Thailand National Root Certification Authority Certificate Policy

Version 4.2

Certificate Policy Identifier (OID): 2.16.764.1.1.1

Publication

Document Revision History

Date	Version	Description
July 2013	1.0	Initial Released
June 2014	2.0	• Translated into English for Web Trust assessment • Reviewed contents to align with RFC3647 • Reviewed consistency of terms in the document • Described the general guideline of log review frequency in topic 5.4.2 • Added topic 6.5.1 Computer Security Technical Requirements • Added topic 6.5.2 Computer Security Rating
May 2015	2.1	• Revised 6.1.5 Key sizes • Revised 7.4 OCSP (Online Certificate Status Protocol) • Revised 9.10.1 • Revised 1.5.2 Contact Person
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 4.9.3 Procedure for Revocation Request • Revised 4.9.1 Circumstances for Revocation • Revised 5.4.8 Vulnerability Assessments • 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 • Revised 9.1 Fees • Revised 9.2 Financial Responsibility • Revised 9.3 Confidentiality of Business Information
August 2018	4.0	• 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 • 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	• Revised 4.2.1 Performing Identification and Authentication Functions • Revised 1.2 Document Name and Identification. • Revised 1.5.1 Organization Administering the Document. • Revised 1.5.2 Contact Person. • Revised 1.6.2 Acronyms.

Oct 2021	4.2	• Revised 1.3.1 Thailand National Root Certification Authority (Thailand NRCA) • Added 1.3.2 Subordinate Certification Authority (Subordinate CA) • Revised 1.3.3 Registration Authority • Revised 1.3.3 Subscribers • Revised 1.5.5 CP Review and Update Procedures • Revised 1.6.1 Definitions • Revised 1.6.2 Acronyms • Revised 3.2.2 Authentication of Organization and Domain Identity. • Revised 3.2.2.4. Validation of Domain Authorization or Control. (Including all sub-Section). • Revised 3.2.2.5. Authentication for an IP Address • Revised 3.2.2.6. Wildcard Domain Validation • Revised 3.2.2.7. Data Source Accuracy • Revised 4.9.9 On-line Revocation/Status Checking Availability • Revised 4.9.10 On-line Revocation Checking Requirements • Revised 4.9.11 Other Forms of Revocation Advertisements Available • Revised 4.9.13 Circumstances for Suspension. • Revised 5.4.3 Retention Period for Audit Log • Revised 6.1.1 Key Pair Generation • Revised 6.2.1 Cryptographic Module Standards and Controls • Revised 6.3.2 Certificate Operational Periods and Key Pair Usage Periods • Revised 7.1 Certificate Profile • Revised 7.1.3 Algorithm Object Identifiers • Revised 7.1.4 Name Forms • Revised 7.3.2 OCSP Extensions • Revised 8. Compliance Audit and Other Assessments • Revised 8.2 Identity/Qualifications of Assessor • Revised 9.2.1 Insurance Coverage • Revised 9.5 Intellectual Property Rights

Table of Contents

1. Introduction

1.1 Overview

The Electronic Transactions Act sets out the legal framework for the public key infrastructure (PKI) with the objectives of facilitating the use of electronic transactions in a secure manner for commercial and other purposes. 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 between each pair of certification authorities, which will be unmanageable in the long run. Therefore, the Electronic Transactions Commission (ETC) has agreed to form a trust relationship in the 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 both locally and internationally.

A 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 the Thailand NRCA. The CP sets forth requirements that subordinate certification authorities under Thailand NRCA must meet.

Mission of Thailand NRCA includes:

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

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

Thailand NRCA conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates 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.

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

1.2 Document Name and Identification

This Certificate Policy is published by the Electronic Transactions Development Agency (ETDA) and specifies the requirements that CAs under Thailand NRCA must employ in providing services.

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:

2.16.764.1.1.1	Common Certificate Policy

1.3 PKI Participants

1.3.1 Thailand National Root Certification Authority (Thailand NRCA)

Thailand NRCA is the highest-level certification authority, trust anchor, of the PKI domain in Thailand. Thailand NRCA is responsible for manage Subordinate CAs through the hierarchical model with the following responsibilities, for example:

- Issuance and publication of Subordinate CA certificates

- Revocation and publication of Certificate Revocation Lists (CRLs)
- Thailand NRCA's key and certificate life cycle management
- Performing domestic and cross-border interoperability

No.	Certification Authority	Type	Support
1	Thailand National Root Certification Authority - G1	Root CA	Subordinate CA Certificate

1.3.2 Subordinate Certification Authority (Subordinate CA)

No.	Certification Authority	Type	Support
1	INET CA - G1	Subordinate CA	Enterprise/Individual Certificate
2	Thai Digital ID CA G3	Subordinate CA	SSL/TLS Certificate Enterprise/Individual Certificate
3	Thai Digital ID CA G2	Subordinate CA	Enterprise/Individual Certificate

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

- Approving the issuance of certificates
- Publication of certificates
- Revocation of certificates
- Publication of certificate status information through Certificate Revocation Lists (CRLs) and/or Online Certificate Status Protocol (OCSP) responders
- Subordinate CA key and certificate life cycle management
- Establishment and maintenance of its Certificate Policy (CP) and Certification Practice Statement (CPS)
- 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 Subordinate CA to perform one or more following functions:

- identifying and authenticating each subscriber's identity and information that is to be entered into the subscriber's public key certificate
- approval or rejection of certificate applications, rekeying requests, and renewal requests
- Initiating certificate revocation and processing requests to revoke certificates

However, The RA may be operated by whether the Subordinate CA or a third parties acting on behalf of the Subordinate CA. These functions must be performed in accordance with the CPS of the Subordinate CA and WebTrust SM/TM Principles and Criteria for Registration Authorities and the CA/B Forum.

1.3.4 Subscribers

A Subscriber is a person, legal entity, or infrastructure components 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.

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 within Thailand NRCA.

1.3.6 Other Participants

1.3.6.1. Policy Authority

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

1. Establishing and maintaining Certificate Policy and Certification Practice Statement of Thailand NRCA;
2. Determining and approving Certificate Policy and Certification Practice Statement of the Subordinate CAs under Thailand NRCA to ensure compliance with this Certificate Policy;
3. Processing and determining applications for becoming a Subordinate CA under Thailand NRCA; and
4. 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 for issuing 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 permitted.
- Subordinate CAs under Thailand NRCA can be used to issue subscriber certificates and Certificate Revocation Lists (CRLs) for checking the status of subscriber certificates. In the case of issuing a Subordinate CA Certificate, only two levels of Subordinate CA certificates are permitted in the Thailand NRCA hierarchy. Cross-certification and recognition are prohibited for the Subordinate CAs.
- Subscriber certificates are permitted for authentication, digital signature and encryption, such as document signing, email signing and encryption, as asserted in subscriber certificates. In protection of data in transit, subscriber certificates are permitted to use for Transport Layer Security (TLS) and Secure Socket Layer (SSL) protocols. Domain Validation (DV), Individual Validation (IV) and Organization Validation (OV) certificates are permitted based on identification and authentication procedures of Subordinate CAs.

However, in considering the appropriation of certificate uses, subscribers must take the following factors into account, for instance, relevant risks, the sensitivity of the information protected, and the degree of assurance provided by Subordinate CAs before using their services.

1.4.2 Prohibited Certificate Uses

A certificate issued in accordance with this CP shall be used only for the purpose as specified in Section 1.4.1. In particular, it shall be used only to the extent of the Policy Authority's approval and the use consistent with applicable laws.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The organization who is responsible for all aspects of this CP is Thailand NRCA which is operated by Electronic Transactions Development Agency (ETDA). In this document, "Thailand NRCA" will refer to Electronic Transaction Development Agency (ETDA).

1.5.2 Contact Person

Thailand National Root Certification Authority
Electronic Transactions Development Agency.
The 9th Tower Grand Rama9 Building (Tower B) Floor 20 - 22
33/4 Rama 9 Road, Huai Khwang, Bangkok 10310
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 shall determine the suitability and conformity of the CPS of each CA based on the results and recommendations of an independent auditor. In the case of establishing its own CP by a Subordinate CA, the suitability and conformity of such CP must also be assessed and included in the results and recommendations.

1.5.4 CPS Approval Procedures

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

1. The applicant CA submits the CPS to the Thailand NRCA.
2. Thailand NRCA reviews and makes recommendations.
3. The CPS submit to the PA for approval.
4. The PA reviews the submitted CPS.
5. The applicant CA publishes the CPS upon approval by the PA.

1.5.5 CP Review and Update Procedures

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

1.6 Definitions and Acronyms

1.6.1 Definitions

See Table 1 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, RFC5280, Baseline Requirements of CA/Browser Forum and ETDA Recommendation.
CAA	From RFC 6844 (http:tools.ietf.org/html/rfc6844): "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 misissue."
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.

Term	Definition
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.
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 1: 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
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
RA	Registration Authority
ETDA	Electronic Transactions Development Agency
SSL	Secure Sockets Layer
TLS	Transport Layer Security
OCSP	Online Certificate Status Protocol

Table 2: Acronyms

2. Publication and Repository Responsibilities

2.1 Repositories

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

2.2 Publication of Information

CAs shall make information publicly available on its repositories such as root certificate, Subordinate CA certificates issued by or to the CA, CRLs, CP, and CPS. The repositories shall be available 24 hours per day and 7 days per week and implemented through trustworthy systems.

2.3 Time or Frequency of Publication

CAs shall publish their certificates and CRLs as soon as possible after issuance. For updating status of subscriber certificates, CRLs for subscriber certificates shall be updated at least every 24 hours and are valid for 7 days. CRLs for CA Certificates are issued at least once every 6 months and within 24 hours if a CA Certificate is revoked. CAs shall review CP and CPS at least annually and make appropriate changes. The latest versions of CP and/or CPS are published within 3 days after approval.

2.4 Access Controls on Repositories

CAs that issues certificates under this CP shall protect information unintended for public dissemination or modification. Certificates and CRLs in the repository shall be publicly available through the Internet. The CAs shall detail what information in the repository shall be exempted from automatic availability and to whom, and under which conditions the restricted information may be made available. The CAs shall maintain effective procedures and controls over the management of its repositories.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

CAs issuing certificates under this CP shall specify the naming convention that it has adopted, such as X.501 Distinguished Names (DN). Subject Alternative Name Forms including, for example, an electronic mail address or a personal identification number may be included to ensure that the certificate of a person can be unambiguously identified.

3.1.2 Need for Names to be Meaningful

Names contained in a certificate must be 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

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

3.1.4 Rules for Interpreting Various Name Forms

Rules in X.501 must be used for interpreting distinguished name forms. Interpreting name forms specified in a distinguished name must follow applicable standards. Rules for interpreting e-mail addresses are specified in RFC 2822. RFC 2253 and RFC 2616 are interpreted as Uniform Resource Identifiers.

3.1.5 Uniqueness of Names

Each certificate issued by each CA under this CP must be ensured that the subject name assigned to a subscriber must uniquely and unambiguously identify.

3.1.6 Recognition, Authentication, and Role of Trademarks

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

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

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

3.2.2 Authentication of Organization and Domain Identity

Requests for certificates shall include the CA name, address, and documentation of the existence of the CA. Thailand NRCA shall verify the information in addition to the authenticity of the requesting representative and the representative' s authorization to act in the name of the CA. However, the information must correspond with the Certificate of Corporate Registration issued by the Department of Business Development, Ministry of Commerce.

For subscriber organization certificates, the CA shall verify the existence of the organization by verifying the Certificate of Corporate Registration issued by the Department of Business Development, Ministry of Commerce. Copies of official documents require Certified True Copy from authorized representative. Public key certificates bind public keys to identities. However, the entity to be identified depends on the application for which the public keys are used. Identifying different types of entity requires different evidence and procedures. The CA that issues certificates under this CP shall state in its CPS the types of entity that the CA will support and details the required evidence and procedures.

3.2.2.1. 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

If the Subject Identity Information is to include a DBA or tradename, the CA SHALL verify the Applicant's right to use the DBA/tradename using at least one of the following:

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

3.2.2.3. Verification of Country

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

1. the IP Address range assignment by country for either (i) the web site's IP address, as indicated by the DNS record for the web site or (ii) the Applicant's IP address;

2. the ccTLD of the requested Domain Name;

3. information provided by the Domain Name Registrar; or

4. a method identified in Section 3.2.2.1. The CA SHOULD implement a process to screen proxy servers in order to prevent reliance upon IP addresses assigned in countries other than where the Applicant is actually located.

3.2.2.4. Validation of Domain Authorization or Control

CAs SHALL verifies and confirms with the Applicant's ownership or control of the domain prior to issuance. CAs validated each Fully-Qualified Domain Name (FQDN) listed in the Certificate using at least one of the methods listed follows:

1. When the FQDN does not contain "onion" as the rightmost label, the CA SHALL validate the FQDN using at least one of the methods listed below; and

2. When the FQDN contains "onion" as the rightmost label, the CA SHALL validate the FQDN in accordance with Appendix B of Baseline Requirements.

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: 1) 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.

2) Delegating this function to Enterprise RA third parties is not permitted.

3.2.2.4.1 Validating the Applicant as a Domain Contact

This method has been retired and MUST NOT be used. Prior validations using this method and validation data gathered according to this method SHALL NOT be used to issue certificates.

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

CAs shall confirm the Applicant's control over the FQDN by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to an email address, fax/SMS number, or postal mail address identified as a Domain

Contact. Each email, fax, SMS, or postal mail MAY confirm control of multiple Authorization Domain Names. The CA MAY send the email, fax, SMS, or postal mail identified under this section to more than one recipient provided that every recipient is identified by the Domain Name Registrar as representing the Domain Name Registrant for every FQDN being verified using the email, fax, SMS, or postal mail. The Random Value SHALL be unique in each email, fax, SMS, or postal mail. The CA MAY resend the email, fax, SMS, or postal mail in its entirety, including re-use of the Random Value, provided that the communication's entire contents and recipient(s) remain unchanged. The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values, in which case the CA MUST follow its CPS.

3.2.2.4.3 Phone Contact with Domain Contact

CAs shall Confirm the Applicant's control over the FQDN by calling the Domain Name Registrant's phone number and obtaining a response confirming the Applicant's request for validation of the FQDN. The CA MUST place the call to a phone number identified by the Domain Name Registrar as the Domain Contact.

Each phone call SHALL be made to a single number and MAY confirm control of multiple FQDNs, provided that the phone number is identified by the Domain Registrar as a valid contact method for every Base Domain Name being verified using the phone call.

CAs SHALL NOT perform validations using this method after May 31, 2019. Completed validations using this method SHALL continue to be valid for subsequent issuance per the applicable certificate data reuse periods.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.4 Constructed Email to Domain Contact

CAs shall confirm the Applicant's control over the FQDN by 1. Sending an email to one or more addresses created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at-sign ("@"), followed by an Authorization Domain Name; and 1. including a Random Value in the email; and 1. receiving a confirming response utilizing the Random Value. Each email MAY confirm control of multiple FQDNs, provided the Authorization Domain Name used in the email is an Authorization Domain Name for each FQDN being confirmed The Random Value SHALL be unique in each email. The email MAY be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient SHALL remain unchanged. The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values.

3.2.2.4.5 Domain Authorization Document

This method has been retired and MUST NOT be used. Prior validations using this method and validation data gathered according to this method SHALL NOT be used to issue certificates.

3.2.2.4.6 Agreed-Upon Change to Website v2

CAs shall confirm the Applicant's control over the FQDN by verifying that the Request Token or Random Value is contained in the contents of a file. 1. The entire Request Token or Random Value MUST NOT appear in the request used to retrieve the file, and 2. the CA MUST receive a successful HTTP response from the request (meaning a 2xx HTTP status code must be received). The file containing the Request Token or Random Number: 1. MUST be located on the Authorization Domain Name, and 2. MUST be located under the "/.well-known/pkivalidation" directory, and 3. MUST be retrieved via either the "http" or "https" scheme, and 4. MUST be accessed over an Authorized Port. pg. 39 If the CA follows redirects the following apply: 1. Redirects MUST be initiated at the HTTP protocol layer (e.g. using a 3xx status code). 2. Redirects MUST be the result of an HTTP status code result within the 3xx Redirection class of status codes, as defined in RFC 7231, Section 6.4. 3. Redirects MUST be to resource URLs with either via the "http" or "https" scheme. 4. Redirects MUST be to resource URLs accessed via Authorized Ports. If a Random Value is used, then: 1. The CA MUST provide a Random Value unique to the certificate request. 2. The Random Value MUST remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values, in which case the CA MUST follow its CPS

3.2.2.4.7 DNS Change

CAs shall confirm the Applicant's control over the FQDN by confirming the presence of a Random Value or Request Token for either in a DNS CNAME, TXT or CAA record for either 1) an Authorization Domain Name; or 2) an Authorization Domain Name that is prefixed with a label that begins with an underscore character. If a Random Value is used, the CA SHALL provide a Random Value unique to the Certificate request and SHALL not use the Random Value after (i) 30 days or (ii) if the Applicant submitted the Certificate request, the timeframe permitted for reuse of validated information relevant to the Certificate

3.2.2.4.8 IP Address

CAs shall confirm the Applicant's control over the FQDN by confirming that the Applicant controls an IP address returned from a DNS lookup for A or AAAA records for the FQDN in accordance with section 3.2.2.5.

3.2.2.4.9 Test Certificate

This method has been retired and MUST NOT be used. Prior validations using this method and validation data gathered according to this method SHALL NOT be used to issue certificates.

3.2.2.4.10 TLS Using a Random Number

CAs Shall confirm the Applicant's control over the FQDN by confirming the presence of a Random Value within a Certificate on the Authorization Domain Name which is accessible by the CA via TLS over an Authorized Port.

3.2.2.4.11 Any Other Method

This method has been retired and MUST NOT be used.

3.2.2.4.12 Validating Applicant as a Domain Contact

CAs Shall Confirming the Applicant's control over the FQDN by validating the Applicant is the Domain Contact. This method may only be used if the CA is also the Domain Name Registrar, or an Affiliate of the Registrar, of the Base Domain Name.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.13 Email to DNS CAA Contact

CAs shall confirm the Applicant's control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to a DNS CAA Email Contact. The relevant CAA Resource Record Set MUST be found using the search algorithm defined in RFC 6844 Section 4, as amended by Errata 5065 (Appendix A).

Each email MAY confirm control of multiple FQDNs, provided that each email address is a DNS CAA Email Contact for each Authorization Domain Name being validated. The same email MAY be sent to multiple recipients as long as all recipients are DNS CAA Email Contacts for each Authorization Domain Name being validated.

The Random Value SHALL be unique in each email. The email MAY be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient(s) SHALL remain unchanged. The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.14 Email to DNS TXT Contact

CAs shall confirm the Applicant's control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to a DNS TXT Record Email Contact for the Authorization Domain Name selected to validate the FQDN. Each email MAY confirm control of multiple FQDNs, provided that each email address is DNS TXT Record Email Contact for each Authorization Domain Name being validated. The same email MAY be sent to multiple recipients as long as all recipients are DNS TXT Record Email Contacts for each Authorization Domain Name being validated. The Random Value SHALL be unique in each email. The email MAY be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient(s) SHALL remain unchanged. The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values.

3.2.2.4.15 Phone Contact with Domain Contact

CAs shall confirm the Applicant's control over the FQDN by calling the Domain Contact's phone number and obtain a confirming response to validate the ADN. Each phone call MAY confirm control of multiple ADNs provided that the same Domain Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN.

In the event that someone other than a Domain Contact is reached, the CA MAY request to be transferred to the Domain Contact.

In the event of reaching voicemail, the CA may leave the Random Value and the ADN(s) being validated. The Random Value MUST be returned to the CA to approve the request.

The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact

CAs shall confirm the Applicant's control over the FQDN by calling the DNS TXT Record Phone Contact's phone number and obtain a confirming response to validate the ADN. Each phone call MAY confirm control of multiple ADNs provided that the same DNS TXT Record Phone Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN.

The CA MAY NOT knowingly be transferred or request to be transferred as this phone number has been specifically listed for the purposes of Domain Validation.

In the event of reaching voicemail, the CA may leave the Random Value and the ADN(s) being validated. The Random Value MUST be returned to the CA to approve the request.

The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.17 Phone Contact with DNS CAA Phone Contact

CAs shall confirm the Applicant's control over the FQDN by calling the DNS CAA Phone Contact's phone number and obtain a confirming response to validate the ADN. Each phone call MAY confirm control of multiple ADNs provided that the same DNS CAA Phone Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN. The relevant CAA Resource Record Set MUST be found using the search algorithm defined in RFC 6844 Section 4, as amended by Errata 5065 (Appendix A).

The CA MUST NOT be transferred or request to be transferred as this phone number has been specifically listed for the purposes of Domain Validation.

In the event of reaching voicemail, the CA may leave the Random Value and the ADN(s) being validated. The Random Value MUST be returned to the CA to approve the request.

The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.18 Agreed-Upon Change to Website v2

CAs shall Confirm the Applicant's control over the FQDN by verifying that the Request Token or Random Value is contained in the contents of a file. 1. The entire Request Token or Random Value MUST NOT appear in the request used to retrieve the file, and 2. the CA MUST receive a successful HTTP response from the request (meaning a 2xx HTTP status code must be received).

The file containing the Request Token or Random Number: 1. MUST be located on the Authorization Domain Name, and 2. MUST be located under the "/.well-known/pki-validation" directory, and 3. MUST be retrieved via either the "http" or "https" scheme, and 4. MUST be accessed over an Authorized Port.

If the CA follows redirects the following apply: 1. Redirects MUST be initiated at the HTTP protocol layer (e.g. using a 3xx status code). 2. Redirects MUST be the result of an HTTP status code result within the 3xx Redirection class of status codes, as defined in RFC 7231, Section 6.4. 3. Redirects MUST be to resource URLs with either via the “http” or “https” scheme. 4. Redirects MUST be to resource URLs accessed via Authorized Ports.

If a Random Value is used, then: 1. The CA MUST provide a Random Value unique to the certificate request. 2. The Random Value MUST remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values, in which case the CA MUST follow its CPS.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.19 Agreed-Upon Change to Website - ACME

CAs shall confirm Confirming the Applicant’s control over a FQDN by validating domain control of the FQDN using the ACME HTTP Challenge method defined in section 8.3 of RFC 8555. The following are additive requirements to RFC 8555.

The CA MUST receive a successful HTTP response from the request (meaning a 2xx HTTP status code must be received).

The token (as defined in RFC 8555, section 8.3) MUST NOT be used for more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values, in which case the CA MUST follow its CPS.

If the CA follows redirects: 1. Redirects MUST be initiated at the HTTP protocol layer (e.g. using a 3xx status code). 2. Redirects MUST be the result of an HTTP status code result within the 3xx Redirection class of status codes, as defined in RFC 7231, Section 6.4. 3. Redirects MUST be to resource URLs with either via the “http” or “https” scheme. 4. Redirects MUST be to resource URLs accessed via Authorized Ports.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.5. Authentication for an IP Address

CAs shall validating the Applicant’s ownership or control of an IP Address listed in a Certificate. The CA SHALL confirm that prior to issuance, the CA has validated each IP Address listed in the Certificate using at

least one of the methods specified in this section. 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 IP Address validation, the term Applicant includes the Applicant's Parent Company, Subsidiary Company, or Affiliate. After July 31, 2019, CAs SHALL maintain a record of which IP validation method, including the relevant BR version number, was used to validate every IP Address. For other method shall follows Section 3.2.2.5.1 to 3.2.2.5.7 of CA/B Forum Baseline Requirements version 1.7.3.

3.2.2.6. Wildcard Domain Validation

Before issuing a certificate with a wildcard character (*) in a CN or subjectAltName of type DNS-ID, the CA MUST establish and follow a documented procedure that determines if the wildcard character occurs in the first label position to the left of a "registry-controlled" label or "public suffix" (e.g. "*.com", "*.co.uk", see RFC 6454 Section 8.2 for further explanation). If a wildcard would fall within the label immediately to the left of a registry-controlled /1 or public suffix, CAs MUST refuse issuance unless the applicant proves its rightful control of the entire Domain Namespace. (e.g. CAs MUST NOT issue "*.co.uk" or "*.local", but MAY issue "*.example.com" to Example Co.). Determination of what is "registry-controlled" versus the registerable portion of a Country Code Top-Level Domain Namespace is not standardized at the time of writing and is not a property of the DNS itself. Current best practice is to consult a "public suffix list" such as the Public Suffix List (PSL), and to retrieve a fresh copy regularly. If using the PSL, a CA SHOULD consult the "ICANN DOMAINS" section only, not the "PRIVATE DOMAINS" section. The PSL is updated regularly to contain new gTLDs delegated by ICANN, which are listed in the "ICANN DOMAINS" section. A CA is not prohibited from issuing a Wildcard Certificate to the Registrant of an entire gTLD, provided that control of the entire namespace is demonstrated in an appropriate way

3.2.2.7. Data Source Accuracy

Prior to using any data source as a Reliable Data Source, the CA SHALL evaluate the source for its reliability, accuracy, and resistance to alteration or falsification. The CA SHOULD consider the following during its evaluation: pg. 43 1. The age of the information provided, 2. The frequency of updates to the information source, 3. The data provider and purpose of the data collection, 4. The public accessibility of the data availability, and 5. The relative difficulty in falsifying or altering the data. Databases maintained by the CA, its owner, or its affiliated companies do not qualify as a Reliable Data Source if the primary purpose of the database is to collect information for the purpose of fulfilling the validation requirements under this Section 3.2.

3.2.2.8. CAA Records

As part of the issuance process, the CA MUST check for CAA records and follow the processing instructions found, for each dNSName in the subjectAltName extension of the certificate to be issued, as

specified in RFC 6844. If the CA issues, they MUST do so within the TTL of the CAA record, or 8 hours, whichever is greater.

When processing CAA records, CAs MUST process the issue, issuewild, and iodef property tags as specified in RFC 6844. Additional property tags MAY be supported. CAs MUST respect the critical flag and not issue a certificate if they encounter an unrecognized property with this flag set.

RFC 6844 requires that CAs "MUST NOT issue a certificate unless either (1) the certificate request is consistent with the applicable CAA Resource Record set or (2) an exception specified in the relevant Certificate Policy or Certification Practices Statement applies." For issuances conforming to these Baseline Requirements, CAs MUST NOT rely on any exceptions specified in their CP or CPS unless they are one of the following:

- CAA checking is optional for certificates for which a Certificate Transparency pre-certificate was created and logged in at least two public logs, and for which CAA was checked.
- CAA checking is optional for certificates issued by a Technically Constrained Subordinate CA Certificate as set out in Baseline Requirements section 7.1.5, where the lack of CAA checking is an explicit contractual provision in the contract with the Applicant.
- CAA checking is optional if the CA or an Affiliate of the CA is the DNS Operator (as defined in RFC 7719) of the domain's DNS.

CAs are permitted to treat a record lookup failure as permission to issue if:

- the failure is outside the CA's infrastructure;
- the lookup has been retried at least once; and
- the domain's zone does not have a DNSSEC validation chain to the ICANN root.

CAs MUST document potential issuances that were prevented by a CAA record in sufficient detail to provide feedback to the CAB Forum on the circumstances and SHOULD dispatch reports of such issuance requests to the contact(s) stipulated in the CAA iodef record(s), if present. CAs are not expected to support URL schemes in the iodef record other than mailto: or https:.

3.2.3 Authentication of Individual Identity

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

3.2.4 Non-verified Subscriber Information

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

3.2.5 Validation of Authority

If the Applicant for a Certificate containing Subject Identity Information is an organization, the CAs SHALL use a Reliable Method of Communication to verify the authenticity of the Applicant Representative's certificate request. The CA MAY use the sources listed in section 3.2.2.1 to verify the Reliable Method of Communication. Provided that the CA uses a Reliable Method of Communication, the CA MAY establish the authenticity of the certificate request directly with the Applicant Representative or with an authoritative source within the Applicant's organization, such as the Applicant's main business offices, corporate offices, human resource offices, information technology offices, or other department that the CA deems appropriate. In addition, the CA SHALL establish a process that allows an Applicant to specify the individuals who may request Certificates. If an Applicant specifies, in writing, the individuals who may request a Certificate, then the CA SHALL NOT accept any certificate requests that are outside this specification. The CA SHALL provide an Applicant with a list of its authorized certificate requesters upon the Applicant's verified written request.

3.2.6 Criteria for Interoperation

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

3.2.7 Authentication of Email addresses

CAs shall confirm that the Applicant has owned/controlled of or right to use email addresses by sending a Random Value to the requested email address and then receiving a confirming response utilizing the Random Value. However, CAs shall demonstrate validation procedure in their CPS.

Noted: Delegating this function to Enterprise RA third parties is not permitted.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

Identification and authentication requirements are specified in Section 3.2.

3.3.2 Identification and Authentication for Re-key after Revocation

Re-keying after revocation requires CAs to follow the initial identity validation process specified in Section 3.2.

3.4 Identification and Authentication for Revocation Request

Identification and authentication requirements are specified in Section 3.2.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

An organization who wishes to operate a CA in Thailand may complete and submit an application for certificates to Thailand NRCA. Other certificate applications may be submitted to the Subordinate CA by the Subscribers listed in Section 1.3.3 and 1.3.4.

4.1.2 Enrollment Process and Responsibilities

CAs shall maintain systems and processes to obtain certificate applications in accordance with this CP and the relevant CPS prior to certificate issuance. All communications among CAs and RAs supporting the certificate application and issuance process shall be authenticated and protected from modification; any electronic transmission of shared secrets and personally identifiable information shall be protected. Communications may be electronic or out-of-band. Where electronic communications are used, cryptographic mechanisms commensurate with the strength of the public/private key pair shall be used. Out-of-band communications shall protect the confidentiality and integrity of the data. Subscribers are responsible for providing accurate information on their certificate applications.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Information in certificate applications must be verified as accurate before certificates are issued. Procedures to verify information in certificate applications shall be specified in the relevant CPS. If the certificate application does not contain all the necessary information about the subscriber, the remaining information shall be obtained from the subscriber or obtained from a reliable source. The identification

and authentication of the subscriber must meet the requirements in this CP. Fully Qualified Domain Name (FQDN) or IP address in TLS/SSL certificates must be also validated in accordance with this CP.

The CA shall develop, maintain, and implement documented procedures that properly identify and verify prior to the Certificate's approval. Further verification for high risk certificate applications is also required. If the CA delegate its obligations under this section to third parties, the delegated third parties shall provide at least the same level of assurance as the CA's own processes.

4.2.2 Approval or Rejection of Certificate Applications

Any certificate application that is received by a CA that issues certificates under this CP, for which the identity and authorization, if applicable, of the applicant has been validated, will be duly processed. The CA must reject any application for which such validation cannot be completed. However, rejection may be considered based on an internal database or other sources identifying revoked certificates and rejected certificate applications regarding suspected or fraudulent uses.

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

4.2.3 Time to Process Certificate Applications

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

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

Upon receiving a certificate application, a CA that issue certificate under this CP and its RA will:

- Perform identification and authentication functions following the requirements specified in Section 3.2;
- Ensure accuracy of the information in the certificate application as specified in Section 4.2.1;
- Ensure accuracy of the information in a Certificate Signing Request (CSR) that conforms with Section 6. If the CSR does not meet the requirements in Section 6, the CA must be reject the CSR;

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

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

Issuing a Subordinate CA certificate shall require trusted roles from Thailand NRCA to deliberately issue a direct command in order for Thailand NRCA to perform a certificate signing operation.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

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

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

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

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

4.4.2 Publication of the Certificate by the CA

All Subordinate certificates shall be published in suitable repositories. Subscriber certificates may be published as specified in the relevant CPS.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Thailand NRCA will notify the PA whenever a Subordinate certificate is issued. Notification of issuing a subscriber certificate may be sent to parties involving such subscriber certificate, for example, RAs, resellers, or partners.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Private key must be protected from unauthorized use and disclosure. A private key must be used corresponding to the purposes for which key usage and extended key usage fields were defined in the corresponding certificate. The certificate shall be lawfully used in accordance with this CP, the CPS and Terms of Service of the issuing CA.

4.5.2 Relying Party Public Key and Certificate Usage

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

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

4.6 Certificate Renewal

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

4.6.1 Circumstance for Certificate Renewal

Not Applicable.

4.6.2 Who May Request Renewal

Not Applicable.

4.6.3 Processing Certificate Renewal Requests

Not Applicable.

4.6.4 Notification of New Certificate Issuance to Subscriber

CAs that issues certificates under this CP shall publish the new certificate according to the procedure in Section 4.3.2.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

After subscribers receive a renewal certificate, the subscribers must follow the procedure in Section 4.4.1 to accept the renewal certificate.

4.6.6 Publication of the Renewal Certificate by the CA

CAs that issues certificates under this CP shall publish the renewal certificate according to the procedure in Section 4.4.2..

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

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

4.7 Certificate Re-key

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

4.7.1 Circumstance for Certificate Re-key

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

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

4.7.2 Who May Request Certification of a New Public Key

Only the subscriber may request a new certificate.

4.7.3 Processing Certificate Re-keying Requests

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

4.7.4 Notification of New Certificate Issuance to Subscriber

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

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

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

4.7.6 Publication of the Re-keyed Certificate by the CA

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

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

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

4.8 Certificate Modification

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

4.8.1 Circumstance for Certificate Modification

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

4.8.2 Who May Request Certificate Modification

Not Applicable.

4.8.3 Processing Certificate Modification Requests

Not Applicable.

4.8.4 Notification of New Certificate Issuance to Subscriber

Not Applicable.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not Applicable.

4.8.6 Publication of the Modified Certificate by the CA

Not Applicable.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not Applicable.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

4.9.1.1. Reasons for Revoking a Subscriber Certificate

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

1. The Subscriber requests in writing that the CA revoke the Certificate;
2. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization;
3. The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6 in Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates;
4. The CA obtains evidence that the Certificate was misused;
5. The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;

6. The CA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
7. The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
8. The CA is made aware of a material change in the information contained in the Certificate;
9. The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement;
10. The CA is made aware that the Certificate was not the CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
11. The CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
12. The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository;
13. The CA is made aware of a possible compromise of the Private Key of the Subordinate CA used for issuing the Certificate;
14. Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement; or
15. The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time).

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

The Issuing CA SHALL revoke a Subordinate CA Certificate within seven (7) days 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 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

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

4.9.3 Procedure for Revocation Request

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

1. The Subscriber submits the revocation request and related documents to the certificate issuing CA, or a RA of the CA, providing that the information is genuine, correct and complete.
2. The issuing CA or RA of the CA verifies and endorses the revocation requests and the 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. The issuing CA with the assistance of the RA will approve and process the revocation request.
5. The issuing CA, or via the RA of the CA, informs the revocation result to the subscriber. For revocation of certificate, the PA must be informed.

4.9.4 Revocation Request Grace Period

There is no grace period for revocation under this CP.

4.9.5 Time within Which CA Must Process the Revocation Request

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

4.9.6 Revocation Checking Requirement for Relying Parties

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

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

- Issuing a CRL whenever a certificate or a subscriber certificate is revoked.
- Thailand NRCA shall update and reissue CRLs every six months whether or not the CRL has any changes.
- Subordinate CA must issue a CRL for subscriber certificates at least once a day whether or not the CRL has any changes.

4.9.8 Maximum Latency for CRLs

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

4.9.9 On-line Revocation/Status Checking Availability

The CA MUST On-line Certificate status Protocol (OCSP) and conform to RFC6960 and/or RFC5019. OCSP responses MUST either:

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

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

In the latter case, the OCSP signing Certificate MUST contain an extension of type id-pkixocsp-nocheck, as defined by RFC6960.

Where on-line status checking is supported, status information shall be regularly updated and available to relying parties.

4.9.10 On-line Revocation Checking Requirements

Relying Parties may optionally check the status of certificates through the Thailand NRCA's Online Certificate Status Protocol (OCSP) service, if provided by Thailand NRCA, and/or check the status of subscriber certificates through the issuing CA's OCSP service, if provided by the Subordinate CA. Client software using on-line status checking need not obtain or process CRLs.

CAs SHALL provide OCSP responses to accordance with CA/Browser Forum Baseline Requirements as requirements below;

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

4.9.11 Other Forms of Revocation Advertisements Available

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

4.9.12 Special Requirements Regarding Key Compromise

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

4.9.13 Circumstances for Suspension

Certificate suspension is not permitted for SSL/TLS Certificate and only allowed for subscriber's certificate as Enterprise, Personnel, Personal or Individual. CA that issues certificates under this CP shall state in its CPS the circumstances for suspension.

4.9.14 Who Can Request Suspension

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

4.9.15 Procedure for Suspension Request

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

4.9.16 Limits on Suspension Period

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

4.10 Certificate Status Services

4.10.1 Operational Characteristics

Certificate status services shall be provided in the forms of CRL and OCSP. Revocation entries on both the CRL and the OCSP responder shall not be removed until after the expiry date of the revoked certificate.

4.10.2 Service Availability

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

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

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

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

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

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5. Facility, Management, and Operational Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

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

5.1.2 Physical Access

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

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

5.1.3 Power and Air Conditioning

CAs shall ensure that the power and air conditioning are maintained to sufficiently support the CA operations.

5.1.4 Water Exposures

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

5.1.5 Fire Prevention and Protection

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

5.1.6 Media Storage

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

5.1.7 Waste Disposal

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

5.1.8 Off-site Backup

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

5.2 Procedural Controls

5.2.1 Trusted Roles

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

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

Trusted roles include without limitation:

1. Certification Authority Officer (CAO) / CA Administrator

   The Certification Authority Officer Staff role is responsible for key life cycle management (e.g., key component custodian, key generation, activation, key backup and recovery), and issuance, revocation, and suspension. Moreover, CAO manage and control the hardware security modules (HSMs).

2. Registration Authority (RA) / RA officer
   Registration Authority is responsible for identifying and authenticating each identity or legal entity and information that is to be subject into the public key certificate. Additionally, To perform approval or rejection of certificate applications, rekeying requests, and renewal requests
   Initiating certificate revocation and processing requests to revoke certificates.
3. System Administrator (SA) / Network Administrator (NA)
   The System Administrator and Network Administrator (NA) role are responsible for installation, configuration and maintenance of the CA system and the audit log system such as servers, routers, firewalls, and networks. Updating software patches, performing backup and recovery, and maintaining system stability are also under responsibility of this role.
4. Security Officer (SO)
   Security Officer (SO) is responsible for reviews and suggestion any security requirement, security compliance, audit logs, Co-ordinate with another security team.
5. Internal Audit (IA)/ Security Auditor
   Internal Audit (IA) is responsible for reviewing and assessment overall operation to ensure that meet Security Standard and compliance related.
6. Executives who manage CA infrastructural trustworthiness / Certification Authority Manager (CAM)
   Certification Authority Manager (CAM) is responsible for planning and managing operation team to ensure that meet Security Standard and compliance related.

Multiple people may hold the same trusted role, with collective privileges sufficient to fill the role. Other trusted roles may be defined in other documents, which describe or impose requirements on the CA operation. The CA shall maintain lists, including names, organizations, contact information, and organizational affiliation for those who act in the trusted roles, and shall make them available during compliance audits.

5.2.2 Number of Persons Required per Task

CAs shall identify the number of persons required per tasks in their relevant CPS. 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. CA key generation, activation, backup and recovery shall require two or more persons.

5.2.3 Identification and Authentication for Each Role

CA personnel shall pass a background check before appointing a trusted role by an appropriate authority. CA personnel shall authenticate themselves to the CA system in a secure manner before access to

perform their trusted roles. The relevant CPS should describe the mechanisms for identification and authentication for each role.

5.2.4 Roles Requiring Separation of Duties

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

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

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

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

The following roles must be performed by trusted officers:

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

5.3 Personnel Controls

5.3.1 Qualifications, Experience and Clearance Requirements

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

5.3.2 Background Check Procedures

Prior to commencement of employment, a CA must conduct the following background checks:

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

- Confirmation letter of previous employment
- Background Check (Recheck at least every three years)

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

5.3.3 Training Requirements

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

- Basic cryptography and Public Key Infrastructure (PKI) concepts
- Authentication and validation policies and procedures, including CP and CPS of the CA.
- Information Security Awareness, including common threats relating to the validation process, for example, phishing and other social engineering attacks.
- Relevant standards and requirements for CA operations, for example, CA/B Forum Baseline Requirements
- Use and operation of deployed hardware and software related to CA operations
- Security Risk Management
- Disaster recovery and business continuity procedures

5.3.4 Retraining Frequency and Requirements

All personnel in trusted roles shall maintain skill levels consistent with CA's training and performance programs.

The CA must provide its personnel 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 related to CA operations.

5.3.5 Job Rotation Frequency and Sequence

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

5.3.6 Sanction for Unauthorized Actions

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

5.3.7 Independent Contractor Requirements

In the case of delegation of a trusted role, independent contractors shall be subjected to the same requirements as a CA personnel. The obligations of such contractors shall also be the same as that of the CA personnel.

To perform tasks without involvement of a trusted role, independent contractors are only permitted to access to the CA's secure facilities if they are escorted and directly supervised by a CA personnel at all times.

5.3.8 Documentation Supplied to Personnel

A CA that issues certificates under this CP must provide its personnel with the requisite documentation needed to perform their job responsibilities competently and satisfactorily. This CP and the relevant CPS should also be provided to them.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

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

- CA Key Life Cycle Management, including:
  - Key generation, backup, storage, recovery, archival, and destruction
  - Cryptographic Module life cycle management events
- CA and Subscriber certificate life cycle management events, including:
  - Certificate Applications, rekey, and revocation
  - Approval or rejection of requests
  - Generation and issuance of certificates and CRL
- Security-related events including:
  - Successful and unsuccessful access attempts to CA systems
  - Security system actions performed by CA officers
  - Security profile changes
  - System crashes, hardware failures and other anomalies

- Firewall and router activity
- CA facility visitor entry/exit

Log entries include the following elements:

- Date and time of entry;
- Identity of the person making the journal entry; and
- Description of the entry.

5.4.2 Frequency of Processing Log

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

5.4.3 Retention Period for Audit Log

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 7 years.
2	Enterprise/Individual Certificate	at least 90 days.

for at least ten years. In case and 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 project the log files from unauthorized actions.

5.4.5 Audit Log Backup Procedures

- Audit Logs stored in an electronic audit log system are backup in two facilities protected through restricted security perimeters.
- Events Records follow the procedures below:
  1) Paper-based event records are converted into electronic format before being stored in the audit log system.
  2) CA backup audit events specified in 5.4.1 in backup media.

5.4.6 Audit Log Accumulation System (Internal vs. External)

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

5.4.7 Notification to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

CAs that issues certificates under this CP shall annually perform risk assessment including:

- Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any certificate data or certificate management processes;
- Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the certificate data or certificate management processes; and
- Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

The CAs must perform security vulnerability assessment at least on a quarterly basis and penetration test at least on annual basis covering the CA systems and related services.

5.5 Records Archival

5.5.1 Types of Records Archived

CA archives:

- CA systems
  - All audit data specified in 5.4.1
  - System configuration
  - Website
- Documentation supporting certificate applications
  - Certificates, CRLs, and expired or revoked certificates
  - CP and CPS
- Certificate lifecycle information
  - Forms such as Application Form, Revocation Request Form, Re-key Request Form, and Certificate Acceptance Form

- Required documents for application
- Internal documents such as procedure manuals and system access approval request
- Letters or memos used for communication between CA and external parties such as, Thailand NRCA, Subscriber and other CAs.

5.5.2 Retention Period for Archive

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

5.5.3 Protection of Archive

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

5.5.4 Archive Backup Procedure

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

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

5.5.5 Requirements for Time Stamping of Records

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

5.5.6 Archive Collection System (Internal or External)

Archive Collection System is internal to the CA only.

5.5.7 Procedures to Obtain and Verify Archive Information

Procedures to obtain and verify archive information are as follows:

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

4) The requester verifies the integrity of information.

5.6 Key Changeover

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

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

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

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

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

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

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

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

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

5.7.3 Entity Private Key Compromise Procedures

In the case of Thailand NRCA compromise, Thailand NRCA shall notify the PA, relying parties, cross-certified PKIs and any Trusted Store via public and/or specified announcement. 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 CA key compromise, the CA shall notify PA and Thailand NRCA. Thailand NRCA shall revoke that CA's certificate, and the revocation information shall be published immediately in the most expedient, authenticated, and trusted manner but within 18 hours after the notification. The compromised CA shall also investigate and report to 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 CA can be securely re-established, then the CA shall be re-established. Upon re-establishment of the CA, new subscriber certificates shall be requested and issued again.

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

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

5.7.4 Business Continuity Capabilities after a Disaster

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

5.8 CA or RA Termination

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

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

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The CAs issuing certificates under this CP generate key pairs and store the private key in a hardware cryptographic module that meets Federal Information Processing Standard (FIPS) 140-2 Level 3, or equivalent standards. Multi-party control is required for CA key pair generation, as specified in section 6.2.2.

The documentation of the key pair generation procedure must be detailed enough to show appropriate role separation. Verifiable audit trails shall be created to demonstrate that the security requirements were followed. An independent third party shall validate the execution of the key generation procedures either by witnessing the key generation or by examining the signed and documented record of the key generation.

Subscriber key pair generation shall be performed by subscribers. If the CA generates key pairs for subscribers, the CA shall generate key within a hardware cryptographic module complying with FIPS 140-2 Level 2.

CAs MUST NOT generate the key pairs for end-entity certificates that have an EKU extension containing the KeyPurposeIds id-kp-serverAuth or anyExtendedKeyUsage.

6.1.2 Private Key Delivery to Subscriber

The Subordinate CA issuing certificates under this CP must generate the key pair by itself. If the Subordinate CA generates key pairs for a subscriber, the Subordinate CA shall develop a procedure to securely distribute the private key to the subscriber.

6.1.3 Public Key Delivery to Certificate Issuer

Where key pairs are generated by subscribers, the CA that issues certificates under this CP shall provide a channel for the subscribers to securely deliver the public key and the subscriber's identity to the issuing CA. The subscribers are required to submit Certificate Signing Request in the form of PKCS #10 standard with the application by themselves.

6.1.4 CA Public Key Delivery to Relying Parties

Relying parties can access a CA public key in the CA certificate corresponding to the CA public key. The CA certificate may be delivered through web browsers and operating systems as well as repositories referenced within the certificates issued the CA.

6.1.5 Key Sizes

This CP requires use of RSA signature algorithm and additional restriction on key sizes and hash algorithms are detailed below.

Subordinate CA Certificates issued under this policy shall contain RSA public keys with the minimum key size of 4,096 bits. with SHA-512.

Subscriber Certificates issued under this policy shall contain RSA public keys with the minimum key size of 2,048 bits with SHA-256, or SHA-384, or SHA-512 hash algorithm or ECDSA with the minimum key size of P-256 or higher.

All Certificates under this CP must not issue certificates signed with SHA-1.

6.1.6 Public Key Parameters Generation and Quality Checking

Not Applicable.

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

The use of a specific key pair is constrained by the key usage field in the X.509 certificate. All certificates shall include key usage field as specified in Section 7.1.2.

Keys corresponding to subscriber certificates shall be used only for digital signature and encryption.

Keys corresponding to CA certificates shall be used only for signing certificates and CRLs.

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 key pair generation as well as certificate and CRL signing operations.

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

A subscriber shall use a FIPS 140-2 Level 1 or higher validated cryptographic module for all cryptographic operations. As per private key corresponding to Adobe signing certificate, cryptographic module requirement shall follow Adobe Approved Trust List – Technical Requirements.

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

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

6.2.3 Private Key Escrow

Private keys of CAs operated under this CP are never escrowed. The CAs must not have any policy to keep their private keys with other parties or keep subscribers' private keys.

6.2.4 Private Key Backup

CAs' private keys shall be backed up under the same multiparty control as the original keys. At least one copy of the private key shall be stored off-site. All copies of the CA private signature key shall be accounted for and protected in the same manner as the original. The private key backups must be kept in FIPS 140-2 Level 3 validated hardware cryptographic module.

6.2.5 Private Key Archival

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

6.2.6 Private Key Transfer into or from a Cryptographic Module

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

6.2.7 Private Key Storage on Cryptographic Module

CAs under this CP shall store their Private Keys on a cryptographic module which complies with FIPS 140-2 Level 3 or above standard.

6.2.8 Method of Activating Private Key

Activation of CA private keys shall be performed by authorized persons and requires a two-factor authentication process. As for a subscriber's private key, activation of the private key stored in the cryptographic module must require authentication of the subscriber.

6.2.9 Method of Deactivating Private Key

CAs shall deactivate hardware cryptographic modules storing private keys when not in use to prevent unauthorized access. Any activated cryptographic modules shall be protected from unauthorized access.

6.2.10 Method of Destroying Private Key

A private key of a CA must be destroyed when it is no longer needed. The CA will delete the private keys from a cryptographic module and its backup following the manufacturer's instructions. The event of destroying the CA must be recorded into the evidence under section 5.4.

6.2.11 Cryptographic Module Rating

See Section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

A public key is stored for a 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. A public key can be used to verify the digital signature even if the certificate is expired but the digital signature to be verified must be created before expiry date of the certificate. For the private key, it can be used to decrypt even if the certificate is expired.

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	23 years.

Subordinate CA Certificate	20 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)
SSL/TLS Certificates	398 days. (Certificates issued after 1 September 2020)

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

Activation data such as Personal Identification Number (PIN) and passwords for accessing the CA systems are user-selected and protected under multi-person control by each of whom holding that activation data. The CA operated under this CP shall use the same data generation mechanism.

6.4.2 Activation Data Protection

The CA operated under this CP shall protect activation data used to unlock private keys by storing the data in secure location.

6.4.3 Other Aspects of Activation Data

activation data must only be held by personnel in trusted roles.

6.5 Computer Security Controls

CAs operated under this CP must implement multi-person control access to information such as sensitive details about customer accounts and passwords. Ultimately CA-related private keys are carefully guarded, along with the machines housing such information. In addition, certificate issuance systems are solely segregated from irrelevant systems. Security procedures are in place to prevent and detect unauthorized access, modification, malicious code or compromise of the CA systems such as firmware and software. Such security controls are subject to compliance assessment as specified in section 8.

6.5.1 Specific Computer Security Technical Requirements

CAs operated under this CP shall limit the number of applications installed on each computer to minimize security risks. Those applications are hardened based on the instructions provided by software manufacturers. In addition, installed applications shall be regularly reviewed for security updates to ensure that no vulnerability is exposed.

6.5.2 Computer Security Rating

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

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

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

6.6.2 Security Management Controls

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

6.6.3 Life Cycle Security Controls

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

6.7 Network Security Controls

The CA network must be equipped with firewall with features to investigate data transmission at application level and detect intruders or network activities that violate the policy. It is to ensure that the system is secure.

Normal users allow accessing the certificate services through the network via the website, OCSP and directories only. For system management, certification authority officers will use dedicated network to access and management purpose. Information contains in this particular network is encrypted.

6.8 Time-stamping

The system clock will be set in the time setting device (NTP Server) 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.

ETDA Recommendation on ICT Standard for Electronic Transactions (15-2560: Certificate and Certificate Revocation List (CRL) Profile) is extension for CAs to use as a guidance for issuing certificate in the appropriate manner of business in Thailand, other than in specified shall be approved by Thailand NRCA.

Public-key and attribute certificate frameworks in which the certificate contains the information shown in Table 3.

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

Table 3 Fields in the Certificate

7.1.1 Version Number

The certificate issued by the CA is in accordance with X.509 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 RFC5280 including the latest version of CA/B Forum Baseline Requirements

Section 7.1.2 and ETDA Recommendation on ICT Standard for Electronic Transactions (ขมธอ. 15-2560: Certificate and Certificate Revocation List (CRL) Profile).

As for issuing a subordinate CA certificate by Thailand NRCA, the pathLenConstraint attribute in the basicConstraints field must set to one. In the case of a subordinate CA issues an issuing CA certificate by itself, the pathLenConstraint attribute in the basicConstraints field must set to zero.

7.1.3 Algorithm Object Identifiers

Certificates issued under this CP shall be signed by using the algorithms specified in Table 4.

Algorithm	Object Identifier
RSAEncryption	1.2.840.113549.1.1.1
SHA512	2.16.840.1.101.3.4.2.3
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 4 Method of Digital Signature and Encryption with Object Identifier

7.1.4 Name Forms

The name format of Issuer and Subject DN are specified in the certificate as reference to RFC 5280. Moreover, the CAs MUST meet requirement in section 7.1.4 of CA/B Forum Baseline Requirements for the SSL/TLS Certificate issuance.

7.1.5 Name Constraints

CAs may assert Name Constraints which follow Section 7.1.5 of CA/B Forum Baseline Requirements. The Thailand NRCA Root Certificate does not assert Name Constraints.

7.1.6 Certificate Policy Object Identifier

CAs shall follow Section 7.1.6 of CA/B Forum Baseline Requirements. Furthermore, all certificates under Thailand NRCA hierarchy shall contain at least a relevant Certificate Policy OID identified in Section 1.2. However, a Subscriber certificate may contain additional Certificate Policy OIDs that begin with OID arc of a Subordinate CA provided by Thailand NRCA.

7.1.7 Usage of Policy Constraints Extension

Not Applicable.

7.1.8 Policy Qualifiers Syntax and Semantics

CAs may include a policy qualifier and suitable information for determining appropriate uses.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Not Applicable.

7.2 CRL Profile

The CA's certificate revocation list must comply with RFC 5280 as the following details as in Table 5. In Additionally, its shall accordance with ETDA Recommendation on ICT Standard for Electronic Transactions (ขมธอ. 15-2560: CERTIFICATE AND CERTIFICATE REVOCATION LIST (CRL) 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 digestion (Hash Function) which is used by Certificate Authority to sign the certificate in form of Object Identifier (OID).
issuer	The name of the Certificate Authority in the certificate must be in the format of Distinguished Name (DN) in accordance with ISO / IEC 9594-2.
thisUpdate	The date and time of the revocation list.
nextUpdate	The specified date and time to the next update of certificate revocation list. If necessary, Thailand NRCA will issue the certificate revocation list before the scheduled date and time.
revokedCertificates	A list of the serialNumber of the certificate has been revoked with the specified date and time of revocation.

Table 5 Item List in Certificate Revocation

7.2.1 Version Number(s)

The version number of certificate revocation list in accordance with RFC 5280 will be specified the value of version to be 2.

7.2.2 CRL and CRL Entry Extensions

CRLs issued by the CAs contains at least the following extensions: Authority Key Identifier and CRL Number.

7.2 OCSP Profile

The Online Certificate Status Protocol (OCSP) is the way for relying parties to obtain certificate status information of a CA. CAs under Thailand NRCA must provide certificate status information through OCSP protocol conforming to RFC6960.

7.3.1 Version Number(s)

CAs shall issue Version 1 OCSP responses.

7.3.2 OCSP Extensions

Not stipulation.

8. Compliance Audit and Other Assessments

The policies within this CP are designed to comply with following industry standards and applicable laws required for CA operations, including:

- WebTrust Principles and Criteria for Certification Authorities
- WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security (if applicable)
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates
- Adobe Approved Trust List – Technical Requirements (if applicable)
- Electronic Transactions Act, B.E. 2544 (2001) and related version.

8.1 Frequency or Circumstances of Assessment

All CAs in the Thailand NRCA hierarchy shall maintain their compliance with relevant standards and applicable laws mentioned in Section 8, as well as this CP and their CPS. A compliance audit shall be performed by an independent auditor on an annual and continuous basis.

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:

- Independence from the subject of the audit;
- The ability to conduct an audit that addresses the criteria specified in an eligible audit scheme (see Section 8.0)
- 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;
- Licensed by WebTrust;
- Bound by law, government regulation, or professional code of ethics; and
- 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 or sufficiently organizationally separated from CAs that provide unbiased and independent evaluation. To ensure independence and objectivity, there must not be a conflict of interest between the auditors and 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

A CA must plan to improve the deficiencies (Non-conformity) based on the assessment results with an explicit operating time. The plan will be submitted to auditors and Thailand NRCA (if the CA is a Subordinate CA) to ensure that the 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 (if any) must be sent to the PA within 30 days of completion. However, the audit compliance report must

be sent to the PA and made it publicly available within three months after the end of the audit period. In the case of delay, the CA shall provide an official letter signed by the qualified auditor.

8.7 Self-Audits

The CA SHALL ensure compliance with this CP and its CPS, as well as strictly control its service quality by performing self-audits on at least a quarterly basis. Randomized samples of the greater of one certificate or at least three percent of the certificates issued since the previous self-audit was performed.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

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

9.1.2 Certificate Access Fees

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

9.1.3 Revocation or Status Information Access Fees

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

9.1.4 Fees for Other Services

The CA operated under this CP shall declare the other fees.

9.1.5 Refund Policy

The CA operated under this CP shall provide reasonable refund policy.

9.2 Financial Responsibility

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

9.2.1 Insurance Coverage CPS

The CA operated under this CP shall maintain and disclose Workers' Compensation, Commercial General Liability insurance and Technology Errors and Omission/ Professional Liability insurance policies. The CA operated under this CP shall disclose insurance related to the CA operation.

9.2.2 Other Assets

The CA operated under this CP shall disclose other assets.

9.2.3 Insurance or Warranty Coverage for End-entities

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

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The CA keeps following information in the scope of confidential information:

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

9.3.2 Information Not within the Scope of Confidential Information

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

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

9.3.3 Responsibility to Protect Confidential Information

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

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

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

9.4.2 Information Treated As Private

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

9.4.3 Information Not Deemed Private

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

9.4.4 Responsibility to Protect Private Information

The CA has implemented security measure to protect private information.

9.4.5 Notice and Consent to Use Private Information

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

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

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

9.4.7 Other Information Disclosure Circumstances

None.

9.5 Intellectual Property Rights

The CAs are the owners of their intellectual property rights associated with the certificate, certificate revocation information and documents relating to their services, including CP and CPS.

The CAs shall not infringe the intellectual property rights, for instance, copyright, patent, trademarks, or trade secrets of third parties. Moreover, in compliance with legal restrictions, the CAs shall use all materials and software products in respect of intellectual property.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

The CAs assures that

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

9.6.2 RA Representations and Warranties

An RA shall assure that

- Its RA registration operation is performed in conformance to the stipulations of the approved CPS of the corresponding CA and related regulations.

- All information contained in the certificate issued by the CA is valid and appropriate. The evidence that due diligence was exercised in validating the information contained in the certificates is maintained.
- The obligations are imposed on subscribers in accordance with section 9.6.3, and subscribers are informed of the consequences of not complying with those obligations.

9.6.3 Subscriber Representations and Warranties

By using the subscriber certificate, the subscriber assures that

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

9.6.4 Relying Party Representations and Warranties

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

9.6.5 Representations and Warranties of Other Participants

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

9.7 Disclaimers of Warranties

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

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

9.9 Indemnities

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

9.10 Term and Termination

9.10.1 Term

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

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

9.10.2 Termination

This CP takes effect until it is terminated.

9.10.3 Effect of Termination and Survival

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

9.11 Individual Notices and Communications with Participants

The CA 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

An amendment of this CP requires approval by the PA before announcement. The amendment shall be performed under laws, regulation or other related service announcements of Thailand NRCA.

9.12.2 Notification Mechanism and Period

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

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

9.13 Dispute Resolution Provisions

9.13.1 Disputes between Issuer and Subscriber

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

9.13.2 Disputes between Issuer and Relying Parties

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

9.14 Governing Law

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

9.15 Compliance with Applicable Law

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

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

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

9.16.2 Assignment

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

9.16.3 Severability

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

9.16.4 Enforcement

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

9.16.5 Force Majeure

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

9.17 Other Provisions

Not Applicable.