Thailand National Root Certification Authority Certification Practice Statement

Version 4.5

Certification Practice Statement Identifier (OID): 2.16.764.1.1.1

Publication

Document Revision History

Date	Version	Description
August 2013	1.0	Initial Release
June 2014	2.0	• Translated into English for WebTrust assessment • Reviewed contents to align with RFC 3647 • Reviewed consistency of terms in the document • Added short description of Thailand NRCA • Introduced Software Developer in topic 5.2.1 • Added topic 6.5.1 Computer Security Technical Requirements • Added topic 6.5.2 Computer Security Rating
May 2015	2.1	• Revised 1.5.2 Contact Person • Revised 2.2 Publication of Certification Information • Revised 9.13.1 Disputes between Issuer and Subscriber
August 2015	3.0	• Revised 1.1 Overview • Revised 1.5.2 Contact Person • Added 1.5.5 CP Review and update Procedures • Revised 4.3.1 CA Actions during Certificate Issuance • Revised 4.9.1 Circumstances for Revocation • Revised 4.9.3 Procedure for Revocation Request • Added 5.4.9 Penetration Test Assessments • Revised 7.1.2.2 Certificate Policies Extension • Revised 8 Compliance Audit and Other Assessments • Revised 8.5 Topics Covered by Assessment
August 2018	4.0	• Revised 1.2 Document Name and Identification • Revised 1.5.2 Contact Person • Revised 2.2 Publication of Information • Revised 2.3 Time or Frequency of Publication • Revised 3.2.2 Authentication of Organization and Domain Identity • Revised 3.2.5 Validation of Authority • Revised 4.2.1 Performing Identification and Authentication Functions

Publication

Date	Version	Description
		• Revised 4.9.1 Circumstances for Revocation
		• Revised 5.3.2 Background Check Procedures
		• Revised 5.4.1 Types of Events Recorded
		• Revised 5.4.5 Audit Log Backup Procedures
		• Revised 6.3.2 Certificate Operational Periods and Key Pair Usage Periods
		• Revised 7.1.2 Certificate Content and Extensions; Application of RFC 5280
		• Revised 7.1.5 Name Constraints
		• Revised 7.1.6 Certificate Policy Object Identifier
		• Revised 7.1.8 Policy Qualifiers Syntax and Semantics
		• Revised 7.2.1 Version Number(s)
		• Revised 7.3 OCSP Profile
		• Revised 8. Compliance Audit and Other Assessments
		• Revised 8.1 Compliance Audit for Subordinate CA to be 8.1 Frequency or Circumstances of Assessment
		• Revised 8.2 Frequency or Circumstances of Assessment to be 8.2 Identity/Qualifications of Assessor
		• Revised 8.3 Identify/Qualifications of Assessor to be 8.3 Assessor's Relationship to Assessed Entity
		• Revised 8.4 Assessor's Relationship to Assessed Entity to be 8.4 Topics Covered by Assessment
		• Added 8.7 Self-Audits
		• Revised 9.12.2 Notification Mechanism and Period
November 2019	4.1	• 4.2.1 Performing Identification and Authentication Functions
		• Revised Organization Name of ETDA in Sections below:
		• 1.3.1 Certification Authority
		• 1.3.5.1 Policy Authority
		• 1.5.2 Contact Person
		• 9.13.1 Disputes between Issuer and Subscriber
October 2020	4.2	• 1. 1.3.2 Subordinate Certification Authority (Subordinate CA)
		• 2. Edited 1.3.4 Subscribers and deleted CA Subscribers

Publication

Date	Version	Description
		• 3. 1.4.1 Appropriate Certificate Uses
		• 4. 1.5.5 CP Review and Update Procedures
		• 5. 1.6.1 Definitions
		• 6. 4.9.9 On-line Revocation/Status Checking Availability
		• 7. 5.4.3 Retention Period for Audit Log
		• 8. 6.1.1 Key Pair Generation
		• 9. 6.3.2 Certificate Operational Periods and Key Pair Usage Periods
		• 10. 6.8 Timestamping
		• 11. 7.1.2.2. Subordinate CA Certificate
		• 12. 7.1.2.3. Subscriber Certificate
		• 7.2 CRL Profile
		• 8. Compliance Audit and Other Assessments
		• 8.2 Identity/Qualifications of Assessor
		• 9. 9.2.1 Insurance Coverage
		• 9.5 9.5 Intellectual Property Rights
December 2022	4.3	• 1.6.2 Vocabulary
		• 2.1 add location of repositories
		• 3.1 Public Organization (G1 G2).
		• 3. Table 4. Remove RAO
		• 5.3.1 Removed Trusted Role for Software Developer
		• 5.5.4 check backup procedure
		• Table 6. Organizational structure update
December 2023	4.4	• Revised items to comply with CA/B TLS version 2.0.1
		• Added sections to comply with CA/B S/MIME version 1.0.1
		• Included the new G2 and G3 Root certificates
December 2024	4.5	• Comply with CA/B TLS version 2.0.2
		• Comply with CA/B S/MIME version 1.0.2
		• Correct typos and consistency

Table of Contents

Publication

Publication

Publication

Publication

Publication

Publication

1 Introduction

1.1 Overviewspelling

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. The PKI is composed of many elements, including legal obligations, policies, hardware, software, databases, networks, personnel, and operating procedures. The center of trust in the 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 among 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 hierarchical 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.

This document is the Thailand National Root Certification Authority (Thailand NRCA) Certification Practice Statement (CPS). It states the practices that Thailand NRCA employs in providing certification services, including without limitation, issuing, managing, revoking, and renewing certificates in accordance with the specific requirements of the Thailand NRCA Certificate Policy (CP).

NRCA conforms to the current versions of both the SSL/TLS and S/MIME Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates, and the Network and Certificate System Security Requirements published at http://www.cabforum.org. In the event of any inconsistency between this document and those requirements, those requirements take precedence over this document.

The Certificate Policy (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 Thailand NRCA. The CP sets forth requirements that subordinate certification authorities under Thailand NRCA MUST meet. This CPS describes how Thailand NRCA meets these requirements. More specifically, this CPS describes the practices that Thailand NRCA employs for:

- Managing and securing the core infrastructure that supports Thailand NRCA, and issuing, managing, revoking, and renewing certificates under Thailand NRCA.

The mission of Thailand NRCA includes:

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

This CPS also sets out the certification service scope and procedures of Thailand NRCA, as well as to specify duties, functions, legal obligations, and potential liabilities of participants in the systems used by Thailand NRCA. The document structure and topics conform to the Internet Engineering Task Force (IETF) RFC 3647 for Internet X.509 Public Key Infrastructure Certificate Policy and Certificate Practices Framework.

1.2   Document Name and Identification

This document is the Thailand National Root Certification Authority (Thailand NRCA) Certification Practice Statement (CPS). This CPS is published for public knowledge on the Thailand NRCA Website.

Thailand NRCA bears an Object Identifier (OID) arc of joint-iso-itu-t (2) country (16) th (764) etda (1) nrca (1). To identify policies of certificates issued under Thailand NRCA, the OID is organized and described as follows:

Type of policy	Policy OID
Common Certificate Policy	2.16.764.1.1.1

Table 1: Type of Policy

NRCA organizes its OIDs for the various Certificates described in this CPS as follows:

Type of Certificate	Policy OID
SSL/TLS – Domain Validation	2.23.140.1.2.1
SSL/TLS – Organization Validation	2.23.140.1.2.2
SSL/TLS – Individual Validation	2.23.140.1.2.3

Table 2: Type of Certificate

NRCA organizes its OIDs for the various S/MIME Certificates described in this CPS as follows:

Type of Certificate	Generation	Policy OID
S/MIME – Mailbox Validation	Multipurpose	2.23.140.1.5.1.2
S/MIME – Mailbox Validation	Strict	2.23.140.1.5.1.3
S/MIME – Organization Validation	Multipurpose	2.23.140.1.5.2.2
S/MIME – Organization Validation	Strict	2.23.140.1.5.2.3
S/MIME – Sponsor Validation	Multipurpose	2.23.140.1.5.3.2

S/MIME – Sponsor Validation	Strict	2.23.140.1.5.3.3
S/MIME – Individual Validation	Multipurpose	2.23.140.1.5.4.2
S/MIME – Individual Validation	Strict	2.23.140.1.5.4.3

Table 3: Type of S/MIME Certificate

1.3   PKI Participants

1.3.1   Certification Authority

Thailand National Root Certification Authority (Thailand NRCA) is an operational unit operated by Electronic Transactions Development Agency under the Ministry of Digital Economy and Society. Thailand NRCA issues digital certificates to a legal entity (who operates a CA in Thailand) by using a collection of hardware, software, personnel, and operating procedures that create, sign, and issue public key certificates to Subordinate CAs. This includes centralized, automated systems such as card management systems. Thailand NRCA is responsible for issuing and managing certificates including:

1) Approving the issuance of all certificates, including those issued to subordinate CAs and RAs.
2) Publication of certificates.
3) Revocation of certificates.
4) Generation and destruction of CA signing keys.
5) Establishing and maintaining Thailand NRCA system.
6) Establishing and maintaining the Certification Practice Statement (CPS).
7) Ensuring that all aspects of the CA services, operations, and infrastructure are performed in accordance with the requirements, representations, and warranties of the CP.

1.3.2   Subordinate Certification Authority (Subordinate CA)

A Subordinate Certification Authority (Subordinate CA) is a legal entity that is primarily responsible for issuance and management of Subscriber certificates including:

1) Approving the issuance of certificates
2) Publication of certificates
3) Revocation of certificates
4) Publication of certificate status information through Certificate Revocation Lists (CRLs) and/or Online Certificate Status Protocol (OCSP) responders
5) Subordinate CA key and certificate life cycle management
6) Establishment and maintenance of its Certificate Policy (CP) and Certification Practice Statement (CPS)
7) Ensuring that all aspects of the CA services, operations, and infrastructures are performed in accordance with this Certificate Policy.

1.3.3 Registration Authority

A Registration Authority (RA) is a person or legal entity delegated certain functions on behalf of a Thailand NRCA to perform one or more of the following functions:

1) Identifying and authenticating each Subscriber's identity and information that is to be entered into the Subscriber's public key certificate
2) Approval or rejection of certificate applications, rekeying requests, and renewal requests
3) Initiating certificate revocation and processing requests to revoke certificates

1.3.4 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 "Subscribers" as used in this CPS refers only to "Subordinate CAs" who request certificates for signing and issuing certificates or certificate status information. CAs who want to apply for a certificate from Thailand NRCA for signing and issuing certificates or certificate status information, and so become a subordinate CA of Thailand NRCA and will be qualified as Subordinate CA.

1.3.5 Relying Parties

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

1.3.6 Other Participants

1.3.6.1 Policy Authority

A Policy Authority (PA) is a committee set up by the Electronic Transactions Development Agency. The members of PA are luminaries on PKI. The duty of PA is to decide 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) Establishing Certificate Policy and Certification Practice Statement of Thailand NRCA and other certification authorities under the Thailand NRCA trust model;
2) Arranging 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) Promoting trust relationship of Thailand NRCA with other domestic or overseas certification authorities.

1.4   Certificate Usage

1.4.1 Appropriate Certificate Uses

Certificates issued under Thailand NRCA MUST be used according to the purposes for which the key usage and extended key usage fields were defined. The usage of a certificate issued under Thailand NRCA is limited to support as follows:

- Thailand NRCA is limited to support only the issuing of Subordinate CA certificates to establish a trust relationship between Thailand NRCA and the Subordinate CAs. Additionally, signing Certificate Revocation Lists (CRLs) and certificates for OCSP responder signing to support certificate status checking are also provided.

1.4.2 Prohibited Certificate Uses

A certificate issued by Thailand NRCA SHALL be used only for the purpose as specified in Section 1.4.1, and in particular SHALL be used only to the extent that is consistent with applicable laws.

1.5   Policy Administration

1.5.1 Organization Administering the Document

This document is administered by Thailand NRCA. This document is publicly available with approval from PA.

1.5.2 Contact Person

Thailand National Root Certification Authority
Electronic Transactions Development Agency
The Government Complex Commemorating His Majesty the King's 80th Birthday (Building B)
120 Moo 3, 6th floor, Chaengwattana Road, Thung Song Hong Subdistrict, Lak Si District,
Bangkok 10210
Tel: (66)-2123-1234
Email: nrca@etda.or.th
Website: https://www.nrca.go.th

1.5.3 Person Determining CPS Suitability for the Policy

The PA determines the suitability and applicability of this CPS.

1.5.4 CPS Approval Procedures

The CPS approval procedures are as follows:

1) Thailand NRCA proposes CPS changes and submits to the PA.

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

    1.2 In case the PA has comments, the PA returns the CPS to Thailand NRCA for proper modification or correction before resubmission.

2) Thailand NRCA announces and publishes the CPS to the channel as listed in Section 2.2.

1.5.5 CP Review and Update Procedures

Thailand NRCA SHALL review the latest SSL/TLS and S/MIME Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates, and the Network and Certificate System Security Requirements from https://cabforum.org/ at least quarterly for the purpose of developing, implementing, and enforcing, and update the Certificate Policy and Certification Practice Statement annually.

1.6 Definitions and Acronyms

1.6.1 Definitions

See Table 4 for a list of definitions.

Term	Definition
Certificate or public-key certificate	A form of electronic document that uses a digital signature to bind a public key and an identity. A certificate is issued in compliance with ITU-T Recommendation X.509, RFC 5280, Baseline Requirements of CA/Browser Forum and ETDA Recommendation.
CAA	From RFC 8659 (http://tools.ietf.org/html/rfc8659): "The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify the Certification Authorities (CAs) authorized to issue certificates for that domain. Publication of CAA Resource Records allows a public Certification Authority to implement additional controls to reduce the risk of unintended certificate mis-issue."
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	An online database containing publicly disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.
Certificate Revocation	A certificate MAY be revoked prior to its expiration date. Once revoked, it can no longer be used.
Certification Authority (CA)	An organization or an entity that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Roots CAs and Subordinate CAs.
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 act in reliance of a certificate.
Cryptographic Module	The specialized equipment used to maintain, manage and operate the key pair.
Cross-certificate	A certification authority (CA) certificate where the issuer and the subject are different CAs. CAs issue cross-certificates to other CAs as a mechanism to authorize the subject CA's existence.
Digital Signature	A mathematical scheme for demonstrating the authenticity, integrity, and non-repudiation of a digital message or document.

Term	Definition
Directory Service	A storage for publication of certificates and certificate revocation lists following the X.500 Standard or LDAP.
End-Entity/Subscriber	A natural person, Legal Entity, server, operating unit, or any device to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use.
Key Pair	The Private Key and its associated Public Key.
OCSP (Online Certificate Status Protocol)	A protocol used for verifying status of a certificate.
Private Key	The key of an entity's key pair which is known only by that entity and used to create a digital signature. Additionally, it 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 of an entity's key pair which is publicly known and used to verify a digital signature to ensure the integrity of electronic message and also to encrypt a message to maintain its confidentiality.
Root Certificate	The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.
Subordinate CA	A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.

Table 4: Terms and Definitions

1.6.2 Acronyms

Acronym	Term
CA	Certification Authority
CAA	Certification Authority Authorization
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DNS	DNS Domain Name System
ETDA	Electronic Transactions Development Agency
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name.
DN	Distinguished Name
OCSP	Online Certificate Status Protocol
OID	Object Identifier
NRCA	National Root Certification Authority
PA	Policy Authority
RA	Registration Authority
PIN	Personal Identification Number
PKI	Public Key Infrastructure
SSL	Secure Sockets Layer
TLS	Transport Layer Security

Table 5: Acronyms

2   Publication and Repository Responsibilities

2.1   Repositories

Thailand NRCA posts all issued certificates on the publicly accessible website at the URL https://nrca.go.th/publish.html,

The repository for the Thailand NRCA's CP and CPS can be found at https://nrca.go.th/publish.html. The fingerprints of root certificate and intermediate certificates can be found at https://nrca.go.th/content/issue-cert.html.

Thailand NRCA has implemented access controls to prevent unauthorized modification or deletion of information.

2.2   Publication of Information

Thailand NRCA makes information publicly available on the website (www.nrca.go.th) such as CPs, CPSs, Certificates and CRLs in repositories. For public services, they are available 24 hours per day and 7 days per week. It SHALL ensure that its repository or repositories are implemented through trustworthy systems.

2.3   Time or Frequency of Publication

Thailand NRCA publishes their certificates and CRLs as soon as possible after issuance. Thailand NRCA reviews CP and CPS at least annually and make appropriate changes. The latest versions of CP and/or CPS are published within three days after updating and of their approval.

2.4   Access Controls on Repositories

Thailand NRCA has implemented physical access control as well as network security measures to authenticate and restrict modification or deletion to the repository. The adding, deleting, or modifying repository entries can be performed only by authorized personnel of Thailand NRCA. Thailand NRCA website is used as repositories for Subscribers and Relying Parties to access the publication documents.

3   Identification and Authentication

3.1   Naming

3.1.1 Types of Names

Thailand NRCA Certificates contain a Distinguished Name (DN) in the Issuer and Subject fields, following the X.501 Information technology – Open Systems Interconnection – The Directory: Models. The Distinguished Names consist of the components specified in Table 6 below.

Root	Attribute Name	Value
G1	Country (C) =	TH
	Organization (O) =	Electronic Transactions Development Agency (Public Organization) or <organization name>
	Common Name (CN) =	Thailand National Root Certification Authority - G1 or <certification authority name>
G2	Country (C) =	TH
	Organization (O) =	Electronic Transactions Development Agency or <organization name>
	Common Name (CN) =	Thailand National Root Certification Authority – G2 or <certification authority name>
G3	Country (C) =	TH
	Organization (O) =	Electronic Transactions Development Agency or <organization name>
	Common Name (CN) =	Thailand National Root Certification Authority – G3 or <certification authority name>

Table 6: Distinguished Name Attributes in certificates

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

Thailand NRCA does not issue anonymous or pseudonymous certificates.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting distinguished name forms follow the X.501 standard. Rules for interpreting e-mail addresses follow RFC 2822.

3.1.5 Uniqueness of Names

The distinguished names of a Subordinate CA MUST be unique within the domain of Thailand NRCA.

3.1.6 Recognition, Authentication, and Role of Trademarks

Thailand NRCA 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 with the relevant laws, regulations, legal obligations or announcements.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

Thailand NRCA requires that an authorized representative of a juristic person submits an application form on behalf of the Subordinate CA and a Certificate Signing Request (CSR) that is signed by the private key of the Subordinate CA. Upon receipt of the CSR, Thailand NRCA will verify that the Subordinate CA is in possession of the corresponding private key by checking the digital signature on the CSR structure containing the public key material. Thailand NRCA will not have possession of the Subordinate CA's private keys.

3.2.2 Authentication of Organization and Domain Identity

Subordinate CAs will submit their applications for certificates with its name, business address in Thailand, and the Certificate of Corporate Registration of the CA issued by the Department of Business Development, Ministry of Commerce. Thailand NRCA verifies 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 other processes, Thailand NRCA SHALL conform to Authentication of Organization and Domain Identity Section in CA/Browser Forum TLS Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates with the latest version.

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

Thailand NRCA follows Section 3.2.2.2 of CA/B Forum TLS Baseline Requirements.

3.2.2.3   Verification of Country

The NRCA SHALL verify the information for Subordinate CAs using the following sources:

1) Commercial entities: The Department of Business Development (DBD)
2) Noncommercial Thai entities: Authorized Thai government organization/agencies
3) Foreign entities: The authorized national government/agencies of that country.

3.2.2.4   SSL/TLS: Validation of Domain Authorization or Control

This section defines the permitted processes and procedures for validating the Applicant's ownership or control of the domain. The CA SHALL confirm that prior to issuance, the CA has validated each Fully Qualified Domain Name (FQDN) listed in the Certificate using at least one of the methods listed below.

Completed validations of Applicant authority MAY be valid for the issuance of multiple Certificates over time. In all cases, the validation MUST have been initiated within the time period specified in the relevant requirement (such as Section 4.2.1 of this document) prior to Certificate issuance. For purposes of domain validation, the term Applicant includes the Applicant's Parent Company, Subsidiary Company, or Affiliate. CAs SHALL maintain a record of which domain validation method, including relevant BR version number, they used to validate every domain.

Note: FQDNs SHALL be listed in Subscriber Certificates using dNSNames in the subjectAltName extension or in Subordinate CA Certificates via dNSNames in permittedSubtrees within the Name Constraints extension.

3.2.2.4.1   Validating the Applicant as a Domain Contact

Thailand NRCA does not issue Subscriber Certificates.

3.2.2.4.2   Email, Fax, SMS, or Postal Mail to Domain Contact

Thailand NRCA does not issue Subscriber Certificates.

3.2.2.4.3   Phone Contact with Domain Contact

Thailand NRCA does not issue Subscriber Certificates.

3.2.2.4.4 Constructed Email to Domain Contact

Thailand NRCA does not issue Subscriber Certificates.

3.2.2.4.5 Domain Authorization Document

Thailand NRCA does not issue Subscriber Certificates.

3.2.2.4.6 Agreed-Upon Change to Website

Thailand NRCA does not issue Subscriber Certificates.

3.2.2.4.7 DNS Change

Thailand NRCA does not issue Subscriber Certificates.

3.2.2.4.8 IP Address

Thailand NRCA does not issue Subscriber Certificates.

3.2.2.4.9 Test Certificate

Thailand NRCA does not issue Subscriber Certificates.

3.2.2.4.10 TLS Using a Random Number

Thailand NRCA does not issue Subscriber Certificates.

3.2.2.4.11 Any Other Method

Thailand NRCA does not issue Subscriber Certificates.

3.2.2.4.12 Validating Applicant as a Domain Contact

Thailand NRCA does not issue Subscriber Certificates.

3.2.2.4.13 Email to DNS CAA Contact

Thailand NRCA does not issue Subscriber Certificates.

3.2.2.4.14 Email to DNS TXT Contact

Thailand NRCA does not issue Subscriber Certificates.

3.2.2.4.15 Phone Contact with Domain Contact

Thailand NRCA does not issue Subscriber Certificates.

3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact

Thailand NRCA does not issue Subscriber Certificates.

3.2.2.4.17 Phone Contact with DNS CAA Phone Contact

Thailand NRCA does not issue Subscriber Certificates.

3.2.2.4.18 Agreed-Upon Change to Website v2

Thailand NRCA does not issue Subscriber Certificates.

3.2.2.4.19 Agreed-Upon Change to Website - ACME

Thailand NRCA does not issue Subscriber Certificates.

3.2.2.4.20 TLS Using ALPN

Thailand NRCA does not issue Subscriber Certificates.

3.2.2.5   SSL/TLS: Authentication for an IP Address

Thailand NRCA does not issue Subscriber Certificates.

3.2.2.5.1   Agreed-Upon Change to Website

Thailand NRCA does not issue Subscriber Certificates.

3.2.2.5.2   Email, Fax, SMS, or Postal Mail to IP Address Contact

Thailand NRCA does not issue Subscriber Certificates.

3.2.2.5.3   Reverse Address Lookup

Thailand NRCA does not issue Subscriber Certificates.

3.2.2.5.4   Any Other Method

Thailand NRCA does not issue Subscriber Certificates.

3.2.2.5.5   Phone Contact with IP Address Contact

Thailand NRCA does not issue Subscriber Certificates.

3.2.2.5.6   ACME "http-01" method for IP Addresses

Thailand NRCA does not issue Subscriber Certificates.

3.2.2.5.7   ACME "tls-alpn-01" method for IP Addresses

Thailand NRCA does not issue Subscriber Certificates.

3.2.2.6   SSL/TLS: Wildcard Domain Validation

Thailand NRCA does not issue Subscriber Certificates.

3.2.2.7   Data Source Accuracy

Thailand NRCA does not issue Subscriber Certificates.

3.2.2.8   CAA Records

Thailand NRCA does not issue Subscriber Certificates.

Thailand NRCA itself lists the following CAA records for the https://www.nrca.go.th website: nrca.go.th, thaidigitalid.com

3.2.2.9   SSL/TLS: Multi-Perspective Issuance Corroboration

Thailand NRCA does not issue Subscriber Certificates.

3.2.2.10 S/MIME: Validation of mailbox authorization or control

3.2.2.10.1 Validating authority over mailbox via domain

Thailand NRCA does not issue Subscriber Certificates.

3.2.2.10.2 Validating control over mailbox via email

Thailand NRCA does not issue Subscriber Certificates.

3.2.2.10.3 Validating applicant as operator of associated mail server(s)

3.2.3   Thailand NRCA does not issue Subscriber Certificates.Authentication of Individual Identity

Thailand NRCA does not issue Subscriber Certificates.

3.2.4   Non-verified Subscriber Information

All Subordinate CA's information contained in a certificate is verified.

3.2.5   Validation of Authority

Thailand NRCA follows Section 3.2.5 of CA/B Forum TLS Baseline Requirements.

3.2.6 Criteria for Interoperation or Certification

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

Thailand NRCA does not issue cross-certificates.

3.2.7 SMIME: Reliability of verification sources

Thailand NRCA does not issue cross-certificates.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

Identification and authentication procedures are specified in Section 3.2.

3.3.2 Identification and Authentication for Re-key after Revocation

Identification and authentication procedures are specified in Section 3.2.

3.4 Identification and Authentication for Revocation Request

Identification and authentication procedures 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

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

4.1.2 Enrollment Process and Responsibilities

Subordinate CAs MUST complete an application and submit it to Thailand NRCA. By submitting a certificate application, the Subordinate CA authorizes the publication of the certificate to any other person or in the Thailand NRCA repository and thus accepts the certificate to be issued to the Subordinate CA.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Thailand NRCA does not perform CAA record verification as there are no SSL certificate being issued based on the current CPS version.

4.2.2 Approval or Rejection of Certificate Applications

Any certificate application that is received by Thailand NRCA for which the identity and authorization of the applicant has been validated, will be duly processed. However, Thailand NRCA will reject any application for which such validation cannot be completed.

The RA will coordinate with Thailand NRCA during the process of approval or rejection of certificate applications and notify the results to Subscribers.

4.2.3 Time to Process Certificate Applications

CA Certificate applications will be processed within 30 business days, counting from the date that the RA endorses the receipt of a CA certification application, to complete the processing of the application.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

Following the identity verification process, Thailand NRCA will notify the Subordinate CA the approval of application. Hence, the certificate issuance process is as follows:

1) The Subordinate CA generates a key pair on its own device and a Certificate Signing Request (CSR) that conforms to PKCS #10: Certificate Request Syntax Standard. The CSR contains the identity of the Subordinate CA organization and the public key. The private key MUST be secured in the hardware security module.

2) Upon receipt of the CSR, Thailand NRCA will verify that the applicant is in possession of the corresponding Private Key by checking the digital signature on the CSR structure containing the public key material and the CAO (Certification Authority Officer) MUST verify and ensure that the information in the CSR MUST conform to Section 6. If it does not conform to Section 6, the CAO should reject. Thailand NRCA will not have possession of the applicants' Private Keys.

3) Upon verifying the applicant's possession of its Private Key, Thailand NRCA will generate the certificate in which the applicant's public key will be included.

4) The certificate will be delivered to the authorized representative in a secure manner such as by hand or by registered mail.

5) Upon Thailand NRCA acknowledgement of certificate acceptance by the authorized representative, the issued certificate will be published in the Thailand NRCA Repository together with its thumbprint for verifying the Subordinate CA authenticity on Thailand NRCA website.

6) Applicants can either verify the information on the certificate by browsing the certificate file or through Thailand NRCA's Repository. Applicants should notify Thailand NRCA immediately of any incorrect information of the certificate.

Backdating of a certificate's notBefore date is not allowed by Thailand NRCA.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

Thailand NRCA, or via the RA, will notify the Subordinate CA of the creation of a certificate and make the certificate available to the Subordinate CA.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Upon the receipt of a certificate, the Subordinate CA MUST verify the information contained in the certificate and determine whether to accept or reject the certificate. The Subordinate CA MAY notify Thailand NRCA if it accepts the certificate or rejects the certificate for some reasons. If the Subordinate CA fails to notify Thailand NRCA the rejection of the issued certificate within ten business days, the certificate will be considered as accepted.

4.4.2 Publication of the Certificate by the CA

Thailand NRCA will publish the issued certificates on the Publication Channel of Certification Information within one business day after being notified by the Subordinate CA.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

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

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subordinate CA can use the Private Key corresponding to the Public Key in the certificate, which is issued by Thailand NRCA, in order to issue Subscriber certificates signing with its digital signature to other Subscribers or sign the certificate revocation list in relation to those Subscriber certificates. Subscriber certificates SHALL be used lawfully in accordance with the CP, CPS and Terms of Service of Thailand NRCA.

4.5.2 Relying Party Public Key and Certificate Usage

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

1) The accuracy of the digital signature in the Subordinate CA's certificate and its hierarchy (e.g.: path validation).
2) The validity period of the certificates of Subordinate CA, e.g.: the certificates should not expire by the time of use.
3) The status of the certificate of Thailand NRCA, Subordinate CA and other parents in every level of the hierarchy involved (if applicable), e.g.: the certificate should not be revoked or suspended.
4) Certificate usage SHALL be in accordance with Section 1.4.

4.6 Certificate Renewal

Certificate renewal means the issuance of a new Certificate without changing the Public Key or any other information in the Certificate. Certificate renewal is not supported by Thailand NRCA.

4.6.1 Circumstance for Certificate Renewal

Certificate renewal is not supported by Thailand NRCA.

4.6.2 Who May Request Renewal

Certificate renewal is not supported by Thailand NRCA.

4.6.3 Processing Certificate Renewal Requests

Certificate renewal is not supported by Thailand NRCA.

4.6.4 Notification of New Certificate Issuance to Subscriber

Certificate renewal is not supported by Thailand NRCA.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Certificate renewal is not supported by Thailand NRCA.

4.6.6 Publication of the Renewal Certificate by the CA

Certificate renewal is not supported by Thailand NRCA.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Certificate renewal is not supported by Thailand NRCA.

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

Thailand NRCA requires its Subordinate CAs to re-key the certificate in the following cases:

1) The Subordinate CA's certificate has less than 5 years before expiration or has already expired.
2) The Subordinate CA's certificate has been revoked.
3) The Subordinate CA needs to modify information in the certificate.

4.7.2 Who May Request Certification of a New Public Key

Only the Subordinate CA may request a new certificate.

4.7.3 Processing Certificate Re-keying Requests

Subordinate CAs 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

Thailand NRCA notifies the result of new certificate issuance to its Subordinate CA according to the procedures specified in Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

After Subordinate CAs receive a re-keyed certificate, they 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

Thailand NRCA publishes 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

Thailand NRCA notifies 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, Thailand NRCA does not offer certificate modification. If a circumstance for certificate modification is deemed to arise, re-certification will be followed, that means the initial registration process as described in Section 3.2 will be performed again. The new certificate SHALL have a different subject public key.

4.8.2 Who May Request Certificate Modification

Certificate modification is not supported by Thailand NRCA.

4.8.3 Processing Certificate Modification Requests

Certificate modification is not supported by Thailand NRCA.

4.8.4 Notification of New Certificate Issuance to Subscriber

Certificate modification is not supported by Thailand NRCA.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Certificate modification is not supported by Thailand NRCA.

4.8.6 Publication of the Modified Certificate by the CA

Certificate modification is not supported by Thailand NRCA.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Certificate modification is not supported by Thailand NRCA.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

Thailand NRCA SHALL revoke a Subordinate CA's certificate in the following circumstances:

4.9.1.1 Reasons for Revoking a Subscriber Certificate

Thailand NRCA does not issue Subscriber Certificates.

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

The Issuing CA SHALL revoke a Subordinate CA Certificate within seven (7) days if one or more of the following occurs:

1) The Subordinate CA requests revocation in writing;
2) The Subordinate CA notifies the Issuing CA that the original certificate request was not authorized and does not retroactively grant authorization;
3) The Issuing CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Section 6.1.5 and 6.1.6 in CA/Browser Forum TLS Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates;
4) The Issuing CA obtains evidence that the Certificate was misused;
5) The Issuing CA is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with this CP or the applicable Certificate Policy or Certification Practice Statement;
6) The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
7) The Issuing CA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;

8) The Issuing CA's or Subordinate CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository;

9) Revocation is required by the Issuing CA's Certificate Policy and/or Certification Practice Statement; or

10) 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

1) The Subordinate CA may make a request to revoke its own certificate.
2) The Subordinate CA may also revoke any issued certificate whenever it knows or reasonably suspects that the circumstances as specified in Section 4.9.1 occurred.
3) The RA may also make a request to revoke a certificate for which a Subordinate CA is responsible whenever it knows or reasonably suspects that the circumstances as specified in Section 4.9.1 occurred.
4) Relying Parties, Application Software Suppliers, and other third parties may submit Certificate Problem Reports informing the issuing CA of reasonable cause to revoke the certificate.
5) Court order.

4.9.3 Procedure for Revocation Request

A CA that issues certificates under this CP SHALL provide the procedure that a requester can request for revocation 24x7 and Certificate Problem Reports. A Subscriber requesting revocation is required to follow the procedures such as:

1) The Subordinate CA submits the revocation request and related documents to Thailand NRCA, or via a RA of Thailand NRCA, providing that the information is genuine, correct and complete.
2) Thailand NRCA verifies and endorses the revocation requests and related documents.
3) The 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) Thailand NRCA, if necessary with the assistance of the RA, will approve and process the revocation request.
5) Thailand NRCA, if necessary with the assistance of the RA, will inform the revocation result to the Subordinate CA and the PA.

More information about submitting Certificate Problem Reports can be found on the "Contact Us" page of the Thailand NRCA website: https://nrca.go.th/contact.html

4.9.4 Revocation Request Grace Period

There is no grace period for revocation under this CPS.

4.9.5 Time within Which CA Must Process the Revocation Request

Thailand NRCA SHALL revoke certificates as quickly as practicable, or within the time set forth in Section 4.9.1.2 after the revocation request is endorsed.

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

Thailand NRCA does not issue Subscriber Certificates and will issue a CRL within the following circumstances:

- Issuing a CRL within 24 hours whenever a certificate is revoked.
- Issuing a CRL for certificates every twelve months whether or not the CRL has any changes.

4.9.8 Maximum Latency for CRLs

Thailand NRCA will publish a CRL within one hour after generation.

4.9.9 On-line Revocation/Status Checking Availability

Online status checking is provided by Thailand NRCA and conforms to RFC 6960 and RFC 5019. Additionally, OCSP responses are signed by Thailand NRCA. Status information is updated and available to Relying Parties within 2 hours of CRL publication.

4.9.10 On-line Revocation Checking Requirements

Relying Parties may optionally check the status of Subscriber certificates through the Subordinate CA's Online Certificate Status Protocol (OCSP) service. Client software using on-line status checking need not obtain or process CRLs.

4.9.11 Other Forms of Revocation Advertisements Available

Thailand NRCA does not employ any method other than OCSP and CRL for advertising revocation status.

4.9.12 Special Requirements Regarding Key Compromise

Thailand NRCA, the Subordinate CA and Subscribers will notify Relying Parties as soon as practical regarding its key compromise.

Thailand NRCA closely monitors our e-mail address nrca@etda.or.th and ticketing system.

4.9.13 Circumstances for Suspension

Under no circumstances will a certificate be suspended. If a certificate is no longer considered as valid, it will be revoked.

4.9.14 Who Can Request Suspension

Thailand NRCA does not suspend certificates.

4.9.15 Procedure for Suspension Request

Thailand NRCA does not suspend certificates.

4.9.16 Limits on Suspension Period

Thailand NRCA does not suspend certificates.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The status of certificates is available through the Thailand NRCA's website and the LDAP server.

4.10.2 Service Availability

Thailand NRCA has implemented backup systems for providing certificate status services and put the best efforts to make such services available 24x7.

4.10.3 Optional Features

No optional features are provided.

4.11 End of Subscription

The Subordinate CA 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

Thailand NRCA does not escrow keys.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Private Keys of a CA that issues certificates under the Thailand NRCA are never escrowed.

5 Facility, Management, and Operational Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

The systems providing Thailand NRCA services are located at two secure facilities, i.e., the main site in Bangkok and the disaster recovery site in a geographic location reasonably apart from the main site. Both secure facilities are equipped with physical access controls as follows:

1) Four layers of physical access controls
2) Two-factor authentication for accessing the server rooms
3) CCTVs (Closed Circuit Televisions) record the activity in the server room at all times
4) Smoke detector and fire extinguisher (using electronic equipment safe agent) systems

The server rooms are accessible by the Thailand NRCA officers only. If a non-Thailand NRCA officer requires access to the room, authorization from Thailand NRCA MUST be provided in order to allow that person to enter the server room. At all times, such a person MUST be accompanied by the Thailand NRCA officer.

Certificate issuing servers and Cryptographic Module are stored in a separate rack where physically accessing to such systems requires a user to perform a two-factor authentication.

5.1.2 Physical Access

Accessing the certificate issuance system is allowed only to Thailand NRCA responsible officers. In case that a third party needs to access the service area of Thailand NRCA, prior authorization MUST be obtained. All visits to the Thailand NRCA premise MUST be recorded in the access log. At all times, third parties MUST be accompanied by the Thailand NRCA officer during the whole visit. Certificate issuing servers and Cryptographic Module are stored in a secure rack where physical access to such systems requires dual-control and two-factor authentication.

5.1.3 Power and Air Conditioning

- Both secure facilities are equipped with power generators and Uninterrupted Power Supplies (UPS) sufficient for a minimum of 6-hour operation in the absence of commercial power, in order to maintain availability and avoid denial of service.
- The air-conditioning systems for both secure facilities maintain the temperature and the humidity of the server rooms to the appropriate level.

5.1.4 Water Exposures

The secure facilities are equipped with water sensors under the raised floor.

5.1.5 Fire Prevention and Protection

The certificate issuing area is equipped with a smoke detector where the fire extinguisher will be automatically activated when smoke is detected. The certificate issuing area is equipped with a fire extinguishing system that operates quickly and effectively without causing damage to electrical equipment.

5.1.6 Media Storage

All magnetic media holding back ups of critical system data, or any other sensitive information are protected from water, fire, or other environmental hazards, and protective measures are in place to deter, detect, and prevent the unauthorized use of, access to, or disclosure of such media.

5.1.7 Waste Disposal

Thailand NRCA has implemented 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

A backup media is stored at the secure disaster recovery 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. Thailand NRCA takes 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:

1) The validation, authentication, and handling of information in Certificate Applications.
2) The acceptance, rejection, or other processing of Certificate Applications, revocation requests renewal requests, or enrollment information.

3) The issuance, or revocation of Certificates, including personnel having access to restricted portions of its repository.

4) Access to safe combinations and/or keys to security containers that contain materials supporting production services.

5) Access to hardware security modules (HSMs), their associated keying material, and the secret share splits of the PINs that protect access to the HSMs.

6) Providing enterprise customer support.

7) Access to any source code for the digital certificate applications or systems.

8) Access to restricted portions of the certificate repository.

9) The ability to grant physical and/or logical access to the CA equipment.

10) The ability to administer the background investigation policy processes.

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.

Thailand NRCA defines trusted roles and rights as follows:

1) Policy Authority (PA)
2) Certification Authority Manager (CAM)
3) Certification Authority Officer (CAO)
4) Registration Authority (RA)
5) Security Officer (SO)
6) System Administrator (SA)
7) Network Administrator (NA)
8) Internal Auditor (IA)

Position	Trusted Roles	Rights
Committee	Policy Authority: PA	• Issue and approve the policy and the CP/CPS of the Thailand NRCA and other certification authorities located in Thailand
The Director of Digital Service Security Center	Certification Authority Manager: CAM	• Access to the certificate issuing facilities. • Access to the Cryptographic Module and give authorization to who can access the Cryptographic Module.
Engineers of Digital Service Security Center	Registration Authority: RA	• Access to the list of Subordinate CAs. • Access to the personal information of Subordinate CAs.
Engineers of Digital Service Security Center	Security Officer: SO	• Access to audit logs • Access to the certificate issuing and supporting facilities. • Hold all privilege account passwords for all systems.
Engineers of Digital Service Security Center	Certification Authority Officer: CAO	• Access to the certificate issuing facilities • Hold the multi-person control token for managing the Cryptographic Module.
Engineers of Digital Service Security Center	System Administrator: SA Network Administrator: NA	• Access to the facilities i n relation to certificate issuance; • Access to the configuration of equipment such as network, firewall, antivirus, backup, etc.;
Independent third-party	Internal Auditor: IA	• Access to information in relation with audit matters on a need to know basis

Table 7: List of the Trusted Roles and their rights

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:

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

For the tasks that require access to the Thailand NRCA's private key, issuing a certificate, and revoking a certificate, such tasks require at least two authorized officers from the trusted roles.

5.2.3 Identification and Authentication for Each Role

Thailand NRCA and its RAs have confirmed 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 Thailand NRCA or RA systems.

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

Thailand NRCA and RA equipment are under strong authenticated access control for remote access using multi-factor authentication. Thailand NRCA and RA equipment require, at a minimum, authenticated access control (e.g., strong passwords) for local multi-party access.

Individuals holding trusted roles will be appointed to the trusted role by an appropriate approving authority. The approvals are recorded in a secure and auditable fashion. Individuals holding trusted roles accept the responsibilities of the trusted role, and this acceptance is recorded in a secure and auditable fashion. Identity proofing of the RA will be performed by a member of the CA Operations Staff. Users MUST 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 Thailand NRCA Operations Staff role SHALL NOT be an RA except that Thailand NRCA Operations Staff MAY perform RA functions when issuing certificates or issuing certificates to RA.

Under no circumstances SHALL Thailand NRCA 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 Thailand NRCA equipment.

The following roles MUST be performed by trusted officers:

1) Verification and validation of forms such as the certificate application forms and the certificate revocation form.
2) CA Certificate issuance and revocation.
3) Access to the Thailand NRCA's private key.

5.3 Personnel Controls

5.3.1 Qualifications, Experience and Clearance Requirements

Thailand NRCA personnel MUST be examined with their qualifications in terms of the requisite background, and experience in order to ensure their prospective job responsibilities, competency and satisfaction. Thailand NRCA conducts investigations of personnel who serve in trusted roles (prior to their employment and periodically thereafter as necessary) to verify such employee's trustworthiness and competence in accordance with the requirements of this CPS and Thailand NRCA's personnel policies. Personnel who fail an initial or periodic investigation are not permitted to serve or to continue to serve in a trusted role.

5.3.2 Background Check Procedures

Prior to commencement of employment, the Human Resource Department of ETDA conducts the following background checks:

1) Identification card
2) House registration
3) Certificate of the highest education
4) Criminal records
5) Professional certificate (if any)

6) Confirmation letter of previous employment
7) Background Check (Recheck at least every five years)

Thailand NRCA MAY also exercise other measurements for background checks. 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 Thailand NRCA.

5.3.3 Training Requirements and Procedures

Thailand NRCA provides 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:

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

5.3.4 Retraining Frequency and Requirements

Thailand NRCA provides 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

Thailand NRCA requires its officers to get their job rotated every two years.

5.3.6 Sanction for Unauthorized Actions

Appropriate disciplinary actions are taken for unauthorized actions or other violations of Thailand NRCA 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 of employment and relevant disciplinary actions as outlined in Thailand NRCA's personnel policies.

5.3.7 Independent Contractor Requirements

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

For system maintenance purposes, operating staffs MUST present their employee identification card to Trusted Persons of Thailand NRCA for verification and recording. They are also escorted and directly supervised by trusted Thailand NRCA officers at all times.

5.3.8 Documentation Supplied to Personnel

Thailand NRCA provides 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

Thailand NRCA logs the following significant events:

1) Key Life Cycle Management of Thailand NRCA, including:
    1.1 Key generation, backup, storage, recovery, archival, and destruction
    1.2 Cryptographic Module life cycle management events
2) CA certificate life cycle management events, including:
    2.1 CA Certificate Applications, rekey, and revocation
    2.2 Approval or rejection of requests
    2.3 Generation and issuance of certificates and CRL
3) Security-related events including:
    3.1 Successful and unsuccessful access attempts to Thailand NRCA systems
    3.2 Security system actions performed by Thailand NRCA officers
    3.3 Security profile changes
    3.4 System crashes, hardware failures and other anomalies
    3.5 Firewall and router activity

Log entries include the following elements:

1) Date and time of entry
2) Identity of the person making the journal entry; and
3) Description of the entry

5.4.2 Frequency of Processing Log

Audit logs are examined at least on a weekly basis for security-related events and biannually for Key Life Cycle Management and CA certificate life cycle management events.

5.4.3 Retention Period for Audit Log

CAs SHALL retain any audit logs generated with periods as below.

No.	Certification type	Retention Period for Audit Log
1	SSL/TLS Certificate	at least 2 years.
2	Enterprise/Individual Certificate	at least 90 days.

Table 8: Log Retention Period

The CA SHALL make these audit logs available to Qualified Auditor upon request.

5.4.4 Protection of Audit Log

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

5.4.5 Audit Log Backup Procedures

1) Audit Logs stored in an electronic audit log system are backed up in two facilities protected through restricted security perimeters.
2) Events Records follow the procedures below:
    2.1 Paper-based event records are converted into electronic format before being stored in the audit log system.
    2.2 Thailand NRCA 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

Thailand NRCA is not required to notify a subject that has been the cause of an auditable event.

5.4.8 Vulnerability Assessments

Thailand NRCA assesses security vulnerabilities at least on a quarterly basis.

5.5   Records Archival

5.5.1 Types of Records Archived

Thailand NRCA archives:

1) Thailand NRCA systems

1.1 All audit data specified in 5.4.1

1.2 System configuration

1.3 Website

2) Documentation supporting certificate applications

2.1 CA Certificates, CRLs, and expired or revoked certificates

2.2 Thailand NRCA CP and CPS

3) Certificate lifecycle information

3.1 Forms such as Application Form, Revocation Request Form, Re- key Request Form, and certificate Acceptance Form

3.2 Required documents for application

3.3 Internal documents such as procedure manuals and system access approval request

3.4 Letters or memos used for communication between Thailand NRCA and external parties such as its subordinate CA.

5.5.2 Retention Period for Archive

The CA and each Delegated Third Party SHALL retain, for at least two (2) years:

1) CA certificate and key lifecycle management event records (as set forth in Section 5.4.1 (1)) after the later occurrence of:

1.1 the destruction of the CA Private Key; or

1.2 the revocation or expiration of the final CA Certificate in that set of Certificates that have an X.509v3 basicConstraints extension with the cA field set to true and which share a common Public Key corresponding to the CA Private Key;

2) Subscriber Certificate lifecycle management event records (as set forth in Section 5.4.1 (2)) after the expiration of the Subscriber Certificate;

3) Any security event records (as set forth in Section 5.4.1 (3)) after the event occurred.)

5.5.3 Protection of Archive

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

5.5.4 Archive Backup Procedure

Records archives are backed up on 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) Thailand NRCA backups event records specified in Section 5.5.1 on 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 the time and date information.

5.5.6 Archive Collection System (Internal or External)

The Archive Collection System is internal to Thailand NRCA only.

5.5.7 Procedures to Obtain and Verify Archive Information

Procedures to obtain and verify archive information are as follows:

1) Thailand NRCA, or via its RA, submits an access request to archived information to the PA, specifying the reasons and necessity of obtaining such information as well as identifying the type of information needed.
2) The PA justifies the appropriateness and necessity of the request and notifies the decision result to the requester.
3) An authorized Thailand NRCA officer obtains the archived information, defines access rights, and forwards it to the requester.
4) The requester verifies the integrity of the information.

5.6 Key Changeover

To minimize the risk from compromise of a Thailand NRCA'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.

Thailand NRCA's signing keys SHALL have a validity period as described in Section 6.3.2.

When Thailand NRCA updates its private signature key and thus generates a new public key, Thailand NRCA SHALL notify all CAs, RAs, and Subscribers that rely on the Thailand NRCA's certificate that it has been changed.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

If compromise of Thailand NRCA is suspected, an independent third-party investigation SHALL be performed in order to determine the nature and the degree of damage. Certificates issuance SHALL be stopped immediately upon detection of a compromise. If a Thailand NRCA 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 Thailand NRCA needs to be rebuilt, only some certificates need to be revoked, and/or the Thailand NRCA private key needs to be declared compromised.

In case that there is an event that affects the security of Thailand NRCA system, the corresponding Thailand NRCA officers SHALL notify the PA if any of the following occur:

1) Suspected or detected compromise of any Thailand NRCA system or subsystem.
2) Physical intrusion or electronic penetration of any Thailand NRCA system or subsystem.
3) Successful denial of service attacks or disruption on any Thailand NRCA system or subsystem.
4) Any incident preventing Thailand NRCA from issuing and publishing a CRL or online status checking prior to the time indicated in the *nextUpdate* field in the currently published CRL, or the certificate for online status checking suspected or detected compromise.

Changes that are motivated by a security concern such as certificate misissuance or a root or intermediate certificate compromise can be reported via email at nrca@etda.or.th or via ETDA Incident Response system. These are treated as security-sensitive, and a security bug filed in Bugzilla.

5.7.2 Recovery Procedures if Computing Resources, Software, and/or Data Are Corrupted

In case of software, hardware or data failure, Thailand NRCA 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 activated and followed to restore Thailand NRCA services.

5.7.3 Recovery Procedures after Key Compromise

In the case of a Thailand NRCA compromise, Thailand NRCA SHALL notify the 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 the 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 Subordinate CA key compromise, the Subordinate CA SHALL notify the PA and Thailand NRCA. Thailand NRCA SHALL revoke that Subordinate 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 Subordinate CA SHALL also investigate and report to the 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 Subordinate CA

can be securely re-established, then the Subordinate CA SHALL be re-established. Upon re-establishment of the Subordinate CA, new Subscriber certificates SHALL be requested and issued again.

When a certificate of the Subordinate CA 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 Subordinate CA, but in no case longer than 6 hours after notification.

In case of an RA compromise, Thailand NRCA will disable the RA. In the case that the RA's key is compromised, Thailand NRCA will revoke it, and the revocation information SHALL be published within 24 hours in the most expedient, authenticated, and trusted manner. The compromise will be investigated by Thailand NRCA 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

Thailand NRCA has prepared a disaster recovery plan which has 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 Thailand NRCA with the approval of the PA, Thailand NRCA will notify the subordinate CAs, the Subscribers and all Relying Parties. The action plan is as follows:

1) Notify the status of the service to all affected users.
2) Revoke all certificates.
3) Long-term store information of Thailand NRCA and its subordinate CA and Subscribers according to the period herein specified.
4) Provide ongoing support and answer questions.
5) Properly handle Thailand NRCA or its subordinate CA 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 Thailand NRCA 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 Thailand NRCA key pair generation, as specified in Section 6.2.2.

Thailand NRCA 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.

Subordinate CA key pair generation SHALL be performed by the Subordinate CA. The Subordinate CA is required to generate the signature key pairs for the purpose of digital signature by FIPS 140 FIPS 140-2 Level 3 validated hardware cryptographic modules to support source authentication. The CA SHALL NOT generate keys for SSL certificates.

6.1.1.1 CA Key Pair Generation

Thailand NRCA follows the CP.

6.1.1.2 RA Key Pair Generation

Thailand NRCA follows the CP.

6.1.1.3 Subscriber Key Pair Generation

Thailand NRCA does not issue Subscriber Certificates.

6.1.2 Private Key Delivery to Subscriber

Subordinate CAs MUST generate the key pair by themselves. Thailand NRCA has no policy or practice to generate a key pair for Subordinate CAs.

6.1.3 Public Key Delivery to Certificate Issuer

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

6.1.4 CA Public Key Delivery to Relying Parties

Relying Parties can access Thailand NRCA public key in the certificate by the published channel.

6.1.5 Key Sizes

Currently, Thailand NRCA has one root certificate, and this root certificate contains a public key of RSA 4,096 bits key length and is signed with the corresponding private key by using a SHA-512 signature algorithm. Key sizes SHALL be assessed by the PA at least once a year or as necessary especially in an incident that is believed to significantly impact trustworthiness of Thailand NRCA.

Subordinate CAs of Thailand NRCA will also use the same signature algorithm of Thailand NRCA and a key size no larger than that of Thailand NRCA.

6.1.6 Public Key Parameters Generation and Quality Checking

Cryptographic keying material used by Thailand NRCA 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 Thailand NRCA key pair generation, as specified in Section 6.2.2.

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 include a critical key usage extension.

Thailand NRCA allows using its key pair for digital signature verification, signing certificate to other certification providers (Certificate Signing) and certificate revocation (CRL Signing).

The Public key that is bound into issued certificates is used only for signing certificates and status information such as CRLs, as well as certificates for infrastructure purposes (administrative role certificates, internal CA, and operational device certificates). Only Thailand NRCA SHALL issue certificates to Subordinate 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.

The Subordinate CAs of Thailand NRCA SHALL use a FIPS 140-2 Level 3 or higher validated hardware cryptographic module for signing operations.

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

Accessing the private key of Thailand NRCA MUST be performed by at least two persons with Trusted Roles.

6.2.3 Private Key Escrow

Thailand NRCA does not have a policy or a practice to keep the private key with other parties or to keep its Subscribers' private key.

6.2.4 Private Key Backup

Thailand NRCA's private signature key is backed up under the same multiparty control as the original signature key. More than one copy of the private signature key is stored off-site. All copies of the CA private signature key are accounted for and protected in the same manner as the original. Thailand NRCA backs up its private signature key in a FIPS 140-2 Level 3 validated hardware cryptographic module.

6.2.5 Private Key Archival

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

6.2.6 Private Key Transfer into or from a Cryptographic Module

The backup of the Thailand NRCA private key MUST be performed through the Cryptographic Module with FIPS 140-2 Level 3 standards. The importing and exporting process of the private key requires at least two persons with Trusted Roles.

6.2.7 Private Key Storage on Cryptographic Module

The Thailand NRCA private key stored in a Cryptographic Module and the backup of the private key in another Cryptographic Module.

6.2.8 Activating Private Key

Activation of Thailand NRCA's private key operations MUST be performed by an authorized person and requires a two-factor authentication process.

6.2.9 Deactivating Private Key

After working with the private key of Thailand NRCA, all Certification Authority officers MUST leave the system (Log Out) to prevent unauthorized access.

6.2.10 Destroying Private Key

Thailand NRCA will delete the private keys from the Cryptographic Module and its backup by overwriting the private key or initialize the module with a zeroization function. The event of destroying Thailand NRCA MUST be recorded into evidence under Section 5.4.

6.2.11 Cryptographic Module Capabilities

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

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The 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. The 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 the expiry date of the certificate. For the private key, it can be used to decrypt even if the certificate is expired.

The validity period of Thailand NRCA root certificate is specified in Table 9 below Certificate operational periods and key pair usage periods SHALL be assessed by the PA at least once a year or as necessary especially in an incident that is believed to significantly impact trustworthiness of Thailand NRCA.

The validity period of Thailand NRCA root certificate and certificate issued under this CP SHALL NOT exceed the maximum validity periods as below.

Type	Maximum Validity Periods
Thailand NRCA Certificate G1	23 years.
Thailand NRCA Certificate G2/G3	20 years.
Subordinate CA Certificate under G1	20 years.
Subordinate CA Certificate under G2/G3	17 years.
Personal Certificate	39 months
Organization or Legal entity Certificate	39 months
AATL End Entity Certificates	39 months
SSL/TLS Certificates	825 days (Certificates issued after 1 March 2018 but prior to 1 September 2020)
SSL/TLS Certificates	398 days (Certificates issued on or after 1 September 2020)
S/MIME Certificates: Strict/Multipurpose	825 days
S/MIME Certificates: Legacy	1185 days

Table 9: Maximum Certificate Validity Periods

However, the certificate validity periods SHALL be assessed by the PA at least once a year or as necessary especially in an incident that is believed to significantly impact trustworthiness of the CA.

6.4   Activation Data

6.4.1 Activation Data Generation and Installation

Thailand NRCA 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 is holding that activation data. Subordinate CAs use the same data generation mechanism.

6.4.2 Activation Data Protection

Data used to unlock private keys is protected from disclosure by storing in a safe and access is allowed only to an authorized person.

6.4.3 Other Aspects of Activation Data

Thailand NRCA activation data are only held by Thailand NRCA personnel in trusted roles as specified in Section 5.2.1.

6.5   Computer Security Controls

Thailand NRCA has implemented multi-person access control 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 Thailand NRCA 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

Thailand NRCA limits the number of applications installed on each computer to minimize security risks. Those applications are hardened based on the instructions provided by the 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

Thailand NRCA applies ISO/IEC 27001 (Information Security Management System) and WebTrust Principles and Criteria for Certification Authorities Version 2.2.2.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

For both readymade software and in-house developed software by Thailand NRCA that are used in certificate management, they SHALL be checked to ensure the software is genuine and fully tested in a non-production environment before deployment in a production environment. Any change to Thailand NRCA systems or components MUST go through the Change Management Control review and approval process.

6.6.2 Security Management Controls

Thailand NRCA has procedures to monitor and control variables of the certificate system. Changes of variables are processed through security management controls.

6.6.3 Life Cycle Security Controls

Thailand NRCA assesses security vulnerabilities at least on a quarterly basis and performs security Penetration Tests at least on an annual basis.

6.7 Network Security Controls

The Thailand NRCA network equips firewalls with features to investigate data transmission at application level and detect intruders or network activities that violate policy to ensure that the system is secure.

Normal users are allowed to access the certificate services through the network via the website, OCSP and directories only. For system management, Certification Authority officers will use a dedicated network to access and for management purposes. Information contained in this particular network is encrypted.

6.8　Time-stamping

The system clock will be set in the time setting device (NTP Server) or a trusted time source 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

The certificate issued by the CA under this CP MUST comply with 'RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile', and certificates used for electronic transactions in Thailand MUST comply with ETDA Recommendation on ICT Standard for Electronic Transactions (15-: Subscriber Certificate Profile). There are Public-key and attribute certificate frameworks in which the certificate contains the information shown in Table 10. In addition, CAs that need to issue Subscriber Certificates with Certificate Profiles apart from specified in this section need to be approved by Thailand NRCA.

Field	Value or Value Constraint
Version	Version of certificate, the details are described in Section 7.1.1
Serial Number	Reference number of each Certification Authority is unique
Signature	The method of digitally sign consists of Asymmetric cryptographic algorithms (Public Key Algorithm) and data digestion (Hash Function) which Certification Authority is used to sign the certificate in form of Object Identifier (OID).
Issuer	The name of the Certification 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 Certification Authority as the owner of public key in the certificate
SubjectPublicKeyInfo	Specify the type of public key and subject value of public key

Table 10: Fields in the Certificate

The CA maintains controls to provide reasonable assurance that Root and Subordinate certificates are generated by the CA contain certificate serial numbers greater than zero (0) containing at least 64 bits of output from a CSPRNG, for all certificates created from 30 September 2016 onwards. For certificates created before 30 September 2016, 32 bits is supported.

Thailand NRCA meets the technical requirements set forth in Section 2.2 - Publication of Information, Section 6.1.5 - Key Sizes, and Section 6.1.6 - Public Key Parameters Generation and Quality Checking.

Prior to 15 September 2023, Thailand NRCA issues certificates in accordance with the profile specified in version 4.3 of the NRCA Certification Practice Statement. Effective 15 September 2023, Thailand NRCA issues certificates in accordance with the profile specified in these Requirements.

7.1.1 Version Number

The certificate issued by Thailand NRCA 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 Content and Extensions; Application of RFC 5280

This section specifies the additional requirements for Certificate content and extensions in compliance with RFC 5280 including the latest version of CA/B Forum TLS Baseline Requirements Section 7.1.2 and ETDA Recommendation on ICT Standard for Electronic Transactions (15-: Subscriber Certificate Profile).

7.1.2.1 Root CA Certificate Profile

Thailand NRCA follows Section 7.1.2.1 of CA/B Forum TLS Baseline Requirements.

7.1.2.2 Cross-Certified Subordinate CA Certificate Profile

Thailand NRCA does not issue cross-certificates.

7.1.2.3 Technically Constrained Non-TLS Subordinate CA Certificate Profile

Thailand NRCA does not have technically constrained Subordinate CAs.

7.1.2.4 Technically Constrained Precertificate Signing CA Certificate Profile

Thailand NRCA does not have technically constrained Subordinate CAs.

7.1.2.5 Technically Constrained TLS Subordinate CA Certificate Profile

Thailand NRCA does not have technically constrained Subordinate CAs.

7.1.2.6 Subordinate CA Certificate Profile

Thailand NRCA follows Section 7.1.2.6 of CA/B Forum TLS Baseline Requirements.

7.1.2.7 Subscriber Certificate Profile

Thailand NRCA does not issue Subscriber certificates.

7.1.2.8 OCSP Responder Certificate Profile

Thailand NRCA follows Section 7.1.2.8 of CA/B Forum TLS Baseline Requirements.

7.1.2.9 Precertificate Profile

Thailand NRCA follows Section 7.1.2.9 of CA/B Forum TLS Baseline Requirements.

7.1.2.10 Common CA Fields

Thailand NRCA follows Section 7.1.2.10 of CA/B Forum TLS Baseline Requirements.

7.1.2.11 Common Certificate Fields

Thailand NRCA follows Section 7.1.2.11 of CA/B Forum TLS Baseline Requirements.

7.1.3 Algorithm object identifiers

The OID of digital signature and encryption of certificate is in Section 1.2.

Algorithm	Object Identifier
RSAEncryption	1.2.840.113549.1.1.1
SHA256WithRSAEncryption	1.2.840.113549.1.1.11
SHA384WithRSAEncryption	1.2.840.113549.1.1.12
SHA512withRSAEncryption	1.2.840.113549.1.1.13
ECDSAWithSHA256	1.2.840.10045.4.3.2
ECDSAWithSHA384	1.2.840.10045.4.3.3
ECDSAWithSHA512	1.2.840.10045.4.3.4

Table 11: Method of digital signature and encryption with Object Identifier

7.1.4 Name Forms

Thailand NRCA follows Section 7.1.4 of CA/B Forum TLS Baseline Requirements. The name formats of Issuer and Subject are specified in the certificate as referenced in Section 3.1.1.

7.1.5 Name Constraints

See Section 7.1.2.

7.1.6 Certificate Policy Object Identifier

Thailand NRCA follows Section 7.1.6 of CA/B Forum TLS Baseline Requirements and the issuing CAs MUST define the Certificate Policy OID provided by Thailand NRCA's OID Structure.

7.1.7 Usage of Policy Constraints Extension

Thailand NRCA does not issue Subscriber Certificates.

7.1.8 Policy Qualifiers Syntax and Semantics

CAs 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

Thailand NRCA does not issue Subscriber Certificates.

7.2   CRL Profile

Prior to 15 September 2023, Thailand NRCA issues certificates in accordance with the profile specified in version 4.3 of the NRCA Certification Practice Statement. Effective 15 September 2023, Thailand NRCA issues certificates in accordance with the profile specified in these Requirements.

Thailand NRCA's certificate revocation list complies with ITU-T Recommendation X.509 standard and RFC 5280 has the following details as in Table 12. In additional CRL Profile SHALL be in accordance with ETDA Recommendation on ICT Standard for Electronic Transactions (15-: Subscriber Certificate Profile)

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 digest (by Hash Function) which Certification Authority uses to sign the certificate in form of Object Identifier (OID).
issuer	The name of the Certification 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	The 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.
extensions	See Section 7.2.2

Table 12: Item list in Certificate Revocation

7.2.1 Version Number(s)

The version number of certificate revocation list in accordance with the RFC 5280 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 the Certification Authority complies with the ISO / IEC 9594-8:2012 standard and contains at least the following:

Extension	Value
CRL Number	Never repeated monotonically increasing integer
Authority Key Identifier	Subject Key Identifier of the CRL issuer certificate
Invalidity Date	Optional date in UTC format
Reason Code	Specify reason for revocation if included.
Issuing Distribution Point	Configured per RFC 5280 requirements, if included.

Table 13: CRL and CRL Entry Extensions

7.2.2.1 CRL Issuing Distribution Point

Thailand NRCA only issues full and complete CRLs.

7.3 OCSP Profile

The Online Certificate Status Protocol [OCSP] is the way for Subscribers to obtain information about the revocation status of a Thailand NRCA issued Certificated. Thailand NRCA uses OCSP to provide information about all its Certificates. The OCSP responses conform to RFC 6960.

If an OCSP response is for a Root CA or Subordinate CA Certificate, and that certificate has been revoked, then the revocationReason field within the RevokedInfo of the CertStatus MUST be present.

The CRLReason indicated MUST contain a value permitted for CRLs.

7.3.1 Version Number(s)

CAs SHALL issue Version 1 OCSP responses.

7.3.2 OCSP Extensions

The singleExtensions of an OCSP response does not contain the reasonCode (OID 2.5.29.21) CRL entry extension.

8 Compliance Audit and Other Assessments

Thailand NRCA has a compliance audit mechanism in place to ensure that the requirements of its CPS are being implemented and audited for complying with the following standards:

1) WebTrust Principles and Criteria for Certification Authorities.
2) WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security.
3) CA/Browser Forum Network and Certificate System Security Requirements.
4) CA/Browser Forum Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates (for SSL/TLS).
5) CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates.
6) Adobe Approved Trust List – Technical Requirements.
7) Electronic Transactions Act, B.E. 2544 (2001) and related version.

8.1 Frequency or Circumstances of Assessment

Thailand NRCA follows the CP.

8.2 Identity/Qualifications of Assessor

A compliance audit MUST be performed by a qualified auditor. A qualified auditor means a natural person, legal entity, or group of natural persons or legal entities that collectively possess the following qualifications and skills:

1) Independence from the subject of the audit;
2) The ability to conduct an audit that addresses the criteria specified in an eligible audit scheme (see Section 8)
3) Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;
4) Licensed by WebTrust;
5) Bound by law, government regulation, or professional code of ethics; and
6) Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage

8.3 Assessor's Relationship to Assessed Entity

Auditors are independent from the Thailand NRCA, or it SHALL be sufficiently organizationally separated from Thailand NRCA 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 Thailand

NRCA's 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 CAs.

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 audit meets the requirements of the audit schemes highlighted in Section 8 under which the assessment is being made. These requirements may vary as audit schemes are updated. An audit scheme is applicable to CAs in the year following the adoption of the updated scheme.

8.5   Actions Taken as a Result of Deficiency

Thailand NRCA'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 the 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

Thailand NRCA does not require fees from its Subordinate CAs.

9.1.1   Certificate Issuance or Renewal Fees

Thailand NRCA does not require fees from its Subordinate CAs.

9.1.2   Certificate Access Fees

Thailand NRCA does not require fees from its Subordinate CAs.

9.1.3   Revocation or Status Information Access Fees

Thailand NRCA does not require fees from its Subordinate CAs.

9.1.4   Fees for Other Services

Thailand NRCA does not require fees from its Subordinate CAs.

9.1.5   Refund Policy

Thailand NRCA does not require fees from its Subordinate CAs.

9.2   Financial Responsibility

9.2.1   Insurance Coverage

Thailand NRCA is responsible for damage only if the damage is caused by intentional acts or gross negligence. Entities, acting as Relying Parties, SHALL determine what financial limits, if any, they wish to impose on certificates used to consummate a transaction.

Thailand NRCA maintain and disclose Workers' Compensation, Commercial General Liability insurance and Technology Errors and Omission insurance policies and Liability for Wrongful Act of Officials Act B.E. 2539.

9.2.2   Other Assets

There are no other assets.

9.2.3   Insurance or Warranty Coverage for End-entities

Thailand NRCA does not issue Subscriber Certificates.

9.3   Confidentiality of Business Information

9.3.1 Scope of Confidential Information

Thailand NRCA keeps the following information in the scope of confidential information:

1) The Private key of Thailand NRCA and required information to access the private key including a password to access Thailand NRCA's hardware and software
2) The Registration of applications of Subordinate CAs for both approved and rejected applications
3) Audit Trail records
4) The Contingency Plan or Disaster Recovery Plan
5) Security controls of Thailand NRCA's hardware and software
6) Sensitive information with a potential to have impact on security and reliability of Thailand NRCA's system

9.3.2 Information Not within the Scope of Confidential Information

The following information is not within the scope of confidential information:

1) The Certificate Practice Policy of the Certification Authority
2) Certificate uses policy
3) Information inside a certificate
4) Certificate revocation
5) Information without impact on security and reliability of Thailand NRCA's system such as articles and news

9.3.3 Responsibility to Protect Confidential Information

Thailand NRCA has security measures in place to protect confidential information.

9.4   Privacy of Personal Information

9.4.1 Privacy Plan

Thailand NRCA develops, implements, and maintains a privacy policy and procedures documenting 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 is not included 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 is included in the certificate or directory.

9.4.4 Responsibility to Protect Private Information

Thailand NRCA has implemented security measures to protect private information.

9.4.5 Notice and Consent to Use Private Information

Thailand NRCA will use private information only if Subscribers are notified and consent to use private information has been given, in compliance with the privacy policy.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

In the event of a court order or administrative order, Thailand NRCA is entitled to disclose personal information required by law or officers under the law.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

Thailand NRCA is the only owner of intellectual property rights associated with the certificate, certificate revocation information, the Certificate Policy, and this Certification Practice Statement.

Thailand NRCA will not knowingly violate the intellectual property rights such as copyright, patent, trademarks, or trade secrets of third parties. Moreover, the CA SHALL comply with legal restrictions on the use of material in respect of intellectual property rights, and on the use of proprietary software products.

This CPS is made publicly available on a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International license (https://creativecommons.org/licenses/by-nc-sa/4.0/legalcode).

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

Thailand NRCA assures that:

1) Procedures are implemented in accordance with the CP of Thailand NRCA.
2) Any certificates issued that assert the policy OIDs identified in this CPS were issued in accordance with the stipulations of this CPS.

3) The Certification Practice Statement (CPS) will be provided, as well as any subsequent changes, for conformance assessment.
4) The CA operation is maintained in conformance to the stipulations of the CPS.
5) The registration information is accepted only from approved RAs operating under an approved CPS.
6) All information regarding certificate issuance and certificate revocation are processed through the procedures specified in the CPS of Thailand NRCA.

9.6.2 RA Representations and Warranties

An RA SHALL assure that:

1) Its RA registration operation is performed in conformance to the stipulations of the approved CPS of Thailand NRCA and related regulations.
2) All information contained in the certificate issued by Thailand NRCA is valid and appropriate. The evidence that due diligence was exercised in validating the information contained in the certificates is maintained.
3) 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 certificate, the Subordinate CA assures that:

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

9.6.4 Relying Party Representations and Warranties

In case Relying Party representations use a 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

No implied or express warranties are given by Thailand NRCA to other participants other than in Subordinate CA agreements, Relying Party agreements and any other agreements signed by Thailand NRCA with Third Parties.

9.7   Disclaimers of Warranties

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

9.8   Limitations of Liability

Thailand NRCA 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 Thailand NRCA. The response to the damage is the amount of actual damages and not more than 2 million baht per time (there may be many transactions in one time).

9.9   Indemnities

In case damage occurs to Thailand NRCA from the actions of Subscribers or Relying Parties, Thailand NRCA reserves the right to claim damages.

9.10   Term and Termination

9.10.1 Term

This CPS of Thailand NRCA takes effect from the date of publication upon the approval of the PA.

9.10.2 Termination

This CPS of Thailand NRCA takes effect until it is terminated.

9.10.3 Effect of Termination and Survival

This CPS remains in effect through the end of the archive period for the last certificate issued.

9.11   Individual Notices and Communications with Participants

Thailand NRCA will communicate to those participants using the 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 CPS is subject to Thailand NRCA and needs to be approved by the PA before announcement. However, all amendments are performed pursuant to laws, regulation or other related service announcements of Thailand NRCA.

9.12.2 Notification Mechanism and Period

Thailand NRCA reserves the right to revise this document. In case there are any significant changes, Thailand NRCA will announce on the website before the date of enforcement.

9.12.3 Circumstances Under Which OID Must Be Changed

In case the PA has the view that it is necessary to change the involved OID numbers, Thailand NRCA will change the OID and enforce the new policy using the new OID.

9.13 Dispute Resolution Provisions

9.13.1 Disputes between Issuer and Subscriber

The decisions of Thailand NRCA pertaining to matters within the scope of this CPS are final. Any claims should be submitted to Thailand NRCA at the following address:

> Thailand National Root Certification Authority
> Electronic Transactions Development Agency
> The Government Complex Commemorating His Majesty the King's 80th Birthday (Building B)
> 120 Moo 3, 6th floor, Chaengwattana Road, Thung Song Hong Subdistrict, Lak Si District,
> Bangkok 10210

In the event of unresolved disputes, the Policy Authority has jurisdiction over the dispute.

9.13.2 Disputes between Issuer and Relying Parties

The same procedure as stated in Section 9.13.1. In the event of undefined situations, the PA has jurisdiction over the dispute.

9.14 Governing Law

The laws of the Kingdom of Thailand SHALL govern this CPS.

9.15 Compliance with Applicable Law

Thailand NRCA is required to comply with the laws of the Kingdom of Thailand.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

This CPS SHALL be considered as part of the agreement between Thailand NRCA and its Subordinate CAs.

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 CPS is incorrect or invalid, the other sections of this CPS SHALL remain in effect until the CPS is updated.

9.16.4 Enforcement

Should it be determined that any section of this CPS 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 that Thailand NRCA and subordinate CAs have exercised a reasonable degree of skill and care to avoid and/or mitigate the effects of matters beyond its control, neither Thailand NRCA, the subordinate CA nor any RA 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

There are no other provisions.