บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน)
Internet Thailand Public Company Limited

One Certification Authority

Certificate Policy

(Certification Policy Identifier (OID): 2.16.764.1.1.3.1)

Document Revision History

Date	Version	Description
12/11/2018	1.0	First baseline

Table of Contents

1. Introduction

1.1 Overview

The Electronic Transactions Act sets out the legal framework for the public key infrastructure (PKI) with the objectives of facilitating the use of electronic transactions in a secure manner for commercial and other purposes. PKI is composed of many elements, including legal obligations, policies, hardware, software, databases, networks, personnel and operating procedures. The center of trust in PKI is Certification Authority (CA), who issues a digital certificate to a person or legal entity (who may be another CA) by using a collection of hardware, software, personnel, and operating procedures. The digital certificate will bind a public key to that person or legal entity. It allows relying parties to trust signatures or assertions made by the person or legal entity using the private key that corresponds to the public key contained in the certificate. A digital certificate when combined with private key can be used to verify the identity in electronic transactions using the Digital Signature mechanism. Any person or legal entity who wishes to use a digital certificate must pass the certification authority's authentication procedures.

In an environment where there are multiple certification authorities, certificate usage and authentication will be troublesome if the certification authorities are not in a Trust Relationship model. The basic way to solve the problem is to build a trust relationship between each pair of certification authorities, which will be unmanageable in the long run. Therefore, the Electronic Transactions Commission (ETC) has agreed to form a trust relationship in the hierarchy model for all certification authorities in Thailand.

In 2007 (B.E. 2550), the Ministry of Information and Communication Technology (MICT) has established the Thailand National Root Certification Authority or Root CA with the objective to centralize the management of trust relationship and serve as the hub of trust, so called Trust Anchor, so that certificates issued by subordinate certification authorities can seamlessly work together both locally and internationally.

The CP is the principal statement of policy governing Internet Thailand Public Company Limited 's CAs under the Thailand NRCA. The CP applies to Internet Thailand Public Company Limited 's all subordinate certification authorities under Thailand NRCA and thereby provides assurances of uniform trust throughout the Thailand NRCA. The CP sets forth requirements that Internet Thailand Public Company Limited 's subordinate certification authorities under Thailand NRCA must meet. At this time only one subordinate CA: One CA is established by INET and operate on INET's infrastructure by One Authen.

Mission of One CA includes:

- Certificate issuance, publication, and revocation for certification authorities owned by Internet Thailand Public Company Limited in Thailand;

The purpose of this document is to identify a baseline set of security controls and practices to support the secure issuance of certificates. This baseline set of controls has been written in the form of a Certificate Policy (CP). As defined by ITU Recommendation X.509, a Certificate Policy is "a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements." That is, a Certificate Policy defines the expectations and requirements of the relying party community that will trust the certificates issued by its CAs. The governance structure that represents the relying party is known as Policy Authority (PA). As such, PA is responsible for identifying the appropriate set of requirements for a given community and oversees the CAs that issue certificates for that community. CAs owned by Internet Thailand Public Company Limited. which operated under Thailand NRCA Trust Model must be conformance to this Certificate Policy.

This Certificate Policy is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) Certificate Policy, RFC 5280 and Certification Practices Framework [RFC3647].

1.2 Document Name and Identification

This Certificate Policy is published by the Internet Thailand Public Company Limited and specifies the baseline set of security controls and practices that CAs owned by Internet Thailand Public Company Limited located in Thailand employ in issuing, revoking or suspending and publishing certificates.

Internet Assigned Numbers Authority (IANA) has assigned the country OID 2.16.764 to Thailand. For identification purpose, this Certificate Policy bears an Object Identifier (OID) "2.16.764.1.1.3.1

1.3 PKI Participants

1.3.1 Certification Authority

A Certification Authority (CA) is responsible for issuance of a digital certificate to a person or legal entity (known as an applicant) by using a collection of hardware, software, personnel, and operating procedures that create, sign, and issue public key certificates to subscribers. This includes centralized, automated systems such as card management systems. The CA is responsible for issuing and managing certificates including:

- Approving the issuance of all certificates, including those issued to RAs
- Publication of certificates
- Revocation of certificates
- Generation and destruction of CA signing keys
- Establishing and maintaining the CA system
- Establishing and maintaining the Certification Practice Statement (CPS)
- Ensuring that all aspects of the CA services, operations, and infrastructure related to certificates issued under this CP are performed in accordance with the requirements, representations, and warranties of the CP.

In this CP, CAs means those established and owned by Internet Thailand Public Company Limited, And have the intention to be first level subordinate CAs under NRCA.

1.3.2 Registration Authority

A Registration Authority (RA) is responsible for collection and authentication of each subscriber's identity and information that is to be entered into the subscriber's public key certificate. RA performs its function in accordance with the CPS of the CA and is responsible for:

- The registration processes
- The identification and authentication process.

1.3.3 Subscribers

A Subscriber is a person or legal entity whose name appears as the subject in a certificate. The Subscriber asserts the use of the key and certificate in accordance with the Certificate Policy asserted in the certificate. The term “Subscriber” as used in this CPS refers only to those who request certificates for uses other than signing and issuing certificates or certificate status information.

1.3.4 Relying Parties

A Relying Party is a person or entity that acts in reliance on the validity of the binding of the Subscriber’s name to a public key. The Relying Party uses a Subscriber’s certificate to verify a digital signature that is generated using the private key corresponding to the public key listed in a certificate. A Relying Party may or may not be a Subscriber within Root CA.

1.3.5 Other Participants

The CA under this CP may select other authorities, which provide related trust services, such as time stamp authority (TSA), and card management center as the collaborative partners, the related information shall be disclosed on the website and the collaboration mechanism and mutual rights and obligations shall be set down in the CPS to ensure the efficiency and reliability of the CA’s quality.

1.3.5.1 Policy Authority

A Policy Authority (PA) decides that a set of requirements for certificate issuance and use are sufficient for a given application. The PA has roles and responsibilities as follows:

1. Establish certificate policy and certification practice statement of subordinate certification authorities owned by Internet Thailand Public Company Limited under the Thailand NRCA trust model;
2. Arrange for a review of certificate policy and certification practice statement of subordinate certification authorities owned by Internet Thailand Public Company Limited under the Thailand NRCA trust model on a regular basis.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The usage of a certificate issued under this CP is suitable to support the following core security needs:

- authentication - provides assurance of the identity of the Subject of the certificate;
- encipherment – encrypt electronic data or key;
- verify a digital signature by the private key corresponding to the public key certificate;

The certificate is appropriate for identity authentication and information encryption required for e-commerce transactions or financial transactions. Including (but not limited to) the following applications: e-bank electronic transactions, account transfer authorization, account notifications, applicant instruction services, Internet orders, Internet tax filing, on-line document approval and Internet identity authentication.

Subscribers must carefully read the CP/CPS and watch for CP/CPS updates before using and trusting the certificate services provided by Internet Thailand Public Company Limited

1.4.2 Prohibited Certificate Uses

A certificate issued in accordance with this CP shall be used only for the purpose as specified in Section 1.4.1, and in particular shall be used only to the extent the use is consistent with applicable laws.

1.5 Policy Administration

1.5.1 Organization Administering the Document

Internet Thailand Public Company Limited is responsible for all aspects of this CP.

1.5.2 Contact Person

INET ONE CA

Address: 1768 Thai Summit Tower, 16th Floor and IT Floor New Petchaburi Road, Khwaeng Bang Kapi, Khet Huay Khwang, Bangkok 10310

Tel: +66-2257-7000

Email: ra@inet.co.th

Website: https://ca.inet.on.th

1.5.3 Person Determining CPS Suitability for the Policy

PA shall determine the CPS of each CA that issues certificates under this CP.

1.5.4 CPS Approval Procedures

CAs issuing under this CP are required to meet all facets of the CP. The CAs shall reviewed CPS at least annually. PA has defined approval procedures as follows:

1. CA issuing certificates under this CP submits CPS to the PA
2. PA reviews and make recommendations
3. Subordinate CAs submitted CPS and propose to PA for Approval.
4. PA reviews the submitted CPS and approves.

    4.1 In case PA has no further comments, PA approves the CPS.

    4.2 In case PA has comments, PA returns the CPS to the applicant CA for proper modification or correction before resubmission.

5. Applicant CA announces and publishes the CPS to the specified channel.

1.5.5 CP Review and update Procedures

CAs operating under this CP shall recheck the latest of Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates from https://cabforum.org/baseline-requirements-documents or http://www.webtrust.org at least quarterly for the purpose of development, implementation, enforcement and annually update of a Certificate Policy and Certificate Practice Statement. https://cabforum.org/baseline-requirements-documents or at least quarterly for the purpose of development, implementation, enforcement and annually update of a Certificate Policy and Certificate Practice Statement.

1.6 Definitions and Acronyms

1.6.1 Definitions

Table 1 Terms and Definitions

Term	Definition
Certificate	A form of electronic documents used for verifying the relationship between entities and public key. A certificate is issued in compliance with ITU-T Recommendation X.509 (11/08): Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks 15782 -- Open Systems Interconnection -- The Directory: Public-key and attribute certificate frameworks.
Certificate Policy (CP)	The document, which is entitled “INET Certification Authority Certificate Policy”, describes the principal statement and applications of certificates.
Certificate Repository	Source for storage and publication of certificates and certificate revocation lists.
Certificate Revocation	A certificate may be revoked prior to its expiration date. Once revoked, it can no longer be used.
Certification Authority (CA)	An entity authorized to issue, manage, revoke, and renew certificates.
Certification Practice Statement (CPS)	The document describes the procedures and scope of the certification authority, duties and obligations of the parties that acts in reliance of a certificate.
Cryptographic Module	Specialized equipment used to maintain, manage and operate the key pair.
Digital Signature	A Digital Signature is a mathematical scheme for demonstrating the authenticity and integrity of a digital message or document.
Directory Service	A storage for publication of certificates and certificate revocation lists following the X.500 Standard or LDAP.
Entity	Individual, Server, Operating Unit/Site, or any Device that is under the control of the individual.
Key Pair	A Key Pair refers to two separate keys of the asymmetric cryptographic system, one of which is secret (Private Key) and another is public (Public Key).

	The two parts of the key pair are mathematically linked in the ways that one key locks or encrypts the plaintext, and the other unlocks or decrypts the cipher text. Neither key can perform both functions by itself. The Key Pair can be used to authenticate the digital signature as well as maintain confidentiality of information.
OCSP (Online Certificate Status Protocol)	A protocol used for verifying status of a certificate.
Private Key	The key used to create a digital signature and can be used to decrypt the message that is encrypted with its pair of public key, to obtain the original message.
Public Key	The key used to verify a digital signature to ensure the integrity of electronic message and also to encrypt message to maintain its confidentiality.

1.6.2 Acronyms

Table 2 Acronyms

Acronym	Term
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
NRCA	National Root Certification Authority
PA	Policy Authority
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RA	Registration Authority
ETDA	Electronic Transactions Development Agency (Public Organization)

2. Publication and Repository Responsibilities

2.1 Repositories

All CAs that issue certificates under this policy are obligated to post all certificates issued by or to the CA and CRLs issued by the CA in a repository that is publicly accessible through all Uniform Resource Identifier (URI) references asserted in valid certificates issued by that CA. To promote consistent access to certificates and CRLs, the repository shall implement access controls and communication mechanism to prevent unauthorized modification or deletion of information.

2.2 Publication of Certification Information

This CP shall be publicly available. The CA that issues certificates under this CP shall make available at least one on-line and publicly accessible repository for the publication of certificates and related information. It shall ensure that its repository or repositories are implemented through trustworthy systems.

2.3 Time or Frequency of Publication

The CA that issues certificates under this CP shall publish its certificates and CRLs as soon as possible after issuance, an updated version of this CP and/or CPS will be made publicly available within three working day of the approval of changes.

2.4 Access Controls on Repositories

The CA that issues certificates under this CP shall protect information not intended for public dissemination or modification. Certificates and CRLs in the repository shall be publicly available through the Internet. The CA shall detail what information in the repository shall be exempt from automatic availability and to whom, and under which conditions the restricted information may be made available. The CA shall maintain effective procedures and controls over the management of its repositories.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

The CAs operating under this CP shall issue certificates with a non-empty Subject name complying with X.501 Distinguished Names (DNs). The CAs shall have the right to decide whether or not to accept the subject alternative name. If used, the Subject Alternative Name extension may be included and marked non-critical.

3.1.2 Need for Names to be Meaningful

The names contained in a certificate must be in English or Thai with commonly understood semantics permitting the determination of the identity of the individual or organization that is the Subject and Issuer of the certificate, for example, through the verification of Jurisdiction of Incorporation and/or Certificate of Registration issued by the Department of Business Development, Ministry of Commerce.

3.1.3 Anonymity or Pseudonymity of Subscribers

The CA that issues certificates under this CP shall not issue anonymous or pseudonymous certificates.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting distinguished name forms are specified in X.501. Rules for interpreting e-mail addresses are specified in RFC 2822.

3.1.5 Uniqueness of Names

The CA that issues certificate under this CP must ensure that the subject name assigned to a subscriber must identify that subscriber uniquely and unambiguously.

3.1.6 Recognition, Authentication, and Role of Trademarks

The CA that issues certificates under this CP reserves no liability to any certificate applicant on the usage of Distinguished Names appearing in a certificate. The right to use the name is the responsibility of the applicant and must be in accordance to the relevant laws, regulations, legal obligations or announcements.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

In all cases where the party named in a certificate generates its own keys, that party shall be required to prove possession on the private key, which corresponds to the public key in the certificate request. In the case where key generation is performed under the CA or RA's direct control, proof of possession is not required. The CA shall state in its CPS the method to prove possession of private key.

3.2.2 Authentication of Organization and Domain Identity

For subscriber organization certificates, the CA shall verify the existence of the organization by verifying the Certificate of Corporate Registration issued by the Department of Business Development, Ministry of Commerce. Copies of official documents require certified true copy from authorized representative.

3.2.2.1 Identity

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

1. A government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;

2. A third party database that is periodically updated and considered a Reliable Data Source;

3. A site visit by the CA or a third party who is acting as an agent for the CA; or

4. An Attestation Letter.

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

3.2.2.2 DBA/Tradename

Not Applicable

3.2.2.3 Verification of Country

Not Applicable

3.2.2.4 Validation of Domain Authorization or Control

Not Applicable

3.2.2.5 Authentication for an IP Address

Not Applicable

3.2.2.6 Wildcard Domain Validation

Not Applicable

3.2.2.7 Data Source Accuracy

Not Applicable

3.2.2.8 CAA Records

Not Applicable

3.2.3 Authentication of Individual Identity

Public key certificates bind public keys to identities. However, the entity to be identified depends on the application for which the public keys are used. Identifying different types of entity requires different evidence and procedures. The CA that issues certificates under this CP shall state in its CPS the types of entity that the CA will support and details the required evidence and procedures.

3.2.4 Non-verified Subscriber Information

Information that is not verified shall not be included in certificates.

3.2.5 Validation of Authority

Registration Authority is responsible for verifying and authenticating an authorized representative of a juristic person by checking the following documents

- Authorized Representative Appointment Letter from the relevant juristic person or other document of the same kind, corporate sealed and singed by the authorized director of the juristic person, as specified under the Certificate of Corporate Registration issued by the Department of Business Development, Ministry of Commerce, with a certified true copy of identification card or passport of the authorized director of such juristic person.
- A certified true copy of identification card or passport of the authorized representative of the juristic person. RA verifies and endorses the integrity of documents.

3.2.6 Criteria for Interoperation

Internet Thailand Public Company Limited's CA under the Thailand NRCA. One CA will follow with the details in Application Form for SubCA Certificate and the notice of NRCA.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-key

Identification and authentication requirements are specified in Section 3.2.

3.3.2 Identification and Authentication for Re-key after Revocation

Identification and authentication requirements are specified in Section 3.2.

3.4 Identification and Authentication for Revocation Request

Identification and authentication requirements are specified in Section 3.2.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Certificate applications may be submitted to the CA that issues certificates under this CP by the Subscribers listed in Section 1.3.3, or an RA on behalf of the Subscriber.

4.1.2 Enrollment Process and Responsibilities

All communications among the CA and the RA supporting the certificate application and issuance process shall be authenticated and protected from modification; any electronic transmission of shared secrets and personally identifiable information shall be protected. Communications may be electronic or out-of-band. Where electronic communications are used, cryptographic mechanisms commensurate with the strength of the public/private key pair shall be used. Out-of-band communications shall protect the confidentiality and integrity of the data.

Subscribers are responsible for providing accurate information on their certificate applications.

4.2 Certificate Application Processing

The CA shall state the initial registration and certificate re-key application procedures, application processing locations and websites in the CPS.

4.2.1 Performing Identification and Authentication Functions

Information in certificate applications must be verified as accurate before certificates are issued. Procedures to verify information in certificate applications shall be specified in the CPS. In cases where the certificate request does not contain all the necessary information about the Applicant, the CA SHALL obtain the remaining information from the Applicant or, having obtained it from a reliable, independent, third-party data source, confirm it with the Applicant. The identification and authentication of the subscriber must meet the requirements specified for subscriber authentication as specified in Sections 3.2 and 3.3. The components of the PKI (e.g., CA or RA) that are responsible for authenticating the subscriber's identity in each case must be identified in the CPS.

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

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

4.2.2 Approval or Rejection of Certificate Applications

Any certificate application that is received by a CA that issues certificates under this CP, for which the identity and authorization of the applicant has been validated, will be duly processed. However, the CA must reject any application for which such validation cannot be completed.

RA will coordinate with the CA to approve or reject certificate applications and notifies the results to subscribers.

4.2.3 Time to Process Certificate Applications

Provided that the applicant submits the information in full which conforms to CP and CPS requirements, the CA and RA shall complete the certification application processing within 30 business days. The time to process certificate applications may be stated in the CPS, subscriber terms and conditions or the certificate applicant contract.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

Upon receiving the request, the CA that issues certificate under this CP and its RA will:

- Verify the identity of the requester as specified in Section 3.2;
- Verify the authority of the requester and the integrity of the information in the certificate request as specified in Section 4.1;
- CAO must ensure the accuracy information in a CSR that conform with Section 6. If not conform in Section 6 CAO must be reject that Sub CA CSR.

- Generate and sign a certificate if all certificate requirements have been met (in the case of an RA, have the CA sign the certificate); and
- Make the certificate available to the subscriber after confirming that the subscriber has formally acknowledged their obligations as described in Section 9.6.3.

All authorization and other attribute information received from a prospective subscriber shall be verified before inclusion in a certificate. The responsibility for verifying prospective subscriber data shall be described in the CA's CPS.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

CAs operating under this CP, or via a RA if applicable, will notify the subscriber of the creation of a certificate and make the certificate available to the subscriber.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Upon the receipt of a certificate, the subscriber must proceed with the following:

- The subscriber must verify the information contained in the certificate and either accept or reject the certificate.
- If the subscriber fails to receive or fails to accept the certificate within ten business days from the CA, the CA shall revoke such certificate.

4.4.2 Publication of the Certificate by the CA

All certificates shall be published in repositories.

Publication arrangements of subscriber certificate are specified in the CPS of the CA.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

CAs operation under this CP will notify the subscriber via email.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers refer to the entities who have applied for and obtained a certificate approved by the CAs operating under this CP. The generation of key pairs for Subscribers shall comply with the regulations in Section 6.1.1 of this CP. Subscribers must have the right and capability to independently possess and control the private key corresponding to the certificate. Subscribers themselves must not issue certificates to others. Subscribers shall protect against unauthorized use and disclosure of the private key and only use the private key for correct key usages (key usages are listed in the key usage extension of the certificate). Subscribers must correctly use the certificate according to regulations specified in the certificate policies extension of the certificate.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties refers to third parties who trust the connecting relationship between the certificate subject name and public key. Relying parties shall use software that complies with ITU-T X.509 and Internet Engineering Task Force (IETF) RFC related standards and specifications.

Relying parties must use the CA certificates and certificate status information to verify the validity of the certificates used. In other words, Relying Parties shall assess the certificates described as follows before any act of reliance:

- The accuracy of the digital signature in the CA`s certificate and subscriber hierarchy (e.g. path validation).
- The validity period of the certificates of CA and subscriber (e.g. the certificates should not expire by the time of use).
- The status of the certificates and all the CAs and their parent in every level of the hierarchy involved (e.g. the certificate should not be revoked or suspended).
- The appropriateness of the certificate usage should be in accordance with this CP and the CPS of the Issuing CA.

After verifying the validity of the certificate, the certificate may be used for the following purposes:

- Verify the integrity of electronic documents with digital signatures

- Verify the identity of the document signature generator.
- Establish secure communication channels between subscribers.

The above certificate status information may be obtained through the CRL or Online Certificate Status Protocol (OCSP) service. The CRL information may be obtained from the CRL distribution points extension of the certificate. In addition, relying parties shall check the CP of Issuing CAs to confirm the assurance level of CA certificates and subscriber certificates.

4.6 Certificate Renewal

4.6.1 Circumstance 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 Certificate by the CA

No stipulation.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.7 Certificate Re-key

Re-keying a certificate consists of creating new certificates with a different public key (and serial number) while retaining the remaining contents of the old certificate that describe the subject. The new certificate may be assigned a different validity period, key identifiers, specify a different CRL distribution point, and/or be signed with a different key. Re-key of a certificate does not require a change to the subject name and does not violate the requirement for name uniqueness. The old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

4.7.1 Circumstance for Certificate Re-key

The CA that issues certificates under this CP requires Subscribers to re-key the certificate to include at least following:

- Subscriber's certificate has less 25% life time before expiration or has already expired.
- Subscriber's certificate has been revoked.
- Subscriber needs to modify information in the certificate.

4.7.2 Who May Request Certification of a New Public Key

Only the subscriber may request a new certificate.

4.7.3 Processing Certificate Re-Keying Requests

Subscribers must follow the procedures of certificate re-keying requests as specified in Section 4.1.2.

4.7.4 Notification of New Certificate Issuance to Subscriber

The CA that issues certificates under this CP shall notify the result of new certificate issuance to subscriber according to the procedures specified in Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

After subscribers receive re-keyed certificate, subscribers must follow the procedure in Section 4.4.1 to accept the re-keyed certificate.

4.7.6 Publication of the Re-Keyed Certificate by the CA

The CA that issues certificates under this CP shall publish the re-keyed according to the procedure in Section 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

The CA that issues certificates under this CP shall notify the result of certificate issuance to other entities according to the procedure in Section 4.4.3.

4.8 Certificate Modification

Modifying a certificate means creating a new certificate that has the same or a different key and a different serial number, and that differs in one or more other fields from the old certificate. The old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

4.8.1 Circumstance for Certificate Modification

Since the interpretation of modifying certificate contents are sometimes complex, CA that issues certificates under this CP shall not offer certificate modification. Re-certification is recommended, that means the initial registration process as described in section 3.2 must be gone through again. The new certificate shall have a different subject public key.

4.8.2 Who May Request Certificate Modification

No stipulation.

4.8.3 Processing Certificate Modification Requests

No stipulation.

4.8.4 Notification of New Certificate Issuance to Subscriber

No stipulation.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

No stipulation.

4.8.6 Publication of the Modified Certificate by the CA

No stipulation.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.9 Certificate Revocation and Suspension

The CA may decide whether or not to provide certificate suspension services depending on certificate usage and service quality.

CAs providing certificate revocation and suspension services shall specify the certificate revocation and suspension service times in the CPS.

CAs providing certificate revocation and suspension services shall specify the service provision methods, certificate revocation request procedures and processing locations and websites in the CPS.

After certificate revocation or suspension, the CA shall list the revoked or suspended certificates in the CRL and post them in the repository at the next scheduled publication time of the CRL at the latest. The published certificate status information shall include the revoked and suspended certificates until the certificates expire or use is resumed.

For expired certificates, the CA may not accept certificate revocation or suspension requests and may not list the certificate revocation or suspension information on the CRL. For revoked or suspended certificates prior to expiry, the CA shall list the revoked or suspended information on the CRL at least once.

4.9.1 Circumstances for Revocation

4.9.1.1 Reasons for Revoking a Subscriber Certificate

The issuing CA shall revoke a subscriber certificate within 24 hours if one or more of the following occurs:

- Subscriber wants to discontinue the use of the certificate.
- Subscriber has violated relevant laws, regulations, legal obligations or announcements.
- Subscriber's private key is lost or compromised.

- Subscriber's information in the certificate is no longer valid.
- Subscriber experiences incident that is believed to significantly impact trustworthiness of the certificate.
- The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization
- The CA obtains evidence that the Subscriber's Private Key (corresponding to the Public Key in the Certificate) has suffered a Key Compromise, or that the Certificate has otherwise been misused
- The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber or Terms of Use Agreement
- The CA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name)
- The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name.
- The CA is made aware of a material change in the information contained in the Certificate.
- The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement
- The CA determines that any of the information appearing in the Certificate is inaccurate or misleading.
- The CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate.
- The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository.
- The CA is made aware of a possible compromise of the Private Key of the Subordinate CA used for issuing the Certificate.
- Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement.

- The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time)

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

The Issuing CA SHALL revoke a Subordinate CA Certificate within seven (7) days in the following circumstances:

- The Subordinate CA requests revocation in writing;
- The Subordinate CA notifies the Issuing CA that the original certificate request was not authorized and does not retroactively grant authorization;
- 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 section 6.1.5 and 6.1.6 in CA/Browser Forum Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates;
- The Issuing CA obtains evidence that the Certificate was misused;
- The Issuing CA is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with this CP or the applicable Certificate Policy or Certification Practice Statement;
- The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
- 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;
- The Issuing CA's or Subordinate CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository;

- Revocation is required by the Issuing CA's Certificate Policy and/or Certification Practice Statement; or
- The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time).

4.9.2 Who Can Request Revocation

- Subscriber may make a request to revoke the certificate for which the subscriber is responsible.
- The CA that issues certificates under this CP may make a request to revoke its own certificate.
- The CA that issues certificates under this CP may also revoke any issued certificate whenever it knows or reasonably suspects that the circumstances as specified in section 4.9.1 occurred.
- Registration Authority (RA) may also make a request to revoke a certificate for which a subscriber is responsible whenever it knows or reasonably suspects that the circumstances as specified in section 4.9.1 occurred.
- Court order

4.9.3 Procedure for Revocation Request

CA that issues certificates under this CP shall provide the procedure that requester can request for revocation 24x7. Subscriber requesting revocation is required to follow the procedures such as:

1. Subscriber submits the revocation request and related documents to the certificate issuing CA, or an RA of the CA, providing that the information is genuine, correct and complete.
2. Issuing CA or RA of the CA verifies and endorses the revocation requests and the related documents.
3. RA is responsible for verifying and authenticating an authorized representative of a juristic person by following the procedures as specified in Section 3.2.
4. Issuing CA with the assistance of RA will approve and process the revocation request.

5. Issuing CA, or via a RA of the CA, informs the revocation result to the subscriber. For revocation of certificate, PA must be informed.

4.9.4 Revocation Request Grace Period

There is no grace period for revocation under this CP.

4.9.5 Time within Which CA Must Process the Revocation Request

The CA that issues certificates under this CP must revoke certificates as quickly as practical upon endorsement of revocation request. Revocation requests should be processed within one business day or, whenever possible, before the next CRL is published.

4.9.6 Revocation Checking Requirement for Relying Parties

Before using certificates, relying Parties shall be responsible for checking the validity of each certificate in the certificate path, including checks for certificate validity, issuer-to-subject name chaining, certificate policy and key usage constraints, and the status of the certificate through the CRL or OCSP service. While using the CRL or OCSP service, the authenticity, integrity, and validity of the CRL and OCSP responses must also be verified. Relying parties must take into consideration the risk, responsibility and possible effects to determine independently the interval for obtaining new certificate revocation information.

4.9.7 CRL Issuance Frequency

The CA that issues certificates under this CP will issue a CRL in the following circumstances:

- Issue a CRL whenever a certificate or a subscriber certificate is revoked.
- Issue a CRL for certificates every six months whether or not the CRL has any changes.
- Issuing CA must issue a CRL for subscriber certificates at least once a day whether the CRL has any changes or not.

4.9.8 Maximum Latency for CRLs

CA that issues certificates under this CP shall publish CRL within commercially acceptance period of time.

4.9.9 On-line Revocation/Status Checking Availability

On-line status checking is optional for CAs operating under this CP. Where on-line status checking is supported, certificate status information shall be regularly updated and available to relying parties.

4.9.10 On-line Revocation Checking Requirements

If OCSP services are provided by CAs, relying Parties may optionally check the status of subscriber certificates through the services. Client software using on-line status checking need not obtain or process CRLs.

4.9.11 Other Forms of Revocation Advertisements Available

Other forms of Revocation Advertisements can be provided in accordance with Trust Service Principles and Criteria for Certification Authorities Version 2.0.

4.9.12 Special Requirements Regarding Key Compromise

The CA that issues certificate under this CP must notify subscribers immediately and Relying Parties as soon as practical.

4.9.13 Circumstances for Suspension

For certificate, suspension is not permitted. For subscriber's certificate, CA that issues certificates under this CP shall state in its CPS the circumstances for suspension.

4.9.14 Who Can Request Suspension

The CA that issues certificates under this CP shall state in its CPS who can request suspension.

4.9.15 Procedure for Suspension Request

The CA that issues certificates under this CP shall state in its CPS the procedure for suspension request.

4.9.16 Limits on Suspension Period

The CA that issues certificates under this CP shall state in its CPS the limits on suspension period.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

CAs operating under this CP shall provide CRLs or OCSP service or both to provide certificate status service. The revocation record of a certificate in the CRL or OCSP response shall only be removed once that revoked certificate expires.

4.10.2 Service Availability

CAs that issue certificates under this CP shall implement backup systems for providing certificate status services and put the best efforts to make such services available 24x7.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

Subscriber may end a subscription by allowing its certificate to expire or revoking its certificate without requesting a new certificate.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

Private keys used for signatures may not be escrowed.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5. Facility, Management, and Operational Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

All CA and RA operations shall be conducted within a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of sensitive information and systems. The site location and construction, when combined with other physical security protection mechanisms such as guards, high security locks, and intrusion sensors, shall provide robust protection against unauthorized access to the CA equipment and records.

5.1.2 Physical Access

Access to certificate issuance systems is only allowed for the responsible officers of the corresponding CA. In case other individuals need to access the service area where the CA systems are located, proper authorization must be obtained in advance. All visiting individuals must be recorded in the access log and must be accompanied by the responsible officer during the whole visit.

Certificate issuing servers and Cryptographic Module must be stored in a secure area where physical access to such systems requires dual-control and two-factor authentication.

5.1.3 Power and Air Conditioning

The CA shall have backup power capability sufficient to lock out input, finish any pending actions, and record the state of the equipment automatically before lack of power or air conditioning causes a shutdown. The repositories (containing certificates and CRLs) shall be provided with uninterrupted power sufficient for a minimum of 6 hours operation in the absence of commercial power, to maintain availability and avoid denial of service.

5.1.4 Water Exposures

The secure facilities of CAs and RAs shall be constructed and equipped, and procedures shall be implemented, to prevent floods or other damaging exposure to water, e.g.: on raised floor equipped with water sensor.

5.1.5 Fire Prevention and Protection

The secure facilities of CAs and RAs shall be constructed and equipped, and procedures shall be implemented, to prevent and extinguish fires or other damaging exposure to flame or smoke. These measures shall meet all local applicable safety regulations.

5.1.6 Media Storage

CAs and RAs shall protect the magnetic media holding back ups of critical system data or any other sensitive information from water, fire, or other environmental hazards, and shall use protective measures to deter, detect, and prevent the unauthorized use of, access to, or disclosure of such media.

5.1.7 Waste Disposal

CAs and RAs shall implement procedures for the disposal of waste (paper, media, or any other waste) to prevent the unauthorized use of, access to, or disclosure of waste containing Confidential/Private Information.

5.1.8 Off-site Backup

Backup media must be stored at a secure off-site facility.

5.2 Procedural Controls

5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. It is essential that the people selected to fill these roles shall be held accountable to perform designated actions correctly or the integrity of the CA is weakened. The functions performed in these roles form the basis of trust in the CA. CA must take two approaches to increase the likelihood that these roles can be successfully carried out:

- The first approach is to minimize the number of trusted roles and ensure that the people filling those roles are trustworthy and properly trained.
- The second is to enforce the concept of least privilege and distribute the functions of the roles among several people, so that any malicious activity requires collusion.

Trusted role operations include:

- The validation, authentication, and handling of information in Certificate Applications
- The acceptance, rejection, or other processing of Certificate Applications, revocation requests, or enrollment information
- The issuance, or revocation of Certificates, including personnel having access to restricted portions of its repository
- Access to safe combinations and/or keys to security containers that contain materials supporting production services
- Access to hardware security modules (HSMs), their associated keying material, and the secret share splits of the PINS that protect access to the HSMs
- Providing enterprise customer support
- Access to any source code for the digital certificate applications or systems
- Access to restricted portions of the certificate repository
- The ability to grant physical and/or logical access to the CA equipment
- The ability to administer the background investigation policy processes

Trusted roles include without limitation:

- CA Administrators
- CA Operations Staff
- RA Operations Staff
- Security Auditors
- Executives who manage CA infrastructural trustworthiness

Multiple people may hold the same trusted role, with collective privileges sufficient to fill the role. Other trusted roles may be defined in other documents, which describe or impose requirements on the CA operation.

The CA shall maintain lists, including names, organizations, contact information, and organizational affiliation for those who act in Administrator, CA Operations Staff, RAs, Security Auditor and CA Executive trusted roles, and shall make them available during compliance audits. RA shall maintain lists, including names, organizations, and contact information of those who act in RA Operations Staff, RA Administrators, and RA Security Auditor roles for that RA.

5.2.2 Number of Persons Required per Task

Where multi-party control is required, all participants shall hold a trusted role. Multi-party control shall not be achieved using personnel that serve in a Security Auditor role with the exception of audit functions. The following tasks shall require two or more persons:

- Generation, activation, and backup of CA keys
- Performance of CA administration or maintenance tasks
- Archiving or deleting CA audit logs. At least one of the participants shall serve in a Security Auditor role
- Physical access to CA equipment
- Access to any copy of the CA cryptographic module
- Processing of third party key recovery requests

5.2.3 Identification and Authentication for Each Role

CAs and RAs shall confirm the identity and authorization of all personnel seeking to become Trusted before such personnel are:

- issued with their access devices and granted access to the required facilities;
- given electronic credentials to access and perform specific functions on Information Systems and the CA or RA systems.

Individuals holding trusted roles shall identify themselves and be authenticated by the CA and RA before being permitted to perform any actions set forth above for that role or identity. CA Operations Staff and RA Staff shall authenticate using a credential that is distinct from any credential they use to perform non-trusted role functions. This credential shall be generated and stored in a system that is protected to the same level as the CA system.

The CA and RA equipment shall require, at a minimum, strong authenticated access control for remote access using multi-factor authentication. Examples of multi factor authentication include use of a password or PIN along with a time-based token, digital certificate on a hardware token or other devices that enforce a policy of what a user has and what a user knows. CA and RA equipment shall require, at a minimum, authenticated access control (e.g., strong passwords) for local multi-party access.

Individuals holding trusted roles shall be appointed to the trusted role by an appropriate approving authority. The approval shall be recorded in a secure and auditable fashion. Individuals holding trusted roles shall accept the responsibilities of the trusted role, and this acceptance shall be recorded in a secure and auditable fashion. Identity proofing of RA shall be performed by a member of the CA Operations Staff. Users shall authenticate themselves to all aspects of the network (servers, operating systems, applications, databases, processes, and so on) before they can access that resource.

5.2.4 Roles Requiring Separation of Duties

Individuals serving as Security Auditors shall not perform or hold any other trusted role. An individual that holds any CA Operations Staff role shall not be an RA except that CA Operations Staff may perform RA functions when issuing certificates or issuing certificates to RA.

Under no circumstances shall a CA operating under this CP be audited for compliance by any subsidiary, parent, or sibling company of its corporate holdings.

Only an individual serving in a Security Auditor role may perform internal auditing functions, with the exception of those security audit functions (e.g., configuring, archiving, deleting) that require multi-person control.

An individual that performs any trusted role shall only have one identity when accessing CA equipment.

The following roles must be performed by trusted officers:

- Verification and validation of forms such as the certificate application forms and the certificate revocation form.
- Certificate issuance and certificate revocation.
- Access to CA's private key.

5.3 Personnel Controls

5.3.1 Qualifications, Experience and Clearance Requirements

All personnel of the CA that issues certificates under this CP must be examined with their qualifications in terms of the requisite background, experience in order to ensure their prospective job responsibilities, competency and satisfaction.

5.3.2 Background Check Procedures

Prior to commencement of employment, the CA Human Resource department must conduct the following background checks:

- Identification card
- House registration
- Certification of the highest education
- Criminal records
- Professional certificate (if any)
- Confirmation letter of previous employment
- Background Check (Recheck at least every three years)

The CA that issues certificates under this CP may also exercise other measurements for background check. If the provided information is found to be false, or if the education/professional background is found unmatched, or if the person has certain criminal convictions, that person shall not be considered to work with the CA.

5.3.3 Training Requirements

The CA that issues certificates under this CP must provide its officers with appropriate training as well as the requisite on-the-job training needed to perform their job responsibilities related to CA operations with competency and satisfaction. The training programs include the following as relevant:

- Basic cryptography and Public Key Infrastructure (PKI) concepts
- Information Security Awareness
- Use and operation of deployed hardware and software related to CA operations
- Security Risk Management
- Disaster recovery and business continuity procedures

5.3.4 Retraining Frequency and Requirements

The CA that issues certificates under this CP must provide its officers with appropriate training at least once a year on the topics related to Information Security Awareness. Additional training may be considered if there is a change in hardware and software related to CA operations.

5.3.5 Job Rotation Frequency and Sequence

The CA that issues certificates under this CP is recommended to specify in its CPS the job rotation frequency and sequence of officers.

5.3.6 Sanction for Unauthorized Actions

Appropriate disciplinary actions are taken for unauthorized actions or other violations of relevant policies and procedures. Disciplinary actions are commensurate with the frequency and severity of the unauthorized actions and may include measures up to and including termination.

5.3.7 Independent Contractor Requirements

In case that independent contractors or consultants is employed and is obliged to pass the background check procedures specified in Section 5.3.2. Any such contractor or consultant are only permitted to access to the CA's secure facilities if they are escorted and directly supervised by trusted officers at all times.

For system maintenance purposes, operating staffs must present their employee identification card to Trusted Persons for verification and record. They must be also escorted and directly supervised by trusted officers at all times.

5.3.8 Documentation Supplied to Personnel

The CA that issues certificates under this CP must provide its personnel the requisite documentation needed to perform their job responsibilities competently and satisfactorily.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

The CA that issues certificates under this CP must log the following significant events:

- CA Key Life Cycle Management, including:
  - Key generation, backup, storage, recovery, archival, and destruction
  - Cryptographic Module life cycle management events
- CA and Subscriber certificate life cycle management events, including:
  - Certificate Applications, rekey, and revocation
  - Approval or rejection of requests
  - Generation and issuance of certificates and CRL

- Security-related events including:
    - Successful and unsuccessful access attempts to CA systems
    - Security system actions performed by CA officers
    - Security profile changes
    - System crashes, hardware failures and other anomalies
    - Firewall and router activity
    - CA facility visitor entry/exit

Log entries include the following elements:

- Date and time of the entry
- Automatic journal entries
- Identity of the entity making the journal entry
- Type of entry

5.4.2 Frequency of Processing Log

The CA operated under this CP shall examine audit logs at a reasonable frequency and at least on a monthly basis.

5.4.3 Retention Period for Audit Log

Audit logs are retained for at least 90 days.

5.4.4 Protection of Audit Log

Audit logs are protected with an electronic audit log system that includes mechanisms to project the log files from unauthorized actions.

5.4.5 Audit Log Backup Procedure

- Audit logs stored in an electronic audit log system are backup in the secure manner.
- Events Records follow the procedures below:

1. Paper-based event records are converted into electronic format before being stored in the audit log system, if provided.
2. CA backup audit events specified in 5.4.1 in backup media.

5.4.6 Audit Log Accumulation System (Internal vs. External)

Audit data is generated and recorded at the machine that the event has occurred and at the audit log system.

5.4.7 Notification to Event-causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

The CA that issues certificates under this CP must assess security vulnerability at least on a quarterly.

5.4.9 Penetration Test Assessments

The CA that issues certificates under this CP must assess security Penetration Test at least on a yearly basis.

5.5 Records Archival

5.5.1 Types of Records Archived

CA archives:

- CA systems
  - All audit data specified in 5.4.1
  - System configuration
  - Website

- Documentation supporting certificate applications
  - Certificates, CRLs, and expired or revoked certificates
  - CP and CPS
- Certificate lifecycle information
  - Forms such as Application Form, Revocation Request Form, Re-key Request Form, and Certificate Acceptance Form
  - Required documents for application
  - Internal documents such as procedure manuals and system access approval request
  - Letters or memos used for communication between CA and external parties such as, Root CA, Subscriber and other CAs.

5.5.2 Retention Period for Archive

Records shall be retained for at least 10 years, unless there are specific requirements (according to the Accounting Act B.E. 2543) Retention Period for Archive

The retention period for One CA file information is 10 years. The application programs used to process file data are kept for 10 years.

5.5.3 Protection of Archive

Records archival are stored in secure facilities and can be accessed only by authorized persons.

5.5.4 Archive Backup Procedure

Records archival are backed up in backup tapes on a monthly basis following the below procedures:

1. Paper-based event records are converted into electronic format before being stored and backed up, if provided.
2. CA backups events records specified in Section 5.5.1 in the backup media.

5.5.5 Requirements for Time Stamping of Records

Any activity performed on or to the certification systems shall be recorded with time and date information.

5.5.6 Archive Collection System (Internal or External)

Archive Collection System is internal to CA only.

5.5.7 Procedures to Obtain and Verify Archive Information

Procedures to obtain and verify archive information are as follows:

1. The requester submits access request to archive information to management of CA specifying reasons and necessity of obtaining such information as well as identifying the type of information needed.
2. management of CA justifies the appropriateness and necessity of the request and notifies the decision result to the requester.
3. An authorized CA officer obtains the archive information, defines access rights, and forwards to the requester.
4. The requester verifies the integrity of information.

5.6 Key Changeover

To minimize risk from compromise of a CA’s private signing key, that key may be changed often. From that time on, only the new key will be used to sign subscriber certificates.

The CA’s signing keys shall have a validity period as described in section 6.3.2.

When a CA updates its private signature key and thus generates a new public key, the CA shall notify all CAs, RAs, and subscribers that rely on the CA’s certificate that it has been changed.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

The CA that issues certificates under this CP shall have an incident response plan and a disaster recovery plan.

If compromise of a CA is suspected, an independent third-party investigation shall be performed in order to determine the nature and the degree of damage. Issuance of certificates from that CA shall be stopped immediately upon detection of a compromise. If a CA private signing key is suspected of compromise, the procedure outlined in section 5.7.3 shall be followed. Otherwise, the scope of potential damage shall be assessed in order to determine if the CA needs to be rebuilt, only some certificates need to be revoked, and/or the CA private key needs to be declared compromised.

In case that there an event affects to security of CA system; the corresponding CA officers shall notify the PA and Root CA if any of the following occur:

- Suspected or detected compromise of any CA system or subsystem
- Physical or electronic penetration of any CA system or subsystem
- Successful denial of service attacks on any CA system or subsystem
- Any incident preventing a CA from issuing and publishing a CRL or on-line status checking prior to the time indicated in the next Update field in the currently published CRL, or the certificate for on-line status checking suspected or detected compromise.

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

In case of software, hardware or data failure, the corresponding CA officers will report such incidents to the upper authorities in order to make decisions and deal with the incident properly. If it is necessary, a disaster recovery plan may be used to restore CA services.

5.7.3 Entity Private Key Compromise Procedures

In case of a CA key compromise, the CA shall notify PA and Root CA. Root CA shall revoke that CA's certificate, and the revocation information shall be published immediately in the most expedient, authenticated, and trusted manner but within 18 hours after the notification. The compromised CA shall also investigate and report to PA and Root CA what caused the compromise or loss, and what measures have been taken to preclude recurrence. If the cause of the compromise can be adequately addressed and it is determined that the CA can be securely re-established, then the CA shall be re-established. Upon re-establishment of the CA, new subscriber certificates shall be requested and issued again.

When a certificate is revoked because of compromise, suspected compromise, or loss of the private key, a CRL shall be published at the earliest feasible time by the CA, but in no case more than 6 hours after notification.

In case of an RA compromise, the CA shall disable the RA. In the case that an RA's key is compromised, the CA that issued RA certificate shall revoke it, and the revocation information shall be published within 24 hours in the most expedient, authenticated, and trusted manner. The compromise shall be investigated by the CA in order to determine the actual or potential date and scope of RA compromise. All certificates approved by that RA since the date of actual or potential RA compromise shall be revoked. In the event that the scope is indeterminate, then the CA compromise procedures as specified in above shall be followed.

5.7.4 Business Continuity Capabilities after a Disaster

The CA that issues certificates under this CP shall prepare a disaster recovery plan which have been tested, verified and continually updated. A full restoration of services will be done within 24 hours in case of disaster.

5.8 CA or RA Termination

If there is any circumstance to terminate the services of CA operating under this CP with the approval of PA, CA operating under this CP will notify the subscribers and all relying parties. The action plan is as follow:

- Notify status of the service to affected users.
- Revoke all certificates.
- Long-term store information of CA and subscribers according to the period herein specified.
- Provide ongoing support and answer questions.
- Properly handle key pair and associated hardware.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Cryptographic keying material used by the CA to sign certificates, CRLs or status information are generated in FIPS 140-2 Level 3 or equivalent standard validated cryptographic modules. Multi-party control is required for the CA key pair generation, as specified in section 6.2.2. the CA key pair generation created a verifiable audit trail demonstrating that the security requirements for procedures were followed. The documentation of the procedure has shown that appropriate role separation was used. An independent third party has validated the execution of the key generation procedures by witnessing the key generation, as well as by examining the signed and documented record of the key generation. The CA key pair generation are performed by the CA staff. CA is required to generate the signature key pairs for the purpose of digital signature by FIPS 140 validated hardware cryptographic modules to support source authentication.

6.1.2 Private Key Delivery to Subscriber

The CA must generate the key pair by themselves.

6.1.3 Public Key Delivery to Certificate Issuer

Subscribers are required to submit Certificate Signing Request in the form of PKCS # 10 standard with application by themselves.

6.1.4 CA Public Key Delivery to Relying Parties

Relying parties can access the CA public key in the certificate by the published channel.

6.1.5 Key Sizes

Certificates for CAs operating under this policy shall contain RSA public keys with the minimum key size of 4,096 bits.

Subscriber certificates issued by the Issuing CA shall contain RSA public keys with the minimum key size of 2,048 bits or other key types of equivalent security strength on and before December 31, 2030. After December 31, 2030, subscriber certificates shall contain RSA public keys with the minimum key size of 3,072 bits or other key types of equivalent security strength.

The CAs should use the SHA-256, SHA-384, or SHA-512 hash algorithm when issuing certificates and CRLs and generating digital signatures. The CAs must not issue certificates signed with SHA-1 hash algorithm.

6.1.6 Public Key Parameters Generation and Quality Checking

Not Applicable.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

The use of a specific key shall be constrained by the key usage extension in the X.509 certificate. All certificates shall include a critical key usage extension.

Public keys that are bound into subscriber certificates shall be used only for digital signature or key/data encipherment.

Public key that are bound into Issuing CA's certificates shall be used only for signing certificates and certificate status information such as CRLs.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

CAs that issue certificates under this CP shall use a FIPS 140-2 Level 3 or higher validated hardware cryptographic module for signing operations.

Subscribers shall use software tokens for all cryptographic operations.

6.2.2 Private Key (n out of m) Multi-person Control

Accessing the private key of CAs operating under this CP must be performed by multi-person control. There are no further regulations for multi-person control of subscriber private key.

6.2.3 Private Key Escrow

Private keys of CAs operating under this CP shall be never escrowed. The CAs must not have policy to keep subscribers' private key.

6.2.4 Private Key Backup

Backup of the signature private key of CAs operating under this CP shall be done in accordance with multi-person control procedures as the original signature private key. At least one copy of the signature private key shall be stored off-site. All copies of the CAs' signature private key shall be accounted for and protected in the same manner as the original. The CAs shall backup the signature private key in FIPS 140-2 Level 3 validated hardware cryptographic module. The CAs shall state in its CPS the backup procedure.

6.2.5 Private Key Archival

The CA private key beyond the validity period will be kept at least 10 years and stored in Cryptographic Module with FIPS 140-2 Level 3 standards.CA

6.2.6 Private Key Transfer into or from a Cryptographic Module

Key generation for CAs operating under this CP shall follow regulations stated in Section 6.1.1. The CAs and their RAs shall not allow their private keys to be stored in plain text outside the cryptographic module. The private key is only imported into the cryptographic module during the key backup/recovery procedures of the CAs/RAs or cryptographic module replacement and the multi-person control method shall be followed in Section 6.2.2 when importing the private key into the cryptographic module. Encryption or key splitting may be used as the private key importation method to ensure that the private key is not exposed ins plain text outside the cryptographic module and guarantee that the encryption key is not disclosed. After the private key importation is completed, the related secret parameters generated during the importation process shall be completely destroyed.

6.2.7 Private Key Storage on Cryptographic Module

CAs operating under this CP shall store its private key on a cryptographic module and back up the private key on another cryptographic module. The cryptographic module shall comply with FIPS 140-2 Level 3 or above standard.

6.2.8 Method of Activating Private Key

Activation of the CA's private key operations performs by authorized person and requires two-factor authentication process.

6.2.9 Method of Deactivating Private Key

The multi-person control methods in section 6.2.2 are used to deactivate the CA private keys.

6.2.10 Method of Destroying Private Key

The CA will delete the private keys from Cryptographic Module and its backup by overwriting the private key or initialize the module with zeroization function. The event of destroying the CA must be recorded into evidence under section 5.4.

6.2.11 Cryptographic Module Rating

Cryptographic Module Rating shall comply with FIPS 140-2 Level 3 standard.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Public key shall be stored for long period in the certificate.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The certificate validity period and key pair associated with the certificate may be used up to the expiry date specified in the certificate. Public key may be used to verify the digital signature even if the certificate is expired but the digital signature to be verified must be created before expiry date of the certificate. For the private key, it may be used to decrypt even if certificate is expired.

The certificate operational period and key pair usage validity period of CAs operating under this CP shall not be more than 20 years and the certificate period and key pair usage validity period of subscribers shall not be more than 10 years. Certificate operational periods and key pair usage periods shall be assessed by PA at least once a year or as necessary especially in an incident that is believed to significantly impact trustworthiness of the CAs.

(With technical limitations on UTC Time, the certificate issued by the CAs shall not have expiry date exceeding year 2580 (AD 2037)).

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Activation data, such as Personal Identification Number (PIN) and password, for accessing the CA systems shall be user-selected and protected under multi-person control by each of whom holding that activation data. If the activation data must be delivered, it should be delivered via proper secure channels.

6.4.2 Activation Data Protection

CAs operating under this CP shall protect activation data used to unlock private keys by storing the data in secure location.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

The CA shall have implemented multi-person control access to information such as sensitive details about customer accounts and passwords. Ultimately CA-related private keys are carefully guarded, along with the machines housing such information. Security procedures are in place to prevent and detect unauthorized access, modification, malicious code or compromise of the CA systems such as firmware and software. Such security controls are subject to compliance assessment as specified in section 8.

6.5.1 Specific Computer Security Technical Requirements

The CA shall limit the number of application installed on each computer to minimize security risks. Those applications are hardened based on the instructions provided by software manufacturer. In addition, installed applications shall be regularly reviewed for security updates to ensure that no vulnerability is exposed.

6.5.2 Computer Security Rating

The CA shall conform to ISO/IEC 27001 (Information Security Management System) and Trust Service Principles and Criteria for Certification Authorities Version 2.0.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

CAs operating under this CP must implement system development controls over the procurement, development and change of the CA system through aspects of its life-cycle. CA systems are implemented and tested in a non-production environment prior to implementation in a production environment. Change control procedures are in place to control and monitor all revisions and enhancements to be made to the components of such systems.

6.6.2 Security Management Controls

CAs operating under this CP shall check if software is the correct and unmodified version provided by the supplier when the CAs install the software for the first time. The CAs' hardware and software shall be dedicated and may not be installed and operated on other unrelated application systems (including hardware devices, network connections and component software). The CAs shall also record and control CA-related system configurations and any revisions and function upgrades as well as detect unauthorized modifications of CA software or configuration systems. In addition, the CAs shall comply with the security measures in CPA WebTrust Principles and Criteria for Certification Authorities regulations at least.

6.6.3 Life Cycle Security Controls

CAs operating under this CP can also address life-cycle security ratings based such as the Software Engineering Institute's Capability Maturity Model (SEI-CMM).

6.7 Network Security Controls

The CA network shall equip firewall with features to investigate data transmission at application level and detect intruders or network activities that violate policy. It is to ensure that system is secure. Normal users allow accessing the certificate services through the network via the website and directories only. For system management, certification authority officers will use dedicated network to access and management purpose. Information contains in this particular network is encrypted.

6.8 Time-stamping

CAs under this CP shall regularly conduct clock synchronization with a reliable time source (e.g., NTP Server) to maintain the correctness of system time and ensure the accuracy of the following time:

- Certificate issuance time.
- Certificate revocation time.
- CRL issuance time.
- System event occurrence time.

Automatic or manual procedures may be used to adjust the system time. The CAs' Clock synchronizations are auditable events.

7. Certificate, CRL and OCSP Profiles

7.1 Certificate Profile

Certificates issued by Issuing CAs operating under this CP must comply with ITU-T Recommendation X.509 and RFC 5280. The CAs shall use cryptographically secure pseudorandom number generator (CSPRNG) to generate the certificate serial numbers which are larger than zero, non-sequential, and containing at least 64-bit entropy.

7.1.1 Version Number(s)

Certificates issued by CAs shall be in accordance with ITU-T Recommendation X.509 and designated to be version 3.

7.1.2 Certificate Content and Extensions; Application of RFC5280

Certificates issued by CAs shall comply with the requirements defined in the latest versions of ITU-T X.509, RFC 5280, and other related standards. The CAs shall state in the CPS the certificate extensions used.

7.1.3 Algorithm object identifiers

Certificates issued by CAs shall use the following algorithm object identifiers (OIDs) during signing:

Algorithm	Object Identifier
sha256WithRSAEncryption	1.2.840.113549.1.1.11
sha384WithRSAEncryption	1.2.840.113549.1.1.12
sha512WithRSAEncryption	1.2.840.113549.1.1.13

Table 3 Algorithm object identifiers used for certificate

Certificates issued by the CAs shall use the following OID to identify the algorithms used with to generate subject key:

Algorithm	Object Identifier
rsaEncryption	1.2.840.113549.1.1.1

Table 4 Object identifiers used to identify the algorithms for generating subject key

7.1.4 Name Forms

The name forms of Issuer and Subject are specified in the certificate as reference to the Section 3.1.1 of this CP.

7.1.5 Name Constraints

It may be asserted in CA certificate if required.

7.1.6 Certificate Policy Object Identifier

Issuing CAs operating under this CP MUST define the Certificate Policy OID provided by Thailand NRCA's OID Structure.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

CAs operating under this CP may issue certificates with a policy qualifier and suitable text to aid relying parties in determining applicability.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2 CRL Profile

7.2.1 Version Number(s)

CRLs issued by CAs shall be in accordance with RFC 5280 and designated to be version 2.

7.2.2 CRL and CRL Entry Extensions

CRL and CRL entry extensions shall comply with the requirements defined in ISO / IEC 9594-8:2012. CAs shall state in the CPS the format of the CRL and CRL entry extensions used, if applicable. It includes at least the following:

7.2.2.1 AuthorityKeyIdentifier

This attribute indicates information associated with the public key of the certificate which is digitally signed by subscribers. The signing uses SHA-256, or SHA -384 or SHA-512 hashing algorithm of public key of Certificate Authority.

7.2.2.2 BaseCRLNumber

This attribute indicates the sequence number that Certificate Authority assigns to each revoked certificate to order the certificate revocation list.

7.2.2.3 ReasonCode

This attribute indicates the Reason Code (0-9) of revoked certificate.

7.2.2.4 IinvalidityDate

This attribution indicates start time when using the pair of private key and the revoked certificate is insecure. It is defined in Greenwich Mean Time (GMT) format.

7.2.2.5 IssuingDistributionPoint

This attribution is used to locate the certificate revocation list (Distribution Point) and indicates that the certificate revocation list is for a Certification Authority or subscribers including the reasons of revocation (Reason Code).

7.3 OCSP Profile

If OCSP services are provided by CAs, the CAs shall disclose the version number of OCSP and standards used for the OCSP extensions.

7.3.1 Version Number(s)

CAs shall issue Version 1 OCSP responses.

7.3.2 OCSP Extensions

Not Applicable

8. Compliance Audit and Other Assessments

CAs operated under this CP shall conduct compliance audit in accordance with WebTrust Principles and Criteria for Certification Authorities to ensure that the requirements of their CPS are being implemented and enforced.

8.1 Frequency or Circumstances of Assessment

CAs and RAs shall be subject to a periodic compliance audit in respect of WebTrust Principles and Criteria for Certification Authorities at least once a year with an audit period of no more than 12 months to ensure that subordinate CA and RAs operations are in compliance with the security regulations and procedures in the CP and CPS. CAs and RAs shall be subject to one non-routine internal audit.

8.2 Identity/Qualifications of Assessor

The auditor must demonstrate competence in the field of compliance audits and must be thoroughly familiar with the CA's CPS and this CP. Subordinate CA shall retain a qualified auditor to perform the CA compliance audit work who is familiar with CA operations and has been authorized by CPA as a licensed WebTrust practitioner to perform WebTrust Principles and Criteria for Certification Authorities to provide fair and impartial audit services. Audit personnel shall be a qualified and authorized Certified Information Systems Auditor (CISA) or have equivalent qualifications and shall at least possess the experience of conducting a WebTrust for CA audit twice at 4 man-days or the experience of conducting a CA information security management audit twice at 8 man-days. Subordinate CA shall conduct identity identification of audit personnel during audits.

8.3 Assessor's Relationship to Assessed Entity

Auditors must be independent from the CAs and RAs being audited, or it shall be sufficiently organizationally separated from those entities and shall provide an unbiased, independent evaluation. To insure independence and objectivity, the compliance auditor may not have served the entity in developing or maintaining the entity's CA facility or certification practice statement. The CA shall determine whether a compliance auditor meets this requirement. There must not be conflict of interest to the CA.

8.4 Topics Covered by Assessment

The purpose of compliance audit is to verify that a CA and its RAs comply with all the requirements of the current version of this CP and the CA's CPS. The scope of assessment shall follow that in WebTrust Principles and Criteria for Certification Authorities Version 2.1 or higher.

The scope of audit is stipulated as follows:

(1) Whether or not the subordinate CA operations comply with the CP/CPS including administrative and technical audit of the physical environment, personnel procedural controls, key control, certificate lifecycle control, hardware security module.

(2) Whether or not the RA operations comply with the CP/CPS and related procedures.

(3) Whether or not the content disclosed from the CPS comply with the corresponding CP and suitable with respect to CA practices.

8.5 Actions Taken as a Result of Deficiency

CA's officers must plan to improve deficiencies (Non-conformity) based on the assessment results with explicit operating time. The plan will be submitted to auditors to ensure that sufficient security of the system is still in place.

8.6 Communication of Results

Except for systems that could possibly be attacked, and the scope specified in section 9.3, CA shall announce the information which should be publicly stated by the qualified auditor. The audit results are displayed on the CA website's front page using WebTrust® for Certification Authorities seals. The compliance audit and management's assertions may be viewed by clicking on the seals. The most recent compliance audit and management's assertions shall be made publicly available in the repository within three months after the end of the audit period. If the posting of the latest audit results needs to be postponed for some reason, the CA shall provide a letter of explanation signed by the qualified auditor.

After the assessment is completed, the audit compliance report and identification of corrective measures will be sent to PA within 30 days of completion.

8.7 Self-Audits

During the period in which the CA issues Certificates, the CA SHALL monitor adherence to its Certificate Policy, Certification Practice Statement and these Requirements and strictly control its service quality by performing self audits on at least a quarterly basis against a randomly selected sample of the greater of one certificate or at least three percent of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

CA operated under this CP shall provide the fee including renewal fee of each type of certificate that CA issued.

9.1.2 Certificate Access Fees

CA operated under this CP shall not include fees for certificate access.

9.1.3 Revocation or Status Information Access Fees

CA operated under this CP shall not include fees for revocation or Status Information access.

9.1.4 Fees for Other Services

CA operated under this CP shall declare the other fees.

9.1.5 Refund Policy

CA operated under this CP shall provide reasonable refund policy.

9.2 Financial Responsibility

This CP contains no limits on the use of certificates issued by CAs under the policy. Rather, entities, acting as relying parties, shall determine what financial limits, if any, they wish to impose for certificates used to consummate a transaction.

9.2.1 Insurance Coverage

- CA operated under this CP shall disclose insurance related to CA operation.

9.2.2 Other Assets

- CA operated under this CP shall disclose other assets.

9.2.3 Insurance or Warranty Coverage for End-entities

- CA operated under this CP shall provide reasonable insurance or warranty for end-entities.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

CA keeps following information in the scope of confidential information:

- Private key of CA and required information to access private key including password to access CA's hardware and software
- Registration application of subscribers for both approved and rejected application
- Audit Trail record
- Contingency Plan or Disaster Recovery Plan
- Security controls of CA's hardware and software
- Sensitive information with potential to have impact on security and reliable of CA's system

9.3.2 Information Not within the Scope of Confidential Information

Following information is not within the scope of confidential information:

- Certificate Practice Statement and Certificate Policy

- Certificate uses policy
- Information inside certificate
- Certificate revocation
- Information without impact on security and reliable of CA's system such as articles and news

9.3.3 Responsibility to Protect Confidential Information

CA under this CP must have security measure in place to protect confidential information.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

CAs under this CP shall develop, implement and maintain a privacy plan. The privacy plan shall document what personally identifiable information is collected, how it is stored and processed, and under what conditions the information may be disclosed.

9.4.2 Information Treated as Private

Private information in this document means related information of subscribers that does not include in the certificate or directory.

9.4.3 Information Not Deemed Private

Not deemed private information in this document means related information of subscribers that include in the certificate or directory.

9.4.4 Responsibility to Protect Private Information

CA has implemented security measure to protect private information.

9.4.5 Notice and Consent to Use Private Information

CA will use private information only if subscribers are noticed and consent to use private information in compliance with privacy policy.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

In the event of court order or administrative order, CA needs to disclose personal information with required by law or officers under the law.

9.4.7 Other Information Disclosure Circumstances

None

9.5 Intellectual Property Rights

CA is the only owner of intellectual property rights associated with the certificate, certificate revocation information and this certificate policy.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

CA assures that

- Procedures are implemented in accordance with this CP.
- Any certificates issued that assert the policy OIDs identified in this CP were issued in accordance with the stipulations of this CP.
- Certification Practice Statement (CPS) will be provided, as well as any subsequent changes, for conformance assessment.
- The CA operation is maintained in conformance to the stipulations of the CPS.
- The registration information is accepted only from approved RAs operating under an approved CPS.
- All information contained in the certificate issued by the CA is valid and appropriate. Evidence that due diligence was exercised in validating the information contained in the certificates is maintained.
- Certificates of subscribers found to have acted in a manner counter to their obligations in accordance with section 9.6.3 will be revoked.
- All information regarding certificate issuance and certificate revocation are processed through the procedure specified in the CPS of the corresponding CA.

9.6.2 RA Representations and Warranties

An RA shall assure that

- Its RA registration operation is performed in conformance to the stipulations of the approved CPS of the corresponding CA and related regulations.
- All information contained in the certificate issued by the CA is valid and appropriate. Evidence that due diligence was exercised in validating the information contained in the certificates is maintained.
- The obligations are imposed on subscribers in accordance with section 9.6.3, and subscribers are informed of the consequences of not complying with those obligations.

9.6.3 Subscriber Representations and Warranties

By using the subscriber certificate, the subscriber assures that

- He/She accurately represents itself in all communications with the CA.
- The private key is properly protected at all times and inaccessible without authorization.
- The CA is promptly notified when the private key is suspected loss or compromise.
- All information displays in the certificate is complete and accurate.
- The certificate will be used legitimately under laws, related regulations, terms, conditions and other related service announcements of the CA by authorized persons.

9.6.4 Relying Party Representations and Warranties

In case of relying party representations use the certificate, the relying party shall properly verify information inside the certificate before use and accepts the fault of single side verification.

9.6.5 Representations and Warranties of Other Participants

Warranties of other participants are optional for CAs under this CP.

9.7 Disclaimers of Warranties

Statement under clause 9.6 cannot be terminated or forfeited unless it is amended to conform to the law.

9.8 Limitations of Liability

CA is responsible for any damage incurred in the event of damage caused by the use of the service systems from the willful act or gross negligence of the corresponding CA. The response to the damage is under determination of CA.

9.9 Indemnities

In case of the damage occurs to the CA from the actions of subscribers or relying parties, the corresponding CA reserves the right to claim damages.

9.10 Term and Termination

9.10.1 Term

This CP takes effect from the date of publication upon the approval of Policy Authority.

In case of changes in technical requirements, subscribers must comply with the changes in a timely manner. The changes must be made within one year from the date that the subscriber has been formally informed.

9.10.2 Termination

This CP takes effect until it is terminated.

9.10.3 Effect of Termination and Survival

The requirements of this CP remain in effect through the end of the archive period for the last certificate issued.

9.11 Individual Notices and Communications with Participants

CA will communicate to those participants using reliable channel as soon as possible in accordance with the importance of information.

9.12 Amendments

9.12.1 Procedure for Amendment

Amendment of this CP requires approval by PA before announcement. The amendment shall be performed under laws, regulation or other related service announcements of Root CA.

9.12.2 Notification Mechanism and Period

In case there are any significant changes to this CP, Root CA will announce on its website.

9.12.3 Circumstances under Which OID Must Be Changed

The OID of this CP contains a version number in the last component of the OID. The version number will be changed if there is any change in this CP.

9.13 Dispute Resolution Provisions

9.13.1 Disputes between Issuer and subscriber

CAs operating under this CP shall state in its CPS a dispute resolution clause and procedures to resolve disputes and claims among CAs operating under this CP and the subscribers. In any case, CAs operating under this CP or subscribers may submit any dispute to PA. PA shall have jurisdiction to settle the dispute.

9.13.2 Disputes between Issuer and Relying Parties

CAs operating under this CP shall state in its CPS a dispute resolution clause and procedures to resolve disputes and claims among CAs operating under this CP and the relying parties. In any case, CAs operating under this CP or relying parties may submit any dispute to PA. PA has jurisdiction over the dispute.

9.14 Governing Law

The laws of the Kingdom of Thailand shall govern this CP.

9.15 Compliance with Applicable Law

All CAs operating under this CP are required to comply with the laws of the Kingdom of Thailand.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

CPS of a CA operating under this CP shall be considered as part of the agreement between CA and the subscribers.

9.16.2 Assignment

Requirements of the assignment must be in accordance with laws, regulations, or announcements relating to Root CA.

9.16.3 Severability

Should it be determined that one section of this CP is incorrect or invalid, the other sections of this CP shall remain in effect until the CP is updated.

9.16.4 Enforcement

Should it be determined that any section of this CP is illegal, unenforceable, or void, then any offending words in it will be deleted to the extent necessary to make it legal and enforceable while preserving its intent.

9.16.5 Force Majeure

Provided CA operating under this CP have exercised a reasonable degree of skill and care to avoid and/or mitigate the effects of matters beyond its control, neither the CA nor any RA operating under this CP is liable for the adverse effects to Subscribers or Relying Parties of any matters outside our control whatsoever, including (without limitation) the availability of the Internet, or telecommunications or other infrastructure systems or the adverse effects of the acts of God, war, military operations, national emergency, epidemic, fire, flood, earthquake, strike or riots or the negligence or deliberate wrongful conduct of other Subscribers or other third parties.

9.17 Other Provisions

No stipulation.