
RevokedCertificates (CRL)	Information about the revoked Certificates; SerialNumber (serial number); and RevocationDate (date of revocation) Reason Code (Reason for revocation) shall be specified.

*1 Used when digitally signing a CRL.

7.2.1 Version Number(s)

The X.509 Format version number of CRLs issued by the CAs is Version2.

7.2.2 CRL and CRL Entry Extensions

The CRLs issued by the CAs use the X.509 CRL Extension field specified in the Table "7.2-2-1 CRL Extension".

reasonCode (OID 2.5.29.21)

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

If present, this extension must not be marked critical.

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

If a CRL entry is for a Certificate not technically capable of causing issuance, 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.

In the CAs, the following reasonCode shall be used.

- keyCompromise (1)
- affiliationChanged (3)
- superseded (4)
- cessationOfOperation (5)

Use the fields shown in Table "7.2-2-1 CRL Extension".

Table 7.2-2-1 CRL Extension

Field	Description
AuthorityKeyIdentifier (CA Key identifier)	A 160-bit SHA-1 hash for CA Public Key

7.3 OCSP Profile

The CAs operates the OCSP server in compliance with RFC6960 and 5019.

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 this CP "7.2.2 CRL and CRL Entry Extensions".

7.3.1 Version Number(s)

The CAs use OCSP Version 1.

7.3.2 OCSP Extensions

Refer to "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

8.1 Frequency and Circumstances of Assessment

Stipulated in the CPS.

8.2 Identity/Qualifications of Assessor

Stipulated in the CPS.

8.3 Assessor's Relationship to Assessed Entity

Stipulated in the CPS.

8.4 Topics Covered by Assessment

Stipulated in the CPS.

8.5 Actions Taken as a Result of Deficiency

Stipulated in the CPS.

8.6 Communication of Results

Stipulated in the CPS.

8.7 Self-Audit

Stipulated in the CPS.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

Stipulated separately in contracts.

9.1.2 Certificate Access Fees

No stipulation

9.1.3 Revocation or Status Information Access Fees

No stipulation

9.1.4 Fees for Other Services

No stipulation

9.1.5 Refund Policy

Stipulated separately in contracts.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

SECOM Trust systems shall maintain a sufficient financial resources in providing the CAs.

9.2.2 Other Assets

No stipulation

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

Information on individuals and organizations in the possession of SECOM as the CAs are subject to confidentiality with the exception of those that were explicitly published as a part of a Certificate, a CRL, this CP, or the CPS. SECOM does not disclose such information externally unless it is required by law or there is a prior consent of the relevant Subscriber. SECOM may disclose the information subject to confidentiality to a legal counsel or a financial adviser who provides advice in connection with such legal,

judicial, administrative or other procedures required by law. It may also disclose information subject to confidentiality to an attorney, an accountant, a legal institution or any other specialist who provides advice on corporate mergers, acquisitions or restructuring.

Subscriber Private Keys are deemed to be information to be kept confidential by the Subscriber's own responsibility. The Services in no circumstances provide access to these Keys.

Information contained in Audit Log and the Audit Reports themselves are subject to the confidentiality and within the Scope of Confidential Information. SECOM will not disclose such information to any external party in other situation than a case stipulated in "8.6 Communication of Results" of the CPS or unless it is required by law.

9.3.2 Information Not Within the Scope of Confidential Information

Information populated in Certificates and CRLs is not considered confidential. In addition, the following information shall not be subject to the confidentiality provisions herein:

- Information that is or came to be known through no fault of SECOM;
- Information that was or is made known to SECOM by a party other than SECOM without confidentiality requirements;
- Information independently developed by SECOM; or
- Information approved for disclosure by the relevant Subscriber.

9.3.3 Responsibility to Protect Confidential Information

SECOM may disclose confidential information retained as the CAs when required by law or there is a prior consent of the relevant Subscriber. In the event of the foregoing, the party having come to acquire the information may not disclose said information to a third party due to contractual or legal constraints.

9.4 Privacy of Personal Information

9.4.1 Personal Information Protection Plan

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

9.4.2 Information Treated as Personal Information

SECOM treats information defined as personal information based on domestic laws

and regulations (such as information collected from subscribers of SECOM authentication services) as personal information and manages it appropriately.

9.4.3 Information that is not considered Personal Information

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

9.4.4 Responsibility for protecting Personal Information

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

9.4.5 Notice and Consent regarding use of Personal Information

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

9.4.6 Disclosure of Information with Judicial or Administrative Procedures

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


9.4.7 Other Information Disclosure Conditions

No stipulation.

9.5 Intellectual Property Rights

Unless otherwise agreed to between SECOM and Subscribers, the following informative materials and data pertaining to the Services shall belong to the parties specified as below:

Subscriber Certificate	An asset belonging to SECOM
CRL	An asset belonging to SECOM
Distinguished Name (DN)	An asset belonging to an entity to which the Name is assigned as long as the fee for the Subscriber Certificate is properly paid
Subscriber	An asset belonging the possessor of the Private Key that completes

Private Key	a Key Pair with the Public Key, regardless of how it is stored or who possesses the storage medium
Subscriber Public Key	An asset belonging the possessor of the Private Key that completes a Key Pair, regardless of how it is stored or who possesses the storage medium
This CP and the CPS	<p>An asset (including the copyrights) belonging to SECOM This CP, CPS 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.</p>  <p>https://creativecommons.org/licenses/by-nd/4.0/</p>

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

SECOM provides certification services including authentication of Subscribers and registration/issuance/revocation of Certificates conforming to the provisions of this CP and the CPS, and secures the reliability of the certification practice including that of the CA Private Keys.

The foregoing warranties by SECOM set forth in this CP and the CPS are in lieu of all other warranties, express or implied, or otherwise.

By issuing a Certificate, the CA or a Subordinate CAs make the certificate warranties listed herein to the following Certificate Beneficiaries:

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

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

1. Right to Use Domain Name or IP Address:
That, at the time of issuance, the Subordinate CA
 - i. implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the Domain Name(s) and IP address(es) listed

in the Certificate's subject field and subjectAltName extension (or, only in the case of Domain Names, was delegated such right or control by someone who had such right to use or control);

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

2. Authorization for Certificate:

That, at the time of issuance, the Subordinate CA

- i. implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject;
- ii. followed the procedure when issuing the Certificate; and
- iii. accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;

3. Accuracy of Information:

At the time of issuance, the Subordinate CA

- i. implemented a procedure for verifying the accuracy of all of the information contained in the Certificate (with the exception of the subject:organizationalUnitName attribute);
- ii. followed the procedure when issuing the Certificate; and
- iii. accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;

4. No Misleading Information:

That, at the time of issuance, the Subordinate CA

- i. implemented a procedure for reducing the likelihood that the information contained in the Certificate's subject:organizationalUnitName attribute would be misleading;
- ii. followed the procedure when issuing the Certificate; and
- iii. accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;

5. Identity of Applicant:

That, if the Certificate contains Subject Identity Information, the Subordinate CA

- i. implemented a procedure to verify the identity of the Applicant in accordance with Section 3.2 and Section 7.1.4.2..2;
- ii. followed the procedure when issuing the Certificate; and
- iii. accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;

6. Subscriber Agreement:

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

7. Status

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

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

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

9.6.2 RA Representations and Warranties

The provisions of "9.6.1 CA Representations and Warranties" hereof shall apply.

9.6.3 Subscriber Representations and Warranties

The CAs or Subordinate 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 CAs and the Certificate Beneficiaries.

Prior to the issuance of a Certificate, the CAs or Subordinate CA shall obtain, for the express benefit of the CAs and the Certificate Beneficiaries, either:

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

The CAs or Subordinate 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 certificates, install the Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate.

Obligation and warranty to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use;

5. Reporting and Revocation

An obligation and warranty to:

- a. Promptly request revocation of the Certificate, and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate, and
- b. Promptly request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate.

6. Termination of Use of Certificate:

An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise.

7. Responsiveness:

An obligation to respond to the CA's instructions concerning Key Compromise or Certificate misuse within a specified time period.

8. Acknowledgment and Acceptance:

An acknowledgment and acceptance that the CA is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber Agreement or Terms of Use or if revocation is required by the CA's CP, CPS, or the

Baseline Requirements.

9.6.4 Relying Party Representations and Warranties

Relying Parties of the CA Services shall bear obligations to:

- Trust Certificates issued by the CAs for use with the intended usage purposes of the CAs set forth in this CP and the CPS;
- Ensure that the Certificate has not been revoked by checking the CRLs in the Repository or the OCSP server in attempting to trust the Certificate;
- Check the validity period of the Certificate to ensure that it has not expired in attempting to trust the Certificate;
- Ensure that the Certificate signature can be authenticated by the CA Certificate in attempting to trust the Certificate issued by the CAs; and
- Agree to bear responsibility as the Relying Party defined in this CP and the CPS in trusting and using the CA Certificates.

9.6.5 Representations and Warranties of Other Participants

No stipulation

9.7 Disclaimers of Warranties

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

9.8 Limitations of Liability

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

- Any damage arising from unlawful conduct, unauthorized use, negligence or any other cause not attributable to SECOM;
- Any damage attributable to the failure of a Subscriber or Relying Party to perform its obligations;
- Any damage attributable to a Subscriber or Relying Party system;
- Damages attributable to the defect or malfunction or any other behavior of SECOM's, Subscriber's, or Relying Party's hardware or software;
- Any damage during the period that a Subscriber neglected to pay the subscription fee as set forth in the agreement thereof;
- Damages caused by information published in a Certificate, a CRL or on the OCSP server due to the reasons not attributable to SECOM;
- Any damage incurred in an outage of the normal communication due to reasons not attributable to SECOM;

- Any damage arising in connection with the use of a Certificate, including transaction debts;
- Damages attributable to improvement, beyond expectations at this point in time, in hardware or software type of cryptographic algorithm decoding skills; and
- Any damage attributable to the suspension of the CA Services, including that of the CAs, due to force majeure, including, but not limited to, natural disasters, earthquakes, volcanic eruptions, fires, tsunamis, floods, lightning strikes, wars, civil commotion and terrorism.

9.9 Indemnities

Each Subscriber and Relying Party shall indemnify and hold harmless SECOM and its related organizations upon applying for, accepting, and trusting Certificates issued by the CAs. Incidents subject to the foregoing include loss, damage, lawsuit, as well as misconduct, omission, act, delay or default that are attributable to any kinds of cost burden, which could have been caused by failure of the Subscriber to provide the latest and accurate information to the CAs. Such incidents also include various liabilities, loss, damage, lawsuit, as well as misconduct, omission, act, delay or default by each Subscriber or Relying Party that are attributable to any kinds of cost burden.

9.10 Term and Termination

9.10.1 Term

This CP goes into effect upon approval by the Certification Services Improvement Committee. This CP will in no way lose effect under any circumstances prior to the termination stipulated in "9.10.2 Termination" hereof.

9.10.2 Termination

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

9.10.3 Effect of Termination and Survival

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

9.11 Individual Notices and Communications with Participants

The CAs provide the necessary notices to Subscribers and Relying Parties through e-mail or in other written forms.

9.12 Amendments

9.12.1 Procedure for Amendment

(1) Critical revisions/amendments

SECOM notifies Subscribers and Relying Parties of amendments of this CP if the amendments thereof are determined to have an obvious impact on the activities for use of Certificates or CRLs by the Subscribers and Relying Parties, by publishing the post-amendment version of this CP (including the Version History/Description/Date) in the Repository, while refreshing the Major Version Number.

(2) Non-critical revisions/amendments

SECOM notifies Subscribers and Relying Parties of amendments of this CP if the amendments thereof are determined to have no or less impact on the activities for use of Certificates or CRLs by the Subscribers and Relying Parties, by publishing the post-amendment version of this CP (including the Version History/Description/Date) in the Repository, while refreshing the Minor Version Number.

9.12.2 Notification Mechanism and Period

If this CP is revised/amended, the prompt publication of the post-amendment version of this CP (including the Version History/Description/Date) in the Repository is deemed to be the notification thereof to Subscribers and Relying Parties. Subscribers may make claims within a week of such notification, while the post-amendment version of this CP is deemed to be approved by the Subscribers unless any claim is made within the said period.

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 Provisions

A party seeking to file a lawsuit, request arbitration, or take any other legal action against SECOM for the resolution of a dispute relating to the Services provided by the CAs, shall notify SECOM to this effect in advance.

9.14 Governing Law

Regardless of the locations of the CAs, Subscribers, or Relying Parties, the laws of Japan will apply to any dispute concerning the interpretation or validity of this CP and the CPS. Regarding the location for arbitration and court proceedings, the parties hereto submit to the exclusive jurisdiction of a dispute settlement institution located within Tokyo.

9.15 Compliance with Applicable Law

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

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

SECOM comprehensively stipulates its policy, warranties as well as the Subscriber and Relying Party obligations and other relevant matters in this CP, the CPS and the agreements for provision of the Services, and any agreement otherwise, whether oral, written, or implied, shall have no effect.

9.16.2 Assignment

When SECOM assigns the Services to a third party, SECOM may also assign its responsibilities and other obligations specified in this CP and the CPS.

9.16.3 Severability

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

In the event of a conflict between Baseline Requirements and a law, regulation or government order (hereinafter 'Law') of any jurisdiction in which the CAs operate or issue certificates, the CAs may modify any conflicting requirement to the minimum extent necessary to make the requirement valid and legal in the jurisdiction.

This applies only to operations or certificate issuances that are subject to that Law. In such event, the CAs shall immediately (and prior to issuing a certificate under the modified requirement) include in the CA's CPS a detailed reference to the Law requiring a modification of Baseline Requirements under this section, and the specific modification to Baseline Requirements implemented by the CAs.

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

Any modification to the CAs 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

Indemnities and attorneys' fees may be sought from parties for disputes arising from the contractual provisions of each prescribed document, damages, losses and costs relating to the parties' actions.

9.16.5 Force Majeure

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

9.17 Other Provisions

No stipulation