Thailand National Root Certification Authority Certificate Policy

Version 2.0

<Document Status>

- ○ *Draft*
- ○ *Internal Use*
- ◉ *Publication*

Document Revision History

Date	Version	Description
July 2013	1.0	Initial Released
June 2014	2.0	• Translated into English for WebTrust assessment • Reviewed contents to align with RFC3647 • Reviewed consistency of terms in the document • Described the general guideline of log review frequency in topic 5.4.2 • Added topic 6.5.1 Computer Security Technical Requirements • Added topic 6.5.2 Computer Security Rating

Table of Contents

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 Thailand NRCA 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 the Thailand NRCA. The CP applies to all subordinate certification authorities under Thailand NRCA and thereby provides assurances of uniform trust throughout the Thailand NRCA. The CP sets forth requirements that subordinate certification authorities under Thailand NRCA must meet.

Mission of Thailand NRCA includes:

- Certificate issuance, publication, and revocation for certification authorities located in Thailand; and
- Coordinate with overseas certification authorities to enable seamless international usage of certificates issued by local certification authorities.

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 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 and Certification Practices Framework [RFC3647].

1.2 Document Name and Identification

This Certificate Policy is published by the Electronic Transactions Development Agency (Public Organization) (ETDA) and specifies the baseline set of security controls and practices that CAs 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) "2.16.764.1.1.1.1".

1.3 PKI Participants

1.3.1 Certification Authority

Certification Authority (CA) is a person or legal entity 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 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 subordinate CAs and 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.

1.3.2 Registration Authority

A Registration Authority ()(RA) is a person or legal entity that collects and verifies 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 process
- 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. CAs are sometimes technically considered "subscribers" in a PKI. However, 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. CAs who want to subscribe a certificate from Thailand NRCA for signing and issuing certificates or certificate status information, and so become a subordinate CA of Thailand NRCA, will be qualified as "CA Subscriber"

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 Thailand NRCA.

1.3.5 Other Participants

1.3.5.1. Policy Authority

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

1. Establish certificate policy and certification practice statement of Thailand NRCA and other certification authorities under the Thailand NRCA trust model;
2. Arrange for a review of certificate policy and certification practice statement of Thailand NRCA and other certification authorities under the Thailand NRCA trust model on a regular basis; and
3. Promote trust relationship of Thailand NRCA with other domestic or overseas certification authorities.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The usage of a certificate issued under Trust model of Thailand NRCA is limited to support the following core security needs:

- authentication and non-repudiation – provides assurance of the identity of the CA Subscriber;
- certificate signing – sign certificates;

- encipherment – encrypt/decrypt electronic data of CA Subscriber. the Private Key used for encipherment shall be used for Digital Signatures;
- digital signature – assist any Relying Party in preventing a CA Subscriber from denying that such CA Subscriber has authorized any particular transaction if that CA Subscriber has digitally signed that certificate; and
- certificate revocation list (CRL) signing – sign and publish CRLs

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

The organization who responsible for all aspects of this CP is Thailand NRCA which operated by Office of Information Technology Infrastructure under Electronic Transactions Development Agency (Public Organization) is responsible for all aspects of this CP. In this document, "Thailand NRCA" will refer to Office of Information Technology Infrastructure.

1.5.2 Contact Person

The Director of Office of Information Technology Infrastructure,

Thailand National Root Certification Authority

Electronic Transactions Development Agency (Public Organization)

The Government Complex Commemorating His Majesty The King's 80th Birthday Anniversary, 5th December, B.E.2550 (2007)

120 Moo 3 Chaeng Wattana Rd. Laksi, Bangkok 10210

Ratthaprasasanabhakti Building (B Building) 7th floor

Tel: (66)-2142-2506

Email: infra@etda.or.th

Website: http://www.nrca.go.th

1.5.3 Person Determining CPS Suitability for the Policy

PAshall 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 under this CP submits CPS to the Thailand NRCA.
2. Thailand NRCA reviews and make recommendations
3. Thailand NRCA 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.

1.6 Definitions and Acronyms

1.6.1 Definitions

See Table 1 for a list of 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 and ISO/IEC 9594-8:2008 Information technology -- Open Systems Interconnection -- The Directory: Public-key and attribute certificate frameworks.
Certificate Policy (CP)	The document, which is entitled "Thailand National Root 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, which is entitled "Thailand National Root Certification Authority Certification Practice Statement", 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

Term	Definition
	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.

Table 1: Terms and Definitions

1.6.2 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)

Table 2: Acronyms

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. 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 will be made publicly available within one working day of the approval of changes. CA that issues certificates under this CP shall update and publish its CPS accordingly within thirty days after update.

2.4 Access Controls on Repositories

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. 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. 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

CA that issues certificates under this CP shall specify the naming convention that it has adopted, such as X.501 Distinguished Names (DN) or other forms of names such as web site certificates. Alternative name forms including for example an electronic mail address or a personal identification number may be included to ensure that the certificate of a person can be unambiguously identified.

3.1.2 Need for Names to be Meaningful

The names contained in a certificate must be in English with commonly understood semantics permitting the determination of the identity of the individual or organization that is the Subject 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

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

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

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. CA shall state in its CPS the method to prove possession of private key.

3.2.2 Authentication of Organization Identity

Requests for certificates shall include the CA name, address, and documentation of the existence of the CA. Thailand NRCA shall verify the information, in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the CA.

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.

3.2.3 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. 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 signed 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

PA promotes interoperation between CAs issuing certificates under this CP and other CAs which may or may not issue certificates under this CP (for example, overseas CA(s)). Thailand NRCA will interoperate with other Certification Authorities after signing the agreement or Memorandum of Understanding (MOU) on behalf of all CAs under Thailand NRCA trust model.

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

Organization who wishes to operate a CA in Thailand may complete and submit an application for certificates to Thailand NRCA. Other 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 CA and 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

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. 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.

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

Certificate applications must be processed within 10 business days, counting from the date that CA or RA endorses the receipt of a certificate application, to complete the processing of the application. For application of certificates, Thailand NRCA will complete the processing of the certificate application within 30 business days, counting from the date that Thailand NRCA endorses the receipt of the certificate application.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

Upon receiving the request, 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;
- 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 a CA's CPS.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

CAs operating under this CP, or via 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, or the applicant CA of a certificate, must proceed with the following:

- The subscriber, or the applicant CA of the certificate, must verify the information contained in the certificate and either accept or reject the certificate.
- If the subscriber, or the applicant CA of the certificate, fails to receive, or fails to accept the certificate within ten business days from the CA or Thailand NRCA, the CA or Thailand NRCA will 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 issuing CA.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Thailand NRCA will notify PA whenever a certificate is issued to a CA.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscriber can use the Private Key corresponding to the Public Key in the certificate, which is issued by CA operating under this CP, in order to generate its digital signature to other subscribers or relying parties. Applicant CA of a certificate can use the Private Key corresponding to the Public Key in the certificate to

issue certificates to its subscribers. The certificate shall be used lawfully in accordance with this CP, the CPS and Terms of Service of the issuing CA.

4.5.2 Relying Party Public Key and Certificate Usage

Before any act of reliance, Relying Parties shall assess the certificate as follows:

- 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 certificate 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 CAs.

4.6 Certificate Renewal

Thailand NRCA issues certificates to CAs located in Thailand under this CP. The validity period of Thailand NRCA certificate is 23 years and that for all subordinate CAs are not more than 20 years. However, PA may review on the proper validity period of such certificates. This is due to the fact that the current specification is determined with technical limitations related to the UTC Time, the certificate issued by Thailand NRCA will last no longer than the year 2580 (AD 2037).

4.6.1 Circumstance for Certificate Renewal

Not Applicable.

4.6.2 Who May Request Renewal

Not Applicable.

4.6.3 Processing Certificate Renewal Requests

Not Applicable.

4.6.4 Notification of New Certificate Issuance to Subscriber

Not Applicable.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Not Applicable.

4.6.6 Publication of the Renewal Certificate by the CA

Not Applicable.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Not Applicable.

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

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

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

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

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

Not Applicable.

4.8.3 Processing Certificate Modification Requests

Not Applicable.

4.8.4 Notification of New Certificate Issuance to Subscriber

Not Applicable.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not Applicable.

4.8.6 Publication of the Modified Certificate by the CA

Not Applicable.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not Applicable.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

Issuing CA shall revoke a subscriber's certificate in the following circumstances:

- 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.

4.9.2 Who Can Request Revocation

- Subscriber may make a request to revoke the certificate for which the subscriber is responsible.
- CA that issues certificates under this CP may make a request to revoke its own certificate.
- 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 state in its CPS the procedure for revocation request. 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

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

Relying Parties are 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 Certificate Revocation List (CRL).

4.9.7 CRL Issuance Frequency

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 or not the CRL has any changes.

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

4.9.10 On-line Revocation Checking Requirements

Relying Parties may optionally check the status of certificates through the Thailand NRCA's Online Certificate Status Protocol (OCSP) service, if provided by Thailand NRCA, and/or check the status of subscriber certificates through the issuing CA's OCSP service, if provided by the issuing CA. 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

CA that issues certificate under this CP must notify Thailand NRCA 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

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

4.9.15 Procedure for Suspension Request

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

4.9.16 Limits on Suspension Period

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

The status of certificates is available through the Thailand NRCA's website and LDAP using the appropriate software. The status of subscriber certificates can be checked through the issuing CA's website and LDAP using the appropriate software.

4.10.2 Service Availability

CA that issues 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

Not Applicable.

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

No Private Key escrow process is planned for Thailand NRCA Private Keys. Private Keys of CA that issues certificates under this CP are never escrowed. Subscriber encipherment keys may be escrowed to provide key recovery. Escrowed keys shall be protected at no less than the level of security in which they are generated, delivered, and protected by the subscriber. Under no circumstances shall a subscriber signature key be held in trust by a third party. CA that issues certificates under this CP that support private key escrow for key management keys shall specify in its CPS the policy and practice of key escrow.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not Applicable.

5. Facility, Management, and Operational Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

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 renewal 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 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.

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 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, CA Human Resource department must conduct the following background checks:

- Identification card
- House registration
- Certificate of the highest education
- Criminal records
- Professional certificate (if any)
- Confirmation letter of previous employment

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

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

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

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 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

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

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

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.
    2) CA backup audit events specified in 5.4.1 in backup media.

5.4.6 Audit Collection 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

Not Applicable.

5.4.8 Vulnerability Assessments

CA that issues certificates under this CP must assess security vulnerability 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, Thailand NRCA, 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)

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.
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 submit 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.

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

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 PA and Thailand NRCA 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 *nextUpdate* 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 the case of Thailand NRCA compromise, Thailand NRCA shall notify PA and relying parties via public announcement, and any cross-certified PKIs, of the Thailand NRCA compromise so that they can revoke any cross certificates issued to the Thailand NRCA or any Subordinate CAs and notify all Subscribers and Relying Parties to remove the trusted self-signed certificate from their trust stores. Notification shall be made in an authenticated and trusted manner. Initiation of notification to PA and any cross-certified PKIs shall be made at the earliest feasible time and shall not exceed 24 hours beyond determination of compromise or loss unless otherwise required by law enforcement. Initiation of notification to relying parties and subscribers will be made after mediations are in place to ensure continued operation of applications and services. If the cause of the compromise can be adequately addressed, and it is

determined that the PKI can be securely re-established, Thailand NRCA shall then generate a new root certificate, solicit requests and issue new certificates, securely distribute the new root certificate, and re-establish any cross certificates.

In case of a CA key compromise, the CA shall notify PA and Thailand NRCA. Thailand NRCA 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 Thailand NRCA 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

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

CA that issues certificates under this CP generates a key pair and store the private key in a cryptographic key management device that meets Federal Information Processing Standard (FIPS) 140-2 Level 3 under multi-person control.

Cryptographic keying material used by CAs to sign certificates, CRLs or status information are required to be generated in FIPS 140-2 Level 3 or equivalent standard validated cryptographic modules. Multi-party control is required for CA key pair generation, as specified in section 6.2.2.

CA key pair generation must create a verifiable audit trail demonstrating that the security requirements for procedures were followed. The documentation of the procedure must be detailed enough to show that appropriate role separation was used. An independent third party shall validate the execution of the key generation procedures either by witnessing the key generation or by examining the signed and documented record of the key generation.

Subscriber key pair generation shall be performed by the subscriber. If the CA that issues certificates under this CP generates key pairs for subscriber, the CA shall generate key within a secure FIPS 140 validated cryptographic hardware.

6.1.2 Private Key Delivery to Subscriber

CA that issues certificates under this CP must generate the key pair by themselves. If the CA that issues certificates under this CP generates key pairs for subscriber, the CA shall develop a procedure to securely distribute private key to subscriber.

6.1.3 Public Key Delivery to Certificate Issuer

Where key pairs are generated by subscriber themselves, CA that issues certificates under this CP shall provide a channel for subscriber to securely deliver the public key and the subscriber's identity to the

issuing CA. the 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 CA public key in the certificate by the published channel.

6.1.5 Key Sizes

This CP requires use of RSA signature algorithm and additional restriction on key sizes and hash algorithms are detailed below. Certificates issued under this policy shall contain RSA public keys.

CAs that issues certificates under this CP shall contains subject public key of 4096 bits RSA and be signed with the corresponding private key.

Thailand NRCA root certificate and CAs that issues certificates and CRLs under this CP should use the SHA-256, or SHA-384, or SHA-512 hash algorithm when generating digital signatures. CAs that issue certificates signed with SHA-256, or SHA-384, or SHA-512 must not issue certificates signed with SHA-1.

Key sizes 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 CA.

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 is 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 signing or encrypting.

Public key that are bound into certificates shall be used only for signing certificates and status information such as CRLs. Only Thailand NRCA shall issue certificates to CAs located in Thailand.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

Thailand NRCA uses a FIPS 140-2 Level 3 validated hardware cryptographic module for signing operations.

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

Subscribers shall use a FIPS 140-2 Level 1 or higher validated hardware cryptographic module for all cryptographic operations.

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

Accessing private key of Thailand NRCA and CAs operated under this CP must be performed by at least two persons.

6.2.3 Private Key Escrow

Private keys of CA operated under this CP are never escrowed. CA that issues certificates under this CP must not have policy to keep private key with other parties or keep subscribers' private key.

6.2.4 Private Key Backup

CA's private signature key shall be backed up under the same multiparty control as the original signature key. At least one copy of the private signature key shall be stored off-site. All copies of the CA private signature key shall be accounted for and protected in the same manner as the original. CA that issues certificate under this CP shall backup its private signature key in FIPS 140-2 Level 3 validated hardware cryptographic module. The CA shall state in its CPS the backup procedure.

6.2.5 Private Key Archival

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.

6.2.6 Private Key Transfer into or from a Cryptographic Module

CA private keys may be exported from the cryptographic module only to perform CA key backup procedure. At no time shall the CA private key exist in plaintext outside the cryptographic module.

6.2.7 Private Key Storage on Cryptographic Module

Thailand NRCA and CA operating under this CP shall store its Private Keys on a cryptographic module which complies with FIPS 140-2 Level 3 or above standard.

6.2.8 Method of Activating Private Key

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

6.2.9 Method of Deactivating Private Key

After working with the private key of CA, all certificate authority officers must leave the system (Log Out) to prevent unauthorized access.

6.2.10 Method of Destroying Private Key

CA will delete the private keys from Cryptographic Module and its backup by overwriting the private key or initialize the module with the destroy function of Cryptographic Module.

The event of destroying CA must be recorded into evidence under section 5.4.

6.2.11 Cryptographic Module Rating

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

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Public key is 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 can be used up to the expiry date specified in the certificate. Public key can 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 can be used to decrypt even if certificate is expired.

The validity period of Thailand NRCA root certificate is 23 years and validity period of certificates is not more than 20 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 CA.

(With technical limitations on UTC Time, the certificate issued by Thailand NRCA and its subordinate CA 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 passwords for accessing the CA systems are user-selected and protected under multi-person control by each of whom holding that activation data. CA operated under this CP shall use the same data generation mechanism.

6.4.2 Activation Data Protection

CA operated 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

Not Applicable.

6.5 Computer Security Controls

CA operated under this CP must implement 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

CA operated under this CP 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

CA operated under this CP should define minimum computer security rating used for the operation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

CA operated 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

CA operated under this CP maintains a list of acceptable products and their versions for each individual CA system component and keeps up-to-date. Changes of variables are processed through security management control.

6.6.3 Life Cycle Security Controls

CA operated under this CP can also address life-cycle security ratings based for example, on the Trusted Software Development Methodology (TSDM) level IV and V, independent life-cycle security controls audit, and the Software Engineering Institute's Capability Maturity Model (SEI-CMM)

6.7 Network Security Controls

CA network must equip with 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

The system clock will be set in the time setting device (NTP Server) which shall be accurate to within three minutes. Any recording time in the system will refer to the same time setting device.

7. Certificate, CRL and OCSP Profiles

7.1 Certificate Profile

Certificate issued by CA under this CP must comply with ITU-T Recommendation X.509 (11/08): Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks and ISO / IEC 9594-8:2008 Information technology standard. - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks in which the certificate contains the information shown in Table 3.

Field	Value or Value Constraint
version	Version of certificate, the details are described in section 7.1.1
serialNumber	Reference number of each Certificate Authority is unique
signature	The method of digitally sign consists of Asymmetric cryptographic algorithms (Public Key Algorithm) and data digestion (Hash Function) which Certificate Authority is used to sign the certificate in form of Object Identifier (OID).
issuer	The name of the Certificate Authority in the certificate must be in the format of Distinguished Name (DN) in accordance with ISO / IEC 9594-2.
validity	Period of certificate usage is specified by the begin date (notBefore) and expiration date (notAfter)
subject	Specify the entity name of Certificate Authority as the owner of public key in the certificate
subjectPublicKeyInfo	Specify the type of public key and subject value of public key

Table 3 Fields in the Certificate

7.1.1 Version Number

Certificate issued by CA is in accordance with ITU-T Recommendation X.509 standard ISO / IEC 9594-8:2008 and designated to be version 3.

7.1.2 Certificate Extensions

Additional information on the certificate issued by CA is complied with ISO / IEC 9594-8:2008 standard, which contains at least the following:

7.1.2.1. Key Usage

This extension shall be marked as critical. Certificates shall assert the minimum required for functionality. Signature certificates shall assert *digitalSignature and nonRepudiation*. Encryption certificates shall assert either *keyencipherment* or *keyagreement*. certificates shall assert *digitalsignature*, *nonRepudiation, keyCertSign* and *CRLSign*.

7.1.2.2. Certificate Policies Extension

All CP and CPS must include OID and designate Critical to True.

7.1.2.3. Subject Alternative Name

See section 3.1.

7.1.2.4. Name Constraints

Name constraints MUST be used only in a certificates. Name constraints may be imposed through explicit inclusion of a name constraints extension in a certificate, but are not required..

7.1.2.5. Basic Constraints

Specify the type of certificate in the CA Field and the maximum number of Certificate Chain that is certified in a hierarchy. The subordinate certificate will have *CA Field* set to True and *pathlen* set to one.

7.1.2.6. Extended Key Usage

This extension shall be marked as noncritical. Certificates shall assert the minimum number required for functionality.

7.1.2.7. CRL Distribution Points

Specify the point where certificate revocation list can be accessed in the form of directoryName, URL.

7.1.2.8. Authority Key Identifier

Specify the related information with public key of Certificate Authority into certificate of subscribers by hashing the public key of Certificate Authority with Hash Algorithm SHA-256, or SHA-384 or SHA-512.

7.1.2.9. Subject Key Identifier

Specify the related information with public key by hashing the public key in the certificate with Hash Algorithm SHA-512.

7.1.2.10. Algorithm Object Identifiers

The OID of digital signature and encryption of certificate is in Table 4

Algorithm	Object Identifier
RSAEncryption	1.2.840.113549.1.1.1
SHA512withRSAEncryption	1.2.840.113549.1.1.13
SHA512	2.16.840.1.101.3.4.2.3

Table 4 Method of digital signature and encryption with Object Identifier

7.1.3 Algorithm object identifiers

7.1.4 Name Forms

The name format of Issuer and Subject are specified in the certificate as reference to the section 3.1.1.

7.1.5 Name Constraints

Not Applicable.

7.1.6 Certificate Policy Object Identifier

Not Applicable.

7.1.7 Usage of Policy Constraints Extension

Not Applicable.

7.1.8 Policy Qualifiers Syntax and Semantics

Not Applicable.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Not Applicable.

7.2 CRL Profile

CA's certificate revocation list must comply with ITU-T Recommendation X.509 standard and ISO / IEC 9594-8:2008 has following details as in Table 5.

Field	Value or Value Constraint
version	Version of the certificate revocation list will be version number 2 as provided in section 7.2.1.
signature	The method of digitally sign consists of Asymmetric cryptographic algorithms (Public Key Algorithm) and data digestion (Hash Function) which Certificate Authority is used to sign the certificate in form of Object Identifier (OID).
issuer	The name of the Certificate Authority in the certificate must be in the format of Distinguished Name (DN) in accordance with ISO / IEC 9594-2.
thisUpdate	The date and time of the revocation list.
nextUpdate	Specified date and time to the next update of certificate revocation list. If necessary Thailand NRCA will issue the certificate revocation list before schedule.
revokedCertificates	A list of the serialNumber of the certificate has been revoked with specific the date and time of revocation.

Table 5 Item list in Certificate Revocation

7.2.1 Version Number(s)

The version number of certificate revocation list in accordance with the ITU-T Recommendation X.509 and ISO / IEC 9594-8:2008 will be specified the value of version to be 2.

7.2.2 CRL and CRL Entry Extensions

The information on certificate revocation lists issued by Certification Authority is complied with ISO / IEC 9594-8:2008 standard and contains 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. invalidityDate

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

Not Applicable.

7.3.1 Version Number(s)

Not Applicable.

7.3.2 OCSP Extensions

Not Applicable.

8. Compliance Audit and Other Assessments

CAs operated under this CP have compliance audit mechanism in place 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 Trust Service Principles and Criteria for Certification Authorities Version 2.0 at least once a year.

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. Assessment must be done by an ISO / IEC 27001:2005 and / or the Trust Service Principles and Criteria for Certification Authorities Version 2.0 certified auditors with the understanding of the certification service business.

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 CAM 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 the Trust Service Principles and Criteria for Certification Authorities Version 2.0.

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

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

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

9.1.3 CA operated under this CP shall not include fees for certificate acess.Revocation or Status Information Access Fees

9.1.4 CA operated under this CP shall not include fees for the request of revocation or status Information.Fees for Other Services

9.1.5 CA operated under this CP shall declare the other fees apart from 9.1.1.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

9.2.2 CA operated under this CP shall disclose insurance related to CA operation. Other Assets

9.2.3 CA operated under this CP shall disclose other assets. Insurance or Warranty Coverage for End-entities

9.3 CA operated under this CP shall provide reasonable insurance or warranty for end-entities.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 Policy of certification authority
- 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 practice statement.

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 stems 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 PA.

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 Thailand NRCA.

9.12.2 Notification Mechanism and Period

In case there are any significant changes to this CP, Thailand NRCA 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 Thailand NRCA.

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

Not Applicable.