

Secom Passport for Member 2.0 PUB
Certificate Policy
Version 5.05

September 29, 2020

SECOM Trust Systems Co., Ltd.

Version History		
Version Number	Date	Description
1.00	2008.04.28	Publication of the first version
1.10	2009.03.19	Revision of Certificate Profile (extendedKeyUsage).
2.00	2009.10.13	Addition of the Policy OID Overall revision of the styles
3.00	2013.11.27	Addition of the revised Policy OID associated with the addition of Sha256 Addition of the RootCA repository information
4.00	2014.05.29	Revision associated with the additional use of server authentication Addition of the Policy OID
5.00	2017.01.20	Addition of the Policy OID Revision associated with the start of OCSP server operation Overall revision of the styles
5.01	2020.02.19	Removal of the Certificate policy for server certificate Addition/revision of contents in BR for Code Signing Overall revision of the descriptions and styles
5.02	2020.03.30	Review of "No stipulation"
5.03	2020.06.15	Addition of Extended Key Usage to CA certificate (sha256) profile Addition of Extended Key Usage to Subscriber certificate (sha256) profile
5.04	2020.07.30	From Extended Key Usage of CA certificate (sha256), remove OCSP Signing, change OU, change CP URL From Subscriber certificate (sha256), change OU, change URL of CP, change OCSP URL of AIA, etc.
5.05	2020.09.29	Revision of Reason code for CRL profile

Table of Contents

1. Introduction.....	1
1.1 Overview	1
1.2 Document Name and Identification.....	2
1.3 PKI Participants.....	2
1.3.1 CA	2
1.3.2 RA	3
1.3.3 Applicants and Subscribers	3
1.3.4 Relying Parties	3
1.3.5 Other Parties	3
1.4 Certificate Usage.....	3
1.4.1 Appropriate Certificate Uses	3
1.4.2 Prohibited Certificate Uses.....	5
1.5 Policy Administration	5
1.5.1 Organization Administering the Document	5
1.5.2 Contact Information	5
1.5.3 Person Determining CP Suitability for the Policy	5
1.5.4 Approval Procedure	5
1.6 Definitions and Acronyms.....	5
2. Publication and Repository Responsibilities.....	10
2.1 Repository	10
2.2 Publication of Certificate Information.....	10
2.3 Time or Frequency of Publication	10
2.4 Access Controls on Repository.....	10
3. Identification and Authentication.....	11
3.1 Naming.....	11
3.1.1 Types of Names	11
3.1.2 Need for Names to Be Meaningful	11
3.1.3 Anonymity or Pseudonymity of Subscribers.....	11
3.1.4 Rules for Interpreting Various Name Forms.....	11
3.1.5 Uniqueness of Names	11
3.1.6 Recognition, Authentication, and Roles of Trademarks	11
3.2 Initial Identity Validation.....	12
3.2.1 Method to Prove Possession of Private Key.....	12
3.2.2 Authentication of Organization Identity.....	12
3.2.3 Authentication of Applicant and Individual Identity.....	12

3.2.4 Non-Verified Subscriber Information.....	13
3.2.5 Validation of Authority	13
3.2.6 Criteria for Interoperation.....	13
3.3 Identification and Authentication for Re-Key Requests.....	13
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 May 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	14
4.2.3 Time to Process Certificate Applications	15
4.3 Certificate Issuance.....	15
4.3.1 CA Actions during Certificate Issuance	15
4.3.2 Notifications to Subscriber of Certificate Issuance.....	15
4.4 Certificate Acceptance.....	15
4.4.1 Conduct Constituting Certificate Acceptance.....	15
4.4.2 Publication of the Certificate by the CA	15
4.4.3 Notification of Certificate Issuance by the CA to Other Entities.....	15
4.5 Key Pair and Certificate Usage.....	15
4.5.1 Subscriber Private Key and Certificate Usage.....	15
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.....	16
4.6.4 Notification of New Certificate Issuance to Subscriber.....	16
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate.....	16
4.6.6 Publication of the Renewal Certificates by the CA.....	16
4.6.7 Notification of Certificate Issuance by the CA to Other Entities.....	16
4.7 Certificate renewal with Re-Key.....	16
4.7.1 Circumstances for Certificate Renewal	17
4.7.2 Who May Request Certificate Renewal	17

4.7.3 Processing Certificate Renewal 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.....	17
4.8 Certificate Modification	17
4.8.1 Circumstances for Certificate Modification.....	17
4.8.2 Who May Request Certificate Modification.....	17
4.8.3 Processing Certificate Modification Requests	17
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 Certificates 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.....	19
4.9.3 Procedure for Revocation Request.....	19
4.9.4 Revocation Request Grace Period.....	19
4.9.5 Time within Which CA Shall Process the Revocation Request.....	19
4.9.6 Revocation Checking Requests	19
4.9.7 CRL Issuance Frequency	20
4.9.8 Maximum Latency for CRLs.....	20
4.9.9 On-Line Revocation/Status Checking Availability	20
4.9.10 On-Line Revocation/Status Checking Requirements.....	20
4.9.11 Other Forms of Revocation Advertisements Available.....	20
4.9.12 Special Requirements Regarding Key Compromise	20
4.9.13 Circumstances for Suspension Who Can Request Suspension	20
4.9.14 Who Can Request Suspension	21
4.9.15 Procedure for Suspension Request.....	21
4.9.16 Limits on Suspension Period	21
4.10 Certificate Status Services	21
4.10.1 Operational Characteristics.....	21
4.10.2 Service Availability	21
4.10.3 Optional Features.....	21
4.11 End of Subscription (Registry)	21
4.12 Key Escrow and Recovery.....	21

4.12.1 Key Escrow and Recovery Policy and Practices	22
4.12.2 Session Key Encapsulation and Recovery Policy and Practices	22
5. Facility, Management, and Operational Controls	23
5.1 Physical Controls.....	23
5.1.1 Site Location and Construction	23
5.1.2 Physical Access	23
5.1.3 Power and Air Conditioning.....	23
5.1.4 Water Exposures.....	23
5.1.5 Fire Prevention and Protection	23
5.1.6 Media Storage	23
5.1.7 Waste Disposal.....	23
5.1.8 Off-Site Backup.....	23
5.2 Procedural Controls	23
5.2.1 Trusted Roles	23
5.2.2 Number of Persons Required per Task	23
5.2.3 Identification and Authentication for Each Role.....	24
5.2.4 Roles Requiring Separation of Duties.....	24
5.3 Personnel Controls	24
5.3.1 Qualifications, Experience, and Clearance Requirements	24
5.3.2 Background Check Procedures	24
5.3.3 Training Requirements	24
5.3.4 Retraining Frequency and Requirements	24
5.3.5 Job Rotation Frequency and Sequence	24
5.3.6 Sanctions for Unauthorized Actions.....	24
5.3.7 Independent Contractor Requirements	24
5.3.8 Documentation Supplied to Personnel.....	24
5.4 Audit Logging Procedures.....	24
5.4.1 Types of Events Recorded	24
5.4.2 Frequency of Processing Audit Log	25
5.4.3 Retention Period for Audit Log.....	25
5.4.4 Protection of Audit Log.....	25
5.4.5 Audit Log Backup Procedure	25
5.4.6 Audit Log Collection System.....	25
5.4.7 Notification to Event-Causing Subject.....	25
5.4.8 Vulnerability Assessments.....	25
5.5 Records Archival.....	25

5.5.1 Types of Records Archived	25
5.5.2 Retention Period for Archive.....	25
5.5.3 Protection of Archive	26
5.5.4 Archive Backup Procedures	26
5.5.5 Requirements for Time-Stamping of Records.....	26
5.5.6 Archive Collection System	26
5.5.7 Procedures to Obtain and Verify Archive Information	26
5.6 Key Changeover	26
5.7 Compromise and Disaster Recovery	26
5.7.1 Incident and Compromise Handling Procedures	26
5.7.2 Procedure when Hardware, Software, and/or Data are Corrupted	27
5.7.3 Entity Private Key Compromise Procedures.....	27
5.7.4 Business Continuity Capabilities after a Disaster	27
5.8 CA or RA Termination.....	27
6. Technical Security Controls	28
6.1 Key Pair Generation and Installation	28
6.1.1 Key Pair Generation.....	28
6.1.2 Private Key Delivery to Subscriber.....	28
6.1.3 Public Key Delivery to Certificate Issuer	28
6.1.4 CA Public Key Delivery to Relying Parties.....	28
6.1.5 Key Sizes	28
6.1.6 Public Key Parameters Generation and Quality Checking.....	28
6.1.7 Key Usage Purposes	29
6.2 Private Key Protection and Cryptographic Module Engineering Controls	29
6.2.1 Cryptographic Module Standards and Controls	29
6.2.2 Private Key Multi-Person Control.....	29
6.2.3 Private Key Escrow	29
6.2.4 Private Key Backup.....	29
6.2.5 Private Key Archive.....	29
6.2.6 Private Key Transfer into or from a Cryptographic Module	29
6.2.7 Private Key Storage on Cryptographic Module.....	30
6.2.8 Method of Activating Private Key	30
6.2.9 Method of Deactivating Private Key	30
6.2.10 Method of Destroying Private Key	30
6.2.11 Cryptographic Module Rating.....	30
6.3 Other Aspects of Key Pair Management	30

6.3.1 Public Key Archival	30
6.3.2 Certificate Operational Periods and Key Pair Usage Periods	30
6.4 Activation Data.....	31
6.4.1 Activation Data Generation and Installation	31
6.4.2 Activation Data Protection.....	31
6.4.3 Other Aspects of Activation Data	31
6.5 Computer Security Controls.....	31
6.5.1 Specific Computer Security Technical Requirements	31
6.5.2 Computer Security Rating	31
6.6 Life-Cycle Security Controls.....	31
6.6.1 System Development Controls.....	32
6.6.2 Security Management Controls.....	32
6.6.3 Life-Cycle Security Controls	32
6.7 Network Security Controls	32
6.8 Time-Stamping	32
7. Certificate, CRL, and OCSP Profiles.....	33
7.1 Certificate Profile	33
7.1.1 Version Number(s).....	41
7.1.2 Certificate Extension.....	41
7.1.3 Algorithm Object Identifier.....	41
7.1.4 Name Format	42
7.1.5 Name Constraints.....	42
7.1.6 Certificate Policy Object Identifier.....	42
7.1.7 Use of Policy Constraint Extensions	42
7.1.8 Policy Qualifier Syntax and Semantics	42
7.1.9 How to interpret Critical Certificate Policy Extensions	42
7.2 CRL Profile	42
7.2.1 Version Number(s).....	44
7.2.2 Certificate Revocation Lists and CRL Entry Extensions	44
7.3 OCSP Profile	45
7.3.1 Version Number(s).....	46
7.3.2 OCSP Extensions.....	46
8. Compliance Audit and Other Assessments	47
8.1 Frequency and Circumstances of Assessment	47
8.2 Identity/Qualifications of Assessor	47
8.3 Assessor's Relationship to Assessed Entity.....	47

8.4 Topics Covered by Assessment	47
8.5 Actions Taken as a Result of Deficiency	47
8.6 Communication of Results.....	47
9. Other Business and Legal Matters.....	49
9.1 Fees	49
9.1.1 Fees for Issuing or Renewing Certificates	49
9.1.2 Certificate Access Fee.....	49
9.1.3 Expiration or Access Fee for Status Information	49
9.1.4 Fees for Other Services	49
9.1.5 Refund Policy	49
9.2 Financial Responsibility	49
9.2.1 Insurance Coverage	49
9.2.2 Other Assets	49
9.2.3 End entity Insurance or Warranty coverage	49
9.3 Confidentiality of Business Information	49
9.3.1 Scope of Confidential Information.....	49
9.3.2 Information Not Within the Scope of Confidential Information	50
9.3.3 Responsibility to Protect Confidential Information	50
9.4 Privacy of Personal Information	50
9.4.1 Personal Information Protection Plan	50
9.4.2 Information Treated as Personal Information.....	50
9.4.3 Information that is not considered Personal Information	50
9.4.4 Responsibility for protecting Personal Information.....	50
9.4.5 Notice and Consent regarding use of Personal Information	50
9.4.6 Disclosure of Information in accordance with Judicial or Administrative Procedures	50
9.4.7 Other Information Disclosure Conditions	50
9.5 Intellectual Property Rights.....	50
9.6 Representations and Warranties	51
9.6.1 CA Representation and Warranties	51
9.6.2 RA Representations and Warranties.....	51
9.6.3 Applicant and Subscriber Representations and Warranties	51
9.6.4 Relying Party Representations and Warranties	52
9.6.5 Representations and Warranties of Other Participants	52
9.7 Disclaimer of Warranties	52
9.8 Limitations of Liability	52

9.9 Indemnities	53
9.10 Term and Termination	53
9.10.1 Term.....	53
9.10.2 Termination.....	53
9.10.3 Effect of Termination and Survival	53
9.11 Individual Notices and Communications with Participants	53
9.12 Amendments	54
9.12.1 Procedure for Amendment	54
9.12.2 Notification Method and Timing	54
9.12.3 Circumstances under Which OID Must Be Changed	54
9.13 Dispute Resolution Procedures	54
9.14 Governing Law	54
9.15 Compliance with Applicable Law	54
9.16 Miscellaneous Provisions.....	54
9.16.1 Entire Agreement	54
9.16.2 Assignment.....	55
9.16.3 Severability	55
9.16.4 Enforcement.....	55
9.16.5 Irresistible Force.....	55
9.17 Other Provisions.....	55

1. Introduction

1.1 Overview

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

This CA has been issued a one-way cross-certification certificate by Security Communication RootCA1 or Security Communication RootCA2, and is operated according to the operational standards set by each CA. The above CA's CP and CPS are published in the following repositories.

1 . Security communication route CA1

<https://repository.secomtrust.net/SC-Root1/index.html>

2 . Security communication route CA2

<https://repository.secomtrust.net/SC-Root2/index.html>

A party seeking to obtain Certificates from the CA must examine its usage purposes against this CP and the CPS, and agree to the both prior to getting the Certificates issued. In the event of a conflict between this CP and the CPS, the order of precedence in the application thereof shall be this CP, and the CPS. Also, if there is a separate contract between SECOM Trust Systems and an organization that has a contractual relationship, the document such as the contract takes precedence over this CP and CPS.

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

This CP conforms to the RFC3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" advocated by the IETF as a CA practice framework. Also if this CA issues a certificate that applies to the code

signing certificate policy, it complies with the CA/Browser Forum's Baseline Requirements for the Issuance and Management of Code Signing Certificates (Hereinafter referred to as "BR for Code Signing") and the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at <https://www.cabforum.org/>.

1.2 Document Name and Identification

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

CP/CPS	OID
Client Certificate Policy (Signature Algorithm: Sha1)	1. 2. 392. 200091. 100. 381. 1
Client Certificate Policy (Signature Algorithm: Sha256)	1. 2. 392. 200091. 100. 381. 4
Certificate Policy for Data Signing (Signature Algorithm: Sha1)	1. 2. 392. 200091. 100. 381. 2
Certificate Policy for Data Signing (Signature Algorithm: Sha256)	1. 2. 392. 200091. 100. 381. 5
Certificate Policy for Code Signing (Signature Algorithm: Sha256)	1. 2. 392. 200091. 100. 381. 8
OCSP server certificate policy (Signature Algorithm: Sha256)	1. 2. 392. 200091. 100. 381. 9
SECOM Digital Certification Infrastructure Certification Practice Statement	1. 2. 392. 200091. 100. 401. 1

1.3 PKI Participants

1.3.1 CA

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

1.3.2 RA

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

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

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

1.3.3 Applicants and Subscribers

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

1.3.4 Relying Parties

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

1.3.5 Other Parties

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

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The certificate issued by this CA based on this CP can be used for the following purposes.

Certificate Policy	Certificate Usage
Client Certificate Policy	<p>According to the method determined based on this CP and the LRA operational standards, certificates certified by LRA will be issued for the following purposes.</p> <ul style="list-style-type: none"> • Digital signature on digital documents and encryption of digital document • Client authentication to identify individuals, devices, etc. <p>Based on this CP and the terms and conditions set forth separately by SECOM Trust Systems, a certificate will be issued to the corporation or organization that has been confirmed by SECOM Trust Systems for the following purposes.</p> <ul style="list-style-type: none"> • E-mail signing and e-mail encryption (S/MIME certificate)
Certificate Policy for Data Signing	<p>Based on this CP and the terms and conditions set forth separately by SECOM Trust Systems, a certificate will be issued to the corporation or organization that has been confirmed by SECOM Trust Systems for the following purposes.</p> <ul style="list-style-type: none"> • Digital signature on electronic documents
Certificate Policy for Code Signing	<p>Based on this CP and the terms and conditions set forth separately by SECOM Trust Systems, a certificate will be issued to the corporation or organization that has been confirmed by SECOM for the following purposes.</p> <ul style="list-style-type: none"> • Digital signature for program files (Code signing certificate)
OCSP Server Certificate Policy	<p>For the certificates issued by the code signing certificate policy, provide an OCSP server. Other certificate policies provide OCSP servers as needed.</p>

1.4.2 Prohibited Certificate Uses

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

1.5 Policy Administration

1.5.1 Organization Administering the Document

This CP is maintained and administered by SECOM Trust Systems.

1.5.2 Contact Information

Contact information for this CP is as follows:

SECOM Trust Systems Co., Ltd.

E-mail address: ca-support@secom.co.jp

1.5.3 Person Determining CP Suitability for the Policy

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

1.5.4 Approval Procedure

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

1.6 Definitions and Acronyms

A~Z

Archive

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

Audit Log

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

Baseline Requirements

A document issued by the CA/Browser Forum that integrates a set of fundamental

requirements for Certificate issuance/administration.

CA (Certification Authority)

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

CA/Browser Forum

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

Certification Service Improvement Committee

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

Code signing

This refers to embedding digital signature data indicating the creator or issuer in a created program file or the like (hereinafter referred to as “code”).

By verifying this digital signature, the code user can obtain information such as the creator, issuer, and expiration date of the code, and can confirm that the code has not been tampered with by a third party.

CP (Certificate Policy)

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

CPS (Certification Practices Statement) :

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

CRL (Certificate Revocation List) :

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

Digital Certificate

Digital data certifying that a public key is owned by the party specified, validity of

which is certified by the digital signature of the relevant CA affixed thereto.

Escrow

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

FIPS140-2

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

HSM (Hardware Security Module)

An encryption device with a tamper-resistant function used for ensuring security in the generation, storage, and use of private keys.

Key Pair

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

LRA Operating Standards

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

OCSP (Online Certificate Status Protocol)

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

OID (Object Identifier) :

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

PKI (Public Key Infrastructure)

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

Private Key

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

Public Key

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

RA (Registration Authority)

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

Repository

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

RFC3647 (Request For Comments 3647)

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

RSA

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

Time-Stamp

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

WebTrustPrinciples and Criteria for Certification Authority (WebTrust for CA)

Standards of internal control and a certification framework based thereon established by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) regarding the reliability of CAs, the security of electronic commerce transactions, and other relevant matters.

WebTrust for Certification Authorities - Publicly Trusted Code Signing Certificates

(WebTrust for CA Code Signing)

Auditing standard established by the American Institute of Certified Public Accountants (AICPA) and the Institute of Chartered Accountants of Canada (CICA) for the examination and certification of certificate authorities when issuing code signing certificates.

X.500

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

2. Publication and Repository Responsibilities

2.1 Repository

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

2.2 Publication of Certificate Information

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

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

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

2.3 Time or Frequency of Publication

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

2.4 Access Controls on Repository

Subscribers and Relying Parties may access the Repository at any time. The protocols used to access the Repository shall be HTTP (Hyper Text Transfer Protocol), HTTPS (HTTP + SSL/TLS data encryption function) and LDAP (Lightweight Directory Access Protocol). Information in the Repository may be accessed via any commonly used Web interface.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

The name of the CA indicated in a Certificate as the issuer and the name of the issuance subject Subscriber are configured according to the X.500 Distinguished Name (DN) format.

3.1.2 Need for Names to Be Meaningful

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

3.1.3 Anonymity or Pseudonymity of Subscribers

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

3.1.4 Rules for Interpreting Various Name Forms

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

3.1.5 Uniqueness of Names

For the certificate issued by this CA, a unique DN is assigned to the certificate subscriber. If the subject name (CN: Common Name) is duplicated, the uniqueness of the DN is ensured by using the Organization, Organizational Unit, or Serial Number attributes.

3.1.6 Recognition, Authentication, and Roles of Trademarks

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

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

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

3.2.2 Authentication of Organization Identity

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

In the case of certification using public documents issued by the national or local governments, a seal certificate (within three months from the date of issuance) or equivalent documents must be submitted.

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

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

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

3.2.3 Authentication of Applicant and Individual Identity

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

Upon issuance of a certificate for a client certificate policy and a data signing certificate policy, an examination of an applicant and a subscriber may be performed by a method determined by the LRA based on the LRA operational standards.

3.2.4 Non-Verified Subscriber Information

SECOM Trust Systems verifies all information specified in BR such as the trade name, name, and location of the certificate subscriber included in the certificate's distinguished name. In addition, in providing the service, there is a case where it is requested to provide information necessary for office procedures such as billing information.

3.2.5 Validation of Authority

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

3.2.6 Criteria for Interoperation

Unilateral cross-certificate by Security Communication RootCA1, or Security Communication RootCA2 has been issued to the CA.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

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

3.3.2 Identification and Authentication for Re-Key after Revocation

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

3.4 Identification and Authentication for Revocation Requests

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

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who May Submit a Certificate Application

An application for this CA can be made by an LRA, corporation, or organization that has been certified by SECOM Trust Systems based on “3.2.2 Authentication of Organization Identity”.

Applications for LRA can be made by persons specified by LRA based on the LRA operational standards.

4.1.2 Enrollment Process and Responsibilities

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

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

SECOM Trust Systems performs identity verification and authentication of the LRA or the corporation, organization in accordance with “3.2 Initial Identification and Authentication”. In applying for a certificate accepted from the LRA, the certificate presented by the LRA is verified and authenticated for the identity of the LRA.

The LRA performs identity verification and authentication based on the LRA operational standards in the manner determined by the LRA.

4.2.2 Approval or Rejection of Certificate Applications

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

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

4.2.3 Time to Process Certificate Applications

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

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

The CA issues a certificate signed using the CA's private key based on the application information.

4.3.2 Notifications to Subscriber of Certificate Issuance

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

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

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

4.4.2 Publication of the Certificate by the CA

The CA does not publish Subscriber Certificates.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

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

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

The use of the private key and certificate of the Subscribers shall be in accordance with "1.4.1 Appropriate Certificate Uses" and the terms and conditions. The

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

4.5.2 Relying Party Public Key and Certificate Usage

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

4.6 Certificate Renewal

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

4.6.1 Circumstances for Certificate Renewal

No stipulation

4.6.2 Who May Request Renewal

No stipulation

4.6.3 Processing Certificate Renewal Requests

No stipulation

4.6.4 Notification of New Certificate Issuance to Subscriber

No stipulation

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

No stipulation

4.6.6 Publication of the Renewal Certificates by the CA

No stipulation

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation

4.7 Certificate renewal with Re-Key

4.7.1 Circumstances for Certificate Renewal

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

4.7.2 Who May Request Certificate Renewal

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

4.7.3 Processing Certificate Renewal Requests

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

4.7.4 Notification of New Certificate Issuance to Subscriber

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

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

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

4.7.6 Publication of the Re-Keyed Certificate by the CA

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

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

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

4.8 Certificate Modification

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

4.8.1 Circumstances for Certificate Modification

No stipulation

4.8.2 Who May Request Certificate Modification

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

4.8.3 Processing Certificate Modification Requests

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

the certificate before the change shall be the same as in “4.9.3 Procedure for Revocation Request”.

4.8.4 Notification of New Certificate Issuance to Subscriber

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

4.8.5 Conduct Constituting Acceptance of Modified Certificate

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

4.8.6 Publication of the Modified Certificates by the CA

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

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Certificate Revocation

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

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

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

- The Subscriber is not performing the obligations thereof set forth in this CP, the CPS, relevant agreements or laws;
- When it has been determined that the Subscriber has been refused to issue a certificate or has been revoked to breach of contract or other reasons;
- When it is determined that the private key of the Subscriber and this CA has been compromised or may be compromised;
- It is recognized that the Certificate is not issued in compliance with BR for code Signing, this CP or CPS;

- It is recognized that the certificate was used for a purpose other than the proper use described in this CP, or was used for a purpose other than that indicated in the contract with SECOM Trust Systems, or the certificate was misused in other ways;
- Use of the domain name or Email address in the certificate gives reasonable evidence that it is no longer legally permitted;
- When it is recognized that a change in the information contained in the certificate;
- When it is recognized that the certificate of the Subscriber has been illegally accessed;
- When it is recognized that the suspicious code was signed using a certificate;
- SECOM Trust Systems recognizes any other situation deemed to necessitate revocation.

4.9.2 Who Can Request Revocation

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

4.9.3 Procedure for Revocation Request

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

4.9.4 Revocation Request Grace Period

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

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

4.9.5 Time within Which CA Shall Process the Revocation Request

Upon receipt of a valid Revocation Request, the CA will promptly process the request and reflect the relevant Certificate information in the CRL.

4.9.6 Revocation Checking Requests

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

4.9.7 CRL Issuance Frequency

The CA will issue a CRL within 24 hours, regardless of whether there has been a revocation processed or not. When a certificate is revoked, a CRL is issued immediately and reflected in the repository.

4.9.8 Maximum Latency for CRLs

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

4.9.9 On-Line Revocation/Status Checking Availability

For the certificates issued under the Code Signing Certificate Policy, online certificate status information is provided through the OCSP server. Policies other than the code signing certificate policy are provided as needed.

4.9.10 On-Line Revocation/Status Checking Requirements

Relying Parties must authenticate the validity of Subscriber Certificates. When verifying a certificate issued by the code signing certificate policy, if not using the CRL posted on the Repository to check for the Revocation registration of a Certificate, the Relying Parties must confirm the Certificate status available through the OCSP server.

4.9.11 Other Forms of Revocation Advertisements Available

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

4.9.12 Special Requirements Regarding Key Compromise

Refer to "4.9.1. Circumstances for Certificate Revocation".

4.9.13 Circumstances for Suspension Who Can Request Suspension

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

4.9.14 Who Can Request Suspension

The suspension of the certificate shall be performed by the Subscriber.

4.9.15 Procedure for Suspension Request

Access the website notified in advance from this CA, and apply for suspension using the login password separately notified.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The revocation information of the CRL or OCSP server shall be confirmed until the expiration date written on the revoked certificate. For the certificates issued by the code signing certificate policy, revocation information shall be confirmed for at least 10 years after the expiration date.

4.10.2 Service Availability

The CA maintains and manages the OCSP server in order to allow 24x7 access to the Certificate status for confirmation. However, the OCSP server may not be available temporarily at times due to maintenance or for any other reason.

4.10.3 Optional Features

No stipulation

4.11 End of Subscription (Registry)

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

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

The CA does not Escrow Subscriber Private Keys.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5. Facility, Management, and Operational Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

Relevant provisions are stipulated in the CPS.

5.1.2 Physical Access

Relevant provisions are stipulated in the CPS.

5.1.3 Power and Air Conditioning

Relevant provisions are stipulated in the CPS.

5.1.4 Water Exposures

Relevant provisions are stipulated in the CPS.

5.1.5 Fire Prevention and Protection

Relevant provisions are stipulated in the CPS.

5.1.6 Media Storage

Relevant provisions are stipulated in the CPS.

5.1.7 Waste Disposal

Relevant provisions are stipulated in the CPS.

5.1.8 Off-Site Backup

Relevant provisions are stipulated in the CPS.

5.2 Procedural Controls

5.2.1 Trusted Roles

Relevant provisions are stipulated in the CPS.

5.2.2 Number of Persons Required per Task

Relevant provisions are stipulated in the CPS.

5.2.3 Identification and Authentication for Each Role

Relevant provisions are stipulated in the CPS.

5.2.4 Roles Requiring Separation of Duties

Relevant provisions are stipulated in the CPS.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

Relevant provisions are stipulated in the CPS.

5.3.2 Background Check Procedures

Relevant provisions are stipulated in the CPS.

5.3.3 Training Requirements

Relevant provisions are stipulated in the CPS.

5.3.4 Retraining Frequency and Requirements

Relevant provisions are stipulated in the CPS.

5.3.5 Job Rotation Frequency and Sequence

Relevant provisions are stipulated in the CPS.

5.3.6 Sanctions for Unauthorized Actions

Relevant provisions are stipulated in the CPS.

5.3.7 Independent Contractor Requirements

Relevant provisions are stipulated in the CPS.

5.3.8 Documentation Supplied to Personnel

Relevant provisions are stipulated in the CPS.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

Relevant provisions are stipulated in the CPS.

5.4.2 Frequency of Processing Audit Log

Relevant provisions are stipulated in the CPS.

5.4.3 Retention Period for Audit Log

Relevant provisions are stipulated in the CPS.

5.4.4 Protection of Audit Log

Relevant provisions are stipulated in the CPS.

5.4.5 Audit Log Backup Procedure

Relevant provisions are stipulated in the CPS.

5.4.6 Audit Log Collection System

Relevant provisions are stipulated in the CPS.

5.4.7 Notification to Event-Causing Subject

Relevant provisions are stipulated in the CPS.

5.4.8 Vulnerability Assessments

Relevant provisions are stipulated in the CPS.

5.5 Records Archival

5.5.1 Types of Records Archived

SECOM Trust Systems stores the following information in addition to logs related to SECOM Passport for Member 2.0 PUB related systems specified in "5.4.1 Types of Events Recorded" in the CPS, as Archive:

- this CP;
- documents associated with agreements of subcontracting if the certification services are outsourced;
- records of audit results and the audit reports;
- Application documents from LRA or corporations, organizations, etc.;
- OCSP server access log.

5.5.2 Retention Period for Archive

SECOM Trust Systems retains its Archive for a minimum of seven (7) years.

5.5.3 Protection of Archive

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

5.5.4 Archive Backup Procedures

If critical data regarding the system related to SECOM Passport for Member 2.0 PUB is changed, the Archive is backed up in a timely manner.

5.5.5 Requirements for Time-Stamping of Records

SECOM Trust Systems uses the NTP (Network Time Protocol) to time synchronize systems related to the Secom Passport for Member 2.0 PUB and Time-Stamps critical information recorded therein.

5.5.6 Archive Collection System

The Archive collection system is included as a function of the systems related to the Secom Passport for Member 2.0 PUB.

5.5.7 Procedures to Obtain and Verify Archive Information

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

5.6 Key Changeover

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

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

SECOM Trust Systems establishes measures against incidents and compromises, including the following, to ensure the prompt recovery of the system related to SECOM Passport for Member 2.0 PUB and relevant operations thereafter:

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

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

In the event of damage to any hardware, software or data of the system related to SECOM Passport for Member 2.0 PUB, SECOM Trust Systems promptly engages in the system recovery efforts using the relevant hardware, software or data that it retains as backup.

5.7.3 Entity Private Key Compromise Procedures

Should it be determined that the CA Private Keys have been or may be compromised or should a disaster or any other unexpected incidents result in a situation that may lead to interruptions or suspensions of the operation of the system related to SECOM Passport for Member 2.0 PUB, SECOM Trust Systems follows the predetermined plans and procedures to securely resume the operation.

5.7.4 Business Continuity Capabilities after a Disaster

In order to ensure prompt recovery to be implemented in the event of an unforeseen circumstance, SECOM Trust Systems deploys preventive measures for the fastest possible recovery of the system related to SECOM Passport for Member 2.0 PUB, including securing of replacement/backup hardware, continual data backups for recovery, and establishment of the recovery procedures.

5.8 CA or RA Termination

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

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The certification infrastructure system generates a CA key pair on a hardware security module (hereinafter, "HSM") compliant with level 3 of FIPS140-2.

The Key Pair generation operation is jointly performed by at least two authorized individuals.

The key pair of the Subscriber is generated on the browser owned by the Subscriber or in the CA facility.

6.1.2 Private Key Delivery to Subscriber

The Subscriber's private key is generated by the Subscriber themselves. When this CA generates a private key for a Subscriber, a PIN for using the private key and a private key are sent by different routes. Or, exchange the PIN and private key in person.

6.1.3 Public Key Delivery to Certificate Issuer

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

6.1.4 CA Public Key Delivery to Relying Parties

Relying Parties may obtain CA Public Keys by accessing the CA Repository.

6.1.5 Key Sizes

The length of a CA Key Pair shall be 2048 bits or 4098 bits in the RSA format.

The length of a Subscriber Key Pair shall be 1024, 2048, 3072 or 4096 bits in the RSA format.

6.1.6 Public Key Parameters Generation and Quality Checking

Parameter generation and parameter strength assessment for the CA Public Keys are performed using the function implemented in the cryptographic module used to generate the Key Pairs.

No stipulation for Subscriber Private Keys.

6.1.7 Key Usage Purposes

"keyCertSign" and "cRLSign" bits shall be specified to the [keyUsage] of the CA Certificate.

One of digitalSignature, nonRepudiation, keyEncipherment, and dataEncipherment is set in the KeyUsage of the certificate of the Subscriber issued by this CA, and the settable combination is appropriately limited for each use of the certificate.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The generation, storage and signing operations of the CA Private Keys are performed using an FIPS140-2 Level 3 conformant HSM.

No stipulation for Subscriber Private Keys.

6.2.2 Private Key Multi-Person Control

Activation, deactivation, backup and other operations relating to CA Private Keys are jointly performed by at least two authorized individuals in a secure environment.

No stipulation for Subscriber Private Keys.

6.2.3 Private Key Escrow

The CA does not Escrow the CA Private Keys.

The CA does not Escrow Subscriber Private Keys.

6.2.4 Private Key Backup

Backup of Private Keys of the CA is jointly performed by at least two authorized individuals and is stored in a secure room as encrypted.

No stipulation for Subscriber Private Keys.

6.2.5 Private Key Archive

The CA does not archive CA Private Keys.

No stipulation for Subscriber Private Keys.

6.2.6 Private Key Transfer into or from a Cryptographic Module

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

No stipulation for Subscriber Private Keys.

6.2.7 Private Key Storage on Cryptographic Module

The private key of this CA is stored in the HSM in an encrypted state.

No stipulation for Subscriber Private Keys.

6.2.8 Method of Activating Private Key

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

6.2.9 Method of Deactivating Private Key

CA Private Keys are jointly deactivated by at least two authorized individuals in a secure room.

No stipulation for Subscriber Private Keys.

6.2.10 Method of Destroying Private Key

CA Private Keys are jointly destroyed by at least two authorized individuals by means of complete initialization or physical destruction. The Private Key backups are also destroyed in the same manner.

No stipulation for Subscriber Private Keys.

6.2.11 Cryptographic Module Rating

Shall be same as specified in "6.2.1 Cryptographic Module Standards and Controls" hereof.

No stipulation for Subscriber Private Keys.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Archives of the CA's public key and the Subscriber's public key are included in this CP "5.5.1 Types of Records Archived".

No stipulation for Subscriber Private Keys.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The validity period of the CA Private Key and Public Key shall not exceed twenty (20) years. No stipulation for Subscriber Private Keys. The validity period of the certificate of the certificate subscriber issued by this CA shall be as follows:

CP/CPS	Validity period
Client certificate policy (Signature Algorithm : Sha1)	Less than 5 Years
Client certificate policy (Signature Algorithm : Sha256)	Less than 5 Years
Certificate Policy for Data Signing (Signature Algorithm : Sha1)	Less than 5 Years
Certificate policy for data signing (Signature Algorithm : Sha256)	Less than 5 Years
Certificate policy for code signing (Signature Algorithm : Sha256)	Less than 3 Years & 3 Months
OCSF Server Certificate Policy (Signature Algorithm : Sha256)	Less than 4 Months

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Relevant provisions are stipulated in the CPS.

6.4.2 Activation Data Protection

Relevant provisions are stipulated in the CPS.

6.4.3 Other Aspects of Activation Data

No stipulation

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

Relevant provisions are stipulated in the CPS.

6.5.2 Computer Security Rating

Relevant provisions are stipulated in the CPS.

6.6 Life-Cycle Security Controls

6.6.1 System Development Controls

Relevant provisions are stipulated in the CPS.

6.6.2 Security Management Controls

Relevant provisions are stipulated in the CPS.

6.6.3 Life-Cycle Security Controls

Relevant provisions are stipulated in the CPS.

6.7 Network Security Controls

Relevant provisions are stipulated in the CPS.

6.8 Time-Stamping

Relevant provisions are stipulated in the CPS.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

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

7.1-1 CA certificate (sha1) profile

Basic Fields		Settings	critical
Version (X.509 certificate version)		Version 3	-
Serial Number (Certificate serial number)		e.g.) 123456789abcdef0	-
Signature Algorithm		SHA-1 with RSAEncryption	-
Issuer	Country	C=JP	-
	Organization	O=SECOM Trust.net	
	Organizational Unit	OU=Security Communication RootCA1	
Validity	NotBefore (Effectiveness start date and time)	e.g.) 2016/10/01 00:00:00 GMT	-
	NotAfter (Validity end date and time)	e.g.) 2026/10/01 00:00:00 GMT * Validity period of less than 10 years	
Subject	Country	C=JP	-
	Organization	O=SECOM Trust Systems CO.,LTD.	
	Organizational Unit	OU=SECOM Passport for Member 2.0 PUB	
	Common Name (CN)	CN=SECOM Passport for Member PUB CA"Number" * "Number" value is optional	
Subject PublicKey Info		Subject RSA Public Key(2048bit)	-
Extension Fields		Settings	
Subject Key Identifier		Subject Public Key Identifier (160-bit SHA-1 hash value of the subject public key)	N
Authority Key Identifier		Authority Public Key Identifier	N

Secom Passport for Member 2.0 PUB
Certificate Policy Ver.5.05

	(160bit SHA-1 hash value of Authority identifier)	
CRL Distribution Points	http://repository.secomtrust.net/SC-Root1/SCRoot1CRL.crl	N
Certificate Policies	Policy: 1.2.392.200091.100.901.1 CPS: https://repository.secomtrust.net/SC-Root1/	N
Key Usage	keyCertSign (Signing a Certificate) cRLSign (Signing a CRL)	Y
Basic Constraints	TRUE (= CA)	Y

7.1-2 CA Certificate (sha256) Profile

Basic Fields		Settings	critical
Version (X.509 Certificate Version)		Version 3	-
Serial Number (Certificate Serial Number)		e.g.) 123456789abcdef0	-
Signature Algorithm		SHA-256 with RSAEncryption	-
Issuer	Country	C=JP	-
	Organization	O=SECOM Trust Systems CO.,LTD.	
	Organizational Unit	The following can be set: OU=Security Communication RootCA2	
Validity	NotBefore (Effectiveness start date and time)	e.g.) 2016/10/01 00:00:00 GMT	-
	NotAfter (Validity end date and time)	e.g.) 2026/10/01 00:00:00 GMT * Validity period of less than 10 years	
Subject	Country	C=JP	-
	Organization	O=SECOM Trust Systems CO.,LTD.	
	Organizational Unit	The following can be set: OU=SECOM Passport for Member 2.0 PUB	
	Common Name (CN)	CN=SECOM Passport for Member PUB CodeSigning CA G"Number" (Certificate Policy for Code Signing)	

Secom Passport for Member 2.0 PUB
Certificate Policy Ver.5.05

	<p>CN=SECOM Passport for CodeSigning CA G"Number" (Certificate Policy for Code Signing)</p> <p>CN=SECOM Passport for Member PUB CA"Number" (Certificate policies other than the above and code signing certificate policies other than the above)</p> <p>* "Number" value is optional</p>	
Subject PublicKey Info	Subject RSA PublicKey (2048 bit or 4096 bit in code signing certificate policy, 2048 bit in other cases)	-
Extension Fields	Settings	
Subject Key Identifier	Subject Public Key Identifier (160-bit SHA-1 hash value of the Subject Public Key)	N
Authority Key Identifier	Authority Public Key Identifier (160-bit SHA-1 hash value of Authority identifier)	N
CRL Distribution Points	http://repository.secomtrust.net/SC-Root2/SCRoot2CRL.crl	N
Authority Information Access	<p>accessMethod ocsp (1.3.6.1.5.5.7.48.1) accessLocation http://scrootca2.ocsp.secomtrust.net</p> <p>accessMethod caIssuers (1.3.6.1.5.5.7.48.2) accessLocation http://repository.secomtrust.net/SC-Root2/SCRoot2ca.cer</p> <p>* Set as required</p>	N
Certificate Policies	<p>Policy: 1.2.392.200091.100.901.4</p> <p>Policy: 2.23.140.1.4.1 (Only a certificate policy for code signing is granted)</p> <p>CPS: URL of repository</p>	N

Secom Passport for Member 2.0 PUB
Certificate Policy Ver.5.05

Key Usage	keyCertSign (Signing a certificate) cRLSign (Signing a CRL)	Y
Extended Key Usage	The followings can be set: clientAuth emailProtection SmartCard Logon codeSigning Adobe Authentic Documents Trust =1.2.840.113583.1.1.5 Microsoft Signer of documents =1.3.6.1.4.1.311.10.3.12 * When SmartCard Logon is selected, clientAuth is also selected. * cordSigning is selected by itself	N
Basic Constraints	TRUE (= CA)	Y

7.1-3 Subscriber Certificate (sha1) Profile

Basic Fields		Settings	critical
X.509 Version (X.509Certificate Version)		Version 3	-
Serial Number (Certificate Serial Number)		e.g.) 123456789abcdef0	-
Signature Algorithm		SHA-1 with RSAEncryption	-
Issuer	Country	C=JP	-
	Organization	O=SECOM Trust Systems CO.,LTD.	
	Organizational Unit	OU=SECOM Passport for Member 2.0 PUB	
	Common Name (CN)	CN=SECOM Passport for Member PUB CA" Number" * "Number" value is optional	
Validity	NotBefore (Effectiveness start date and time)	e.g.) Feb 10 09:55:27 2017 GMT	-
	NotAfter (Validity end date and time)	e.g.) Feb 10 10:25:27 2018 GMT * comply to each certificate policy	
Subject	Country	C=JP	-
	stateOrProvinceName	ST="State or Province Name" 【Optional】	

Secom Passport for Member 2.0 PUB
Certificate Policy Ver.5.05

	localityName	L="Locality Name" 【Optional】
	Organization	O="Organization Name"
	Organizational Unit	OU=" Organizational Unit " 【Optional】
	Organizational Unit	OU="Optional Value" 【 Can be specified arbitrarily】
	Organizational Unit	OU="Optional Value" 【 Can be specified arbitrarily】
	Common Name (Subject name)	CN="Subscriber Name"
	Serial Number	SerialNumber=" Serial Number " 【Can be specified arbitrarily】
Subject PublicKey Info		Subject Public Key Data -

Extension Fields (x.509 v3)	Settings	critical
Authority Key Identifier	Authority Public Key Identifier (160-bit SHA-1 hash value of Authority Public Key)	N
Subject Key Identifier	Subject Public Key Identifier (160-bit SHA-1 hash value of the Subject Public Key)	N
Key Usage	The following can be set: digitalSignature (Digital signature) Non Repudiation (Non Repudiation) keyEncipherment (Key Encipherment) dataEncipherment (Data Encipherment)	Y
Certificate Policies	The following can be set: Policy: 1.2.392.200091.100.381.1 Policy: 1.2.392.200091.100.381.2 Policy: 1.2.392.200091.100.381.6 CPS: https://repo1.secomtrust.net/spcpp/pfm20pub/	N
Subject Alt Name (Subject Alternate Name)	The following can be set: OtherName: UPN="User Principal Name " OtherName: "OID"="Arbitrary String " Rfc822Name:" Mail Address"	N

Secom Passport for Member 2.0 PUB
Certificate Policy Ver.5.05

	dNSName:" Server Name "	
Extended Key Usage	<p>The following can be set:</p> <p>clientAuth (Client Authentication)</p> <p>emailProtection (E-mail Protection)</p> <p>SmartCard Logon (Smart Card Log in)</p> <p>codeSigning (Code Signing)</p> <p>* When SmartCard Logon is selected, also select clientAuth</p> <p>* codeSigning is selected by itself</p>	N
CRL Distribution Points	<p>http://repo1.secomtrust.net/spcpp/pfm20pub/ca"数字 "/fullCRL.crl</p> <p>* "Number" value is optional</p> <p>ldap://repo1.secomtrust.net/"IssuerDN"?certificateRevoc ationList</p>	N
Netscape Certificate Type	<p>The following can be set (Optional):</p> <p>SSL Client</p> <p>S/MIME Client</p> <p>codeSigning</p>	N

7.1-4 Subscriber Certificate (sha256) Profile

Basic Fields		Settings	critical
X.509 Version (X.509 Certificate Version)		Version 3	-
Serial Number (Certificate Serial Number)		e.g.) 123456789abcdef0	-
Signature Algorithm		SHA-256 with RSAEncryption	-
Issuer	Country	C=JP	-
	Organization	O=SECOM Trust Systems CO.,LTD.	
	Organizational Unit	<p>The following can be set:</p> <p>OU=SECOM Passport for Member 2.0 PUB</p>	
	Common Name (CN)	<p>CN=SECOM Passport for Member PUB</p> <p>CodeSigning CA G"Number" (Certificate Policy for Code Signing)</p> <p>CN=SECOM Passport for CodeSigning CA G"Number" (Certificate Policy for Code Signing)</p>	

Secom Passport for Member 2.0 PUB
Certificate Policy Ver.5.05

		CN=SECOM Passport for Member PUB CA"Number" (Certificate policies other than the above and code signing certificate policies other than the above) * "Number" value is optional	
Validity	NotBefore (Effectiveness start date and time)	e.g.) Feb 10 09:55:27 2017 GMT	-
	NotAfter (Validity end date and time)	e.g.) Feb 10 10:25:27 2018 GMT * Comply with each certificate policy	
Subject	Country	C=JP	-
	stateOrProvinceName (State or Province)	ST="State or Province Name" 【Optional】	
	localityName (Locality)	L="Locality Name" 【Optional】	
	Organization	O="Organization Name"	
	Organizational Unit	OU=" Organizational Unit " 【Optional】	
	Organizational Unit	OU="Optional Value" 【 Can be specified arbitrarily】	
	Organizational Unit	OU="Optional Value" 【 Can be specified arbitrarily】	
	Common Name (Subject Name)	CN="Subscriber Name"	
	Serial Number	SerialNumber=" Serial Number " 【 Can be specified arbitrarily】	
Subject PublicKey Info (Subject Public Key Information)		Subject's Public Key Data 2048 bit, 3072 bit or 4096 bit in the code signing certificate policy, 2048 bit in other cases	-

Extension Fields (x.509 v3)	Settings	critical
Authority Key Identifier	Authority Public Key Identifier (160-bit SHA-1 hash value of Authority public key)	N

Secom Passport for Member 2.0 PUB
Certificate Policy Ver.5.05

Subject Key Identifier	Subject Public Key Identifier (160-bit SHA-1 hash value of the Subject Public key)	N
Key Usage	The following can be set: digitalSignature (Digital Signature) Non Repudiation (Repudiation) keyEncipherment (Key Encipherment) dataEncipherment (Data Encipherment)	Y
Certificate Policies	The following can be set: Policy: 1.2.392.200091.100.381.4 Policy: 1.2.392.200091.100.381.5 Policy: 1.2.392.200091.100.381.8 CPS: URL of repository Policy: 2.23.140.1.4.1 (Only a Certificate Policy for Code Signing is granted)	N
Subject Alt Name (Subject Alternate Name)	The following can be set: OtherName: UPN="User Principal Name " OtherName: "OID"=" Any character string " Rfc822Name:" Mail address" * Do not use code signing certificate policies	N
Extended Key Usage	The following can be set: clientAuth (Client Authentication) emailProtection (E-mail Protection) SmartCard Logon (Smart Card Logon) codeSigning (Code Signing) Adobe Authentic Documents Trust =1.2.840.113583.1.1.5 Microsoft Signer of documents =1.3.6.1.4.1.311.10.3.12 * When SmartCard Logon is selected, also select clientAuth * codeSigning (Code Signing) is selected by itself	N
CRL Distribution Points (CRL Distribution Points)	http://repo1.secomtrust.net/spcpp/pfm20pub/codecag"Number"/fullCRL.crl (Certificate policy for code signing) http://repo1.secomtrust.net/spcpp/pfm20pub/ca"Number"/fullCRL.crl (Certificate policies other than the above and code signing certificate policies other than the above)	N

	<p>* "Number" value is optional</p> <p>ldap://repo1.secomtrust.net/"IssuerDN"?certificateRevocationList</p>	
Authority Information Access	<p>accessMethod</p> <p>ocsp (1.3.6.1.5.5.7.48.1)</p> <p>accessLocation</p> <p>URL of OCSP responder</p> <p>accessMethod</p> <p>caIssuers (1.3.6.1.5.5.7.48.2)</p> <p>accessLocation</p> <p>URL of Intermediate CA certificate</p> <p>* This part should be set as required</p>	N
Netscape Certificate Type	<p>The following can be set (Optional):</p> <p>SSL Client</p> <p>S/MIME Client</p> <p>codeSigning</p>	N

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

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

7.1.1 Version Number(s)

This CA applies version 3.

7.1.2 Certificate Extension

Certificates issued by this CA use certificate extension fields.

7.1.3 Algorithm Object Identifier

The algorithm OID used in this service is as follows:

Security Communication RootCA1 algorithm OID

Algorithm	Object Identifier
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

Security Communication RootCA2 algorithm OID

Algorithm	Object Identifier
sha256 With RSA Encryption	1.2.840.113549.1.1.11
RSA Encryption	1 2 840 113549 1 1 1

7.1.4 Name Format

This CA and the subscribers are uniquely identified by the DN defined according to the X.500 distinguished name.

7.1.5 Name Constraints

Set in the CA if necessary.

7.1.6 Certificate Policy Object Identifier

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

7.1.7 Use of Policy Constraint Extensions

Not set.

7.1.8 Policy Qualifier Syntax and Semantics

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

7.1.9 How to interpret Critical Certificate Policy Extensions

Not set.

7.2 CRL Profile

7.2-1 CRL (sha1) Profile

Basic Fields		Settings	critical
Version (X.509CRL Version)		Version 2	-
Signature Algorithm		SHA-1 with RSAShAEncryption	-
Issuer	Country	C=JP	-

Secom Passport for Member 2.0 PUB
Certificate Policy Ver.5.05

	Organization	O=SECOM Trust Systems CO.,LTD.	
	Organizational Unit	OU=SECOM Passport for Member 2.0 PUB	
	Common Name (CN)	CN= SECOM Passport for Member PUB CA"Number" * "Number" value is optional	
This Update (Update date and time)		e.g.) Oct 1 00:00:00 2016 GMT	-
Next Update (Next scheduled update date and time)		e.g.) Oct 5 00:00:00 2016 GMT * Actual update interval 24 hours, validity period 96 hours	
Revoked Certificates	Serial Number (Revoked certificate serial number)	e.g.) 1234567890	-
	Revocation Date	e.g.) 2016/09/01 12:00:00 GMT	
	Reason Code (Revocation reason)	e.g.) cessation of operation (operation suspension) * Setting is optional	
Extension Fields		Settings	
CRL Number		e.g.) 1 (Integer value indicating the order in which CRLs are issued)	N
Authority Key Identifier		Authority public key identifier (Public key SHA-1 hash value)	N

7.2-2 CRL (sha256) Profile

Basic Fields		Settings	critical
Version (X.509CRL Version)		Version 2	-
Signature Algorithm		SHA-256 with RSAEncryption	-
Issuer	Country	C=JP	-
	Organization	O=SECOM Trust Systems CO.,LTD.	
	Organizational Unit	The following can be set: OU=SECOM Passport for Member 2.0 PUB	

	Common Name (CN)	CN=SECOM Passport for Member PUB CodeSigning CA G"Number" (Certificate Policy for Code Signing) CN=SECOM Passport for CodeSigning CA G"Number" (Certificate Policy for Code Signing) CN=SECOM Passport for Member PUB CA"Number" (Certificate policies other than the above and code signing certificate policies other than the above) * "Number" value is optional	
This Update (Update date and time)		e.g.) Oct 1 00:00:00 2016 GMT	-
Next Update (Next scheduled update date and time)		e.g.) Oct 5 00:00:00 2016 GMT * Actual update interval 24 hours, validity period 96 hours	
Revoked Certificates	Serial Number (Revoked Certificates Serial Number)	e.g.) 1234567890	-
	Revocation Date	e.g.) 2016/09/01 12:00:00 GMT	
	Reason Code (Revocation reason)	e.g.) cessation of operation (operation suspension) * Setting is optional	
Extension Fields		Settings	
CRL Number		e.g.) 1 (Integer value indicating the order in which CRLs are issued)	N
Authority Key Identifier		Authority Public Key Identifier (SHA- 1 hash value of the Public Key)	N

7.2.1 Version Number(s)

This CA applies CRL version 2.

7.2.2 Certificate Revocation Lists and CRL Entry Extensions

Use the CRL extension field issued by this CA.

7.3 OCSP Profile

7.3-1 OCSP Profile (sha256)

Basic Fields		Settings	critical
Version		Version 3	-
Serial Number		e.g.)0123456789	-
Signature Algorithm		SHA-256 with RSAEncryption	-
Issuer	Country	C=JP	-
	Organization	O=SECOM Trust Systems CO.,LTD.	
	Organizational Unit	The following can be set: OU=SECOM Passport for Member 2.0 PUB	
	Common Name (CN)	CN=SECOM Passport for Member PUB CodeSigning CA G"Number" (Certificate policy for code signing) CN=SECOM Passport for CodeSigning CA G"Number" (Certificate policy for code signing) CN=SECOM Passport for Member PUB CA"number" (Certificate policies other than the above and code signing certificate policies other than the above) * "Number" value is optional	
Validity	NotBefore (Effectiveness start date and time)	e.g.) 2017/1/1 00:00:00 GMT	-
	NotAfter (Validity end date and time)	e.g.) 2017/5/1 00:00:00 GMT * Validity period 4 months	-
Subject	Country	C=JP	-
	Organization	O=SECOM Trust Systems CO.,LTD.	-
	Organizational Unit	OU=SECOM Passport for Member 2.0 PUB Service	-
	Common Name (CN)	OCSP Server Name (Required)	-
Subject Public Key Info (Subject Public Key Information)		Subject Public Key Data	-
Extension Fields		Settings	
KeyUsage (Key Usage)		digitalSignature	Y
ExtendedKeyUsage (Extended Key Usage)		OCSPSigning	N

OCSP No Check	null	N
CertificatePolicies (Certificate Policy)	policyIdentifier OID= 1.2.392.200091.100.381.9 policyQualifiers policyQualifierId=CPS qualifier= URL of repository	N
Authority Key Identifier	SHA-1 hash value of Authority public key (160 bits)	N
Subject Key Identifier	SHA-1 hash value of Subject Public Key (160 bits)	N

7.3.1 Version Number(s)

The CA uses OCSP Version 1.

7.3.2 OCSP Extensions

Use the OCSP extended field issued by the CA.

8. Compliance Audit and Other Assessments

8.1 Frequency and Circumstances of Assessment

The CA performs compliance audits at least once a year to examine if the operation of the services is in compliance with this CP and the CPS. Regarding the operation of the S/MIME certificate and the Code Signing Certificate, a compliance audit based on the WebTrust standard shall be conducted more than once a year to ensure that the operation is performed in compliance with this CP and CPS.

8.2 Identity/Qualifications of Assessor

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

8.3 Assessor's Relationship to Assessed Entity

The auditor shall select an auditor who is independent of the operations of the audited department or has no special interest in SECOM trust Systems, except for matters relating to the audit. In performing the audit, the audited department shall cooperate with the audit.

8.4 Topics Covered by Assessment

Audits are performed with respect to business activities for operation of the CA.

Audits may also be performed, conforming to the standards for CA set forth in WebTrust for CA, and WebTrust for CA Code Signing.

8.5 Actions Taken as a Result of Deficiency

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

8.6 Communication of Results

Audit results are reported to SECOM Trust Systems from Auditor. SECOM Trust Systems never would disclose audit results to the outside, except when there is a request for disclosure based on law, when there is a request for disclosure from related organizations based on a contract with SECOM Trust Systems, and when approved by the Certification Service Improvement Committee.

Verification reports based on WebTrust for CA, and WebTrust for CA Code Signing are

made available on a specific website conforming to the rules thereof.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Fees for Issuing or Renewing Certificates

Stipulated separately in contracts.

9.1.2 Certificate Access Fee

No stipulation.

9.1.3 Expiration or Access Fee for Status Information

No stipulation.

9.1.4 Fees for Other Services

No stipulation.

9.1.5 Refund Policy

Stipulated separately in contracts.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

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

9.2.2 Other Assets

No stipulation.

9.2.3 End entity Insurance or Warranty coverage

No stipulation.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

Relevant provisions are stipulated in the CPS.

9.3.2 Information Not Within the Scope of Confidential Information

Relevant provisions are stipulated in the CPS.

9.3.3 Responsibility to Protect Confidential Information

Relevant provisions are stipulated in the CPS.

9.4 Privacy of Personal Information

9.4.1 Personal Information Protection Plan

Relevant provisions are stipulated in the CPS.

9.4.2 Information Treated as Personal Information

Relevant provisions are stipulated in the CPS.

9.4.3 Information that is not considered Personal Information

Relevant provisions are stipulated in the CPS.

9.4.4 Responsibility for protecting Personal Information

Relevant provisions are stipulated in the CPS.

9.4.5 Notice and Consent regarding use of Personal Information

Relevant provisions are stipulated in the CPS.

9.4.6 Disclosure of Information in accordance with Judicial or Administrative Procedures

Relevant provisions are stipulated in the CPS.

9.4.7 Other Information Disclosure Conditions

Relevant provisions are stipulated in the CPS.

9.5 Intellectual Property Rights

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

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

9.6 Representations and Warranties

9.6.1 CA Representation and Warranties

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

- Secure generation and management of CA Private Keys;
- Accurate issuance, revocation and management of certificates based on LRA and applicant's application;
- management and operational monitoring of the systems;
- issuance and publication of CRLs;
- provision of access to the OCSP server; and
- maintenance and administration of the Repository.

9.6.2 RA Representations and Warranties

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

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

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

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

9.6.3 Applicant and Subscriber Representations and Warranties

Applicants and Subscribers shall bear obligations to the following:

- provide accurate and complete information to this CA or LRA when applying for a certificate;
- promptly notify this CA or LRA of any change in the information provided therein;
- protect their own Private Keys against compromise;
- use the Certificates conforming to the provisions of this CP and CPS; and
- promptly request this CA or LRA to revoke the Subscriber Certificate in case the Subscriber determines that the Private Key corresponding to the Public Key

indicated therein has or may have been compromised, or there has been a change in the registered information, or if this CA instructs to revoke a certificate based on "4.9.1 Reason for Certificate Revocation".

9.6.4 Relying Party Representations and Warranties

Relying Parties shall bear the obligations to the following:

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

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimer of Warranties

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

9.8 Limitations of Liability

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

- Any damage arising from unlawful conduct, unauthorized use, negligence or any other cause not attributable to SECOM Trust Systems;
- any damage attributable to the failure of a Subscriber to perform its obligations;
- any damage attributable to LRA or a Subscriber system;
- damages attributable to a hardware or software defect or malfunction or any other behavior of LRA or the Subscriber system;
- damages caused by information published in a Certificate, a CRL or on the OCSP server due to the reasons not attributable to SECOM Trust Systems;
- any damage incurred in an outage of the normal communication due to reasons not attributable to SECOM Trust Systems;

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

9.9 Indemnities

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

9.10 Term and Termination

9.10.1 Term

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

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

9.10.2 Termination

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

9.10.3 Effect of Termination and Survival

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

9.11 Individual Notices and Communications with Participants

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

9.12 Amendments

9.12.1 Procedure for Amendment

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

9.12.2 Notification Method and Timing

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

9.12.3 Circumstances under Which OID Must Be Changed

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

9.13 Dispute Resolution Procedures

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

9.14 Governing Law

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

9.15 Compliance with Applicable Law

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

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

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

9.16.2 Assignment

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

9.16.3 Severability

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

9.16.4 Enforcement

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

9.16.5 Irresistible Force

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

9.17 Other Provisions

No stipulation