Table of Contents

1 INTRODUCTION

Turnkey Communication Services Public Company Limited (hereby referred to as TKC) is a Certification Authority (CA) that issues digital Certificates to entities and individuals according to the ThaiCA Certificate Policy and Certification Practice Statement (CP/CPS). ThaiCA performs Public Key life-cycle functions that include receiving certificate requests, issuing, revoking and renewing digital Certificates. In addition, ThaiCA maintains and publishes the Certificate Revocation Lists (CRLs) for participants within the ThaiCA Public Key Infrastructure (PKI).

1.1 Overview - The ThaiCA CP/CPS

This document incorporates the ThaiCA Certificate Policy (CP) and ThaiCA Certification Practice Statement (CPS) into a single document, henceforth referred to as the ThaiCA CP/CPS. It sets forth the business, legal, and technical requirements, principles and practices surrounding digital certification services provided by TKC.

This CP/CPS conforms to the current version of guidelines adopted by the Certification Authority/Browser Forum ("CAB Forum") and published to their site (https://www.cabforum.org).

The ThaiCA CP/CPS uses the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 3647). In accordance with RFC 3647, this CP/CPS is organized using numbered paragraphs. Items that do not currently apply to ThaiCA PKI will have the statement "Not applicable" or "No stipulation".

TKC's Policy Management Authority (PMA) will continuously keep track of changes in ThaiCA policies and applicable guidelines, incorporate required changes before their effective dates, and update this CP/CPS accordingly. In the event of any inconsistency between this CP/CPS and the guidelines given above, the relevant CAB Forum publication shall take precedence over this document.

This CP/CPS applies to all entities and individuals utilizing ThaiCA certification services.

Other important documents also apply to ThaiCA certification services. These include public documents (such as agreements with Subscribers and other ThaiCA customers, Relying Party agreements, and the ThaiCA privacy policy) and private documents governing internal operations.

1.2 Identification Number and Document Name

1.2.1 Document Identification Number

The OID assigned to ThaiCA by IANA is `iso (1) org (3) dod (6) internet (1) private (4) enterprise (1) ThaiCA (62483)`.

A special OID arc has been allocated by ThaiCA for Certificate Policy / Certification Practice Statement:

```
iso (1) org (3) dod (6) internet (1) private (4) enterprise (1) ThaiCA
(62483) certificationServicesProvision (1)
certificatePolicyCertificationPracticeStatement (1)
```

The globally unique Identification Number (OID) of the ThaiCA CP/CPS (this document) is:

1.3.6.1.4.1.62483.1.1.1.6

OID Arc	Description
1.3.6.1.4.1.**62483**	Identification Number (OID) of TKC, registered to IANA (www.iana.org)
1	Certification Services Provision
1	Certificate Policy / Certification Practice Statement
1.6	First and Second number of the version identifying this document

Version Control

Version	Date	Information
1.0	**July 1 2024**	First release
1.1	**August 1 2024**	Release update after internal review
1.2	**September 1 2024**	Release update after comments from External Auditor
1.3	**November 1 2024**	Release update after comments from External Auditor
1.4	**November 12 2024**	Release updated after comments from External Auditor
1.5	**November 13 2024**	Release updated after comments from NRCA
1.6	**May 25 2025**	Release updated after comment from NRCA

1.2.2 Document Name

This document is the ThaiCA CP/CPS and constitutes the documentation and regulatory frame for TKC's PKI. This document incorporates both the Certificate Policy and the Certification Practice Statement for TKC's operations. In abbreviation, it will be referred as the "TKC CP/CPS" or "CP/CPS".

1.2.3 Certification Practice Statements and specific scenarios

Should the need arise to follow any additional practice beyond what is outlined in this CP/CPS, a corresponding alternate certification practice statement (alternate CPS) will be created and referenced in this document. The resulting document(s) will be a separate CPS that applies to specific cases. The new alternate CPS will describe particular cases where it applies, the different procedures that will apply in those particular cases, and the specific sections of the ThaiCA CP/CPS which the alternate CPS modifies or supersedes.

1.2.4 Provision and amendment of ThaiCA CP/CPS

The provisions of the ThaiCA CP/CPS, as amended from time to time, are publicly available via the ThaiCA repository. Amendments to this document will be made in accordance with Sections 1.5 and 9.12.

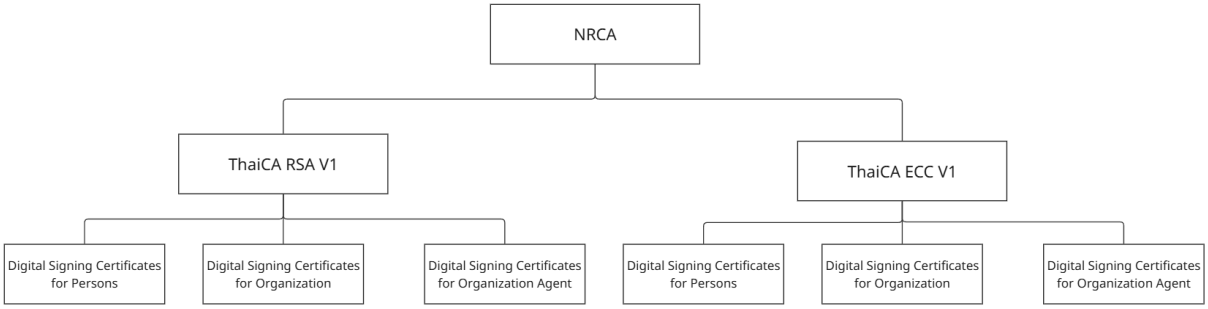
1.3 PKI participants and their roles

The roles which comprise TKC's PKI include Certification Authorities (CAs), Registration Authorities (RAs), Subscribers and Relying Parties.

- A Certification Authority (CA) is the entity responsible for issuing Certificates.
- A CA utilises at least one Registration Authority (RA) for identifying, authenticating and managing a Subscriber's certificate request information.
- A Subscriber is any party which has been issued a certificate by TKC.
- A Relying Party is any party who performs transactions, communications and/or functions that rely on a certificate issued by TKC.

Also refer to Section 1.6.1 for definition of these terms.

The diagrams below indicate the relationship between these components:



1.3.1 Certification Authority

Within the ThaiCA PKI hierarchy, ThaiCA functions as an Issuing CA.

1.3.1.1 Root CA role

Within this PKI infrastructure, the NRCA performs the role as the Root CA. The NRCA operates according to its own CP and CPS. The ThaiCA CA is compliant to the NRCA CP and CPS and adds additional constrains and business logic.

1.3.1.2 Issuing CA role

In its role as an issuing CA, ThaiCA performs functions associated with Public Key operations that include:

- ThaiCA RSA V1 for
  - Digital Signing Certificates for Persons
  - Digital Signing Certificates for Organisations
  - Digital Signing Certificates for Authorised Organisation Agents
  - Digital Signing Short Lived Certificates for legal Persons
- ThaiCA ECC V1 for
  - Digital Signing Certificates for Persons
  - Digital Signing Certificates for Organisations
  - Digital Signing Certificates for Authorised Organisation Agents
  - Digital Signing Short Lived Certificates for legal Persons

1.3.1.3 General CA roles

In its capacity as a CA, TKC:

- Conforms its operations to the ThaiCA CP/CPS
- Conforms its operations to the NRCA CP/CPS
- Issues and publishes Certificates in a timely manner
- Revokes Certificates upon receipt of a valid and authorised request, or on its own initiative when circumstances warrant
- Notifies Certificate holders of the imminent expiry of their Certificates.

1.3.2 Registration Authority

Any CA utilizes at least one RA for identifying, authenticating and managing a Subscriber's certificate request information. Depending on the type of CA, registration requirements of this CA and the assurance level, a Subscriber may need to perform specific registration operations (for example face-to-face proof of identity, inquiries to official local government list of commercial organizations, etc). These operations are performed by RAs operated under the supervision of TKC, utilizing trusted personnel and/or trustworthy systems providing equivalent assurance. ThaiCA operates the central RA of the ThaiCA hierarchy.

With the exception of sections 3.2.2.4 and 3.2.2.5, ThaiCA may delegate the performance of all or any part of these requirements to a Delegated Third Party, provided that the process as a whole fulfills all of the requirements of Section 3.2 of this CP/CPS. Before ThaiCA

authorizes a Delegated Third Party to perform a delegated function, ThaiCA shall contractually require the Delegated Third Party to:

1. Meet the qualification requirements of Section 5.3.1, when applicable, to the delegated function;
2. Retain documentation in accordance with Section 5.5.2;
3. Comply with (a) the ThaiCA CP/CPS or (b) the Delegated Third Party's (TKC-approved) CP/CPS; and
4. Abide by the other provisions (i.e. Contract between ThaiCA and Delegated Third Parties) that are applicable to the delegated function.

TKC may designate an Enterprise RA to verify certificate requests from the Enterprise RA's own organization. ThaiCA shall not accept certificate requests authorized by an Enterprise RA unless the following requirements are satisfied:

1. TKC shall confirm that the identity of the person requesting the certificate is verified against a physical document in person OR
2. TKC shall confirm that the identity of the person requesting the certificate is verified against a physical document via a video call using a video mechanism initiated and vetted by ThaiCA
3. TKC shall confirm that the organisation certificate is requested by an authorised agent
4. TKC shall confirm that the organisation is a valid organisation

TKC may delegate the performance of all or any part of validation to an affiliate or a Registration Authority (RA) or subcontractor, provided that the process employed fulfils all of the requirements of the guidelines. Affiliates and/or RAs must comply with the qualification requirements of Sections 5.2 and 5.3.

TKC shall verify that the Delegated Third Party's personnel involved in the issuance of a Certificate meet the training and skills requirements of Section 5.3.

1.3.3 Enterprise RAs

TKC may contractually authorize an appointed enterprise to perform the RA function and authorize ThaiCA to issue additional. In such case, the Subject shall be considered an Enterprise RA, and the following requirements shall apply:

(1) An Enterprise RA shall not authorize ThaiCA to issue an Enterprise or digital signing certificate at the third or higher domain levels to any Subject other than the Enterprise RA or a business that is owned or directly controlled by the Enterprise RA;

(2) In all cases, the Enterprise RA must be an organization verified by ThaiCA

(3) TKC must impose these limitations as a contractual requirement with the Enterprise RA and monitor compliance by the Enterprise RA;

(4) The Final Cross-Correlation and Due Diligence requirements of may be performed by a single person representing the Enterprise RA; and

(5) The audit requirements of Section 8.4 shall apply to the Enterprise RA, except in the case where ThaiCA maintains control over the CA private key used to issue the Enterprise Certificates, in which case, the Enterprise RA may be exempted from the audit requirements.

(6) TKC does NOT contractually authorize the Enterprise RA to perform the RA function and authorize ThaiCA to issue additional certificates for other organisations.

1.3.4 Guidelines Compliance Obligation

In all cases, ThaiCA contractually obligates each Affiliate, RA, subcontractor, and Enterprise RA to comply with all applicable requirements in this CP/CPS and to perform them as required of ThaiCA itself. ThaiCA shall enforce these obligations and internally audit each Affiliate's, RA's, subcontractor's, and Enterprise RA's compliance with this CP/CPS on an annual basis.

1.3.5 Subscribers

A Subscriber is any natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use.

1.3.5.1 Applicants

An Applicant is any natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Prior to verification of identity and issuance of a certificate, any requesting Subscriber is defined as an Applicant. Once the Certificate is issued, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual certificate request. Prior to verification of identity and issuance of a certificate, any requesting Subscriber is defined as an Applicant.

1.3.5.2 Role of Applicants and/or Subscribers

Before accepting and using a certificate, an Applicant must:

1. Generate a unique Key Pair.
2. Submit an application for the type of certificate requested which must be approved by TKC's RA
3. Agree to and accept the terms and conditions of the applicable ThaiCA Subscriber Agreement

For Key Pair generation on behalf of the Subscriber, the provisions of section 6.2.1 apply.

1.3.5.3 Applicant and/or Subscriber responsibilities

Each Applicant and/or Subscriber is solely responsible for the generation of the Key Pair associated with an ThaiCA certificate. For Key Pair generation on behalf of the Subscriber, the provisions of section 6.2.1 apply.

Each Applicant and/or Subscriber is solely responsible for the protection of the Private Key related to their ThaiCA certificate.

A Subscriber shall immediately notify ThaiCA if any information contained in an issued ThaiCA certificate changes or becomes false or misleading, or in the event that its Private Key has been compromised or the Subscriber has reason to believe that it has been compromised. A Subscriber must immediately stop using and uninstall any ThaiCA certificate upon that certificate's revocation or expiration.

Applicants and Subscribers are required to operate under the ThaiCA CP/CPS and agree to the ThaiCA Subscriber Agreement.

1.3.5.4 Machine Subscribers

Machine subscribers are certificates issued to natural persons for the purpose of authenticating a machine. In this case the certificate contains identifiers for both the person as well as the machine identifier to which it is bound to. These are any one of the following:

- MAC Address
- IP Address
- Domain name (internal)

1.3.6 Relying Parties

A Relying Party is any entity performing transactions, communications and/or functions which rely on a certificate issued by TKC.

Before relying on or using an ThaiCA certificate, Relying Parties should:

- Read the ThaiCA CP/CPS in its entirety
- Review the ThaiCA repository to determine whether the certificate has expired or been revoked (per the CRL and/or OCSP) and/or to collect more information concerning the certificate

Relying Parties should make their own judgment as to what degree, if any, they rely on any certificate and must make a trust decision based on the content of the corresponding certificate in order to proceed to specific actions or justified belief. In order to verify the validity of the certificate, Relying Parties must check that:

- The validity period of the certificate has begun and has not expired
- The certificate is correctly signed by an ThaiCA Trusted Certification Authority
- The certificate has not been revoked/suspended

- Subject identification matches the details that the signer presents
- The usage for which the certificate was originally intended corresponds with those presented and abides by the terms and the conditions that are described in TKC's CP/CPS.

1.3.7 Other participants in the ThaiCA PKI

TKC shall contractually guarantee that all applicable requirements specified in the CP/CPS, external RAs, Enterprise RAs, and/or subcontractors that involve or relate to the issuance or maintenance of Certificates.

1.4 Certificate usage

1.4.1 Allowed certificate usage

A certificate issued by ThaiCA under the guidelines of the ThaiCA CP/CPS shall be used only as designated by the key usage or extended key usage fields defined in the certificate profile for that product (including authentication, encryption, access control, and digital signature purposes).

1.4.2 Prohibited certificate usage

A certificate issued by ThaiCA under the guidelines of this ThaiCA CP/CPS may not be used for any purpose other than those defined in the certificate profile of the respective product.

1.5 Policy Administration

1.5.1 Organisation administering the ThaiCA CP/CPS

The ThaiCA CP/CPS, related procedural or security policy documents, and any other related agreements referenced, are administered by the ThaiCA Policy Management Authority (PMA), appointed by ThaiCA management.

1.5.2 Contact information for the ThaiCA PMA

The ThaiCA PMA can be contacted via the following methods:

- Mail: Policy Creation Authority, Turnkey Communication Services Public Company Limited. 44/44 Vibhavadi-Rangsit 60 Yake 18-1-2, Talad Bangkhen, Laksi, Bangkok, Thailand, 10210
- Email: support@thaica.com
- Phone: +6624018222

Instructions on how to submit a Certificate Problem Report is provided in section 4.9.3.3.

1.5.3 Person determining CP/CPS suitability for the policy

Compliance and suitability with the ThaiCA CP/CPS is monitored and managed by the ThaiCA PMA, with reference to results and recommendations made by Qualified Auditors and Self-Audits (Section 8).

1.5.4 CPS approval procedures

The ThaiCA CP/CPS is approved and amended by the ThaiCA PMA per the provisions of section 9.12.

1.6 Definitions and acronyms

1.6.1 Definitions

Account Dashboard: User interface for management of ThaiCA Certificates. Any Applicant will be directed to log in to or create an ThaiCA account before any request shall be processed.

Affiliate: A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.

Applicant: The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual certificate request.

Applicant Representative: A natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: (i) who signs and submits, or approves a certificate request on behalf of the Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or (iii) who acknowledges the Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of ThaiCA or is TKC.

Application Software Supplier: A supplier of Internet browser software or other Relying Party application software that displays or uses Certificates and incorporates Root Certificates.

Attestation Letter: A letter attesting that Subject Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information.

Audit Period: In a period-of-time audit, the period between the first day (start) and the last day of operations (end) covered by the auditors in their engagement. (This is not the same as the period of time when the auditors are on-site at the CA.) The coverage rules and maximum length of audit periods are defined in Section 8.1.

Audit Report: A report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the mandatory provisions of industry standards Requirements.

Authorization Domain Name: The FQDN used to obtain authorization for a given FQDN to be included in a Certificate. ThaiCA may use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. If a Wildcard Domain Name is to be included in a Certificate, then ThaiCA MUST remove "`*.`" from the left-most portion of the Wildcard Domain Name to yield the corresponding FQDN. ThaiCA may prune zero or more Domain Labels of the FQDN from left to right until encountering a Base Domain Name and may use any one of the values that were yielded by pruning (including the Base Domain Name itself) for the purpose of domain validation.

Authorized Port: One of the following ports: 80 (http), 443 (https), 25 (smtp), 22 (ssh).

Base Domain Name: The portion of an applied-for FQDN that is the first Domain Name node left of a registry-controlled or public suffix plus the registry-controlled or public suffix (e.g. "example.co.uk" or "example.com"). For FQDNs where the right-most Domain Name node is a gTLD having ICANN Specification 13 in its registry agreement, the gTLD itself may be used as the Base Domain Name.

Baseline Requirements: The "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" as published by the CA/Browser Forum and any amendments to such document.

Business Entity: Any entity that is not a Private Organization, Government Entity, or Non-Commercial Entity as defined herein. Examples include, but are not limited to, general partnerships, unincorporated associations, sole proprietorships, etc.

CAA: From RFC 8659 (http:tools.ietf.org/html/rfc8659): "The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify one or more Certification Authorities (CAs) authorized to issue certificates for that domain name. CAA Resource Records allow a public CA to implement additional controls to reduce the risk of unintended certificate mis-issue".

CA Key Pair: A Key Pair where the Public Key appears as the Subject Public Key Info in one or more Root CA Certificate(s) and/or Subordinate CA Certificate(s).

CAB Forum: The Certification Authority/Browser Forum, a voluntary group of certification authorities (CAs), vendors of Internet browser software, and suppliers of other applications that use X.509 v.3 digital certificates for SSL/TLS and Code Signing. The CAB Forum determines guidelines and requirements to establish public trust in browsers and other software using digital certificates.

CCADB: A repository of information about externally operated Certificate Authorities (CAs) whose root and intermediate certificates are included within the products and services of Application Software Suppliers who are CCADB root store members. The repository is available at https://ccadb.org.

Certificate: An electronic document that uses a digital signature to bind a public key and an identity.

Certificate Approver: A natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant to (i) act as a Certificate Requester and to authorize other employees or third parties to act as a Certificate Requester.

Certificate Data: Certificate requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA's possession or control or to which the CA has access.

Certificate Management Process: Processes, practices, and procedures associated with the use of keys, software, and hardware, by which ThaiCA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.

Certificate Management System: A system used by ThaiCA or Delegated Third Party to process, approve issuance of, or store certificates or certificate status information, including the database, database server, and storage.

Certificate Policy: A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.

Certificate Problem Report: Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.

Certificate Profile: A set of requirements for Certificate content and Certificate extensions.

Certificate Requester: A natural person who is either the Applicant, employed by the Applicant, an authorized agent who has express authority to represent the Applicant, or a third party (such as an ISP or hosting company)

Certificate Revocation List: A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.

Certificate Systems: The systems used by ThaiCA or Delegated Third Party in providing identity verification, registration and enrolment, certificate approval, issuance, validity status, support, and other PKI-related services.

Certification Authority: An organization 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: One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.

Code Signature: A Signature logically associated with a signed Object

Confirmation Request: An appropriate out-of-band communication requesting verification or confirmation of the particular fact at issue.

Contract Signer: A natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant, and who has authority on behalf of the Applicant to sign Subscriber Agreements.

Control: "Control" (and its correlative meanings, "controlled by" and "under common control with") means possession, directly or indirectly, of the power to: (1) direct the management, personnel, finances, or plans of such entity; (2) control the election of a majority of the directors ; or (3) vote that portion of voting shares required for "control" under the law of the entity's Jurisdiction of Incorporation or Registration but in no case less than 10%.

Country: Either a member of the United Nations OR a geographic region recognized as a Sovereign State by at least two UN member nations.

Cross Certificate: A certificate that is used to establish a trust relationship between two Root CAs.

CSPRNG: A random number generator intended for use in a cryptographic system.

Dashboard: See Account Dashboard.

Delegated Third Party: A natural person or Legal Entity that is not TKC, and whose activities are not within the scope of TKC's external audits, but is authorized by ThaiCA to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.

Delegated Third Party System: Any part of a Certificate System used by a Delegated Third Party while performing the functions delegated to it by TKC.

DNS CAA Email Contact: The email address defined as a property in a DNS CAA record. Example: `CAA 0 contactemail "domainowner@example.com"`. The CAA contactemail property takes an email address as its parameter. The entire parameter value MUST be a valid email address as defined in RFC 6532 section 3.2, with no additional padding or structure, or it cannot be used. The contactemail property MAY be critical, if the domain owner does not want CAs who do not understand it to issue certificates for the domain.

DNS CAA Phone Contact: The phone number defined as a property in a DNS CAA record. Example: `CAA 0 contactphone "+1 (555) 123-4567"`. The CAA contactphone property takes a phone number as its parameter. The entire parameter value MUST be a valid Global Number as defined in RFC 3966 section 5.1.4, or it cannot be used. Global Numbers MUST have a preceding + and a country code and MAY contain visual separators. The contactphone property MAY be critical if the domain owner does not want CAs who do not understand it to issue certificates for the domain.

DNS TXT Record Email Contact: The email address placed in a DNS TXT record. The DNS TXT record MUST be placed on the `"_validation-contactemail"` subdomain of the domain being validated. The entire RDATA value of this TXT record MUST be a valid email address as defined in RFC 6532 section 3.2, with no additional padding or structure, or it cannot be used.

DNS TXT Record Phone Contact: An email address placed in a DNS TXT record. This DNS TXT record MUST be placed on the "_validation-contactphone" subdomain of the domain being validated. The entire RDATA value of this TXT record MUST be a valid Global Number as defined in RFC 3966 section 5.1.4, or it cannot be used.

Domain Authorization Document: Documentation provided by, or a CA's documentation of a communication with, a Domain Name Registrar, the Domain Name Registrant, or the person or entity listed in WHOIS as the Domain Name Registrant (including any private, anonymous, or proxy registration service) attesting to the authority of an Applicant to request a Certificate for a specific Domain Namespace.

Domain Contact: The Domain Name Registrant, technical contact, or administrative contact (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record, or as obtained through direct contact with the Domain Name Registrar.

Domain Label: From RFC 8499 (http://tools.ietf.org/html/rfc8499): "An ordered list of zero or more octets that makes up a portion of a domain name. Using graph theory, a label identifies one node in a portion of the graph of all possible domain names."

Domain Name: An ordered list of one or more Domain Labels assigned to a node in the Domain Name System.

Domain Name Registrant: Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.

Domain Name Registrar: A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns).

Domain Namespace: The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.

Enterprise RA: An employee or agent of an organization unaffiliated with ThaiCA who authorizes issuance of Certificates to that organization.

Expiry Date: The "notAfter" date in a Certificate that defines the end of a Certificate's validity period.

Fully-Qualified Domain Name: A Domain Name that includes Domain Labels of all superior nodes in the Internet Domain Name System.

Government Agency: In the context of a Private Organization, the government agency in the Jurisdiction of Incorporation under whose authority the legal existence of Private Organizations is established (e.g., the government agency that issued the Certificate of Incorporation). In the context of Business Entities, the government agency in the

jurisdiction of operation that registers business entities. In the case of a Government Entity, the entity that enacts law, regulations, or decrees establishing the legal existence of Government Entities.

Government Entity: A government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).

High Risk Certificate Request: A Request which ThaiCA flags for additional scrutiny by reference to internal criteria and databases maintained by the CA, which may include names at higher risk for phishing or other fraudulent usage, names contained in previously rejected certificate requests or revoked Certificates, names listed on the Miller Smiles phishing list or the Google Safe Browsing list, or names which ThaiCA identifies using its own risk-mitigation criteria.

High Risk Region of Concern (HRRC): A geographic location where the detected number of Code Signing Certificates associated with signed Suspect Code exceeds 5% of the total number of detected Code Signing Certificates originating or associated with the same geographic area. This information is provided in Appendix D of the "Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates" document.

Incorporating Agency: In the context of a Private Organization, the government agency in the Jurisdiction of Incorporation under whose authority the legal existence of the entity is registered (e.g., the government agency that issues certificates of formation or incorporation). In the context of a Government Entity, the entity that enacts law, regulations, or decrees establishing the legal existence of Government Entities.

Individual: A natural person.

Intermediate CA Certificate: A Certificate issued by a Root Certificate or another Intermediate CA Certificate which is deemed as capable of being used to issue new Certificates and which contains an X.509v3 basicConstraints extension, with the cA boolean set to true. If an Intermediate CA Certificate is issued to a non-affiliated organization, then this Intermediate CA Certificate is also referred to as an Intermediate CA Certificate of a Subordinate CA.

Internal Name: A string of characters (not an IP address) in a Common Name or Subject Alternative Name field of a Certificate that cannot be verified as globally unique within the public DNS at the time of certificate issuance because it does not end with a Top Level Domain registered in IANA's Root Zone Database.

IP Address: A 32-bit or 128-bit number assigned to a device that uses the Internet Protocol for communication.

Issuing CA: In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.

Jurisdiction of Incorporation: In the context of a Private Organization, the country and (where applicable) the state or province or locality where the organization's legal existence

was established by a filing with (or an act of) an appropriate government agency or entity (e.g., where it was incorporated). In the context of a Government Entity, the country and (where applicable) the state or province where the Entity's legal existence was created by law.

Jurisdiction of Registration: In the case of a Business Entity, the state, province, or locality where the organization has registered its business presence by means of filings by a Principal Individual involved in the business.

Key Compromise: A Private Key is said to be compromised if its value has been disclosed to an unauthorized person or an unauthorized person has had access to it.

Key Generation Script: A documented plan of procedures for the generation of a CA Key Pair.

Key Pair: The Private Key and its associated Public Key.

LDH Label: From RFC 5890 (http://tools.ietf.org/html/rfc5890): "A string consisting of ASCII letters, digits, and the hyphen with the further restriction that the hyphen cannot appear at the beginning or end of the string. Like all DNS labels, its total length must not exceed 63 octets."

Latin Notary: A person with legal training whose commission under applicable law not only includes authority to authenticate the execution of a signature on a document but also responsibility for the correctness and content of the document. A Latin Notary is sometimes referred to as a Civil Law Notary.

Legal Entity: An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.

Legal Existence: A Private Organization, Government Entity, or Business Entity has Legal Existence if it has been validly formed and not otherwise terminated, dissolved, or abandoned.

Legal Practitioner: A person who is either a lawyer or a Latin Notary (see above) and competent to render an opinion on factual claims of the Applicant.

Lifetime Signing OID: An optional extended key usage OID (1.3.6.1.4.1.311.10.3.13) used by Microsoft Authenticode to limit the lifetime of the Code Signature to the expiration of the Code Signing certificate.

Non-Reserved LDH Label: From RFC 5890 (http://tools.ietf.org/html/rfc5890): "The set of valid LDH labels that do not have '–' in the third and fourth positions."

Notary: A person whose commission under applicable law includes authority to authenticate the execution of a signature on a document.

Object Identifier: A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.

OCSP: See Online Certificate Status Protocol.

OCSP Responder: An online server operated under the authority of ThaiCA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.

OID: see Object Identifier.

Onion Domain Name: A Fully Qualified Domain Name ending with the RFC 7686 ".onion" Special-Use Domain Name. For example, `2gzyxa5ihm7nsggfxnu52rck2vv4rvmdlkiu3zzui5du4xyclen53wid.onion` is an Onion Domain Name, whereas `torproject.org` is not an Onion Domain Name.

Online Certificate Status Protocol: An online Certificate-checking protocol that enables Relying Party application software to determine the status of an identified Certificate. See also OCSP Responder.

P-Label: A XN-Label that contains valid output of the Punycode algorithm (as defined in RFC 3492, Section 6.3) from the fifth and subsequent positions.

Parent Company: A company that Controls a Subsidiary Company.

PKI: See Public Key Infrastructure.

Place of Business: The location of any facility (such as a factory, retail store, warehouse, etc.) where the Applicant's business is conducted.

Policy Management Authority: Administrative body appointed by ThaiCA management to create and maintain policies described in the ThaiCA CP/CPA and related procedural or security policy documents.

Principal Individual: An individual of a Private Organization, Government Entity, or Business Entity that is either an owner, partner, managing member, director, or officer, as identified by their title of employment, or an employee, contractor or agent authorized by such entity or organization to conduct business related to the request, issuance, and use of Certificates.

Private Organization: A non-governmental legal entity (whether ownership interests are privately held or publicly traded) whose existence was created by a filing with (or an act of) the Incorporating Agency or equivalent in its Jurisdiction of Incorporation.

Private Key: The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

Public Key: The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

Public Key Infrastructure: A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.

Public Suffix: 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 http://publicsuffix.org/ (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. ThaiCA 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.

Publicly-Trusted Certificate: A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software.

Qualified Auditor: A natural person or Legal Entity that meets the requirements of Section 8.2 (Auditor Qualifications).

Qualified Government Information Source: A regularly-updated and current, publicly available, database designed for the purpose of accurately providing the information for which it is consulted, and which is generally recognized as a dependable source of such information, provided that it is

```
i)maintained by a Government Entity,
ii)the reporting of data is required by law, and
iii)false or misleading reporting is punishable with criminal or civil
penalties.
```

RA: See Registration Authority

Random Value: A value specified by ThaiCA to the Applicant that exhibits at least 112 bits of entropy.

Registered Domain Name: A Domain Name that has been registered with a Domain Name Registrar.

Registration Agency: A Governmental Agency that registers business information in connection with an entity's business formation or authorization to conduct business under a license, charter or other certification. A Registration Agency may include, but is not limited to (i) a State Department of Corporations or a Secretary of State; (ii) a licensing agency, such as a State Department of Insurance; or (iii) a chartering agency, such as a state office or department of financial regulation, banking or finance, or a federal agency such as the Office of the Comptroller of the Currency or Office of Thrift Supervision.

Registration Authority: Any Legal Entity that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence does not sign or issue

Certificates. An RA may assist in the certificate application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.

Re-keying: Creation of an entirely new certificate, using some or all of the information submitted for an existing certificate and using a newly generated Private Key.

Reliable Data Source: An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate.

Relying Party: Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such Supplier merely displays information relating to a 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. ThaiCA maintains its repository at https://www.thaica.com/repository.

Request Token: A value derived in a method specified by ThaiCA which binds this demonstration of control to the certificate request.

The Request Token SHALL incorporate the key used in the certificate request.

A Request Token MAY include a timestamp to indicate when it was created.

A Request Token MAY include other information to ensure its uniqueness.

A Request Token that includes a timestamp SHALL remain valid for no more than 30 days from the time of creation.

A Request Token that includes a timestamp SHALL be treated as invalid if its timestamp is in the future.

A Request Token that does not include a timestamp is valid for a single use and ThaiCA SHALL NOT re-use it for a subsequent validation.

The binding SHALL use a digital signature algorithm or a cryptographic hash algorithm at least as strong as that to be used in signing the certificate request.

Required Website Content: Either a Random Value or a Request Token, together with additional information that uniquely identifies the Subscriber, as specified by TKC.

Reserved IP Address: An IPv4 or IPv6 address that is contained in the address block of any entry in either of the following IANA registries:

- https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml

- https://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special-registry.xhtml

Root CA: A top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.

Root CA System: A system used to create a Root Certificate or to generate, store, or sign with the Private Key associated with a Root Certificate.

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.

Root Program Policy: Policy set by an Application Software Supplier to establish the minimum requirements for CA certificates to be distributed in their software.

Sovereign State: A state or country that administers its own government, and is not dependent upon, or subject to, another power.

Subject: The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.

Subject Identity Information: Information that identifies the Certificate Subject. Subject Identity Information does not include a Domain Name listed in the `subjectAltName` extension or the Subject `commonName` field.

Subordinate CA: A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.

Subscriber: A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use. For Code Signing and, the Subscriber is

```
i) the Subject of the Code Signing Certificate and
ii) the entity responsible for distributing the software, but does not
necessarily hold the copyright to the software.
```

Subscriber Agreement: An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.

Subsidiary Company: A company that is controlled by a Parent Company.

Suspect code: Code that contains malicious functionality or serious vulnerabilities, including spyware, malware and other code that installs without the user's consent and/or resists its own removal, and code that can be exploited in ways not intended by its designers to compromise the trustworthiness of the platforms on which it executes.

Takeover Attack: An attack where a Signing Service or Private Key associated with a Code Signing Certificate has been compromised by means of fraud, theft, intentional malicious act of the Subject's agent, or other illegal conduct

Technically Constrained Subordinate CA Certificate: A Subordinate CA certificate which uses a combination of Extended Key Usage settings and Name Constraint settings to limit the scope within which the Subordinate CA Certificate may issue Subscriber or additional Subordinate CA Certificates.

Terms of Use: Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with these Requirements when the Applicant/Subscriber is an Affiliate of ThaiCA or is TKC.

Test Certificate: A Certificate with a maximum validity period of 30 days and which: (i) includes a critical extension with the specified Test Certificate CABF OID (2.23.140.2.1), or (ii) is issued under a CA where there are no certificate paths/chains to a root certificate subject to the Baseline Requirements.

Timestamp Authority: An organization that timestamps data, thereby asserting that the data existed at the specified time.

Unregistered Domain Name: A Domain Name that is not a Registered Domain Name.

Valid Certificate: A Certificate that passes the validation procedure specified in RFC 5280.

Validation Specialist: Someone who performs the information verification duties specified in this CP/CPS.

Validity Period: As defined within RFC 5280, Section 4.1.2.5: the period of time from notBefore through notAfter, inclusive.

WebTrust Program for CAs: The AICPA/CPA Canada WebTrust Program for Certification Authorities.

WebTrust Seal of Assurance: An affirmation of compliance resulting from the WebTrust Program for CAs.

WHOIS: information retrieved directly from the Domain Name Registrar or registry operator via the protocol defined in RFC 3912, the Registry Data Access Protocol defined in RFC 7482, or an HTTPS website.

Wildcard Certificate: A Certificate containing at least one Wildcard Domain Name in the Subject Alternative Names in the Certificate.

Wildcard Domain Name: A string starting with "*." (U+002A ASTERISK, U+002E FULL STOP) immediately followed by a Fully-Qualified Domain Name.

XN-Label: From RFC 5890 (http://tools.ietf.org/html/rfc5890): "The class of labels that begin with the prefix `"xn--"` (case independent), but otherwise conform to the rules for LDH labels."

1.6.2 Acronyms

Short Term	Explained Term
ADN	Authorization Domain Name
AI	Artificial Intelligence
CA	Certification Authority
CAA	Certification Authority Authorization
CCADB	Common CA Database
ccTLD	Country Code Top-Level Domain
CP	Certificate Policy
CPA	Chartered Professional Accountant
CP/CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSO	Chief Security Officer
CSR	Certificate Signing Request
CT	Certificate Transparency
DN	Distinguished Name
EKU	Extended Key Usage
EV	Extended Validation
EVCP	Extended Validation Certificates Policy
FIPS	United States Federal Information Processing Standards
FQDN	Fully-Qualified Domain Name
gTLD	Generic Top-Level Domain
HSM	Hardware Security Module
HTTP	Hyper Text Transfer Protocol
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers

Short Term	Explained Term
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ISP	Internet Service Provider
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
OCSP	On-line Certificate Status Protocol
OID	International Standards Organization's Object Identifier
OVCP	Organizational Validation Certificates Policy
PIN	Personal identification number
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PKIX	IETF Working Group on PKI
PMA	Policy Management Authority
RA	Registration Authority
SHA	Secure Hashing Algorithm
S/MIME	Secure multipurpose Internet mail extensions
SSL	Secure Socket Layer
subCA	Subordinate Certification Authority
TLD	Top Level Domain
TLS	Transport Layer Security
URL	Uniform Resource Locator
X.509	ITU-T standard for Certificates and authentication framework

1.6.3 References

The definitions, acronyms and terminology used in the ThaiCA CP/CPS may draw from the documents and publications listed below:

Document	Title
RFC 822	Standard For the Format of ARPA Internet Text Messages
RFC 2119	Key words for use in RFCs to Indicate Requirement Levels
RFC 2527	Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework
RFC 3161	Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)
RFC 3492	Punycode: A Bootstring encoding of Unicode for Internationalized Domain Names in Applications (IDNA)
RFC 3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
RFC 3912	WHOIS Protocol Specification
RFC 3986	Punycode: Uniform Resource Identifier (URI): Generic Syntax
RFC 4210	Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)
RFC 4366	Transport Layer Security (TLS) Extensions
RFC 5019	The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments
RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
RFC 5890	Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework
RFC 5952	A Recommendation for IPv6 Address Text Representation
RFC 6454	The Web Origin Concept
RFC 6960	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
RFC 6962	Certificate Transparency
RFC 7231	Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content
RFC 7482	Registration Data Access Protocol (RDAP) Query Format
RFC 7538	The Hypertext Transfer Protocol Status Code 308 (Permanent Redirect)
RFC 8499	DNS Terminology

Document	Title
RFC 8659	Request for Comments: 8659, DNS Certification Authority Authorization (CAA) Resource Record
X.509v3	ITU-T Recommendation X.509 (2005) ISO/IEC 9594-8:2005, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks

The ThaiCA CP/CPS also observes the most current versions of the following documents:

Document	Link
Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates	https://cabforum.org/baseline-requirements-documents/
Guidelines For The Issuance And Management Of Extended Validation Certificates	https://cabforum.org/extended-validation/
Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates	https://cabforum.org/baseline-requirements-code-signing/
Network and Certificate System Security Requirements	https://cabforum.org/network-security/

1.6.4 Conventions

Terms not otherwise defined in this document shall be defined in applicable agreements, user manuals, Certificate Policies and Certification Practice Statements, of TKC.

1.6.4.1 Definitions per RFC 2119

The key words “must”, “must not”, “required”, “shall”, “shall not”, “should”, “should not”, “recommended”, “may”, and “optional” in these documents shall be interpreted in accordance with RFC 2119.

2 TKC DOCUMENTS AND REPOSITORY

2.1 Repositories

TKC maintains a central Repository to allow access to documents related to TKC's policies and practices, including this CP/CPS, Subscriber and Relying Party agreements and root Certificates. TKC's central Repository is available at https://www.thaica.com/repository.

TKC's central Repository is maintained with resources sufficient to provide a commercially reasonable response time for access at all times. Distributed repositories that include at least the same type of information as the central repository may also exist.

2.1 Publication of certification information

CRL distribution points are included in intermediate and end-entity Certificates. CRLs and OCSP services are publicly available online.

2.1.1 TKC PKI CP/CPS

The ThaiCA CP/CPS shall always be publicly accessible in the ThaiCA Repository.

2.1.2 Certificate Revocation List and On-line Certificate Status Protocol

TKC maintains Certificate Revocation Lists (CRLs) and Online Certificate Status Protocol (OCSP) responders as public resources which provide Relying Parties with pertinent information regarding the validity or current status of an ThaiCA certificate. CRL distribution points are included in intermediate and end-entity Certificates. CRLs and OCSP services are publicly available online.

2.1.2.1 CRLs

CRLs maintained by ThaiCA contain lists of serial numbers for all revoked, un-expired Certificates issued by TKC. These lists adhere to the standards set out in RFC 5280 for X.509 Certificate Revocation Lists. ThaiCA maintains CRLs as described in Sections 4.9.7, 4.9.8 and 4.10 of this CP/CPS.

2.1.2.2 OCSP

OCSP is part of TKC's Repository and documents all relevant status information for each certificate issued by TKC. This status information is presented by TKC's OCSP responding server(s) (also known as the OCSP responder). This resource adheres to the standards set out in RFC 6960. See also Sections 4.9.9, 4.9.10 and 4.10 of this CP/CPS.

2.1.3 TKC Certificate Subscriber Agreement

A copy of the latest ThaiCA Certificate Subscriber Agreement is available in the ThaiCA repository (https://www.thaica.com/repository).

2.1.4 TKC Relying Party Agreement and Warranty

A copy of the latest ThaiCA Certificate Relying Party Agreement and ThaiCA Relying Party Warranty are available in the ThaiCA repository at https://www.thaica.com/repository/relying-party-agreement and https://www.thaica.com/repository/relying-party-warranty, respectively.

2.1.5 TKC Root and Intermediate Certificates

All CA Certificates utilized by the ThaiCA PKI are available in the ThaiCA Repository listed in Section 2.1.

2.1.6 Audit Reports

Copies of auditor report letters certification and other relevant statuses, are available in the ThaiCA Repository listed in Section 2.1.

2.1.7 Disclosure of Verification Sources

The ThaiCA Repository contains agency information about the Incorporating Agency or Registration Agency used to validate certificates

This agency information SHALL include at least the following:

- Sufficient information to unambiguously identify the Incorporating Agency or Registration Agency (such as a name, jurisdiction, and website); and,
- The accepted value or values for each of the `subject:jurisdictionLocalityName` (OID: 1.3.6.1.4.1.311.60.2.1.1), `subject:jurisdictionStateOrProvinceName` (OID: 1.3.6.1.4.1.311.60.2.1.2), and `subject:jursidictionCountryName` (OID: 1.3.6.1.4.1.311.60.2.1.3) fields, when a certificate is issued using information from that Incorporating Agency or Registration Agency, indicating the jurisdiction(s) that the Agency is appropriate for; and,
- The acceptable form or syntax of Registration Numbers used by the Incorporating Agency or Registration Agency, if ThaiCA restricts such Numbers to an acceptable form or syntax; and,
- A revision history that includes a unique version number and date of publication for any additions, modifications, and/or removals from this list.

2.1.8 Other ThaiCA Legal Documents

The ThaiCA repository contains copies of the following ThaiCA legal documents:

- Terms of Service
- Privacy Policy

2.1.9 Documents not included in the ThaiCA Repository

TKC does not make publicly available documents or elements of documents deemed as internal, which include security controls, internal security polices, etc. However, these documents are fully disclosed in audits associated with any formal accreditation process that ThaiCA adheres to.

2.2 Time or Frequency of Publication

2.2.1 Frequency of Publication of Certificates

Certificate information is published immediately upon acceptance by the Subscriber or when a Certificate is revoked. More information is available in Section 4.4.2.

2.2.2 Frequency of Publication of CRLs

Frequency of CRL updating and publication is described in Section 4.9.7

2.2.3 Frequency of Publication of CP/CPS, Terms & Conditions

The ThaiCA CP/CPS will be revised and/or amended, and the updated document published, as described in Section 1.5.4.

2.2.4 Notification of major changes

Major changes to any documents, agreements and resources will be clearly noted in the relevant item when published. ThaiCA reserves the right to make minor changes to any item in the Repository if such changes do not substantially affect or modify ThaiCA PKI operations, practices and policies. More information is available in Section 9.12.3.

2.3 Access Controls on Repositories

All online repositories described in Section 2.2 are publicly and anonymously available on the Internet with read-only access. Only authorized entities within ThaiCA have rights to perform modification to documents in these repositories. Restrictions and access-controls are applied to public repositories for protection against enumeration and Denial of Service attacks.

Any participant in the ThaiCA PKI (including Applicants, Subscribers and Relying Parties) shall have unlimited read-only access to any item in the ThaiCA Repository.

Any participant in the ThaiCA PKI accessing the ThaiCA Repository and/or other ThaiCA directory resources are deemed to have agreed with the provisions of the ThaiCA CP/CPS and to any other conditions of usage that ThaiCA makes available.

3 NAMING, IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Type of names

All ThaiCA Certificates adhere to rules for naming and identification, and (except as specifically detailed in the profile for that certificate type) shall require a Distinguished Name that is in compliance with the ITU X.500 standard for Distinguished Names (DN). Names shall be interpreted using the X.500 and RFC822 standards.

3.1.2 Need for names to be meaningful, unambiguous and unique

Names submitted to ThaiCA during the certificate application process must be meaningful, unambiguous, and unique.

Certificates issued by ThaiCA will utilize a meaningful, unambiguous, and unique Distinguished Name (DN). The only exception to this practice shall be for products with a profile specifically detailed to utilize other naming methodology (see Section 7). Otherwise, all Certificates issued by ThaiCA will utilize a meaningful, unambiguous, and unique Distinguished Name (DN).

In cases where the Common Name (CN) or any other element would produce an ambiguous or non-unique DN, or where for any reason a CN is not present, ThaiCA will utilize a unique ID and/or serial integer to clearly identify a certificate as unique.

3.1.3 Anonymous, pseudonymous and role-based Certificates

TKC does not allow Certificates to be issued with anonymous or pseudonymous Subscriber information. However, for IDNs, ThaiCA may include the Punycode version of the IDN as a Subject Name.

TKC may allow Certificates to include role-based Subscriber information. This information must be verified, validated, and must be submitted along with other verified Subscriber information included in the Subject Identity Information field.

3.1.4 Rules for interpreting various name forms

TKC Certificates shall be issued with Distinguished Names interpreted using X.500 standards and ASN.1 syntax.

3.1.5 Uniqueness of names

The full combination of the Subject Attributes (Distinguished name) has to be unique in TKC's PKI. Depending on the type of certificate (SSL, S/MIME, Code Signing), different elements/attributes of the certificate ensure uniqueness.

3.1.6 Recognition, authentication, and role of trademarks

Applicants agree by submitting a certificate request to ThaiCA that their request does not contain data which in any way interferes with or infringes upon the rights of any third parties in any jurisdiction with respect to trademarks, service marks, trade names, company names, "doing business as" (DBA) names, or any other intellectual property right, and that they are not presenting the data for any unlawful purpose whatsoever. Data covered by this agreement includes but is not limited to any domain name, domain name space, Distinguished Name (DN), or Fully-Qualified Domain Name (FQDN), and/or any trade name or DBA name, contained in any portion of the certificate request.

If the certificate is to include a DBA or trade name in any field whatsoever, ThaiCA shall verify the Applicant's right to use the DBA or trade name using the steps detailed in Section 4.2.

Applicants requesting ThaiCA Certificates shall be responsible for the legality of the information they present for verification and/or use in Certificates for any jurisdiction in which such content may be used or viewed.

Any certificate issued using information which is deemed to violate Section 3.1.6 may be revoked by TKC.

Subscribers shall defend, indemnify, and hold ThaiCA harmless for any loss or damage resulting from any interference or infringement upon the rights of third parties and shall be responsible for defending all actions against TKC.

3.2 Initial identity validation

A valid certificate request shall establish possession of the Private Key related to the request. All requests for Certificates sent to ThaiCA must be verified at the level of assurance appropriate to the certificate requested.

TKC shall inspect any document relied upon for verification for alteration or falsification. ThaiCA shall verify the identity and status of any Applicant as appropriate and required for the certificate requested. Alteration or falsification of any document used in this process, and/or falsification or misrepresentation of the identity or status of any Applicant and/or organization referenced in this process, shall constitute grounds for disapproval of a certificate request and/or immediate revocation of any existing certificate relying upon altered or falsified documents or false or misrepresented identity or status.

3.2.1 Method to prove possession of Private Key

Any Applicant for any ThaiCA certificate must submit a Certificate Signing Request (CSR). This establishes that the Applicant holds the Private Key corresponding to the Public Key to be included in the requested certificate.

This requirement does not apply when a Key Pair is generated by ThaiCA on behalf of a Subscriber . In these cases ThaiCA shall ensure control of Key Pairs as described in 6.2.1.

3.2.2 Authentication of organization identity

Requests for Certificates which include an organization identity shall be verified using the criteria described below. Items to be verified include the legal existence, legal name, assumed name, legal form and requested address of the organization, and the authority of the requesting party shall be confirmed. ThaiCA shall inspect any document relied upon for these purposes for alteration or falsification.

In particular, whenever validation steps of this section require the use of documentation obtained by an Incorporating Agency or Registration Agency, ThaiCA uses only agencies included in its approved, at time of issuance, List of Approved Incorporating and Registration Agencies, which is publicly available at https://www.thaica.com/repository. See section 2.2.8.

3.2.2.1 Identity

If the Subject Identity Information is to include the name or address of an organization, ThaiCA shall verify the identity and address of the Applicant. This verification shall use documentation provided by, or through communication with, at least one of the following:

1. A government agency or Incorporating Agency or Registration 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 as defined in Section 3.2.2.7;
3. A site visit by ThaiCA or a third party who is acting as an agent for TKC; or
4. An Attestation Letter, as defined in Section 1.6.1

TKC may use the same documentation or communication described in 1) through 4) above to verify both the Applicant's identity and address.

Alternatively, ThaiCA may verify the address of the Applicant (but not the identity of the Applicant) using a utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that ThaiCA determines to be reliable.

3.2.2.2 DBA/Trade Name

If the Subject Identity Information is to include a DBA or trade name, ThaiCA shall verify the Applicant's right to use the DBA/trade name with at least one of the following criteria:

1. Documentation provided by, or communication with, government agency or Incorporating Agency or Registration Agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;
2. A Reliable Data Source as defined in Section 3.2.2.7;
3. Communication with a government agency responsible for the management of such DBAs or trade names;
4. An Attestation Letter accompanied by verifying practitioner credentials; or
5. A utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that ThaiCA determines to be reliable.

Use of a DBA or trade name is governed by and further described in Section 3.1.6.

3.2.2.3 Verification of Country

If the subject:countryName field is present, then ThaiCA 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.

3.2.2.4 Validation of Domain Authorization or Control

This Section defines the permitted processes and procedures for validating the Applicant's ownership or control of the domain.

TKC shall confirm that, prior to the date of Certificate issuance, ThaiCA has validated each Fully-Qualified Domain Name (FQDN) listed in the Certificate using at least one of the methods listed below.

TKC shall confirm that prior to issuance, ThaiCA has validated each Fully-Qualified Domain Name (FQDN) listed in the Certificate as follows:

1. When the FQDN is not an Onion Domain Name, ThaiCA SHALL validate the FQDN using at least one of the methods listed below; and

2. When the FQDN is an Onion Domain Name, ThaiCA SHALL validate the FQDN in accordance with Appendix B of the "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" document.

Completed confirmations of Applicant authority may be valid for the issuance of multiple certificates over time. In all cases, the confirmation 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.

TKC shall maintain a record of which domain validation method was used to validate each domain, including the relevant Baseline Requirements version number applicable.

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

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

TKC 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.

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

Each email, fax, SMS, or postal mail MAY confirm control of multiple Authorization Domain Names.

TKC 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.

TKC 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.

3.2.2.4.2 Phone Contact with Domain Contact

This method is not allowed.

3.2.2.4.3 Constructed Email to Domain Contact

TKC shall confirm the Applicant's control over the FQDN by (i) 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, (ii) including a Random Value in the email, and (iii) receiving a confirming response utilizing the Random Value.

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

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.

3.2.2.4.4 Agreed-Upon Change to Website

This method is not allowed.

3.2.2.4.5 DNS Change

TKC shall confirm the Applicant's control over the FQDN by confirming the presence of a Random Value or Request Token in a DNS CNAME, TXT or CAA record for either i) an Authorization Domain Name or ii) an Authorization Domain Name that is prefixed with a Domain Label that begins with an underscore character.

If a Random Value is used, ThaiCA 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 (such as in Section 4.2.1 of this CP/CPS).

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

3.2.2.4.6 IP Address

TKC 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.

Note: Once the FQDN has been validated using this method, ThaiCA SHALL NOT also issue Certificates for other FQDNs that end with all the Domain Labels of the validated FQDN, unless ThaiCA performs a separate validation for that FQDN using an authorized method. This method is NOT suitable for validating Wildcard Domain Names.

3.2.2.4.7 Test Certificate

This method is not allowed.

3.2.2.4.8 Validating Applicant as a Domain Contact

[Reserved]

3.2.2.4.9 Email to DNS CAA Contact

[Reserved]

3.2.2.4.10 Email to DNS TXT Contact

TKC 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 a 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.

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

3.2.2.4.11 Phone Contact with Domain Contact

TKC 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 Authorization Domain Name. Each phone call MAY confirm control of multiple Authorization Domain Names provided that the same Domain Contact phone number is listed for each Authorization Domain Name being verified and they provide a confirming response for each Authorization Domain Name.

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

In the event of reaching voicemail, ThaiCA may leave the Random Value and the Authorization Domain Name(s) being validated. The Random Value MUST be returned to ThaiCA 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.

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

3.2.2.4.12 Phone Contact with DNS TXT Record Phone Contact

TKC 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 Authorization Domain Name. Each phone call MAY confirm control of multiple Authorization Domain Names provided that the same DNS TXT Record Phone Contact phone number is listed for each Authorization Domain Name being verified and they provide a confirming response for each Authorization Domain Name.

This call from ThaiCA MAY NOT knowingly be transferred or requested to be transferred, as this phone number has been specifically listed for the purposes of Domain Validation.

In the event of reaching voicemail, ThaiCA may leave the Random Value and the Authorization Domain Name(s) being validated. The Random Value MUST be returned to ThaiCA 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.

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

3.2.2.4.13 Phone Contact with DNS CAA Phone Contact

TKC 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 8659 Section 3.

TKC 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, ThaiCA may leave the Random Value and the ADN(s) being validated. The Random Value MUST be returned to ThaiCA 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.

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

3.2.2.4.14 Agreed-Upon Change to Website v2

Confirming 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. TKC 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 ThaiCA follows redirects, the following apply:

1. Redirects MUST be initiated at the HTTP protocol layer.
    i. For validations performed on or after July 1, 2021, redirects MUST be the result of a 301, 302, or 307 HTTP status code response, as defined in RFC 7231, Section 6.4, or a 308 HTTP status code response, as defined in RFC 7538, Section 3. Redirects MUST be to the final value of the Location HTTP response header, as defined in RFC 7231, Section 7.1.2.
    ii. For validations performed prior to July 1, 2021, 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.
2. Redirects MUST be to resource URLs with either the “http” or “https” scheme.
3. Redirects MUST be to resource URLs accessed via Authorized Ports.

If a Random Value is used, then:

1. TKC 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.

Note:

- For Certificates issued prior to 2021-09-01, ThaiCA MAY also issue Certificates for other FQDNs that end with all the Domain Labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.
- For Certificates issued on or after 2021-09-01, ThaiCA MUST NOT issue Certificates for other FQDNs that end with all the Domain Labels of the validated FQDN unless it performs a separate validation for that FQDN using an authorized method. This method is NOT suitable for validating Wildcard Domain Names.

3.2.2.4.15 Agreed-Upon Change to Website - ACME

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.

TKC 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.

If ThaiCA follows redirects, the following apply:

1. Redirects MUST be initiated at the HTTP protocol layer.

    i. For validations performed on or after July 1, 2021, redirects MUST be the result of a 301, 302, or 307 HTTP status code response, as defined in RFC 7231, Section 6.4, or a 308 HTTP status code response, as defined in RFC 7538, Section 3. Redirects MUST be to the final value of the Location HTTP response header, as defined in RFC 7231, Section 7.1.2.

    ii. For validations performed prior to July 1, 2021, 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.

2. Redirects MUST be to resource URLs with either the “http” or “https” scheme.

3. Redirects MUST be to resource URLs accessed via Authorized Ports.

Note:

- For Certificates issued prior to 2021-09-01, ThaiCA MAY also issue Certificates for other FQDNs that end with all the Domain Labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.
- For Certificates issued on or after 2021-09-01, ThaiCA MUST NOT issue Certificates for other FQDNs that end with all the Domain Labels of the validated FQDN unless it performs a separate validation for that FQDN using an authorized method. This method is NOT suitable for validating Wildcard Domain Names.

3.2.2.4.16 TLS Using ALPN

[Reserved]

3.2.2.5 Authentication for an IP Address

TKC SHALL confirm that prior to issuance, ThaiCA has validated the Applicant’s ownership or control of each IP Address listed in a 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 Section 4.2.1 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, ThaiCA SHALL maintain a record of which IP validation method, including the relevant BR version number, was used to validate every IP Address.

Note: IP Addresses verified in accordance with this section 3.2.2.5 may be listed in Subscriber Certificates as defined in section 7.1.4.2 or in Subordinate CA Certificates via iPAddress in permittedSubtrees within the Name Constraints extension. ThaiCA is not required to verify IP Addresses listed in Subordinate CA Certificates via iPAddress in

excludedSubtrees in the Name Constraints extension prior to inclusion in the Subordinate CA Certificate.

3.2.2.5.1 Agreed-Upon Change to Website

TKC SHALL confirm the Applicant's control over the requested IP Address by confirming the presence of a Request Token or Random Value contained in the content of a file or webpage in the form of a meta tag under the "/.well-known/pki-validation" directory, or another path registered with IANA for the purpose of validating control of IP Addresses, on the IP Address that is accessible by ThaiCA via HTTP/HTTPS over an Authorized Port. The Request Token or Random Value MUST NOT appear in the request.

If a Random Value is used, ThaiCA SHALL provide a Random Value unique to the certificate request and SHALL not use the Random Value after the longer of (i) 30 days or (ii) if the Applicant submitted the certificate request, the timeframe permitted for reuse of validated information relevant to the certificate (see Section 4.2.1).

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

TKC SHALL confirm the Applicant's control over the IP Address 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 an IP Address Contact.

Each email, fax, SMS, or postal mail MAY confirm control of multiple IP Addresses.

TKC 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 IP Address Registration Authority as representing the IP Address Contact for every IP Address being verified using the email, fax, SMS, or postal mail.

The Random Value SHALL be unique in each email, fax, SMS, or postal mail.

TKC 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.

3.2.2.5.3 Reverse Address Lookup

TKC SHALL confirm the Applicant's control over the IP Address by obtaining a Domain Name associated with the IP Address through a reverse-IP lookup on the IP Address and then verifying control over the FQDN using a method permitted under Section 3.2.2.4.

3.2.2.5.4 Any Other Method

This method has been retired and MUST NOT be used.

3.2.2.5.5 Phone Contact with IP Address Contact

TKC SHALL confirm the Applicant's control over the IP Address by calling the IP Address Contact's phone number and obtaining a response confirming the Applicant's request for validation of the IP Address. ThaiCA MUST place the call to a phone number identified by the IP Address Registration Authority as the IP Address Contact. Each phone call SHALL be made to a single number.

In the event that someone other than an IP Address Contact is reached, ThaiCA MAY request to be transferred to the IP Address Contact.

In the event of reaching voicemail, ThaiCA may leave the Random Value and the IP Address(es) being validated. The Random Value MUST be returned to ThaiCA 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.

3.2.2.5.6 6 ACME "http-01" method for IP Addresses

TKC SHALL confirm the Applicant's control over the IP Address by performing the procedure documented for an "http-01" challenge in draft 04 of "ACME IP Identifier Validation Extension," available at https://tools.ietf.org/html/draft-ietf-acme-ip-04#section-4.

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

TKC SHALL confirm the Applicant's control over the IP Address by performing the procedure documented for a "tls-alpn-01" challenge in draft 04 of "ACME IP Identifier Validation Extension," available at https://tools.ietf.org/html/draft-ietf-acme-ip-04#section-4.

3.2.2.6 Wildcard Domain Validation

TKC shall follow specific practices to validate any certificate containing a wildcard character (*).

Before issuing a Wildcard Certificate, ThaiCA shall determine if the FQDN portion of any Wildcard Domain Name in the Certificate is "registry-controlled" or is a "public suffix" (e.g. "*.com", "*.co.uk", see RFC 6454 Section 8.2 for further explanation).

If the FQDN portion of any Wildcard Domain Name is "registry-controlled" or is a "public suffix", ThaiCA SHALL NOT issue a Certificate unless the Applicant proves its rightful control of the entire Domain Namespace. (e.g. ThaiCA SHALL NOT issue "*.co.uk" or "*.local", but MAY issue "*.example.com" to Example Co.).

In all such cases, ThaiCA shall observe stipulations and considerations as given in RFC 6454 Section 8.2.

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. ThaiCA follows the current best practice and consults the Public Suffix List (PSL), and regularly retrieves a fresh copy.

3.2.2.7 Data Source Accuracy

Prior to using any data source as a Reliable Data Source, ThaiCA shall evaluate the source for its reliability, accuracy, and resistance to alteration or falsification.

Criteria for this evaluation shall include:

- The age of the information provided
- The frequency of updates to the information source
- The data provider and purpose of the data collection
- The public accessibility of the data availability, and
- The relative difficulty in falsifying or altering the data.

3.2.2.8 CAA Records

As part of the Certificate issuance process, ThaiCA MUST retrieve and process CAA records in accordance with RFC 8659 for each `dNSName` in the `subjectAltName` extension that does not contain an Onion Domain Name. If ThaiCA issues, it shall take place within the TTL of the CAA record, or 8 hours, whichever is greater.

This stipulation does not prevent ThaiCA from checking CAA records at any other time.

When processing CAA records, ThaiCA must process the issue, issuewild, and iodef property tags as specified in RFC 8659, although they are not required to act on the contents of the iodef property tag. Additional property tags may be supported, but must not conflict with or supersede the mandatory property tags set out in this document. ThaiCA must respect the critical flag and not issue a certificate if they encounter an unrecognized property with this flag set.

RFC 8659 requires that a CA "MUST NOT issue a certificate unless the CA determines that either (1) the certificate request is consistent with the applicable CAA RRset or (2) an exception specified in the relevant CP or CPS applies." For issuances conforming to this CP/CPS, ThaiCA must not rely on any exceptions specified in this CP/CPS unless they are one of the following:

1. 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.
2. 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.

3. For certificates issued prior to July 1, 2021, CAA checking is optional if ThaiCA or an Affiliate of ThaiCA is the DNS Operator (as defined in RFC 7719) of the domain's DNS.

TKC is permitted to treat a record lookup failure as permission to issue if:

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

TKC 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. ThaiCA is not expected to support URL schemes in the iodef record other than mailto: or https:.

3.2.2.9 Validation of Email Address Control

Where required, ThaiCA or an RA may verify an Applicant's control of any email address listed in a certificate via one of the methods listed in the following subsections.

TKC SHALL NOT delegate validation of the domain portion of an email address.

3.2.2.9.1 Validation the email address recipient

TKC shall confirm the Applicant's control over the email address by sending an email to that address which includes a Random Value, and receiving a confirming response utilizing the Random Value.

Each email SHALL confirm control of a single email address.

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.

3.2.2.9.2 Validating the domain part of an email address

TKC MAY confirm control of an email address by validating the domain part of an email address, using the domain validation methods as described in section 3.2.2.4.

An Applicant that confirms control of the domain part of an email address is authorized for any local part followed by the at-sign ("@"), followed by the Authorization Domain Name or by any other Domain Name that ends with all the Domain Labels of the validated Authorization Domain Name.

3.2.2.9.3 Any other method

Using any other method of confirmation, including variations of the methods defined in section 3.2.2.9, provided that ThaiCA maintains documented evidence that the method of confirmation establishes that the Applicant has control over the email address to at least the same level of assurance as the methods described in section 3.2.2.9.

3.2.3 Authentication of individual identity

3.2.3.1 Natural Person as an individual Applicant

If an Applicant is a natural person applying as an individual, then ThaiCA shall verify the Applicant's name and the authenticity of the certificate request. For Server Authentication certificates, Code Signing certificates, or when the Applicant's address is displayed in the SubjectDN of the certificate, ThaiCA shall also verify the Applicant's address.

For server certificates, verification shall be through one or more of the methods described in the Baseline Requirements.

For Code Signing certificates, verification shall be through one or more of the methods described in the Minimum Requirements for Code Signing.

For Document Signing Certificates, ThaiCA shall rely on strong identity proofing, based on a face to face meeting with the Applicant, or a procedure that provides an equivalent assurance. The latter may include any of the following:

- means of secure video communication;
- use of identity verification software/AI;
- hybrid or other methods.

3.2.3.2 Natural Person associated with a Legal Entity

For Document Signing, S/MIME and Client Authentication Certificates issued to Natural Persons associated with Legal Entities, TKC

- shall validate the Legal Entity following the requirements of section 3.2.2.1;
- shall obtain evidence that the individual is associated with the Legal Entity.

For Document Signing Certificates, ThaiCA shall perform identity verification of individual natural persons associated with that Legal Entity following the requirements of section 3.2.3.1. For S/MIME and Client Authentication Certificates, ThaiCA may also rely on the Legal Entity to perform identity verification of individual natural persons associated with that Legal Entity.

3.2.4 Non-verified information

TKC does not verify information contained in the Organization Unit (OU) field in any certificate request, and only ensures that the OU attribute meets the requirements described

in 7.1.4.2.2 i. Other information may be designated as non-verified in specific certificate profiles. Non-verified information other than the OU field will be detailed in the certificate profile and in the verification process for that certificate type as given in Section 4.

3.2.5 Validation of authority

TKC shall verify the authorization of all certificate requests.

For server certificate requests, verification of this authority shall be through one or more of the methods described in the Baseline Requirements.

For Code Signing certificate requests, verification of this authority shall be through one or more of the methods described in the Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates.

3.2.6 Criteria for interoperation

TKC shall issue cross-Certificates as required in order to assist root roll-over operations. This shall only apply in cases where all Subordinate CAs remain under control of TKC.

3.3 Identification and authentication for re-keying

Re-keying (sometimes called reissuing) refers to the creation of an entirely new certificate, using some or all of the information submitted for an existing certificate and using a newly generated Private Key. Subscribers may request re-keying of an ThaiCA certificate prior to the certificate's expiration. Subordinate CAs of ThaiCA may request re-keying of a certificate registered by them prior to the certificate's expiration. The re-keying process is detailed fully in Section 4.7.

3.3.1 Re-keying request by Subscriber

3.3.1.1 Subscriber re-keying request via ThaiCA Account Dashboard

A Subscriber may request re-key of any unexpired ThaiCA certificate via their ThaiCA Account Dashboard. Any changes made when requesting re-keying by this method may require validation and/or authentication steps as described in Section 4.7.

3.3.1.2 Subscriber re-keying request via other means

A Subscriber requesting re-keying of an unexpired ThaiCA certificate by any method other than their ThaiCA Account Dashboard requires validation and/or authentication steps as described in Section 4.7.

3.3.2 Identification and authentication for re-key after revocation

A Subscriber requesting re-key of an ThaiCA certificate after that certificate has been revoked will need to apply for and follow all validation and/or authentication procedures for a new certificate.

3.4 Identification and authentication for revocation requests

TKC may revoke any certificate issued within the ThaiCA PKI at its sole discretion. In all cases, identification and/or authorization for a revocation request must follow the procedures detailed in Section 4.9.3.

3.4.1 Identification and authentication for revocation requests by Subscribers

A Subscriber, or the Subscriber's authorized agent, may request revocation of any unexpired ThaiCA certificate via their ThaiCA Account Dashboard.

Revocation requests from a Subscriber or authorized agent for an unexpired ThaiCA certificate by any method other than their ThaiCA Account Dashboard may, at TKC's sole discretion, require further validation and/or authentication steps as described in Section 4.9.

TKC may, if necessary, and at its sole discretion, confirm a revocation request by other means, including (but not limited to) contact with the Subscriber or authorized representatives of the Subscriber.

3.4.2 Revocation requests by non-Subscribers

Non-Subscribers (such as Relying Parties, Application Software Suppliers, and other third parties) may file a Certificate Revocation Request in order to register:

- Complaints related to certificate issuance
- Suspected Private Key compromise
- Certificate misuse
- Other types of fraud, compromise, misuse, or inappropriate conduct related to the certificate.

Non-Subscriber Certificate Revocation Requests must follow the procedures detailed in Section 4.9.3.

3.4.3 Identification and authentication for revocation requests by other participants in the ThaiCA PKI

A revocation request for an TKC-issued certificate by any other authorized participant in the ThaiCA PKI (such as a Subordinate CA or external RA) shall be identified and/or authenticated by that authorized participant.

Identification and/or authorization for a revocation request must in all cases follow the procedures detailed in Section 4.9.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

This chapter specifies the policy, procedures and requirements for the management of Certificates across the entire life cycle, including:

- Application processing
- Certificate issuance
- Certificate acceptance
- Key pair and certificate usage
- Certificate re-issuance
- Certificate renewal
- Certificate re-key
- Certificate modification
- Certificate revocation and suspension
- Certificate status services
- End of subscription
- Key escrow and recovery

Any request to re-issue a certificate without changing the expiration date (the `validTo` field) and the Subject Information (the `Subject Distinguished Name` field), shall be defined as a "re-issuance" and addressed in Section 4.2.5.

Any request to re-issue a certificate without changing the Public Key or any other information, with the sole exception of the expiration date (the `validTo` field), shall be defined as a "renewal" and addressed in Section 4.6.

Any request to change the Key Pair in a certificate shall be defined as "re-keying" and addressed in Section 4.7. Note that, apart from the Key Pair, any other information (such as the CN, SAN entries, email addresses etc.) may also be changed in the re-key process.

Any request to change any information in a certificate (such as the CN, SAN entries, email addresses etc.), without changing the Public Key, shall be defined as "modification" and addressed in Section 4.8.

TKC's PKI operations follow the Certificate Management Protocol (CMP) as defined in RFC 4210.

4.1 Certificate Application

4.1.1 Who may submit a certificate application

Either the Applicant or an authorized Certificate Requester may submit certificate requests. Applicants are responsible for the accuracy of any data submitted.

In all cases ThaiCA or any Enterprise RA shall require identification and authentication sufficient to meet the requirements relevant to the type of certificate requested.

TKC shall not issue Certificates to organizations or entities on a government denied list maintained by the Government of Thailand, or which is located in a country with which the laws of Thailand prohibit doing business.

4.1.2 Enrolment process and responsibilities

The enrolment process to obtain an ThaiCA certificate shall include:

- Applying for a certificate
- Generating a Key Pair
- Delivering the Public Key of the Key Pair to TKC
- Agreeing to the applicable Subscriber Agreement, and
- Paying any applicable fees

The order in which these events occur may vary, depending on the method used and product ordered.

4.1.2.1 Enrolment process for ThaiCA central RA

In most cases, a request for an ThaiCA certificate is made through the ThaiCA Account Dashboard. Any Applicant will be directed to log in to or create an ThaiCA account before any request shall be processed. A request submitted via the ThaiCA Account Dashboard is identified with the account holder and considered authentic.

TKC may, at its sole discretion, and on a case by case basis, accept requests which are not submitted via the Applicant's ThaiCA Account. Additional verification and/or authentication may be required for requests submitted outside of the ThaiCA Account Dashboard.

4.1.2.2 Enrolment process for Enterprise RAs

Any Enterprise RA authorized to use the ThaiCA PKI to issue Certificates must have appropriate processes in place to receive certificate requests, as detailed in chapter 3. Any Enterprise RA authorized to use the ThaiCA PKI may submit certificate requests by an authorized call to the ThaiCA API. Requests submitted to the ThaiCA CA by an enterprise RA must be digitally signed by the enterprise RA using a certificate issued by the ThaiCA CA for this purpose.

4.1.2.3 The Certificate Signing Request (CSR)

With the exception of ThaiCA generating Key Pairs on behalf of an Applicant as described in section 6.2.1, a valid Certificate Signing Request (CSR) must be created and submitted by the Applicant. A valid CSR will be derived from a Key Pair generated by the Applicant or the Applicant's agent. A valid CSR will incorporate the generated Public Key and other such information as is required to create the requested certificate.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

The Certificate request may include all factual information about the Applicant to be included in the Certificate, and such additional information as is required for ThaiCA to comply with this CP/CPS. In cases where the Certificate request does not contain all the necessary information about the Applicant, ThaiCA shall obtain the remaining information from the Applicant or, having obtained it from a reliable, independent, third-party data source, confirm it with the Applicant.

TKC maintains systems and processes to authenticate the identity of any Applicant, and follows documented procedures to verify all data requested for inclusion in the Certificate by the Applicant.

Initial identity verification and any additional validation required for specific certificate types shall follow the procedures detailed in Chapter 3.

Successful validation through these identification and authentication procedures must occur prior to issuance of any certificate.

Section 6.3.2 limits the validity period of Subscriber Certificates. ThaiCA may use the documents and data provided in Section 3.2 to verify certificate information, provided that ThaiCA obtained the data or document from a source specified under Section 3.2 no more than 825 days prior to issuing the Certificate. Effective 2021-09-30, for validation of Domain Names and IP Addresses according to Section 3.2.2.4 and 3.2.2.5, any reused data, document, or completed validation MUST be obtained no more than 397 days prior to issuing the Certificate.

In no case may a prior validation be reused if any data or document used in the prior validation was obtained more than the maximum time permitted for reuse of the data or document prior to issuing the Certificate.

TKC shall develop, maintain, and implement documented procedures that identify and require additional verification activity for High Risk Certificate Requests prior to the Certificate's approval, as reasonably necessary to ensure that such requests are properly verified under this CP/CPS.

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

4.2.2 Approval or rejection of certificate applications

Any certificate request which cannot be verified shall be rejected.

TKC SHALL NOT issue Certificates containing Internal Names or Reserved IP Addresses.

TKC reserves the right to reject any certificate application for any reason, including but not limited to:

- Correlation with previously revoked Certificates
- Correlation with previously rejected certificate requests
- Presence on a government denied list maintained by the United States or location in a country with which the laws of the United States prohibit doing business
- Insufficient, incorrect or inapplicable supporting documentation

TKC may reject the request for any certificate the issuance of which may harm, diminish or otherwise negatively impact TKC's business or reputation. ThaiCA shall be the sole determinant of what meets these criteria, and is not obligated to provide a reason for rejection of any Certificate Request.

TKC shall not issue new or replacement Code Signing Certificates to an entity that ThaiCA determined intentionally signed Suspect Code. ThaiCA shall keep meta-data about the reason for revoking a Code Signing Certificate as proof that the Code Signing Certificate was not revoked because the Applicant was intentionally signing Suspect Code.

TKC may issue new or replacement Code Signing Certificates to an entity who is the victim of a documented Takeover Attack, resulting in either a loss of control of their code-signing service or loss of the Private Key associated with their Code Signing Certificate.

If ThaiCA is aware that the Applicant was the victim of a Takeover Attack, ThaiCA MUST verify that the Applicant is protecting its Code Signing Private Keys under section 6.2.1. ThaiCA MUST verify the Applicant's compliance with section 6.2.1 (i) through technical means that confirm the Private Keys are protected using the method described in section 6.2.1 or (ii) by relying on a report provided by the Applicant that is signed by an auditor who is approved by ThaiCA and who has IT and security training.

Documentation of a Takeover Attack MAY include a police report (validated by TKC) or public news report that admits that the attack took place. The Subscriber MUST provide a report from an auditor with IT and security training that provides information on how the Subscriber was storing and using Private keys and how the intended solution for better security meets this CP/CPS for improved security.

Except where issuance is expressly authorized by the Application Software Supplier, ThaiCA MUST not issue new Code Signing Certificates to an entity where ThaiCA is aware that the entity has been the victim of two Takeover Attacks or where ThaiCA is aware that entity breached a requirement under this Section to protect Private Keys under Section 6.2.1.

Other than in the cases given above, ThaiCA shall approve any successfully validated certificate application which meets the criteria for the certificate requested.

4.2.3 Time to process certificate applications

TKC shall process certificate applications in a commercially reasonable time frame. ThaiCA shall not be responsible for delays in application processing resulting from action or inaction by the Applicant or the Applicant's agent, including omitted or incorrect details and/or documentation in the application. ThaiCA shall not be responsible for events outside of TKC's control which delay application processing.

4.2.4 Certificate Authority Authorization (CAA)

TKC supports CAA as described in Section 3.2.2.8. Subscribers who wish to authorize ThaiCA to issue Certificates for their FQDNs should include a CAA record property "issue" or "issuewild", including the value "TKC" in their respective DNS zone.

Subscribers who already have CAA entries in their respective DNS zone and need a Certificate from ThaiCA must add a CAA record property "issue" or "issuewild", including the value "TKC".

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Any RA, internal or external, utilizing TKC's PKI shall perform validation of all information sent before issuing any certificate.

Certificate issuance by a Root CA shall require an individual authorized by ThaiCA (i.e. the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command in order for the Root CA to perform a certificate signing operation.

4.3.2 Notification to Subscriber by the CA of issuance of Certificate

Any RA, internal or external, utilizing TKC's PKI shall notify the Subscriber of the successful issuance of a certificate. Notification shall be by email, using an email address provided by the Subscriber. Notification may, at TKC's sole discretion, be provided by other means as required. Notification shall also constitute acknowledgement that the certificate is available for review, access and download from the ThaiCA Account Dashboard correlating to the certificate ordered.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

The Subscriber or Subscriber's agent is responsible for review and verification of information contained in the issued certificate. The Subscriber or agent shall be deemed to have accepted the certificate:

- By downloading, installing or taking delivery by any other method of the certificate
- After 30 (thirty) days have passed from the communication of fulfilment.

4.4.2 Publication of the certificate by the CA

Any certificate issued by ThaiCA shall be published by email to the address corresponding to the Subscriber or agent requesting the certificate.

The certificate may also be published by other means, including:

- Publication to the corresponding ThaiCA Account
- Publication to a public repository, such as an x.500 or LDAP repository
- Publication to other entities as required by the ThaiCA PKI CP/CPS

4.4.3 Notification of certificate issuance by the CA to other Entities

Any RA, internal or external, may be notified regarding the issuance of a certificate. Notification may include transmission of the certificate by ThaiCA as the issuing CA to a corresponding Enterprise RA.

4.5 Key pair and certificate usage

4.5.1 Subscriber Private Key and certificate usage

Subscribers using any certificate issued through the ThaiCA PKI are required to protect the Private Key for that certificate, including:

- Securing the Private Key (and any copies made) to prevent disclosure or compromise
- Using the Private Key and/or certificate only as authorized by the relevant terms of service and/or Subscriber Agreement
- Ceasing use of the Private Key after expiration or revocation of the associated certificate
- Contacting the issuing entity if the Private Key is compromised
- Using the certificate only as applicable and for the intended purpose (per the key usage field of that certificate)

Subscribers requesting or utilizing Document Signing, Code Signing Certificates must observe the requirements for Private Key generation and protection given in Section 6.2.1 of this CP/CPS.

4.5.2 Relying party Public Key and certificate usage

Any party relying on a certificate issued using the ThaiCA PKI accepts responsibilities for the use of a Subscriber's Public Key and certificate. These responsibilities include:

- Obligation to rely on the certificate only for applications appropriate for the Certificate type (as set forth in this CP/CPS) and consistent with applicable certificate content (e.g., key usage field)
- Successful performance of Public Key operations as a condition of relying on a certificate

- Assumption of responsibility to check the certificate's status, including using one of the required or permitted mechanisms set forth in this CP/CPS (as referenced in Section 4.9)
- Assent to the terms of the applicable Relying Party Agreement as a condition of relying on the certificate

4.6 Certificate renewal

For the purposes of this CP/CPS, "certificate renewal" means the issuance of a new certificate without changing the Public Key or any other information used in the original certificate, with the sole exception of the `notAfter` field (i.e. the renewal date).

4.6.1 Circumstance for certificate renewal

Unless otherwise specifically prohibited in this CP/CPS, any certificate issued utilizing the ThaiCA PKI may be renewed if the certificate meets the following criteria:

- The original certificate has not been revoked or otherwise flagged
- The Public Key from the original certificate has not been blocklisted
- The Private Key corresponding to the original certificate has not been compromised
- The key lifetime is not exceeded as stated in Section 6.3.2
- All information within the certificate, other than the `notAfter` field, remains accurate
- The renewed certificate's cryptographic security is deemed to remain sufficient for the certificate's intended lifetime
- The information provided in the request still passes the appropriate validation checks
- No further or additional validation is required beyond repeating the same steps performed originally

Certificates which have either been previously renewed or previously re-keyed may be renewed again so long as the criteria above are met. The original certificate may be revoked after renewal is complete. Revocation after renewal shall be at the sole discretion of ThaiCA or the authorized entity utilizing the ThaiCA PKI to process the renewal. Regardless of revocation status, the original certificate shall not be further renewed, re-keyed or modified.

4.6.2 Who may request renewal

Renewal of a certificate issued utilizing the ThaiCA PKI may be requested by the Subscriber or the Subscriber's agent. Subscribers with Certificates issued directly by ThaiCA may request renewal via their ThaiCA Account Dashboard. Any RA, internal or external, utilizing the ThaiCA PKI shall require a specific request for renewal. Certificates issued by any entity utilizing the ThaiCA PKI shall not be automatically renewed.

4.6.3 Processing certificate renewal requests

Renewal requests shall require validation and/or authentication identical to that for a new certificate. Subscribers with Certificates issued directly by ThaiCA may request renewal via

their ThaiCA Account Dashboard. Any certificate slated for renewal shall re-use all information in the original request, with the sole exception of the expiration date (the `notAfter` field). Any certificate slated for renewal which for any reason fails re-verification and/or re-authentication of the certificate shall not be renewed. Certificates which cannot be renewed may be capable of re-keying as defined and described in Section 4.7.

4.6.4 Notification of renewed certificate issuance to Subscriber

Any certificate renewed via the ThaiCA PKI shall utilize a notification method identical to that for a new certificate, in compliance with Section 4.4.2.

4.6.5 Conduct constituting acceptance of a renewal certificate

Acceptance of any certificate renewed via the ThaiCA PKI shall use the same methods described for a new certificate in Section 4.4.1.

4.6.6 Publication of the renewal certificate by the CA

Any certificate renewed via the ThaiCA PKI may be published via email to the Subscriber using the same methods described for a new certificate in Section 4.4.2.

4.6.7 Notification of certificate issuance by the CA to other Entities

Notification to other entities may also be performed for any renewed certificate using the same methods described for a new certificate in Section 4.4.3.

4.7 Certificate re-key

For the purposes of this CP/CPS, "certificate re-keying" means the re-issuance of a certificate which utilizes a new Key Pair. Other information used in the original certificate may or may not be changed when a certificate is re-keyed. In all cases where re-keying is requested and/or performed a new Certificate Signing Request (CSR) must be submitted (per Section 4.1.2.3) to obtain the new Public Key required.

4.7.1 Circumstances for certificate re-key

Any certificate issued utilizing the ThaiCA PKI may be re-keyed, unless otherwise specifically prohibited in the ThaiCA PKI CP/CPS.

4.7.1.1 Revocation

In certain cases, an original certificate or previously issued certificate must be revoked as a condition of re-keying. For instance, if the `subject:commonName` or a `subjectAltName:dNSName` field is altered for the following certificate categories with relation to the previously issued certificate, the original certificate must be revoked as a condition of re-keying:

- Digital Signing Certificate

In all other cases, the original certificate may be revoked after re-keying is complete. In these cases, revocation after re-keying shall be at the sole discretion of ThaiCA or the authorized entity utilizing the ThaiCA PKI to process the re-key request.

4.7.1.2 Loss, theft or compromise

Any Subscriber, agent or authorized entity utilizing the ThaiCA PKI to create a certificate whose Private Key has been stolen, lost or otherwise compromised should immediately request re-keying of that certificate. The Subscriber should also request revocation of the Public Key that is associated with the lost, stolen or compromised Private Key.

For Server Certificates, if the Subscriber requests that ThaiCA revoke a Certificate for the reason of Key Compromise, and has not previously demonstrated and cannot currently demonstrate possession of the associated Private Key of the Certificate, ThaiCA MAY revoke all certificates associated with that Subscriber that contain that Public Key. ThaiCA SHALL NOT assume that it has evidence of Private Key compromise for the purposes of revoking the certificates of other subscribers, but MAY block issuance of future certificates with that key.

TKC is not responsible for loss, damages or injury resulting from any compromise of a Private Key. Reference should be made to the Subscriber Agreement and/or Relying Party Agreement applicable to the certificate for more information regarding compromised Private Keys.

4.7.1.3 Key pair expiration

Any expired certificate issued from a Key Pair whose usage period has also expired must be re-keyed, unless otherwise specifically prohibited in the ThaiCA CP/CPS.

4.7.2 Who may request certification of a new Public Key

Re-keying of a certificate issued via the ThaiCA PKI may be requested by the Subscriber or the Subscriber's agent. Subscribers with Certificates issued directly by ThaiCA may request re-keying directly via their ThaiCA Account Dashboard. Any RA, internal or external, utilizing the ThaiCA PKI may request a certificate re-key if compromise of that certificate's Private Key is known or suspected to have occurred. This re-keying shall occur at the discretion of ThaiCA and/or the internal or Enterprise RA concerned.

4.7.3 Processing certificate re-keying requests

Re-keying requests must be accompanied by a new CSR. Any certificate slated for re-keying may be re-issued using any or all information in the original request, with the exception of the Public Key and the date of issuance date (the `validFrom` field). Other information may be changed in a re-key request, as requested by the Subscriber or the Authorized Entity requesting the re-key. Re-keying requests shall require validation and/or authentication, as described in Section 4.2. Any certificate submitted for re-keying which for any reason fails verification and/or authentication shall not be issued.

4.7.4 Notification of new certificate issuance to Subscriber

Any certificate re-keyed via the ThaiCA PKI shall utilize a notification method which is in compliance with Section 4.4.2.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Acceptance of any certificate re-keyed via the ThaiCA PKI shall use the same methods described for a new certificate in Section 4.4.1.

4.7.6 Publication of the re-keyed certificate by the CA

Any certificate re-keyed via the ThaiCA PKI may be published via email to the Subscriber using the same methods described for a new certificate in Section 4.4.2.

4.7.7 Notification of certificate issuance by the CA to other Entities

Notification to other entities may also be performed for any re-keyed certificate using the same methods as described in Section 4.4.3

4.8 Certificate modification

For the purposes of the ThaiCA CP/CPS, "certificate modification" means the issuance of a new certificate in which non-essential information has changed, without changing the Key Pair related to the original certificate.

4.8.1 Circumstance for certificate modification

Certificate modification may be requested by a Subscriber when non-essential attributes change, including but not limited to:

- Country change
- Role change
- Address change
- A reorganization resulting in alteration of a DN

Any re-issuance of a certificate in which information other than the Key Pair changes, shall be considered certificate modification. The original Certificate may be revoked after modification is complete, but the original Certificate shall not be further renewed, re-keyed or modified.

4.8.2 Who may request certificate modification

Modification of a certificate issued via the ThaiCA PKI may be requested by the Subscriber or the Subscriber's agent. Subscribers with Certificates issued directly by ThaiCA may request modification directly via their ThaiCA Account Dashboard.

4.8.3 Processing certificate modification requests

Modification requests shall require validation and/or authentication, as described in Section 4.2. Any certificate slated for modification which for any reason fails verification and/or authentication of the certificate shall not be renewed.

4.8.4 Notification of modified certificate issuance to Subscriber

Any certificate modified via the ThaiCA PKI shall utilize a notification method which is in compliance with Section 4.4.2.

4.8.5 Conduct constituting acceptance of modified certificate

Acceptance of any certificate modified via the ThaiCA PKI shall use the same methods described for a new certificate in Section 4.4.1.

4.8.6 Publication of the modified certificate by the CA

Any certificate modified via the ThaiCA PKI may be published via email to the Subscriber using the same methods described for a new certificate in Section 4.4.2.

4.8.7 Notification of modified certificate issuance by the CA to other Entities

Notification to other entities may also be performed for any modified certificate using the same methods as described in Section 4.4.3.

4.9 Certificate revocation and suspension

For the purposes of the ThaiCA CP/CPS, “revocation” is defined as adding the serial number of a certificate issued via the ThaiCA PKI to a Certificate Revocation List (CRL), an Online Certificate Status Protocol (OSCP) and any other relevant database used for blocklisting.

4.9.1 Circumstances for revocation

4.9.1.1 Reasons for Revoking a Subscriber Certificate

Each new CRL entry MUST contain the RFC 5280 revocation reason code (CRLReason) indicated by this section, unless the CRLReason is “unspecified (0)”. Only the following CRLReasons MAY be present in the CRL:

- keyCompromise (RFC 5280 CRLReason #1);
- privilegeWithdrawn (RFC 5280 CRLReason #9);
- cessationOfOperation (RFC 5280 CRLReason #5);
- affiliationChanged (RFC 5280 CRLReason #3); or
- superseded (RFC 5280 CRLReason #4).

Except for CRLReason "privilegeWithdrawn", CAs MUST inform Subscribers about these revocation reasons and explain when to choose each option. Tools that the CA provides to the Subscriber MUST allow for these options to be easily specified when the Subscriber requests revocation of their Certificate, with the default value being that no revocation reason (unspecified (0)) is provided.

TKC shall begin the revocation procedure of a Subscriber certificate within 24 hours, if it meets one or more of the following criteria:

1. The Subscriber requests in writing that ThaiCA revoke the Certificate for:

- keyCompromise (RFC 5280 CRLReason #1) (i.e., the Subscriber's Private Key is suspected of compromise);
- cessationOfOperation (RFC 5280 CRLReason #5) (i.e., the Subscriber will no longer be using the Certificate because they are discontinuing their website);
- affiliationChanged (RFC 5280 CRLReason #3) (i.e., identifying information about the Subscriber in the Certificate has changed); or
- superseded (RFC 5280 CRLReason #4) (i.e., the Subscriber requests a new certificate to replace an existing certificate).

If the Subscriber requests revocation for Key Compromise and cannot demonstrate possession of the associated Private Key of that Certificate, then the CA MAY revoke all certificates associated with that Subscriber that contain that Public Key. The CA MUST NOT assume that it has evidence of Key Compromise for the purposes of revoking the Certificates of other Subscribers, but MAY block issuance of future certificates with that key;

1. The Subscriber notifies ThaiCA that the original certificate request was not authorized and does not retroactively grant authorization (CRLReason #9, privilegeWithdrawn);
1. TKC obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise (CRLReason #1, keyCompromise);
2. TKC is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys) (CRLReason #1, keyCompromise);
3. TKC obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon (CRLReason #4, superseded or CRLReason #9, privilegeWithdrawn).

TKC should revoke a certificate within 24 hours and must revoke a Certificate within 5 days if one or more of the following occurs:

1. The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6 (CRLReason #4, superseded);
2. TKC obtains evidence that the Certificate was misused (CRLReason #9, privilegeWithdrawn);

3. TKC is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use (CRLReason #9, privilegeWithdrawn);
4. TKC 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) (CRLReason #5, cessationOfOperation);
5. TKC is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name (CRLReason #9, privilegeWithdrawn);
6. TKC is made aware of a material change in the information contained in the Certificate (CRLReason #9, privilegeWithdrawn);
7. TKC is made aware that the Certificate was not issued in accordance with this CP/CPS (CRLReason #4, superseded);
8. TKC determines or is made aware that any of the information appearing in the Certificate is inaccurate (CRLReason #9, privilegeWithdrawn);
9. TKC's right to issue Certificates is revoked or terminated, unless ThaiCA has made arrangements to continue maintaining the CRL/OCSP Repository (CRLReason #5, cessationOfOperation);
10. Revocation is required by TKC's CP/CPS (CRLReason #4, superseded); or
11. TKC is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, or if there is clear evidence that the specific method used to generate the Private Key was flawed (CRLReason #1, keyCompromise);
12. TKC receives a lawful and binding ruling from a Government or regulatory body to revoke the Certificate (CRLReason #9, privilegeWithdrawn).

When ThaiCA obtains verifiable evidence of Key Compromise for a Certificate whose CRL entry does not contain a reasonCode extension or has a reasonCode extension with a non-keyCompromise reason, ThaiCA SHOULD update the CRL entry to enter keyCompromise as the CRLReason in the reasonCode extension. Additionally, ThaiCA SHOULD update the revocation date in a CRL entry when it is determined that the Private Key of the Certificate was compromised prior to the revocation date that is indicated in the CRL entry for that Certificate.

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

TKC shall begin the revocation procedure of a Subordinate CA Certificate within seven (7) days, if it meets one or more of the following criteria:

1. The Subordinate CA requests revocation in writing;
2. The Subordinate CA notifies ThaiCA that the original certificate request was not authorized and does not retroactively grant authorization;

3. TKC 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 Sections 6.1.5 and 6.1.6,
4. TKC obtains evidence that the Certificate was misused;
5. TKC is made aware that the Certificate was not issued in compliance with this CP/CPS or an applicable alternate CPS;
6. TKC determines that any of the information appearing in the Certificate is inaccurate or misleading;
7. TKC or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
8. TKC's or Subordinate CA's right to issue Certificates under this CP/CPS 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 TKC's CP/CPS.
10. TKC receives a lawful and binding ruling from a Government or regulatory body to revoke a CA Certificate.

Applicable revocation reasons (per RFC 5280 and ITU-T X.509) for CA Certificates, are:

- **cACompromise** is used in revoking a CA certificate; it indicates that it is known or suspected that the subject's private key, or other aspects of the subject validated in the CA certificate, have been compromised.
- **affiliationChanged** indicates that the subject's name or other information in the public-key certificate has been modified but there is no cause to suspect that the private key has been compromised.
- **superseded** indicates that the public-key certificate has been superseded but there is no cause to suspect that the private key has been compromised.
- **cessationOfOperation** indicates that the public-key certificate is no longer needed for the purpose for which it was issued but there is no cause to suspect that the private key has been compromised.
- **privilegeWithdrawn** indicates that a public-key certificate was revoked because a privilege contained within that public-key certificate has been withdrawn.

4.9.2 Who can request revocation

Revocation of a certificate issued utilizing the ThaiCA PKI may be requested by the Subscriber or the Subscriber's agent. Any RA, internal or external, utilizing the ThaiCA PKI may request revocation of a certificate. Non-Subscribers meeting one or more of the criteria given in Section 4.9.1 may file a Certificate Problem Report to initiate a certificate revocation, as described in Sections 3.4.2 and 4.9.3.3.

4.9.3 Procedure for revocation request

Revocation may be initiated by submitting a request to the appropriate RA (internal or external). A Subscriber can submit a revocation request via an email account associated with the corresponding ThaiCA certificate order. Other approved methods of

communication may be allowed, provided that corresponding account credentials are sufficiently presented.

TKC shall maintain a continuous 24x7 ability to accept and respond to revocation requests and Certificate Problem Reports.

Relying Parties, Application Software Suppliers, and other non-Subscribers may report suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates and request certificate revocation as described in Section 4.9.3.3.

4.9.3.1 Revocation requested by Subscriber or Subscriber's agent

TKC shall respond within 24 hours to a Subscriber's valid revocation request. A valid revocation request is one in which the corresponding account credentials, in conjunction with one or more of the criteria outlined in Section 4.9.1, are sufficiently presented.

For Server Certificates, if a Subscriber requesting revocation for the reason of Key Compromise has previously demonstrated or can currently demonstrate possession of the private key of the certificate as described in section 4.9.12, then ThaiCA SHALL revoke all non-expired Server Certificates associated with that key across all Subscribers.

4.9.3.2 Revocation Requested by an Enterprise RA

Any authorized Enterprise RA utilizing the ThaiCA PKI may request revocation of a certificate only if proper credentials are presented. Should the request meet any of the criteria given in Section 4.9.1, along with approved account credentials, ThaiCA CA shall complete the revocation. For any revocation request received from an External RA, ThaiCA shall provide a signed acknowledgement of the request and confirmation of actions to the requesting RA.

4.9.3.3 Revocation requested by Non-Subscribers

Relying Parties, Application Software Suppliers, and other non-Subscribers seeking to request revocation of a Certificate will find instructions for filing a Certificate Problem Report at https://www.thaica.com/revoke/. Certificate Problem Reports should be filed to report suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates. ThaiCA shall proceed with the revocation process if the request meets any of the scenarios described in Section 3.4.2 and/or 4.9.1.1.

For Server Certificates, if anyone requesting revocation for the reason of Key Compromise has previously demonstrated or can currently demonstrate possession of the private key of the certificate as described in section 4.9.12, then ThaiCA SHALL revoke all non-expired Server Certificates associated with that key across all Subscribers.

4.9.3.4 Revocation requested by an Application Software Supplier

If an Application Software Supplier requests ThaiCA to revoke a Certificate because the Application Software Supplier believes that a Certificate attribute is deceptive, or that the Certificate is being used for malware, bundle ware, unwanted software, or some other illicit purpose, then the Application Software Supplier may request that ThaiCA revoke the certificate.

Within two (2) business days of receipt of the request, ThaiCA MUST either revoke the certificate or inform the Application Software Supplier that it is conducting an investigation. If ThaiCA decides to conduct an investigation, it MUST inform the Application Software Supplier whether or not it will revoke the Certificate, within two (2) business days. If ThaiCA decides that the revocation will have an unreasonable impact on its customer, then ThaiCA MUST propose an alternative course of action to the Application Software Supplier based on its investigation.

4.9.4 Revocation request grace period

The grace period given for SSL/TLS certificates is the maximum allowed by the CA/B Forum Baseline Requirements.

For all incidents involving malware, ThaiCA SHALL revoke the Code Signing Certificate in accordance with and within the following maximum timeframes. Nothing herein prohibits ThaiCA from revoking a Code Signing Certificate prior to these timeframes.

1. TKC SHALL contact the software publisher within one (1) business day after ThaiCA is made aware of the incident.
2. TKC SHALL determine the volume of relying parties that are impacted (e.g., based on OCSP logs) within 72 hours after being made aware of the incident.
3. TKC SHALL request the software publisher send an acknowledgement to ThaiCA within 72 hours of receipt of the request.
    a. If the publisher responds within 72 hours, ThaiCA and publisher SHALL determine a “reasonable date” to revoke the certificate based on discussions with TKC.
    b. If the publisher does NOT respond within 72 hours, ThaiCA SHALL notify the publisher that ThaiCA will revoke the certificate in 7 days if no further response is received.
        i. If the publisher responds within 7 days, ThaiCA and the publisher will determine a “reasonable date” to revoke the certificate based on discussion with TKC.
        ii. If the publisher does NOT respond after 7 days, ThaiCA SHALL revoke the certificate, except if ThaiCA has documented proof (e.g., OCSP logs) that this will cause significant impact to the general public.

4.9.4.1 Code Signing Certificate revocation dates

A Certificate MAY have a one-to-one relationship or one-to-many relationship with the signed Code. Regardless, revocation of a Certificate may invalidate the Code Signatures on all signed Code, some of which could be perfectly sound. Because of this, after working with the Subscriber, ThaiCA MAY specify the time at which the Certificate is first considered to be invalid in the `revocationDate` field of a CRL entry or the `revocationTime` field of an OCSP response to time-bind the set of software affected by the revocation, and software should continue to treat objects containing a timestamp dated before the revocation date as valid. This is called a back dated revocation and applies only to signing Certificates.

Backdating the revocationDate field is an exception to best practice described in RFC 5280 (section 5.3.2); however, the "Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates" specify the use of the `revocationDate` field to convey the "invalidity date" to support Application Software Supplier software implementations that process the `revocationDate` field as the date when the Certificate is first considered to be invalid.

If a Code Signing Certificate previously has been revoked, and the ThaiCA later becomes aware of a more appropriate revocation date, then ThaiCA MAY use that revocation date in subsequent CRL entries and OCSP responses for that Code Signing Certificate.

4.9.5 Time within which CA must process the revocation request

TKC SHALL provide a preliminary report on its findings within 24 hours after receiving a Certificate Problem Report to both the Subscriber and the entity who filed the Certificate Problem Report.

Based on these findings, ThaiCA SHALL work with the Subscriber and any entity reporting the Certificate Problem Report or other revocation-related notice to establish whether or not the certificate will be revoked, and if so, a date upon which ThaiCA will revoke the certificate. The period from receipt of the Certificate Problem Report or revocation-related notice to published revocation MUST NOT exceed the time frame set forth in Section 4.9.1.1.

TKC SHALL determine whether revocation or other appropriate action is warranted and set a revocation date based on at least the following criteria:

1. The nature of the alleged problem (scope, context, severity, magnitude, risk of harm);
2. The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties);
3. The number of Certificate Problem Report received about a particular Certificate or Subscriber;
4. The entity making the complaint (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that she didn't receive the goods she ordered);

5. Relevant legislation; and
6. The consequences of revocation (including direct and collateral impacts to Subscribers and Relying Parties).

4.9.6 Revocation checking requirement for relying parties

Relying parties should validate the authenticity and intended usage of a Certificate using the resources described in Section 4.10.1.

4.9.7 CRL issuance frequency

For the status of SSL/TLS and Client Subscriber Certificates, if ThaiCA publishes a CRL then it shall be updated and reissued at least once every **seven (7) days**, and the value of the `nextUpdate` field must not be more than **ten (10) days** beyond the value of the `thisUpdate` field.

For the status of Code Signing Certificates, ThaiCA SHALL publish a CRL then it shall be updated and reissued at least once every **seven (7) days**, and the value of the `nextUpdate` field must not be more than **ten (10) days** beyond the value of the `thisUpdate` field.

For the status of NAESB Subscriber Certificates, the CRL shall be updated and reissued at least once every **twenty-four (24) hours**, and the value of the `nextUpdate` field must not be more than **ten (10) days** beyond the value of the `thisUpdate` field.

For the status of Subordinate CA Certificates and time-stamping Certificates, ThaiCA shall update and reissue CRLs at least:

- once every **twelve (12) months** and
- within **twenty-four (24) hours** after revoking a Subordinate CA Certificate,

and the value of the `nextUpdate` field must not be more than **twelve (12) months** beyond the value of the `thisUpdate` field.

For the status of CA Certificates issuing NAESB Subscriber Certificates, ThaiCA shall update and reissue CRLs at least:

- once every **six (6) months** and
- within **three (3) hours** after revoking a NAESB Issuing Subordinate CA Certificate,

and the value of the `nextUpdate` field must not be more than **twelve (12) months** beyond the value of the `thisUpdate` field.

Under normal conditions, ThaiCA posts new entries to the CRL as soon as a revocation request is confirmed.

TKC shall provide accurate and up-to-date revocation status information for a period not less than ten (10) years beyond expiry of a Code Signing, Document Signing and Timestamp Certificate (see also 4.10.1). After the expiration of a Code Signing or Timestamp Issuing CA, the associated CRLs shall remain published for at least five (5) years beyond the expiry of that Issuing CA.

4.9.8 Maximum latency for CRLs

Where applicable, the maximum latency for the Certificate Revocation List is ten (10) minutes.

4.9.9 On-line revocation/status checking availability

OCSP responses, they shall conform to RFC 6960 and/or RFC 5019. 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-pkix-ocsp-nocheck`, as defined by RFC 6960.

4.9.10 On-line revocation checking requirements

If ThaiCA provides OCSP responses, it shall support an OCSP capability using the GET method, as described in RFC 6960 for Certificates issued.

For the status of Subscriber Certificates:

- OCSP responses MUST have a validity interval greater than or equal to eight hours;
- OCSP responses MUST have a validity interval less than or equal to ten days;
- For OCSP responses with validity intervals less than sixteen hours, then ThaiCA SHALL update the information provided via an Online Certificate Status Protocol prior to one-half of the validity period before the nextUpdate.
- For OCSP responses with validity intervals greater than or equal to sixteen hours, then ThaiCA 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.

For the status of Subordinate CA Certificates:

- If the Issuing CA provides OCSP responses, it shall update information provided via an Online Certificate Status Protocol at least
- every **twelve (12) months** and
- within **24 hours** after revoking a Subordinate CA Certificate.

OCSP responders for CAs which are not Technically Constrained in line with Section 7.1.5, shall not respond with a “good” status for Certificates that have not been issued.

4.9.11 Other forms of revocation advertisements available

No stipulation

4.9.12 Special requirements regarding key compromise

Third parties must use the Certificate Problem report process, as described in section 3.4.2 and may follow at least one of the following methods to demonstrate that a Private Key is indeed Compromised:

1. Submission of the private key itself;
2. Submission of a signed CSR with a Common Name indicating that the key is compromised e.g. “This key is compromised”. This CSR can be generated using the following OpenSSL command:

```
openssl req -new -key privkey.pem -subj "/CN=This key is compromised/" -out proofofcompromise.csr;
```

3. Submission of signed data indicating that the key is compromised e.g. “This key is compromised” by following the instructions at Proving Possession of a Private Key.

4.9.13 Circumstances for suspension

The ThaiCA PKI does not support Certificate suspension.

4.9.14 Who can request suspension

No entity is permitted to request suspension of any Certificate issued utilizing the ThaiCA PKI.

4.9.15 Procedure for suspension request

Certificate suspension is not provided.

4.9.16 Limits on suspension period

Certificate suspension is not provided.

4.10 Certificate status services

TKC shall maintain services to provide certificate status information for any certificate issued by the ThaiCA PKI.

4.10.1 Operational characteristics

If ThaiCA provides OCSP responses for Code Signing, Document Signing and Timestamp Certificates, then it shall provide them beyond expiry of such a Certificate which MAY be at least ten (10) years after the expiration of the certificate. Application Software Suppliers

MAY request ThaiCA to support a longer life-time according to their trust store requirements.

If a Code Signing Certificate contains the Lifetime Signing OID, the digital signature becomes invalid when the Code Signing Certificate expires, even if the digital signature is timestamped.

TKC CAs shall include URLs to revocation information within any issued Certificate in `CRL Distribution Points` (where applicable) and `Authority Information Access` extensions.

4.10.2 Service availability

TKC shall operate and maintain its CRL and OCSP capability with resources sufficient to provide a response time of ten (10) seconds or less under normal operating conditions. ThaiCA shall maintain an online 24x7 Repository that application software can use to automatically check the current status of all unexpired Certificates issued by TKC. ThaiCA shall maintain a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke any Certificate which is the subject of such a complaint.

4.10.3 Optional features

Not stipulated

4.11 End of subscription

Subscribers have two options in terms of ending a certificate subscription. A certificate subscription is deemed to end when the certificate:

1. is revoked prior to the date found in the `validTo` field, or
2. reaches the `validTo` date and expires.

Either of these options shall result in the termination of subscription. TKC, or the appropriate Authorized Third Party or Enterprise RA, shall notify a Subscriber of the need for renewal prior to the expiration of any certificate issued via the ThaiCA PKI. Notifications can be configured through the Subscriber's ThaiCA Account.

4.12 Key escrow and recovery

The ThaiCA PKI does not support key escrow.

4.12.1 Key escrow and recovery policy and practices

The ThaiCA PKI does not support key escrow.

4.12.2 Session key encapsulation and recovery policy and practices

The ThaiCA PKI does not support key escrow.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

TKC implements and maintains a comprehensive security program to protect Certificate Data and all aspects of the Certificate Management Process.

TKC's security plan is based on an annual risk assessment designed to identify and assess threats and to implement appropriate steps to address these threats.

5.1 Physical controls

TKC implements and maintains physical security controls to restrict access to the hardware and software used for ThaiCA PKI operations.

5.1.1 Site location and construction

TKC operates from a secure commercial datacenter. All critical facilities are housed in secure areas with appropriate security barriers and entry controls. These are protected from unauthorized access, damage and/or interference.

5.1.2 Physical access

TKC equipment is physically secured and protected from unauthorized access. Measures to secure datacenter equipment include two-factor access control through physical cards and biometric readers, 24-hour video surveillance and full-time human security presence which monitors and logs all access.

Support and vetting rooms where RA functions are performed are secured by controlled access and keyed-lock doors. Access card use is logged by the building security system. Video monitoring is employed to record all access to the location. Unauthorized personnel needing to enter into the physical location of a secure datacenter or the area where RA functions are performed shall never be left without oversight by an authorized person.

5.1.3 Power and air conditioning

TKC equipment is maintained in a facility which utilizes uninterrupted power supply (UPS) units and automatic backup generators to ensure multiple redundant power sources. HVAC systems for heating, cooling and ventilation are sufficient to support the operation of the CA system.

5.1.4 Water exposures

TKC equipment is maintained in a facility which provides protection against water exposures.

5.1.5 Fire prevention and protection

TKC equipment is maintained in a facility equipped with automatic engineered fire suppression systems designed to preserve electronic equipment.

5.1.6 Media storage

Any media used by ThaiCA is securely handled and stored to protect it from damage, theft and unauthorized access.

Media containing Private Key material is handled, packaged and stored in a manner compliant with the requirements for the sensitivity level of the information it protects or to which it provides access. Storage protection of CA Private Key material shall be consistent with stipulations in Section 5.1.2.

5.1.7 Waste disposal

Paper documents or any other printed material containing ThaiCA PKI information or related confidential information are securely disposed of by shredding or destruction by an approved service. Removable media containing ThaiCA PKI information or related confidential information are securely disposed of by complete destruction of the media, or by the use of an approved utility to wipe or overwrite removable media.

5.1.8 Off-site backup

An off-site location is used for the storage and retention of ThaiCA PKI backup software and data. The off-site storage facility is available to authorized personnel 24 hours per day 7 days per week for the purpose of retrieving software and data. The off-site storage facility has appropriate levels of physical security in place and is protected against fire and unauthorized access.

5.2 Procedural controls

5.2.1 Trusted roles

PKI functions are performed by individuals working within clearly defined trusted roles. These trusted roles are established and maintained to share responsibility, limit the ability for action by individual participants, and securely separate duties and functions within the PKI. Trusted roles include but are not limited to:

- **CA Administrator:** Authorized to install, configure and maintain the CA systems used for Certificate life-cycle management.
- **RA Administrator:** Certificate generation and revocation, and end entity creation and deletion
- **System Administrator:** Responsible for operating the CA and RA systems on a day-to-day basis.
- **Network Administrator:** Responsible for operating networking equipment on a day-to-day basis.
- **Vetting Agent:** Responsible for validating the authenticity and integrity of data to be included within Certificates via a suitable RA system
- **Security Auditor** Responsible for internal auditing of CAs and RAs and responsible for administering the implementation of the security practices. This sensitive role shall

not be combined with any other sensitive role, e.g. the Security Auditor shall not also be a CA Administrator. Security Auditors shall review, maintain, and archive audit logs, and perform or oversee internal audits (independent of formal compliance audits) to ensure that CAs and RAs are operating in accordance with any applicable CP/CPS.

5.2.2 Number of persons required per task

PKI-sensitive operations shall require active participation by ThaiCA personnel. This participation shall require at least two trusted individuals to perform the required duties of their specified roles. CA Private Keys shall be backed up, stored, and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment.

Multi-party control shall not be achieved using personnel that serve in the Security Auditor role with the exception of audit functions. The following tasks shall require two or more persons:

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

Systems used to process and approve Certificate Requests shall require actions by at least two persons in Trusted Roles before issuing an Certificate.

5.2.3 Identification and authentication for each role

All individuals authorized in trusted roles must properly authenticate themselves to the relevant CA or RA before performing their duties.

5.2.4 Roles requiring separation of duties

Any trusted role as defined in 5.2.1 intrinsically possesses duties and/or capabilities separate from those in other trusted roles.

As described in 5.2.2, validation of certificate requests shall require the participation of at least two validation specialists. For example, one Validation Specialist may review and verify all the Applicant information and a second Validation Specialist may approve issuance of the certificate.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

TKC verifies the identity and trustworthiness of all personnel, whether as an employee, agent, or an independent contractor, prior to the engagement of such person(s).

Any personnel occupying a trusted role (as defined in 5.2.1) must possess suitable experience and be deemed qualified by TKC. Personnel in trusted roles shall undergo ThaiCA training prior to performing any duties as part of that role.

In addition, the identity, trustworthiness and competence of assigned personnel is verified on a yearly basis by the policy management authority to ensure their continued qualification to act appropriately in such a role.

5.3.2 Background check procedures

All individuals performing trusted role functions have cleared current ThaiCA security screenings or background checks appropriate for that role. Background check procedures verify information relevant to the role and may include identity verification (through government-issued photo), as well as examination of one's public record (through research of previous employment history, relevant qualifications and criminal records).

5.3.3 Training requirements

TKC shall provide comprehensive training to all personnel performing information verification duties with skills-training that covers:

- Basic Public Key Infrastructure knowledge
- Authentication and vetting policies and procedures (including TKC's CP/CPS)
- Common threats to the information verification process (including phishing and other social engineering tactics).

TKC shall ensure that all personnel performing validation duties be trained to and maintain an appropriate skill level. Training shall include an initial examination and periodic retraining as required to reflect changes in PKI operations. All training shall be thoroughly documented.

5.3.4 Retraining frequency and requirements

All personnel occupying any Trusted Role shall maintain skill levels consistent with that Trusted Role and shall undergo periodic retraining related to that Role. TKC's retraining programs shall reflect and address any relevant changes to the ThaiCA PKI and related operations.

TKC shall maintain records of all retraining performed.

5.3.5 Job rotation frequency and sequence

TKC shall ensure that changes in personnel, including changes in personnel occupying Trusted Roles, shall not affect the operations, services and/or security of the ThaiCA PKI and related functions.

5.3.6 Sanctions for unauthorized actions

TKC employees and agents failing to comply with the ThaiCA CP/CPS, whether through negligence or malicious intent, are subject to administrative or disciplinary actions, including termination of employment or agency and criminal sanctions. Any ThaiCA employee holding a Trusted Role shall be immediately removed from that role following identification of any unauthorized actions. ThaiCA management will review the underlying details of an incident and promptly issue an applicable resolution report once a conclusion has been reached. Resolution may result in termination, other sanctions, and/or demotion to a new non-trusted role within the ThaiCA PKI. Resolution may also require retained personnel to undergo additional training programs as determined by ThaiCA management.

5.3.7 Independent contractor requirements

Any independent contractor or Delegated Third Party's personnel involved in the issuance of a Certificate via the ThaiCA PKI shall be fully subject to the TKC's CP/CPS, including training and skills requirements (Section 5.3.3), sanctions (5.3.6), document retention and event logging requirements (5.4.1).

5.3.8 Documentation supplied to personnel

TKC shall provide authorized personnel with any relevant documentation needed to carry out job functions or duties. All documentation required for duties, functions and obligations for any personnel utilizing the ThaiCA PKI and related functions shall be available to authorized personnel and properly maintained/updated. Documentation which accurately reflects current operations and processes shall be made readily available. Access to documentation related to specific Trusted Roles may be limited to personnel occupying those roles. Relevant materials are systematically disseminated through TKC's training and retraining programs. Any changes to operations, processes or practices related to the ThaiCA PKI shall be recorded and reflected in the related documentation.

5.4 Audit logging procedures

5.4.1 Types of events recorded

All events relating to the security of Certificate Systems, Certificate Management Systems, Root CA Systems and delegated Third Party Systems of ThaiCA and of each Delegated Third Party are recorded in audit log files.

Security audit logs shall be automatically generated whenever possible. Where this is not an option, a logbook, paper form, or other physical mechanism shall be used.

All security audit logs are retained (per 5.4.3 and 5.5) and made available to Qualified Auditors as requested.

Log entries include the following elements:

1. Date and time of event;

2. Identity of the person making the journal entry; and
3. Description of the event.

5.4.1.1 Types of events recorded for publicly-trusted TLS and Code Signing Certificates

For publicly-trusted TLS and Code Signing Certificates, ThaiCA shall record at least the following events:

1. CA certificate and key lifecycle events, including:
    i. Key generation, backup, storage, recovery, archival, and destruction;
    ii. Certificate requests, renewal, and re-key requests, and revocation;
    iii. Approval and rejection of certificate requests;
    iv. Cryptographic device lifecycle management events;
    v. Generation of Certificate Revocation Lists;
    vi. Signing of OCSP Responses (as described in Sections 4.9 and 4.10); and
    vii. Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.
2. Subscriber Certificate lifecycle management events, including:
    i. Certificate requests, renewal, and re-key requests, and revocation;
    ii. All verification activities stipulated in the Baseline Requirements and this CP/CPS;
    iii. Approval and rejection of certificate requests;
    iv. Issuance of Certificates;
    v. Generation of Certificate Revocation Lists; and
    vi. Signing of OCSP Responses (as described in Sections 4.9 and 4.10).
3. Security events, including:
    i. Successful and unsuccessful PKI system access attempts;
    ii. PKI and security system actions performed;
    iii. Security profile changes;
    iv. Installation, update and removal of software on a Certificate System;
    v. System crashes, hardware failures, and other anomalies;
    vi. Firewall and router activities; and
    vii. Entries to and exits from the CA facility.

5.4.1.2 Types of events recorded for publicly-trusted Time-stamping Certificates

For publicly-trusted Time-stamping Certificates, ThaiCA shall record at least the following events:

1. Physical or remote access to a timestamp server, including the time of the access and the identity of the individual accessing the server,
2. History of the timestamp server configuration,
3. Any attempt to delete or modify timestamp logs,

4. Security events, including:
    i. Successful and unsuccessful Timestamp Authority access attempts;
    ii. Timestamp Authority actions performed;
    iii. Security profile changes;
    iv. System crashes, hardware failures, and other anomalies; and
    v. Firewall and router activities;
5. Revocation of a timestamp certificate,
6. Major changes to the timestamp server's time, and
7. System startup and shutdown.

5.4.2 Frequency of processing audit log

TKC shall monitor the integrity of the logging processes for application and system logs through continuous automated monitoring and alerting or through a human review to ensure that logging and log-integrity functions are effective. If a human review is utilized and the system is online, the process shall be performed at least once every 31 days.

TKC shall monitor audit logs through continuous automated monitoring and alerting or through a human review for possible issues, such as:

- Anomalies and/or irregularities
- Malicious activity

Each review should be reported to the appropriate personnel by summarizing findings, if any.

Investigations which result from reported findings, recommendations made based on these investigations, and actions taken to address reported issues are recorded and made available to auditors as requested.

5.4.3 Retention period for audit log

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

1. CA certificate and key lifecycle management event records (as set forth in Section 5.4.1.1 (1)) after the later occurrence of:
    i. the destruction of the CA Private Key; or
    ii. the revocation or expiration of the final CA Certificate in that set of Certificates that have an X.509v3 `basicConstraints` extension with the `cA` field set to true and which share a common Public Key corresponding to the CA Private Key;
2. Subscriber Certificate lifecycle management event records (as set forth in Section 5.4.1.1 (2)) after the expiration of the Subscriber Certificate;
3. Timestamp Authority data records (as set forth in Section 5.4.1.2) after the revocation or renewal of the Timestamp Certificate private key;

4. Any security event records (as set forth in Section 5.4.1.1 (3)) after the event occurred.

TKC shall further retain the following Subscriber Certificate lifecycle management event records (as set forth in Section 5.4.1.1 (2)), for at least seven (7) years after the revocation or expiration of the Subscriber Certificate:

1. Certificate requests, renewal, and re-key requests, and revocation;
2. All verification activities stipulated in the Baseline Requirements and this CP/CPS;
3. Approval and rejection of certificate requests; and
4. Issuance of Certificates.

This extended retention period of seven (7) years aligns with the retention period of documentation relating to certificate requests and the verification thereof, and all Certificates and revocation thereof, as set forth in Section 5.5.2.

Note: While these Requirements set the minimum retention period, ThaiCA MAY choose a greater value as more appropriate in order to be able to investigate possible security or other types of incidents that will require retrospection and examination of past audit log events.

5.4.4 Protection of audit log

TKC shall collect and regularly analyse relevant audit data for any attempts to violate the integrity of any element of the ThaiCA PKI. ThaiCA audit logs may be viewed only by authorized personal and auditors.

TKC shall decide whether and which audit records may be viewed by others and under what circumstances it shall make those records available.

TKC shall protect logs from modification and destruction and maintain digital logs in an encrypted format.

5.4.5 Audit log backup procedures

TKC shall perform an onsite backup of the audit log daily. The backup process includes at least a weekly copy of the audit log from the ThaiCA facility and storage at a secure, offsite location.

5.4.6 Audit collection system (internal vs. external)

The security audit process shall run independently of the ThaiCA PKI certificate issuance software. Security audit processes shall be invoked at system start up and cease only at system shutdown. Security audit processes shall not be capable of being circumvented.

5.4.7 Notification to event-causing subject

TKC shall not be required to give any notice to the individual, Organization, device, or application that caused any event which invoked logging.

5.4.8 Vulnerability assessments

TKC and Delegated Third Parties perform regular vulnerability assessments and penetration tests (at least once a year) covering all Certificate Systems. These assessments document and implement a vulnerability correction process to identify, review and remediate issues and threats.

Vulnerability assessments may also be performed:

- Within one week of receiving a request from the CA/Browser Forum
- After any system or network changes that the CA determines are significant, and
- At least once per quarter, on public and private IP addresses identified by the CA or Delegated Third Party as the CA's or Delegated Third Party's Certificate Systems

Additionally, ThaiCA and Delegated Third Parties perform an annual Risk Assessment to:

- Identify foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;
- Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
- Assess the sufficiency of the policies, procedures, information systems, technology, and other arrangements that ThaiCA has in place to counter such threats.

5.5 Records archival

5.5.1 Types of records archived

TKC and each Delegated Party shall archive all documentation relating to certificate requests and the verification thereof, and all Certificates and revocation thereof.

Additionally, ThaiCA and each Delegated Party SHALL archive: 1. Documentation related to the security of their Certificate Systems, Certificate Management Systems, Root CA Systems, and Delegated Third Party Systems; and 2. Documentation related to their verification, issuance, and revocation of certificate requests and Certificates.

TKC may also archive other records relating to: 1. CA certificate and key lifecycle 2. Subscriber Certificate lifecycle management 3. Security operations

TKC may also archive any other documents deemed relevant to ThaiCA PKI operations.

5.5.2 Retention period for archive

Archived audit logs (as set forth in Section 5.5.1 SHALL be retained for a period of at least two (2) years from their record creation timestamp, or as long as they are required to be retained per section 5.4.3, whichever is longer.

Additionally, ThaiCA and each delegated party SHALL retain, for at least two (2) years:

1. All archived documentation related to the security of Certificate Systems, Certificate Management Systems, Root CA Systems and Delegated Third Party Systems (as set forth in Section 5.5.1); and

2. All archived documentation relating to the verification, issuance, and revocation of certificate requests and Certificates (as set forth in Section 5.5.1) after the later occurrence of:

    i. such records and documentation were last relied upon in the verification, issuance, or revocation of certificate requests and Certificates; or

    ii. the expiration of the Subscriber Certificates relying upon such records and documentation.

Note: While these Requirements set the minimum retention period, ThaiCA MAY choose a greater value as more appropriate in order to be able to investigate possible security or other types of incidents that will require retrospection and examination of past records archived.

For any other archived records, set forth in Section 5.5.1 (1) to (3), ThaiCA shall apply mutatis mutandis the retention rules set forth in Section 5.4.3.

For any other archived documents deemed relevant to ThaiCA PKI operations, set forth in Section 5.5.1, appropriate retention period shall be applied.

5.5.3 Protection of archive

Archives shall be retained and protected against modification or destruction for the minimum time period specified in Section 5.5.2. ThaiCA shall take all appropriate measures to ensure that only authorized access is allowed with respect to any archives.

5.5.4 Archive backup procedures

TKC shall utilize secure and verifiable backup procedures to provide a complete and readily accessible backup archive in the event of loss or damage to a primary archive. Any backup archive shall be maintained at a separate, secure location from the primary archive. Access to any backup archive shall employ protections equivalent to the security protocols of its primary archive. Backup archive maintenance shall include periodic transfer of archived data to new media to prevent data loss.

5.5.5 Requirements for time-stamping of records

All archived documents shall include the date and time of creation, occurrence or modification. The date and time for any document archived shall derive these from a trusted time source as defined in Section 6.8.

5.5.6 Archive collection system (internal or external)

TKC shall employ internal systems to collect and maintain a primary archive.

5.5.7 Procedures to obtain and verify archive information

TKC's primary and backup archives shall only be accessible by authorized ThaiCA personnel and qualified auditors.

TKC may upon request, at its sole discretion, release specific records related to requests by a Subscriber, a Relying Party or an authorized agent of a Subscriber or Relying Party.

TKC shall not release archives in their entirety, except as required by law.

TKC may require compensation and fees for any costs incurred in accessing or retrieving any requested archival data.

TKC shall verify the integrity and readability of primary and backup archives through periodic random testing.

5.5.8 Archive Destruction

At the end of the archive period, the archive may be permanently destroyed through:

- Secure deletion procedures of the archive media for logical data removal
- Physical destruction of the storage media

5.6 Key changeover

TKC shall ensure a securely managed changeover of Private Keys for any expiring Root Certificate utilized by the ThaiCA PKI.

For any key changeover, ThaiCA shall maintain, for a temporary and strictly delimited period, concurrent Root Certificates (the original, expiring Root Certificate with the expiring Private Key and the new Root Certificate with the new Private Key) to maintain a seamless transition of functions and services. This period shall end upon the expiration of the original Root Certificate's Private Key.

TKC shall provide the new Public Key to Subscribers and Relying Parties through the delivery methods detailed in Section 6.1.4.

Similar key changeover and key distribution methods shall be employed to manage the expiration of any cross-certified certificate.

5.7 Compromise and disaster recovery

TKC maintains a Business Continuity Plan which details required steps, procedures and actions to restore operations in a timely manner when any function of the ThaiCA PKI has been negatively impacted by incidents or disasters.

5.7.1 Incident and compromise handling procedures

TKC maintains policies and procedures to respond to potential or actual security compromises, natural disasters, and similar events. Documents addressing these needs include (but are not limited to) an Incident Management Policy (IMP), a Business Continuity and Disaster Recovery Plan and other related resources.

TKC shall review, test and update these policies and procedures as needed.

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

TKC's Business Continuity Plan includes measures to address any incident in which Computing Resources, Software, and/or Data related to the ThaiCA PKI are corrupted. Any affected operations shall be investigated and suspended as required. Any suspended activities shall be restored as quickly as possible commensurate with secure operation of the ThaiCA PKI.

The Disaster Recovery Plan shall be tested at least annually.

5.7.3 Recovery Procedures After Key Compromise

TKC maintains procedures to address any incident wherein a CA Private Key is lost, destroyed, compromised, or suspected to be compromised. The same applies to the event of a compromise of the algorithms and parameters used to generate the Private Key and certificate. Steps taken after thorough investigation of the incident may include, but are not limited to:

- Revocation of the affected CA Private Key
- Generation of a new CA Key Pair
- Notification of all affected Subscribers
- Revocation of all Certificates signed with the affected CA Private Key

5.7.4 Business continuity capabilities after a disaster

TKC's Business Continuity Plan is designed to ensure secure continuous operations, and/or timely and secure restoration of affected operations, in the event of an incident or disaster.

5.8 CA or RA termination

In the event of the termination of any CA and/or RA associated with the ThaiCA PKI, ThaiCA shall provide timely notice of this information to all affected parties. In addition to prompt notification of termination to the appropriate parties, ThaiCA shall:

- Destroy all associated Private Keys
- Revoke all affected unexpired Certificates in existence
- Transfer all responsibilities for the affected CA and/or RA to an entity approved by TKC.

In case of a transfer of ThaiCA operations to another Trust Service Provider (TSP), a thorough migration plan will be created. All ThaiCA Subscribers will receive due notice of this transfer. During the transfer, all critical operations are expected to continue to function properly according to this CP/CPS.

In the event that ThaiCA decides upon a full CA business termination, ThaiCA will provide a timely notice (including a schedule for business termination) to allow Subscribers and other affected parties to switch to another TSP. When the scheduled termination time is reached, ThaiCA will revoke all issued Certificates, update the relevant CRLs and revoke its own root Certificates. Furthermore, it will inform interested third parties (such as Application Software Suppliers) about the end of its operation.

In either case, all files relating to certificate requests and the verification thereof, and all Certificates and revocation thereof, is kept for at least seven (7) years after any Certificate based on that documentation ceases to be valid in order to be available for any lawful control.

6 TECHNICAL SECURITY CONTROLS

TKC shall implement and maintain appropriate technical security controls to govern all operations of the ThaiCA PKI.

6.1 Key Pair Generation and Installation

TKC shall generate and install all CA Key Pairs in a physically secure environment on secure cryptographic equipment by personnel in trusted roles and using the methodology detailed in Section 6.1.1.

Access to physical modules shall be controlled as detailed in Section 6.2.

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

TKC CA Key Pairs shall be generated only within cryptographic modules as detailed in Section 6.2.

TKC shall generate CA Key Pairs only by means of a Key Generation Script ceremony. Key pairs and related Certificates are generated by multiple trusted individuals acting in specific trusted roles. The creation of intermediate CA keys is witnessed by an internal or external audit team. Especially for the issuance of a Root Certification Authority or for a subordinate Authority which is not under the control of the operator of the Root CA, the process is witnessed by an external Auditor or the CA Key Pair generation process is recorded and submitted to an external auditor who issues an appropriate opinion report.

6.1.1.2 Subscriber Key Pair Generation

TKC SHALL reject a certificate request if one or more of the following conditions are met:

1. The Key Pair does not meet the requirements set forth in Section 6.1.5 and/or Section 6.1.6;
2. There is clear evidence that the specific method used to generate the Private Key was flawed;
3. TKC is aware of a demonstrated or proven method that exposes the Applicant's Private Key to compromise;
4. TKC has previously been made aware that the Applicant's Private Key has suffered a Key Compromise, such as through the provisions of Section 4.9.1.1;
5. TKC is aware of a demonstrated or proven method to easily compute the Applicant's Private Key based on the Public Key (such as a Debian weak key, see https://wiki.debian.org/SSLkeys).

If the Subscriber Certificate will contain an extKeyUsage extension containing either the values id-kp-serverAuth [RFC5280] or anyExtendedKeyUsage [RFC5280], ThaiCA SHALL NOT generate a Key Pair on behalf of a Subscriber, and SHALL NOT accept a certificate request using a Key Pair previously generated by TKC.

With the exception of Key Pairs associated with TLS Certificates, ThaiCA MAY generate a Key Pair on behalf of a Subscriber.

Applicants requesting Document Signing must observe the criteria given in 6.2.1 regarding Key Pair generation and protection.

6.1.2 Private Key Delivery to Subscriber

In case ThaiCA generates a Key Pair on behalf of a Subscriber, the Private Key shall be provided to the Subscriber via a secure method. Private Keys may be delivered electronically (such as through secure email or storage in a secure cloud-based system) or in a hardware cryptographic module meeting the hardware requirements described in section 6.2.1.

TKC MAY generate and manage a Key Pair on behalf of a Subscriber as documented in section 6.2.1.

In all cases of Private Key delivery:

- TKC shall not retain access to the Subscriber's Private Key after delivery;
- TKC shall protect the Private Key from activation, compromise, or modification during the delivery process;
- The Subscriber must acknowledge receipt of the Private Key(s), and
- TKC must deliver the Private Key in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers, including:

```
a. For hardware modules, ThaiCA maintaining accountability for the
location and state of the module until the Subscriber accepts
possession of it and
b. For electronic delivery of Private Keys, ThaiCA encrypting key
material using a cryptographic algorithm and key size at least as
strong as the Private Key.
```

TKC shall deliver activation data to the Subscriber using a separate secure channel. The activation data shall be used to activate the Subscriber token or private keys on behalf of the Subcriber in a hardware cryptographic module meeting the requirements described in section 6.2.1.

TKC shall maintain a record of the Subscriber's acknowledgement of receipt of the device containing the Subscriber's Key Pair.

6.1.3 Public key delivery to certificate issuer

Public key delivery to ThaiCA must be by methods conforming to Section 3.2.1.

6.1.4 CA Public Key delivery to Relying Parties

TKC shall deliver Public Keys to Relying Parties in a secure manner that helps prevent opportunities for substitution attacks.

Third parties supporting ThaiCA Certificates (including but not limited to Application Software Suppliers, commercial browsers, and operating system trust stores), Subscribers and Relying Parties are permitted to use and redistribute any current, issued ThaiCA Root Certificate. These are published and maintained in the ThaiCA repository.

6.1.5 Key sizes

Certificates must meet the following requirements for algorithm type and key size.

(1) Root CA Certificates

Algorithm	Values
Digest algorithm	SHA-256, SHA-384 or SHA-512
Minimum RSA modulus size (bits)	2048
ECC curve	NIST P-256, P-384, or P-521

(2) Subordinate CA Certificates

Algorithm	Values
Digest algorithm	SHA-256, SHA-384 or SHA-512
Minimum RSA modulus size (bits)	2048
ECC curve	NIST P-256, P-384, or P-521

(3) Subscriber Certificates

Algorithm	Values
Digest algorithm	SHA-256, SHA-384 or SHA-512
Minimum RSA modulus size (bits)	2048
ECC curve	NIST P-256, P-384, or P-521

(4) All RSA key pairs shall have a modulus size, in bits, evenly divisible by 8.

6.1.6 Public key parameters generation and quality checking

RSA: ThaiCA SHALL confirm that the value of the public exponent is an odd number equal to 3 or more. Additionally, the public exponent SHOULD be in the range between 216+1 and 2256-1. The modulus SHOULD also have the following characteristics: an odd number, not the power of a prime, and have no factors smaller than 752. [Source: Section 5.3.3, NIST SP 800-89]

ECDSA: ThaiCA SHALL confirm the validity of all keys using either the ECC Full Public Key Validation Routine or the ECC Partial Public Key Validation Routine. [Source: Sections 5.6.2.3.2 and 5.6.2.3.3, respectively, of NIST SP 800-56A: Revision 2]

TKC generates CA Key Pairs using secure algorithms and parameters based on current research and industry standards.

TKC uses CA software that performs quality checks on generated keys for both RSA and ECC algorithms and also performs regular internal audits against randomly selected samples of Subscriber Certificates per section 8.7.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

TKC Issuing CA Private Keys shall only be utilized to sign Certificates for the following purposes:

1. Certificates for infrastructure purposes (e.g. administrative role Certificates, internal CA operational device Certificates)
2. Certificates for OCSP Response verification
3. Subscriber Certificates

6.2 Private Key Protection and Cryptographic Module Engineering Controls

TKC shall implement physical and logical safeguards to prevent unauthorized certificate issuance. Protection of CA Private Keys outside the validated system or device specified above must consist of physical security, encryption, or a combination of both, implemented in a manner that prevents disclosure of the CA Private Key. ThaiCA shall encrypt its Private Key with an algorithm and key-length that, according to the state of the art, are capable of withstanding cryptanalytic attacks for the residual life of the encrypted key or key part.

6.2.1 Cryptographic module standards and controls

All CA Private Keys shall be stored in a secure Hardware Security Module in order to perform key signing operations.

All CA Private Keys are stored and used only in a secure Hardware Security Module meeting FIPS 140-2 level 3 standards.

6.2.1.1 Secure cryptographic hardware devices for Key Pairs associated with Document Signing Certificates

For Document Signing Subscribers, ThaiCA shall ensure that the Subscriber's Private Key is generated:

1. either by using a trustworthy system, taking all reasonable precautions to prevent any loss, disclosure, or unauthorized use of the private key, and then securely transferred and protected by cryptographic means using a secure cryptographic hardware device conforming to this section 6.2.1.2, or,
2. directly generated and protected by a secure cryptographic hardware device
3. be stored in a secure cryptographic hardware device according to this section 6.2.1.2

All key pairs associated with Document Signing Certificates must be stored in a secure cryptographic hardware device that:

- is certified by:
    - FIPS 140-2 Level 2; or
    - Common Criteria (ISO 15408 & ISO 18045) - Protection Profiles CEN prEN 14169 (all parts applicable to the device type) or standards such as CEN EN 419 241 series or equivalent, for remotely managed devices; or
    - an EU Member State as a Qualified Signature Creation Device (QSCD) after 1 July 2016, or that was recognized as a Secure Signature Creation Device (SSCD) by an EU Member State designated body before 1 July 2016.
- is controlled by the signer (or by the subscriber if the signer is not a Natural Person):
    - either directly, by possession (after secure hand-over to the subscriber when applicable). In this case:
        - the activation of the private key must require the signer's authentication and
        - the device must prevent exportation or duplication of the private key.
    - or via a third party managing the secure cryptographic hardware device on behalf of the signer. In this case:
        - the key activation must rely on at least a 2-factor authentication (2FA) process, except from cases in which more flexibility is desirable; for example, in automated e-signing / e-sealing scenarios or when the Subscriber acknowledges and accepts the associated risks, and
        - no duplication of the private key is allowed, except for duly documented service availability purpose, and the duplicated key must abide at least the same security measures as the original;

Special controls are in place to ensure that any cryptographic hardware used has not been tampered with and is functioning correctly. The integrity of the hardware and software used for key generation, and of any interfaces used to access the hardware and software, is tested before production usage.

6.2.2 Private key (n out of m) multi-person control

TKC CA Private Keys (including backups) may only be activated and/or accessed by multiple persons acting in designated trusted roles (i.e., "n-of-m multi-person control") and using multi-factor authentication methods.

6.2.3 Private key escrow

No stipulation

6.2.4 Private key backup

TKC CA Private Keys are backed up via a secure and verifiable process by multiple persons acting in designated trusted roles.

Backup copies of ThaiCA CA Private Keys are securely maintained. The backup copy of any CA Private Keys is encrypted and the procedures referenced in Section 5.1.6 must be followed regarding media storage. Only authorized personnel are allowed access to any backup copy of any CA Private Key.

Private key backup for Subscriber Certificates (if such an action is technically feasible) is exclusively under the control of the Subscriber.

Backup keys of ThaiCA CA Private Keys shall only exist in encrypted form and shall never exist as plain text outside of a cryptographic module (see Section 6.2.1).

All copies of the CA Private Keys, including signing keys, are put beyond use at the end of their life cycle.

6.2.5 Private key archival

TKC shall not archive Private Keys.

6.2.6 Private key transfer into or from a cryptographic module

Transfer of any ThaiCA CA Private Keys into or from any hardware security module shall follow a secure and verifiable process conducted by multiple persons acting in designated trusted roles.

Transferred ThaiCA CA Private Keys shall only exist in encrypted form and shall never exist as plain text outside of a cryptographic module (see Section 6.2.1).

6.2.7 Private key storage on cryptographic module

TKC creates, stores and utilizes CA Private Keys within a secure Hardware Security Module as described in Section 6.2.1. Root Private Keys are stored offline in cryptographic modules or backup tokens.

6.2.8 Method of activating Private Key

TKC activates CA Private Keys using only methods which observe the instructions and specifications of the manufacturer of the relevant cryptographic module and via a secure and verifiable process, conducted by multiple persons acting in designated trusted roles and using multi-factor authentication.

Applicants and Subscribers are instructed to protect their Private Keys using the standards described in the appropriate Subscriber Agreement. Subscribers are solely responsible for protecting their Private Keys.

6.2.9 Method of deactivating Private Key

TKC CA Private Keys maintained in any cryptographic hardware shall be deactivated when not in use, using documented procedures which ensure that appropriate physical and logical security controls are observed.

6.2.10 Method of destroying Private Key

CA Private Keys shall be destroyed when they are no longer needed. As part of the process of destruction of a CA Private Key:

- Any CA Private Key stored in any Hardware Security Module (HSM) is destroyed using the secure deletion function of the HSM, per the manufacturer's instructions. Only the physical instance of the CA Private Key stored in the HSM under consideration will be destroyed.
- Any other encrypted copies and fragments of the CA Private Key shall be destroyed over a reasonable amount of time.

If a CA cryptographic device is being permanently removed from service, then any CA Private Key contained within the device used for any cryptographic purpose is erased from the device. If a CA cryptographic device case is intended to provide tamper-evident characteristics and the device is being permanently removed from service, then the case is destroyed.

The destruction of any CA Private Key and/or CA cryptographic device shall only be performed by appropriate personnel acting in trusted roles and documented using verifiable methods.

Subscribers are solely responsible for the complete and secure destruction of all copies and fragments of the Subscriber's Private Key at the end of the Key Pair life cycle.

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

TKC archives Public Keys as described in Section 5.5.

6.3.2 Certificate operational periods and Key Pair usage periods

The maximum validity period of CA Certificates is:

- **Twenty-five (25) years** for Root CAs,
- **Fifteen (15) years** for Intermediate CAs.

The maximum validity period of end-entity Certificates is:

- **Twenty four (24) months** for digital signing certificates
- **One (1) day for short lived digital signing certificates**

The operational period must be defined according to the size of the keys and the current technological developments at the field of cryptography to guarantee the best level of security and efficiency of use.

Subscribers should not reuse Key Pairs when requesting new certificates.

6.3.3 Public key destruction

Public keys are stored in the database for the duration of the archival period. Once the archival period is over, public keys may be destroyed by secure delete of the information in the archive database.

6.4 Activation data

TKC shall protect and secure any data used to activate any CA Private Key utilized in the ThaiCA PKI, including any PIN, passphrase, or portion of a Private Key used in a key-splitting scheme. See also Section 6.2.8.

6.4.1 Activation Data Generation and Installation

TKC shall activate and install ThaiCA CA Private Keys into any cryptographic module using only methods which observe the instructions and specifications of the manufacturer of the relevant cryptographic module. Initial generation, activation and installation shall be via a CA key ceremony as described in Section 6.1.1.1.

Separately generated and secured Activation Data is used to protect access to Private Keys in cases where ThaiCA generates Key Pairs for Subscribers.

6.4.2 Activation data protection

TKC shall protect activation data from compromise or disclosure. Appropriate cryptographic and physical access controls shall be implemented to prevent unauthorized use of any CA Private Key activation data.

In cases where ThaiCA generates Key Pairs for Subscribers, ThaiCA shall only provide Activation Data via a secure channel which is separate from delivery of the cryptographic module containing the related Private Key.

6.4.3 Other aspects of activation data

All activation data related to ThaiCA CA Private Keys and associated root Certificates is held only by ThaiCA personnel holding clearly defined trusted roles.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

All systems used as part of the ThaiCA PKI (including CA servers, support and vetting workstations, and systems utilized by trusted third parties) are:

- Configured, maintained and secured using industry best practices
- Operated on trustworthy software
- Regularly scanned for malicious code and protected against spyware and viruses
- Updated with recommended security patches within six months of the security patch's availability, unless documented testing determines that the security patch would introduce additional vulnerabilities

All systems are configured to:

- Authenticate the identity of users before permitting access to the system or applications
- Manage the privileges of users and limit users to their assigned roles
- Generate and archive audit records for all transactions
- Enforce domain integrity boundaries for security critical processes, and
- Support recovery from key or system failure.

Where practicable, ThaiCA shall implement multi-factor authentication to each PKI component that supports multi-factor authentication, including accounts capable of directly causing certificate issuance.

6.5.2 Computer security rating

No stipulation.

6.6 Life cycle technical controls

6.6.1 System development controls

TKC CA's system development controls include (but are not limited to) the following:

- All software used for CA systems follows a documented development process prior to implementation
- All components of the CA system, including all hardware and software, are obtained in a manner that reduces the probability that hardware or software has been falsified, modified or tampered with in any way
- All hardware used in CA systems shall be shipped and/or delivered using secure packing methodology (including tamperproof packaging where appropriate) along with complete tracking records
- The hardware and software used for CA systems are specifically used to performing CA activities, and only software, hardware or network connections directly required for CA operations are installed or permitted
- All hardware and software updates to CA systems are documented, and are securely purchased, developed, and/or installed only by personnel holding a Trusted role

6.6.2 Security management controls

TKC incorporates system-wide security controls and monitoring to CA software configurations. A documented process is used to authenticate modification, installation, and management of software utilized in or interacting with CA systems.

6.6.3 Life cycle security controls

No stipulation.

6.7 Network security controls

TKC maintains network security controls to protect all operations related to the ThaiCA PKI.

These controls observe the standards established in the most recent version of the CAB Forum Network and Certificate System Security Requirements (https://cabforum.org/network-security-requirements/)

All ThaiCA PKI-related systems are segmented into networks or zones based on their functional, logical, and/or physical relationship. The same security controls are applied to all systems co-located in the same zone or network. To protect data confidentiality, integrity, and availability, systems, networks and communications are protected by appropriate physical and logical controls to protect data confidentiality, integrity, and availability including (but not limited to) firewalls, filters, port blocking and any other hardware or software methods deemed appropriate.

TKC implements measures to protect PKI-related systems and communications within and between these zones and networks, and to also secure all communications between these zones and networks and:

- Non-PKI-related systems, networks and/or zones, including those ThaiCA and/or third party systems that do not provide PKI-related services) and
- Any systems on public networks

All network boundary control devices or systems (including firewalls, switches, routers, gateways, or other devices) are configured with rules to allow only services, protocols, ports, and communications necessary for operations. All systems supporting ThaiCA PKI operations (including third-party systems) are configured to use only accounts, applications, services, protocols, and ports approved by TKC.

Physical access to hardware utilized for ThaiCA CA Private Keys, including cryptographic modules and related devices, is secured within a facility which meets the approval of Qualified Auditors (see Section 5.1.2).

Administrator (or higher) access to systems is only granted to a person acting in an accountable Trusted Role (per Section 5.2.1) and any such access is logged (see Section 5.4.1).

TKC continually reviews system configurations to detect and correct departures from these security controls.

6.8 Time-stamping

TKC shall ensure that the accuracy of time sources used in all time-stamping operations are properly maintained, trusted and verifiable via NTP (Network Time Protocol). ThaiCA incorporates a manual and digital process which work in tandem to ensure authenticity of system time. ThaiCA used the Swedish Distributed Time Service (NTS) is a time synchronization service provided by Swedish to offer highly accurate and reliable time for systems, networks, and various applications. It is part of a broader initiative to ensure that the country's critical infrastructure and technological systems remain synchronized, contributing to a stable and precise timekeeping environment.

More information is also available in Section 5.5.5.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profiles

TKC shall meet the technical requirements set forth in Sections 2.2, 6.1.5 and 6.1.6 of the ThaiCA CP/CPS.

TKC shall generate Certificate serial numbers greater than zero (0) containing at least 64 bits of output from a CSPRNG.

7.1.1 Version Numbers

The ThaiCA PKI issues Certificates in compliance with the X.509 Version 3, which corresponds to certificate version number 2.

7.1.2 Certificate Content and Extensions

TKC Certificates comply with RFC 5280 and with applicable best industry practices.

A tabled view of the most common certificate profiles used by ThaiCA are listed in Annex A (TKC Certificate Profiles).

7.1.2.1 Root CA Certificate

Root CA certificate is issued by NRCA and is specified in the CP/CPS document released and maintained by NRCA

7.1.2.2 Subordinate CA Certificate

a. certificatePolicies

   This extension must be present and should not be marked critical.

- certificatePolicies:policyIdentifier (Required): See Section 7.1.6

  The following fields may be present if the Subordinate CA is not an Affiliate of TKC.

  - certificatePolicies:policyQualifiers:policyQualifierId (Optional)
    - id-qt 1 [RFC 5280]
    - certificatePolicies:policyQualifiers:qualifier:cPSuri (Optional)
  - HTTP URL for the Root CA's Certificate Policy, Certification Practice Statement, Relying Party Agreement, or other pointer to online policy information provided by ThaiCA and the Subordinate CA.

b. cRLDistributionPoints (if applicable)

   This extension must be present. It contains the HTTP URL of the Issuing CA's CRL service.

c. authorityInformationAccess (if applicable)

If the Issuing CA issues Code Signing or Time-stamping Certificates, this extension MUST be present and MUST NOT be marked critical. The extension MUST contain the HTTP URL of the Issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2) and if the CA provides OCSP responses, the HTTP URL for the CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1).

For all other Issuing CAs this extension SHOULD be present. It MUST NOT be marked critical. It SHOULD contain the HTTP URL of the Issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2) and it MAY contain the HTTP URL of the Issuing CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1).

d. basicConstraints (critical)

The cA field is set true. The pathLenConstraint field may be present.

e. keyUsage (critical)

keyCertSign and cRLSign bits are set. Optionally, digitalSignature can be set.

f. nameConstraints (optional)

If present, this extension should not be marked critical*.

* Non-critical Name Constraints are an exception to RFC 5280 (4.2.1.10), however, they may be used until the Name Constraints extension is supported by Application Software Suppliers whose software is used by a substantial portion of Relying Parties worldwide.

g. extkeyUsage (optional)

For Cross Certificates that share a Subject Distinguished Name and Subject Public Key with a Root Certificate operated in accordance with this CP/CPS, this extension MAY be present. If present, this extension SHOULD NOT be marked critical. This extension MUST only contain usages for which the issuing CA has verified the Cross Certificate is authorized to assert. This extension MAY contain the `anyExtendedKeyUsage` [RFC5280] usage, if the Root Certificate(s) associated with this Cross Certificate are operated by the same organization as the issuing Root Certificate.

For all other Subordinate CA Certificates, including Technically Constrained Subordinate CA Certificates:

This extension MUST be present and SHOULD NOT be marked critical.

For Subordinate CA Certificates that will be used to issue TLS certificates, the value `id-kp-serverAuth` [RFC5280] MUST be present. The value `id-kp-clientAuth` [RFC5280] MAY be present. The values `id-kp-emailProtection` [RFC5280], `id-kp-codeSigning` [RFC5280], `id-kp-timeStamping` [RFC5280], and `anyExtendedKeyUsage` [RFC5280] MUST NOT be present. Other values SHOULD NOT be present.

For Subordinate CA Certificates that are not used to issue TLS certificates, then the value `id-kp-serverAuth` [RFC5280] MUST NOT be present. Other values MAY be present, but SHOULD NOT combine multiple independent key purposes (e.g. including `id-kp-timeStamping` [RFC5280] with `id-kp-codeSigning` [RFC5280]).

h. authorityKeyIdentifier (required)

This extension MUST be present and MUST NOT be marked critical. It MUST contain a keyIdentifier field and it MUST NOT contain a authorityCertIssuer or authorityCertSerialNumber field.

By issuing a Subordinate CA Certificate, ThaiCA represents that it followed the procedure set forth in this CP/CPS to verify that, as of the CA Certificate's issuance date, all of the Subject Information was validated and found to be accurate.

7.1.2.3 Subscriber Certificate

a. certificatePolicies

This extension must be present and should not be marked critical.

- certificatePolicies:policyIdentifier (Required): (See Section 7.1.6)

The following extensions may be present:

- certificatePolicies:policyQualifiers:policyQualifierId (Recommended)
  - id-qt 1 [RFC 5280]
- certificatePolicies:policyQualifiers:qualifier:cPSuri (Optional)
  - HTTP URL for the Subordinate CA's Certificate Policyies, Certification Practice Statement, Relying Party Agreement, or other pointer to online policy information provided by ThaiCA and the Subordinate CA.

g. cRLDistributionPoints (if applicable)

For TLS Certificates, this extension MAY be present and for Code Signing or Timestamping Certificates it MUST be present. If present, it MUST NOT be marked critical and it MUST contain the HTTP URL of the Issuing CA's CRL service.

h. authorityInformationAccess (if applicable)

For TLS, Code Signing and Time-stamping Certificates this extension MUST be present and for other types of Certificates it MAY be present. If present, it MUST NOT be marked critical. For TLS Certificates it MUST contain the HTTP URL of the Issuing CA's OCSP responder (`accessMethod` = 1.3.6.1.5.5.7.48.1) and SHOULD contain the HTTP URL of the Issuing CA's certificate (`accessMethod` = 1.3.6.1.5.5.7.48.2). For Code Signing or Timestamping Certificates, it MUST contain the HTTP URL of the Issuing CA's certificate (`accessMethod` = 1.3.6.1.5.5.7.48.2) and if the CA provides OCSP responses, the HTTP URL for the CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1). For all other Subscriber Certificates, it MAY

contain the HTTP URL of the Issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2) and if the CA provides OCSP responses, the HTTP URL for the CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1).

i. basicConstraints (optional)

This extension should not be present. If present, the cA field must be set false.

j. keyUsage (required)

If present, bit positions for keyCertSign and cRLSign must not be set.

For signing certificates digitalSigning must be set. nonRepudiation may be set

For authentication certificates digitalSigning must be set

k. extKeyUsage (required)

Depending on the usage of the certificate, the proper extended key usage (EKU) will be applied. More information available in Annex A.

For digital signing certificates no extension is set

For machine authentication certificates id-kp-clientAuth

For Timestamp Certificates, this extention MUST be marked critical. For other types, the extention SHOULD NOT be marked critical.

For SSL/TLS Certificates either the value `id-kp-serverAuth` [RFC5280] or `id-kp-clientAuth` [RFC5280] or both values MUST be present. `id-kp-emailProtection` [RFC5280] MAY be present. Other values SHOULD NOT be present. The value `anyExtendedKeyUsage` MUST NOT be present.

For Code Signing Certificates the value `id-kp-codeSigning` [RFC5280] MUST be present. The value `lifetimeSigning` (1.3.6.1.4.1.311.10.3.13) MAY be present. The value `anyExtendedKeyUsage` (2.5.29.37.0), `serverAuth` (1.3.6.1.5.5.7.3.1), `emailProtection` (1.3.6.1.5.5.7.3.4) and `timeStamping` (1.3.6.1.5.5.7.3.8) MUST NOT be present. Other values SHOULD NOT be present. If any other value is present, ThaiCA MUST have a business agreement with a Platform vendor requiring that EKU in order to issue a Platform-specific code signing certificate with that EKU.

For Timestamp Certificates the value `id-kp-timeStamping` [RFC5280] MUST be present. The value `anyExtendedKeyUsage` (2.5.29.37.0), `serverAuth` (1.3.6.1.5.5.7.3.1), `emailProtection` (1.3.6.1.5.5.7.3.4) and `codeSigning` [RFC5280] MUST NOT be present. Other values SHOULD NOT be present. If any other value is present, ThaiCA MUST have a business agreement with a Platform vendor requiring that EKU in order to issue a Platform-specific code signing certificate with that EKU.

It is forbidden for Intermediate CAs to issue end-entity Certificates which blend the serverAuth (1.3.6.1.5.5.7.3.1), emailProtection (1.3.6.1.5.5.7.3.2) and codeSigning (1.3.6.1.5.5.7.3.3) extended key usages.

7.1.2.4 All Certificates

All other fields and extensions must be set in accordance with RFC 5280. ThaiCA shall not issue a Certificate that contains a keyUsage flag, extKeyUsage value, Certificate extension, or other data not specified in Sections 7.1.2.1, 7.1.2.2, 7.1.2.3 and Annex A unless ThaiCA is aware of a reason for including the data in the Certificate.

All Certificates include the following extensions:

- Authority Key Identifier: Provides information to identify the Public Key corresponding to the Private Key used to sign a Certificate. This field contains the "Subject Key Identifier" of the issuing CA's Certificate
- Subject Key Identifier: Identifies a particular Public Key uniquely. It contains the ID of the Certificate Holder's key

7.1.2.5 Application of RFC 5280

For purposes of clarification, a Precertificate, as described in RFC 6962 - Certificate Transparency, shall not be considered to be a "certificate" subject to the requirements of RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

7.1.3 Algorithm object identifiers

7.1.3.1 SubjectPublicKeyInfo

The following requirements apply to the `subjectPublicKeyInfo` field within a Certificate or Precertificate. No other encodings are permitted.

7.1.3.1.1 RSA

TKC SHALL indicate an RSA key using the rsaEncryption (OID: 1.2.840.113549.1.1.1) algorithm identifier. The parameters MUST be present, and MUST be an explicit NULL. ThaiCA SHALL NOT use a different algorithm, such as the id-RSASSA-PSS (OID: 1.2.840.113549.1.1.10) algorithm identifier, to indicate an RSA key.

When encoded, the `AlgorithmIdentifier` for RSA keys MUST be byte-for-byte identical with the following hex-encoded bytes: `300d06092a864886f70d0101010500`

7.1.3.1.2 ECDSA

TKC SHALL indicate an ECDSA key using the id-ecPublicKey (OID: 1.2.840.10045.2.1) algorithm identifier. The parameters MUST use the `namedCurve` encoding.

- For P-256 keys, the `namedCurve` MUST be secp256r1 (OID: 1.2.840.10045.3.1.7).
- For P-384 keys, the `namedCurve` MUST be secp384r1 (OID: 1.3.132.0.34).

- For P-521 keys, the `namedCurve` MUST be secp521r1 (OID: 1.3.132.0.35).

When encoded, the `AlgorithmIdentifier` for ECDSA keys MUST be byte-for-byte identical with the following hex-encoded bytes:

- For P-256 keys, `301306072a8648ce3d020106082a8648ce3d030107`.
- For P-384 keys, `301006072a8648ce3d020106052b81040022`.
- For P-521 keys, `301006072a8648ce3d020106052b81040023`.

7.1.3.2 Signature AlgorithmIdentifier

All objects signed by a CA Private Key MUST conform to this CP/CPS on the use of the `AlgorithmIdentifier` or `AlgorithmIdentifier`-derived type in the context of signatures.

In particular, it applies to all of the following objects and fields:

- The `signatureAlgorithm` field of a Certificate or Precertificate.
- The `signature` field of a TBSCertificate (for example, as used by either a Certificate or Precertificate).
- The `signatureAlgorithm` field of a CertificateList
- The `signature` field of a TBSCertList
- The `signatureAlgorithm` field of a BasicOCSPResponse.

No other encodings are permitted for these fields.

7.1.3.2.1 RSA

TKC SHALL use one of the following signature algorithms and encodings. When encoded, the `AlgorithmIdentifier` MUST be byte-for-byte identical with the specified hex-encoded bytes.

- RSASSA-PKCS1-v1_5 with SHA-256:

  Encoding: `300d06092a864886f70d01010b0500`.

- RSASSA-PKCS1-v1_5 with SHA-384:

  Encoding: `300d06092a864886f70d01010c0500`.

- RSASSA-PKCS1-v1_5 with SHA-512:

  Encoding: `300d06092a864886f70d01010d0500`.

- RSASSA-PSS with SHA-256, MGF-1 with SHA-256, and a salt length of 32 bytes:

  Encoding:

  ```
  304106092a864886f70d01010a3034a00f300d060960864801650304020105
  00a11c301a06092a864886f70d010108300d060960864801650304020105
  00a203020120
  ```

- RSASSA-PSS with SHA-384, MGF-1 with SHA-384, and a salt length of 48 bytes:

  Encoding:

  ```
  304106092a864886f70d01010a3034a00f300d060960864801650304020205
  00a11c301a06092a864886f70d010108300d060960864801650304020205
  00a203020130
  ```

- RSASSA-PSS with SHA-512, MGF-1 with SHA-512, and a salt length of 64 bytes:

  Encoding:

  ```
  304106092a864886f70d01010a3034a00f300d060960864801650304020305
  00a11c301a06092a864886f70d010108300d060960864801650304020305
  00a203020140
  ```

In addition, ThaiCA MAY use the following signature algorithm and encoding if all of the following conditions are met:

- If used within a Certificate, such as the `signatureAlgorithm` field of a Certificate or the `signature` field of a TBSCertificate:
  - The new Certificate is a Root CA Certificate or Subordinate CA Certificate that is a Cross-Certificate; and,
  - There is an existing Certificate, issued by the same issuing CA Certificate, using the following encoding for the signature algorithm; and,
  - The existing Certificate has a `serialNumber` that is at least 64-bits long; and,
  - The only differences between the new Certificate and existing Certificate are one of the following:
    - A new `subjectPublicKey` within the `subjectPublicKeyInfo`, using the same algorithm and key size; and/or,
    - A new `serialNumber`, of the same encoded length as the existing Certificate; and/or
    - The new Certificate's `extKeyUsage` extension is present, has at least one key purpose specified, and none of the key purposes specified are the id-kp-serverAuth (OID: 1.3.6.1.5.5.7.3.1) or the anyExtendedKeyUsage (OID: 2.5.2937.0) key purposes; and/or
    - The new Certificate's `basicConstraints` extension has a pathLenConstraint that is zero.
- If used within an OCSP response, such as the `signatureAlgorithm` of a BasicOCSPResponse:
  - The `producedAt` field value of the ResponseData MUST be earlier than 2022-06-01 00:00:00 UTC; and,
  - All unexpired, un-revoked Certificates that contain the Public Key of the CA Key Pair and that have the same Subject Name MUST also contain an `extKeyUsage` extension with the only key usage present being the id-kp-ocspSigning (OID: 1.3.6.1.5.5.7.3.9) key usage.

- If used within a CRL, such as the `signatureAlgorithm` field of a CertificateList or the `signature` field of a TBSCertList:
    - The CRL is referenced by one or more Root CA or Subordinate CA Certificates; and,
    - The Root CA or Subordinate CA Certificate has issued one or more Certificates using the following encoding for the signature algorithm.

Note: The above requirements do not permit ThaiCA to sign a Precertificate with this encoding.

- RSASSA-PKCS1-v1_5 with SHA-1:

  Encoding: `300d06092a864886f70d0101050500`

7.1.3.2.2 ECDSA

TKC SHALL use the appropriate signature algorithm and encoding based upon the signing key used.

If the signing key is P-256, the signature MUST use ECDSA with SHA-256. When encoded, the `AlgorithmIdentifier` MUST be byte-for-byte identical with the following hex-encoded bytes: `300a06082a8648ce3d040302`.

If the signing key is P-384, the signature MUST use ECDSA with SHA-384. When encoded, the `AlgorithmIdentifier` MUST be byte-for-byte identical with the following hex-encoded bytes: `300a06082a8648ce3d040303`.

If the signing key is P-521, the signature MUST use ECDSA with SHA-512. When encoded, the `AlgorithmIdentifier` MUST be byte-for-byte identical with the following hex-encoded bytes: `300a06082a8648ce3d040304`.

7.1.4 Name forms

TKC Certificates support name chaining as specified in RFC 5280. All issued Certificates incorporate a unique identifying serial number.

7.1.4.1 Name Encoding

The content of the Certificate Issuer Distinguished Name field must match the Subject DN of the Issuing CA to support Name chaining as specified in RFC 5280, Section 4.1.2.4.

For every valid Certification Path (as defined by RFC 5280, Section 6):

- For each Certificate in the Certification Path, the encoded content of the Issuer Distinguished Name field of a Certificate SHALL be byte-for-byte identical with the encoded form of the Subject Distinguished Name field of the Issuing CA certificate.
- For each CA Certificate in the Certification Path, the encoded content of the Subject Distinguished Name field of a Certificate SHALL be byte-for-byte identical among all Certificates whose Subject Distinguished Names can be compared as equal according to RFC 5280, Section 7.1, and including expired and revoked Certificates.

7.1.4.2 Subject Information - Subscriber Certificates

By issuing a Server Certificate, ThaiCA represents that it followed the procedures set forth in this CP/CPS to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate. ThaiCA shall not include a Domain Name or IP Address in a Subject attribute except as specified in Section 3.2.2.4 or Section 3.2.2.5. Subject attributes MUST NOT contain only metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.

By issuing a Personal/Client/CodeSigning Certificate, ThaiCA represents that it followed the procedures set forth in this CP/CPS to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate. ThaiCA shall not include a commonName, emailAddress in a Subject attribute except as specified in Section 3.2.3. Because Subject name attributes for individuals (e.g. givenName (2.5.4.42) and surname (2.5.4.4)) are not broadly supported by application software, ThaiCA may use the subject:organizationName field to convey a natural person Subject's name or DBA.

7.1.4.2.1 Subject Alternative Name Extension

Certificate Field: extensions:subjectAltName

- Required/Optional:
  - **Optional** for Digital Signing Certificates

This extension must contain at least one entry. Each entry SHALL be one of the following types:

- `dNSName`: The entry SHALL contain either a Fully-Qualified Domain Name or Wildcard Domain Name that ThaiCA has validated in accordance with Section 3.2.2.4. Wildcard Domain Names SHALL be validated for consistency with Section 3.2.2.6. The entry SHALL NOT contain an Internal Name. Underscore characters ("_") SHALL NOT be present in `dNSName` entries.

  The Fully-Qualified Domain Name or the FQDN portion of the Wildcard Domain Name contained in the entry SHALL be composed entirely of LDH Labels joined together by a U+002E FULL STOP (".") character. The zero-length Domain Label representing the root zone of the Internet Domain Name System SHALL NOT be included (e.g. "example.com" SHALL be encoded as "example.com" and SHALL NOT be encoded as "example.com.").

  Effective 2021-10-01, the Fully-Qualified Domain Name or the FQDN portion of the Wildcard Domain Name SHALL consist solely of Domain Labels that are P-Labels or Non-Reserved LDH Labels.

- `iPAddress`: The entry SHALL contain an IPv4 or IPv6 address that ThaiCA has validated in accordance with Section 3.2.2.5. The entry SHALL NOT contain a Reserved IP Address.

7.1.4.2.2 Subject Distinguished Name Fields

a. Certificate Field: subject:commonName (OID 2.5.4.3)

- Required/Optional:
  - **Deprecated** (Discouraged, but not prohibited) for SSL Certificates or S/MIME Certificates
  - **Required** for Code Signing
- **Contents for SSL Server Certificates:** If present, this field MUST contain exactly one entry that is one of the values contained in the Certificate's `subjectAltName` extension (see Section 7.1.4.2.1). The value of the field MUST be encoded as follows:
  - If the value is an IPv4 address, then the value MUST be encoded as an IPv4Address as specified in RFC 3986, Section 3.2.2.
  - If the value is an IPv6 address, then the value MUST be encoded in the text representation specified in RFC 5952, Section 4.
  - If the value is a Fully-Qualified Domain Name or Wildcard Domain Name, then the value MUST be encoded as a character-for-character copy of the `dNSName` entry value from the `subjectAltName` extension. Specifically, all Domain Labels of the Fully-Qualified Domain Name or FQDN portion of the Wildcard Domain Name must be encoded as LDH Labels, and P-Labels MUST NOT be converted to their Unicode representation.
- **Contents for Code Signing Certificates:** This field must contain the Subject's legal name as verified under Section 3.2.2.2.
- **Contents for SSL or Code Signing or S/MIME Certificates:** If present, the subject:organizationName field must contain either the Subject's name or DBA as verified under Section 3.2.2.2. ThaiCA may include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that ThaiCA documents the difference and any abbreviations used are locally accepted abbreviations; e.g., if the official record shows "Company Name Incorporated", ThaiCA may use "Company Name Inc." or "Company Name". Because Subject name attributes for individuals (e.g. givenName (2.5.4.42) and surname (2.5.4.4)) are not broadly supported by application software, ThaiCA may use the subject:organizationName field to convey a natural person Subject's name or DBA.

If the combination of names or the organization name by itself exceeds 64 characters, ThaiCA may abbreviate parts of the organization name, and/or omit non-material words in the organization name in such a way that the text in this field does not exceed the 64-character limit. ThaiCA shall check this field in accordance with Section 4.2.1 and a Relying Party will not be misled into thinking that they are dealing with a different organization.

c. Certificate Field: subject:givenName (2.5.4.42) and subject:surname (2.5.4.4)

- **Contents:** If present, the subject:givenName field and subject:surname field MUST contain a natural person Subject's name as verified under Section 3.2.3. A SSL/TLS Certificate containing a subject:givenName field or subject:surname field MUST contain the (2.23.140.1.2.3) Certificate Policy OID.

d. Certificate Field: Number and street: subject:streetAddress (OID: 2.5.4.9)

- Required/Optional:

- **Optional** if the subject:organizationName field, subject:givenName field, or subject:surname field are present.
- **Prohibited** if the subject:organizationName field, subject:givenName, and subject:surname field are absent.

- **Contents for SSL, Code Signing or S/MIME Certificates:** If present, the subject:streetAddress field must contain the Subject's street address information as verified under Section 3.2.2.1.
- **Contents for SSL, Code Signing or S/MIME Certificates:** If the subject:organizationName field is present, the subject:countryName must contain the two-letter ISO 3166-1 country code associated with the location of the Subject verified under Section 3.2.2.1. If the subject:organizationName field is absent, the subject:countryName field may contain the two-letter ISO 3166-1 country code associated with the Subject as verified in accordance with Section 3.2.2.3. If a Country is not represented by an official ISO 3166-1 country code, ThaiCA may specify the ISO 3166-1 user-assigned code of XX indicating that an official ISO 3166-1 alpha-2 code has not been assigned.

7.1.4.3 Subject Information –Subordinate CA Certificates

By issuing a Subordinate CA Certificate, ThaiCA represents that it followed the procedure set forth in this CP/CPS to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate.

7.1.4.3.1 Subject Distinguished Name Fields

a. Certificate Field: subject:commonName (OID 2.5.4.3)

- Required/Optional: **Required**
- **Contents:** This field MUST be present and the contents SHOULD be an identifier for the certificate such that the certificate's Name is unique across all certificates issued by the issuing certificate.

b. Certificate Field: subject:organizationName (OID 2.5.4.10)

Required/Optional: **Required**

- **Contents:** This field MUST be present and the contents MUST contain either the Subject CA's name or DBA as verified under Section 3.2.2.2. ThaiCA may include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that ThaiCA documents the difference and any abbreviations used are locally accepted abbreviations; e.g., if the official record shows "Company Name Incorporated", ThaiCA MAY use "Company Name Inc." or "Company Name".

c. Certificate Field: subject:countryName (OID: 2.5.4.6)

- Required/Optional: **Required**
- **Contents:** This field MUST contain the two-letter ISO 3166-1 country code for the country in which the CA's place of business is located.

7.1.5 Name Constraints

TKC reserves the right to issue Certificates with name constraints and/or marked as critical when deemed necessary.

If ThaiCA decides to apply Name Constraints and if the Subordinate CA Certificate includes the "id-kp-serverAuth" [RFC 5280] extended key usage, then the Subordinate CA Certificate must include the Name Constraints X.509v3 extension with constraints on dNSName, iPAddress and DirectoryName as follows:

a. For each dNSName in permittedSubtrees, ThaiCA must confirm that the Applicant has registered the dNSName or has been authorized by the domain registrant to act on the registrant's behalf in line with the verification practices of Section 3.2.2.4.

b. For each iPAddress range in permittedSubtrees, ThaiCA must confirm that the Applicant has been assigned the iPAddress range or has been authorized by the assigner to act on the assignee's behalf.

c. For each DirectoryName in permittedSubtrees ThaiCA must confirm the Applicant's and/or Subsidiary's Organizational name and location such that end entity Certificates issued from the subordinate CA Certificate will be in compliance with Section 7.1.2.4 and 7.1.2.5.

If the Subordinate CA Certificate is not allowed to issue Certificates with an iPAddress, then the Subordinate CA Certificate must specify the entire IPv4 and IPv6 address ranges in excludedSubtrees. The Subordinate CA Certificate must include within excludedSubtrees an iPAddress GeneralName of 8 zero octets (covering the IPv4 address range of 0.0.0.0/0). The Subordinate CA Certificate must also include within excludedSubtrees an iPAddress GeneralName of 32 zero octets (covering the IPv6 address range of ::0/0). Otherwise, the Subordinate CA Certificate must include at least one iPAddress in permittedSubtrees.

A decoded example for issuance to the domain and sub domains of example.com by organization: "Example LLC, Boston, Massachusetts, US" would be:

X509v3 Name Constraints: Permitted: DNS:example.com DirName: C=US, ST=MA, L=Boston, O=Example LLC Excluded: IP:0.0.0.0/0.0.0.0 IP:0:0:0:0:0:0:0:0/0:0:0:0:0:0:0:0

If the Subordinate CA is not allowed to issue Certificates with dNSNames, then the Subordinate CA Certificate must include a zero-length dNSName in excludedSubtrees. Otherwise, the Subordinate CA Certificate must include at least one dNSName in permittedSubtrees.

7.1.6 Certificate Policy object identifier

The OID (Object Identifier) of this CP/CPS is documented in section 1.2.1.

A special OID arc has been allocated by ThaiCA based on a certain certificate type:

```
iso (1) org (3) dod (6) internet (1) private (4) enterprise (1) ThaiCA
(62483) certificationServicesProvision (1) certificateTypes (3)
```

TKC issues Certificates containing the following OIDs / OID arcs:

Digitally Signed Object	Policy Object Identifier (OID)
Digital Signing Certificates	**1.3.6.1.4.1.642483.1.3.1**
Digital Signing Certificates for Legal Persons (RSA)	**1.3.6.1.4.1.62483.1.3.1.1**
Digital Signing Certificates for Organisations (RSA)	**1.3.6.1.4.1.62483.1.3.1.2**
Digital Signing Certificates for Organisation Representatives (RSA)	**1.3.6.1.4.1.62483.1.3.1.3**
Digital Signing Certificates – Short lived for legal persons (ECC)	**1.3.6.1.4.1.62483.1.3.1.8**
Digital Signing Certificates for Legal Persons (ECC)	**1.3.6.1.4.1.62483.1.3.1.4**
Digital Signing Certificates for Organisations (ECC)	**1.3.6.1.4.1.62483.1.3.1.5**
Digital Signing Certificates for Organisation Representatives (ECC)	**1.3.6.1.4.1.62483.1.3.1.6**
Digital Signing Certificates – Short lived for legal persons (ECC)	**1.3.6.1.4.1.62483.1.3.1.7**
Time-Stamping	**1.3.6.1.4.1.62483.1.3.3**
OCSP Responder Certificate	**1.3.6.1.4.1.62483.1.3.7**

These ThaiCA custom Policy OIDs are used when Certificates are signed pursuant to this CP/CPS are indicated in the certificate's respective certificatePolicies extension. When a Certificate is issued containing a certain policy identifier which is indicated as compatible with the "CA/B Forum Policy OID X" , it asserts that the Certificate was issued and is managed in accordance with those applicable requirements AND the provisions of this CP/CPS.

SSL/TLS Subscriber Certificates MUST contain, within the Certificate's certificatePolicies extension, one or more policy identifier(s) that are specified beneath the CA/Browser Forum's reserved policy OID arc of {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1)} (2.23.140.1).

Subordinate CAs that are Affiliated with ThaiCA can use the reserved `AnyPolicy` OID **2.5.29.32.0**.

7.1.7 Usage of Policy Constraints extension

No stipulation

7.1.8 Policy qualifiers syntax and semantics

TKC's policy qualifier field includes information relying parties may consult in order to determine any limitations a certificate may have.

7.1.9 Processing semantics for the critical Certificate Policies extension

No stipulation

7.2 CRL Profile

7.2.1 Version Numbers

TKC's PKI issues version 2 CRLs which comply with RFC 5280 and contain the following:

- Issuer Signature Algorithm: The algorithm used to sign the CRL.
- Issuer Distinguished Name: The Distinguished Name of the Certification Authority that has signed and issued the CRL.
- thisUpdate: Issue date of the CRL in UTCTime or GeneralizedTime.
- nextUpdate: Date by which the next CRL will be issued in UTCTime or GeneralizedTime.
- Revocation list (Identified by certificate serial number): List of all revoked Certificates including their serial number and the date and time of the revocation in UTCTime or GeneralizedTime.
- Serial Number
- Issuer's Signature

7.2.2 CRL and CRL Entry Extensions

CRL and CRL Entry Extensions follow the requirements of section 5 of RFC 5280.

If a CRL has a thisUpdate field value of 2022-07-01 00:00:00 UTC or later and the CA includes the Invalidity Date CRL entry extension in a CRL entry for a Code Signing Certificate, then the time encoded in the Invalidity Date CRL extension SHALL be equal to the time encoded in the revocationDate field of the CRL entry.

7.2.2.1 CRL Number

Sequentially increasing unique number for each CRL.

7.2.2.2 Authority Key Identifier

The Authority Key Identifier of an issuing CA used for chaining and validation.

7.2.2.3 Revocation reasonCode (OID 2.5.29.21)

If present, this extension MUST NOT be marked critical.

If a CRL entry is for a Root CA or Subordinate CA Certificate, including Cross Certificates technically capable of issuing SSL/TLS Certificates, this CRL entry extension MUST be present.

If a CRL entry is for a Certificate not technically capable of causing issuance, this CRL entry extension SHOULD be present, but MAY be omitted, subject to the following requirements.

The `CRLReason` indicated MUST NOT be unspecified (0). If the reason for revocation is unspecified, CAs MUST omit `reasonCode` entry extension, if allowed by the previous requirements.

If a CRL entry is for a SSL/TLS Certificate, the `CRLReason` MUST NOT be certificateHold (6).

If a `reasonCode` CRL entry extension is present, the `CRLReason` MUST indicate the most appropriate reason for revocation of the certificate (see sections 4.9.1.1 and 4.9.1.2).

7.3 OCSP Profile

TKC's PKI system operates an Online Certificate Status Profile (OCSP) responder in compliance with RFC 5019 and highlights this via an OCSP responder URL. OCSP version 1 defined by RFC 6960 is also supported.

7.3.1 Version Numbers

TKC's OCSP responders conform to version 1 of RFC 6960.

7.3.2 OCSP Extensions

The `singleExtensions` of an OCSP response MUST NOT contain the `reasonCode` (OID 2.5.29.21) CRL entry extension.

The `singleExtensions` of an OCSP response MAY contain the `ArchiveCutOff` (OID 1.3.6.1.5.5.7.48.1.6) as described in section 4.4.4 of RFC 6960 with values according to section 4.10.1 of this CP/CPS.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

TKC's operations and practices meet or exceed generally accepted industry standards (including the requirements described in Section 8.4). This is ensured by the implementation of regularly scheduled external assessments and audits, as well as ongoing internal assessments and audits.

8.1 Frequency or circumstances of assessment

TKC is audited on an annual basis in order to ensure compliance with the standards identified in this section. Audits are performed by a Qualified Auditor and cover all ThaiCA activities.

8.2 Identity/qualifications of assessor

Any external audit shall be performed by a Qualified Auditor who can demonstrate the following:

- Independence from the subject of the audit
- The ability to conduct an audit that addresses the criteria specified in an Eligible Audit as stipulated in Section 8.4
- The employment of individuals proficient in the examination of Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function
- Status as certified, accredited, licensed, or otherwise meeting the qualification requirements of auditors under the audit scheme
- Adherence to applicable laws, government regulation, and professional code of ethics
- Maintains Professional Liability/Errors & Omissions insurance with a minimum of one million ($1,000,000) US dollars in coverage.

8.3 Assessor's relationship to assessed entity

Any external auditor shall be independent from any relationships that might constitute a conflict of interest, or that could in any way impair the external auditor's objective assessment.

8.4 Topics covered by assessment

All external audits and assessments shall be performed in accordance with the WebTrust for Certification Authorities (WTCA) latest applicable program, and comply with industry standards as detailed in the current versions of the following documents:

- WebTrust Principles and Criteria for Certification Authorities

Relevant aspects of TKC's operations undergo regularly scheduled external audits which adhere to all of the industry standards listed in chapter 8. These audits are conducted by a Qualified Auditor, as specified in Section 8.2.

Internal audits and assessments, as described in Section 8.7, shall address all aspects of TKC's operations as required to ensure integrity and security.

For Delegated Third Parties which are not Enterprise RAs, ThaiCA SHALL obtain an audit report, issued under the auditing standards that underlie the accepted audit schemes found in this Section 8.4, which provides an opinion whether the Delegated Third Party's performance complies with either the Delegated Third Party's practice statement or TKC's Certificate Policy and Certification Practice Statement.

If the opinion is that the Delegated Third Party does NOT comply with the above requirements, then ThaiCA SHALL NOT allow the Delegated Third Party to continue performing delegated functions.

The audit period for any Delegated Third Party SHALL NOT exceed one year (ideally aligned with TKC's audit).

8.5 Actions taken as a result of deficiency

TKC shall create and implement an appropriate action plan to correct any deficiency deemed to constitute material non-compliance with applicable law, the ThaiCA CP/CPS, or any standard listed in Section 8.4.

Any corrective action plan shall be submitted to ThaiCA management. Any plan which affects ThaiCA policy shall also be referred to the ThaiCA Policy Management Authority (PMA). Any plan shall also be communicated to any appropriate party legally obligated to be notified. Any corrective actions deemed necessary shall be implemented and documented. Corrective actions which result in changes to ThaiCA policies or procedures shall be documented and incorporated into any subsequent ThaiCA PKI CP/CPS.

In addition any corrective action plan shall be submitted to NRCA.

8.6 Communication of results

Audit results are communicated to ThaiCA management, the ThaiCA PMA and to any third party entities entitled or required to be notified of audit results by law, regulation, or agreement. Audit compliance will be communicated to other interested parties (such as Application Service Suppliers and browser vendors) as appropriate. ThaiCA makes letters showing compliance with annual external Audit Reports publicly available in the legal Repository (www.thaica.com/repository).

8.7 Self-Audits

TKC performs regular internal audits (on at least a quarterly basis) drawing upon populations of Certificates issued since the last internal audit. These audits MUST be drawn against randomly selected samples of each of the following populations:

- Document Signing Certificates.

For each population, samples will consist of at least the greater of one certificate or three percent of issued Certificates.

Self-audits are performed in accordance with applicable CA/B Forum Guidelines.

Beginning in 2023, ThaiCA shall perform an annual self-assessment evaluating the conformance of this CP/CPS against CA/B Forum Baseline Requirements and the applicable Root Program Policies.

Completed self-assessments shall be submitted to the CCADB within 90 days from the "BR Audit Period End Date" field specified in the root CA's "CA Owner/Certificate" CCADB record (i.e. End Date of the Audit Period). If a self-assessment covers multiple CAs operating under this CP/CPS, ThaiCA shall enumerate the CAs in the scope of the assessment on the provided cover sheet.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

All fees are made clear to Applicants during the enrolment process through a web interface and/or in any marketing content presented by TKC.

9.1.2 Certificate access fees

TKC reserves the right to charge for access to any database that stores information corresponding to issued Certificates.

9.1.3 Revocation or status information access fees

TKC may charge Subscribers who decide not to use current OCSP responders or similar systems.

9.1.4 Fees for other services

TKC may charge fees for additional services beyond the standard certificate procurement process.

9.1.5 Refund policy

TKC's Subscriber Agreement at https://www.thaica.com/repository/ includes information regarding the refund policy for all Subscribers.

9.2 Financial responsibility

9.2.1 Insurance coverage

The CA has electronic device insurance, property insurance against public unrest, and fire insurance for electronic certificate service providers.

9.2.2 Other assets

No stipulation

9.2.3 Insurance or warranty coverage for end-entities

TKC's Subscriber Agreement at https://www.thaica.com/repository/ includes information regarding limited warranties extended to Subscribers.

9.3 Confidentiality of business information

9.3.1 Scope of Confidential Information

TKC classifies the following items as confidential information subject to requirements of reasonable care for protection from disclosure and misuse:

- Private Keys
- Any data regarding access to or activation of Private Keys
- Any data utilized to access the ThaiCA PKI infrastructure, other than that made available to Subscribers per the ThaiCA Subscriber Agreement and related agreements
- TKC's business continuity plans, including incident response, contingency and disaster recovery plans
- TKC's security documentation, including security practices and methodology
- Any data designated as private information per Section 9.4
- Audit logs and archive records related to any part of the ThaiCA PKI
- TKC's transaction records, financial audit records and external or internal audit trail records related to TKC
- External auditor reports related to TKC, except for any auditor's letter or document designed for public release and confirming the results of that external audit

9.3.2 Information Not Within the Scope of Confidential Information

Any information not defined as confidential in Section 9.3.1 shall be deemed public. Certificate status information and Certificates issued via the ThaiCA PKI are also deemed public.

9.3.3 Responsibility to Protect Confidential Information

TKC and all employees, agents and contractors thereof are responsible for protecting confidential information. ThaiCA shall maintain and protect confidential information through thorough training and enforcement programs for all personnel.

9.4 Privacy of personal information

9.4.1 Privacy plan

All personal information utilized by any element of the ThaiCA PKI is protected in accordance with TKC's Privacy Policy. The Privacy Policy is published at https://www.thaica.com/privacy-policy.

9.4.2 Information treated as private

All personally identifiable information received from certificate Applicants that is not ordinarily placed into a Certificate is considered private.

In accordance with Section 5.3, ThaiCA shall train and periodically retrain all personnel to ensure secure handling of and access to private information.

9.4.3 Information not deemed private

Information contained in Certificates, certificate signing requests, or certificate revocation lists is not considered private. Any official document published to the ThaiCA Repository (https://www.thaica.com/repository) is not considered private.

9.4.4 Responsibility to protect private information

All ThaiCA personnel are subject to policies and confidentiality agreements that require them to handle private information in accordance with the ThaiCA Privacy Policy.

9.4.5 Notice and consent to use private information

TKC complies with its Privacy Policy as to use of personal information, including any notice and consent requirements stated in the Privacy Policy.

In addition to permissions, consent must be specifically granted from an Applicant or Subscriber before seeking any additional information from third parties that may be required for an ThaiCA product, service or operation.

9.4.6 Disclosure pursuant to judicial or administrative process

TKC may disclose private information without notice to Applicants or Subscribers when required to do so by law or regulation.

9.4.7 Other information disclosure circumstances

If ThaiCA requires information from a third party to provide a product or service, it will obtain the Applicant's consent before seeking the information from the third party.

9.5 Intellectual property rights

TKC owns the intellectual property rights in TKC's services, and does not knowingly violate the intellectual property rights of third parties.

TKC retains ownership of all Certificates issued through the ThaiCA PKI and associated revocation information. However, ThaiCA grants permission to reproduce and distribute Certificates on a non-exclusive and royalty-free basis, provided that they are reproduced and distributed in full.

Public and Private Keys remain the property of Subscribers who legitimately hold them. All ThaiCA CA Private Keys are the property of TKC.

The CCADB is granted permission to make and store copies of this CP and CPS as well as all pervious and future versions of this document.

9.6 Representations and warranties

9.6.1 CA representations and warranties

By issuing a Certificate, ThaiCA makes the certificate warranties listed herein to the following Certificate Beneficiaries:

1. The Subscriber that is a party to the Subscriber Agreement or Terms of Use for the Certificate;
1. All Application Software Suppliers with whom the Root CA has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Supplier; and
2. All Relying Parties who reasonably rely on a Valid Certificate.

TKC represents and warrants to the Certificate Beneficiaries that, during the period when the Certificate is valid, ThaiCA has complied with its CP/CPS in issuing and managing the Certificate.

The Certificate Warranties specifically include, but are not limited to, the following:

1. **Right to Use Domain Name or IP Address:** That, at the time of issuance, TKC
    i. implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the Domain Name(s) and IP address(es) listed in the Certificate's subject field and subjectAltName extension (or, only in the case of Domain Names, was delegated such right or control by someone who had such right to use or control);
    ii. followed the procedure when issuing the Certificate; and
    iii. accurately described the procedure in TKC's Certificate Policy and/or Certification Practice Statement;
2. **Authorization for Certificate:** That, at the time of issuance, TKC
    i. implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject;
    iv. followed the procedure when issuing the Certificate; and
    v. accurately described the procedure in TKC's CP/CPS;
3. **Accuracy of Information:** That, at the time of issuance, TKC
    i. implemented a procedure for verifying the accuracy of all of the information contained in the Certificate (with the exception of the subject:organizationalUnitName attribute)
    vi. followed the procedure when issuing the Certificate; and
    vii. accurately described the procedure in TKC's CP/CPS;
4. **No Misleading Information:** That, at the time of issuance, TKC
    i. implemented a procedure for reducing the likelihood that the information contained in the Certificate's subject:organizationalUnitName attribute would be misleading;

viii. followed the procedure when issuing the Certificate; and
ix. accurately described the procedure in TKC's CP/CPS;

5. **Identity of Applicant:** That, if the Certificate contains Subject Identity Information, TKC
   i. implemented a procedure to verify the identity of the Applicant in accordance with Section 3.2;
   x. followed the procedure when issuing the Certificate; and
   xi. accurately described the procedure in TKC's CP/CPS;
6. **Subscriber Agreement:** That, if ThaiCA and Subscriber are not Affiliated, the Subscriber and ThaiCA are parties to a legally valid and enforceable Subscriber Agreement that satisfies the requirements of this CP/CPS, or, if ThaiCA and Subscriber are the same entity or are Affiliated, the Applicant Representative acknowledged the Terms of Use;
7. **Status:** That ThaiCA maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates; and
8. **Revocation:** That ThaiCA will revoke the Certificate for any of the reasons specified in this CP/CPS.

TKC shall be responsible for the performance and warranties of the Subordinate CAs and for all liabilities and indemnification obligations of the Subordinate CAs under this CP/CPS.

9.6.2 RA representations and warranties

Any Registration Authority (RA) utilizing TKC's PKI shall warrant that:

1. All certificate management operations conform to the ThaiCA CP/CPS and any other related or relevant documents.
3. Information provided by the RA does not contain any false or misleading information.
4. Any translations provided by the RA are accurate.
5. Any RA shall abide by the terms of any Registration Authority Agreement (RAA) signed with TKC.

Additional RA-specific contractual stipulations may apply.

9.6.3 Subscriber representations and warranties

TKC shall require each Applicant to enter into a Subscription Agreement that is legally enforceable against the Applicant/Subscriber and covers each Certificate request and resulting Certificate. The Subscription Agreement shall include the following commitments and warranties by the Subscriber for the benefit of ThaiCA and the Certificate Beneficiaries:

1. **Accuracy of Information:** all information provided by the Applicant/Subscriber is accurate, complete, and up to date, both in the Certificate request and as otherwise requested by ThaiCA in connection with the issuance of the Certificate(s) to be supplied by TKC;

6. **Protection of Private Key:** Subscriber shall take all reasonable measures to maintain sole control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token); Where the key is available outside a Signing Service, to maintain sole control of, keep confidential, and properly protect, at all times in accordance with Section 4.5.1, the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token). ThaiCA MUST provide the Subscriber with documentation on how to protect a Private Key. ThaiCA MAY provide this documentation as a white paper or as part of the Subscriber Agreement. The Subscriber MUST represent that it will generate and operate any device storing private keys in a secure manner, as described in a document of Code Signing best practices, which ThaiCA MUST provide to the Subscriber during the ordering process. ThaiCA MUST obligate the Subscriber to use passwords that are randomly generated with at least 16 characters containing uppercase letters, lowercase letters, numbers, and symbols to transport private keys.
7. **Prevention of Misuse:** For Code Signing, Subscriber has an obligation to provide adequate network and other security controls to protect against misuse of the Private Key and that ThaiCA will revoke the Certificate without requiring prior notification if there is unauthorized access to the Private Keys
8. **Private Key Reuse:** Subscriber has an obligation to not apply for a Code Signing Certificate if the Public Key in the Certificate is or will be used with a non-Code Signing Certificate
9. **Acceptance of Certificate:** Subscriber will review and verify the Certificate contents for accuracy;
10. **Use of Certificate:** Subscriber shall install and use the Certificate solely in compliance with all applicable laws, solely in accordance with the Subscriber Agreement and solely for the purposes it was intended to be used for. For Code Signing, the Subscriber shall not knowingly sign software that contains Suspect Code and use the Code Signing as follows:
    i. only to sign code that complies with the requirements set forth in these Guidelines;
    ii. solely in compliance with all applicable laws;
    iii. solely for authorized company business; and
    iv. solely in accordance with the Subscriber Agreement;
11. **Reporting and Revocation:** Subscriber has an obligation and warranty to:
    i. promptly request revocation of the Certificate, and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate,
    ii. promptly request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate, and

iii. for Code Signing, promptly request revocation of the Certificate, and cease using it and its associated Private Key, if there is evidence that the certificate was used to sign Suspect Code;
iv. for Server Certificates, when requesting revocation of the Certificate, report the most relevant revocation reason per Section 4.9.1.1;

12. **Termination of Use of Certificate:** Subscriber has an obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon expiration or revocation of that Certificate;
13. **Responsiveness:** Subscriber has an obligation to respond to TKC's instructions concerning Key Compromise or Certificate misuse within a specified time period;
14. **Acknowledgment and Acceptance:** Subscriber acknowledges and accepts that ThaiCA is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber Agreement or if revocation is required by TKC's CP/CPS, or if ThaiCA discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware.

9.6.4 Relying party representations and warranties

A Relying Party utilizing any certificate created using TKC's PKI makes the following warranties and commitments in a Relying Party Agreement:

1. It shall verify that any third party issuing a Certificate is an authorized subordinate Certification Authority of ThaiCA and that the Certificate was issued in accordance with the policies set out in TKC's CP/CPS;
15. It shall check the CRL/OSCP to ensure that the Certificate is valid and not revoked or terminated;
16. It acknowledges that ThaiCA performs differing degrees of Certificate validation depending on the type of Certificate and intended use, and that it must take those factors into consideration when deciding whether or not to rely on a Certificate;
17. It complies with all applicable policies and procedures set out in the ThaiCA CP/CPS, including, without limitation, a requirement that the Certificate not be used for any purpose other than as set forth in the relevant section of this CP/CPS for the particular class and type of Certificate.

A copy of the latest ThaiCA Certificate Relying Party Agreement and ThaiCA Relying Party Warranty are available in the ThaiCA repository when requested.

9.6.5 Representations and warranties of other participants

No stipulation

9.7 Disclaimers of warranties

EXCEPT AS EXPRESSLY STATED IN SECTION 9.6.1, ALL CERTIFICATES AND ANY RELATED SOFTWARE AND SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE".

TO THE MAXIMUM EXTENT PERMITTED BY LAW, ThaiCA DISCLAIMS ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING ALL WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT.

TKC DOES not WARRANT THAT ANY SERVICE OR PRODUCT WILL MEET ANY EXPECTATIONS OR THAT ACCESS TO CERTIFICIATES WILL BE TIMELY OR ERROR-FREE.

TKC does not guarantee the availability of any products or services and may modify or discontinue any product or service offering at any time.

No fiduciary duty is created or implied though use of ThaiCA services by any entity.

9.8 Limitations of liability

For delegated tasks, ThaiCA and any Delegated Third Party may allocate liability between themselves contractually as they determine, but ThaiCA shall remain fully responsible for the performance of all parties in accordance with this CP/CPS, as if the tasks had not been delegated.

If ThaiCA has issued and managed the Certificate in compliance with this CP/CPS, ThaiCA may disclaim liability to the Certificate Beneficiaries or any other third parties for any losses suffered as a result of use or reliance on such Certificate beyond those specified in TKC's CP/CPS. If ThaiCA has not issued or managed the Certificate in compliance with its CP/CPS, ThaiCA may seek to limit its liability to the Subscriber and to Relying Parties, regardless of the cause of action or legal theory involved, for any and all claims, losses or damages suffered as a result of the use or reliance on such Certificate by any appropriate means that ThaiCA desires. If ThaiCA chooses to limit its liability for Certificates that are not issued or managed in compliance with its CP/CPS, then ThaiCA shall include the limitations on liability in TKC's CP/CPS.

9.9 Indemnities

9.9.1 Indemnification by CAs

Notwithstanding any limitations on its liability to Subscribers and Relying Parties, ThaiCA understands and acknowledges that the Application Software Suppliers who have a Root Certificate distribution agreement in place with the Root CA do not assume any obligation or potential liability of ThaiCA under this CP/CPS or that otherwise might exist because of the issuance or maintenance of Certificates or reliance thereon by Relying Parties or others. Thus, ThaiCA shall defend, indemnify, and hold harmless each Application Software Supplier for any and all claims, damages, and losses suffered by such Application Software Supplier related to a Certificate issued by TKC, regardless of the cause of action or legal theory involved. This does not apply, however, to any claim, damages, or loss suffered by such Application Software Supplier related to a Certificate issued by ThaiCA where such claim, damage, or loss was directly caused by such Application Software Supplier's software displaying as not trustworthy a Certificate that is still valid, or displaying as trustworthy:

1. a Certificate that has expired, or

18. a Certificate that has been revoked (but only in cases where the revocation status is currently available from ThaiCA online, and the application software either failed to check such status or ignored an indication of revoked status).

9.9.2 Indemnification by Subscribers

To the extent permitted by law, each Subscriber shall indemnify TKC, its partners, and any cross-signed entities, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to

1. any misrepresentation or omission of material fact by Subscriber, regardless of whether the misrepresentation or omission was intentional or unintentional;
19. Subscriber's breach of the Subscriber Agreement, this CP/CPS, or applicable law;
20. the compromise or unauthorized use of a certificate or Private Key caused by the Subscriber's negligence or intentional acts; or
21. Subscriber's misuse of the certificate or Private Key.

9.9.3 Indemnification by Relying Parties

To the extent permitted by law, each Relying Party shall indemnify TKC, its partners, and any cross-signed entities, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to the Relying Party's

1. breach of the Relying Party Agreement, an End-User License Agreement, this CP/CPS, or applicable law;
22. unreasonable reliance on a certificate; or
23. failure to check the certificate's status prior to use.

9.10 Term and termination

9.10.1 Term

This version of the ThaiCA CP/CPS is effective until otherwise communicated through the ThaiCA repository. (https://www.thaica.com/repository)

9.10.2 Termination

The termination of any ThaiCA CP/CPS becomes effective immediately following the publication of a more recent version. Some sections of the CP/CPS may include specific future dates after which certain policies or practices will become effective.

9.10.3 Effect of termination and survival

TKC will publicly communicate any CA termination through its public repository and the Application Software Suppliers who have a Root Certificate distribution agreement in place with TKC.

9.11 Individual notices and communications with participants

TKC accepts forms of notice related to this CP/CPS which either implement a digital signature or employ a physical mail service. Paper forms of notice must be delivered with a courier service that confirms delivery or via certified mail. Only digitally signed messages of notice that are judged to be valid shall receive an ThaiCA response. ThaiCA contact information for notices using certified mail is provided in Section 1.5.2. Valid communications will be reviewed and replied to as appropriate in a timely manner.

9.12 Amendments

9.12.1 Procedure for amendment

TKC's Policy Management Authority (PMA) may enact amendments to this CP/CPS as required.

Any significant changes made to the ThaiCA CP/CPS shall be noted in a version control table incorporated into this CP/CPS.

Minor changes (e.g. correction of grammatical, syntactical, spelling errors) may, at TKC's sole discretion, be carried out without any prior notice and by adding a sub-minor number in the document OID.

On an annual basis, if no other changes are made to the document, its version number shall be incremented and a dated changelog entry shall be added to denote that.

9.12.2 Notification mechanism and period

TKC shall upload updated versions of this CP/CPS to its legal Repository and the CCADB within 7 days of being updated.

Subscribers shall be duly notified in case of major changes to this CP/CPS, especially in regards to any specific effective dates that enable policy and procedural changes.

9.12.3 Circumstances under which OID must be changed

TKC reserves the right to amend content of any published CP/CPS. Any major change of the ThaiCA CP/CPS will also alter the OID of the CP/CPS published via the ThaiCA repository.

9.13 Dispute resolution provisions

Parties are required to notify ThaiCA and attempt to resolve disputes directly with ThaiCA before resorting to any dispute resolution mechanism, including adjudication or any type of alternative dispute resolution.

9.14 Governing law

The laws of the kingdom of Thailand govern the interpretation, construction, and enforcement of this CP/CPS and all proceedings related to TKC's products and services,

including tort claims, without regard to any conflicts of law principles. The kingdom of Thailand has non-exclusive venue and jurisdiction over any proceedings related to this CP/CPS or any ThaiCA product or service.

9.15 Compliance with applicable law

This CP/CPS is subject to all applicable laws and regulations.

Subject to Section 9.4.5's Notice and Consent to Use Private Information contained in Certificates, ThaiCA meets the requirements of the European data protection laws and has established appropriate technical and organization measures against unauthorized or unlawful processing of personal data and against the loss, damage, or destruction of personal data.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

TKC contractually obligates each RA to comply with this CP/CPS and applicable industry guidelines. ThaiCA also requires each party using its products and services to enter into an agreement that delineates the terms associated with the product or service. If an agreement has provisions that differ from this CP/CPS, then the agreement with that party controls, but solely with respect to that party. Third parties may not rely on or bring action to enforce such agreement.

9.16.2 Assignment

Any entities operating under this CP/CPS may not assign their rights or obligations without the prior written consent of TKC. Unless specified otherwise in a contact with a party, ThaiCA does not provide notice of assignment.

9.16.3 Severability

In the event of a conflict between the ThaiCA CP/CPS and a law, regulation or government order (hereinafter 'Law') of any jurisdiction in which ThaiCA operates or issues certificates, ThaiCA MAY modify any conflicting requirement to the minimum extent necessary to make the requirement valid and legal in the jurisdiction.

This applies only to operations or certificate issuances that are subject to that Law.

In such event, ThaiCA SHALL immediately (and prior to issuing a certificate under the modified requirement) include in Section 9.16.3 of this CP/CPS a detailed reference to the Law requiring a modification of this CP/CPS under this section, and the specific modifications to the CP/CPS as implemented by TKC.

TKC MUST also (prior to issuing a certificate under the modified requirement) notify the CA/Browser Forum of the relevant information newly added to its CPS by sending a message to questions@cabforum.org and receiving confirmation that it has been posted to the Public

Mailing List and is indexed in the Public Mail Archives available at https://cabforum.org/pipermail/public/ (or such other email addresses and links as the Forum may designate), so that the CA/Browser Forum may consider possible revisions to the Baseline Requirements accordingly.

Any modification to CA practice enabled under this section MUST be discontinued if and when the Law no longer applies, or the CA/Browser Forum Baseline Requirements (and therefore the ThaiCA CP/CPS) are modified to make it possible to comply with both them and the Law simultaneously without reliance on specific modifications within 9.16.3.

An appropriate change in practice, modification to TKC's CP/CPS and a notice to the CA/Browser Forum, as outlined above, must be made within 90 days from the date the law becomes effective as to TKC.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

TKC may seek indemnification and attorneys' fees from a party for damages, losses, and expenses related to that party's conduct. TKC's failure to enforce a provision of this CP/CPS does not waive TKC's right to enforce the same provision later or right to enforce any other provision of this CP/CPS. To be effective, waivers must be in writing and signed by TKC.

9.16.5 Force Majeure

TKC is not liable for any delay or failure to perform an obligation under this CP/CPS to the extent that the delay or failure is caused by an occurrence beyond TKC's reasonable control. The operation of the Internet is beyond TKC's reasonable control.

9.17 Other provisions

No stipulation

ANNEX A - ThaiCA CERTIFICATE PROFILES

Table of Certificate Profiles

Friendly Name	Policy IDs	Key Usages	Other Extensions
TKC Sub CA Certificate	**2.5.29.32.0 (anyPolicy)**	KU: **Certificate Signing, CRL Signing, Digital Signature (optional)** EKU: (Optional) Depending on the Intermediate CA Certificate usage	None
OCSP Responder Certificate	**1.3.6.1.4.1.62483.1.3.3**	KU: **Digital Signature** EKU: **OCSP Signing** (1.3.6.1.5.5.7.3.9)	**OCSP No Check**
TKC Digital Signing Certificate	**1.3.6.1.4.1.62483.1.3.1**	KU: **Digital Signature**	

1: **"Key Encipherment"** is included in certificates that use RSA public key algorithm. It is not included in certificates that use ECDSA keys.