Thai Digital ID CA G3

**Certificate Policy/Certification Practice Statement**

*Certification Policy/Certificate Practice Statement Identifier (OID):* 2.16.764.1.1.2.1.0.2.0

**Revision History**

| Doc. Version | Status | Date of Issue | Issued By | Comments | Date of PA Approval |
|---|---|---|---|---|---|
| 1.0 | Published | 11-07-16 | TDID PCA | The first version for TDID CA G3 | 29-Jul-16 |
| 1.1 | Published | 28-03-17 | TDID PCA | (1) Specify applicable standards used to develop this CP/CPS (secion 1.1)<br>(2) Update CPS Approval Procedures 1.5.4<br>(3) Update Certificate Authority Authorization (CAA) 4.2.4<br>(4) Update suspension process time (4.9.15)<br>(5) Update Limited period of Suspension (4.9.16)<br>(6) Review backup off-site backup (5.1.8)<br>(7) Classify Events Recorded (5.5.1)<br>(8) Review Public Key Archival (6.3.1)<br>(9) Review Certificate operational periods and key pair usage periods (6.3.2) | 21-Apr-17 |
| 1.2 | Published | 26/06/2017 | TDID PCA | (1) Update CRL and OCSP link in section (4.9.6), (4.9.9) and (4.10.1)<br>(2) Add organizationIdentifier in Name Forms (7.1.4) | 26/06/2017 |
| 1.3 | Published | 18/10/2018 | TDID PCA | (1) Update certificate validity to be upto 2 years (1.4)<br>(2) Update company address (1.5, 4.1.2) | 18/10/2018 |
| 1.4 | Published | 09/09/2019 | TDID PCA | (1) Update Notification to Subscriber by the CA of Issuance of Certificate (4.3.2)<br>(2) Update Certificate Acceptance (4.4.1,4.4.3) | 09/09/2019 |
| 1.5 | Published | 31/10/2019 | TDID PCA | (1) Update 4.2.4 CAA record “thaidigitalid.com”<br>(2) Change 4.9.7 to CRL Issuance Frequency<br>(3) Change 4.9.8 to Maximum Latency for CRLs<br>(4) Update 5.4.3 Retention Period for | 07/11/2019 |

| | | | | | |
|---|---|---|---|---|---|
| | | | | Audit Log to 10 years | |
| 1.6 | Published | 05/03/2021 | TDID PCA | (1) Update 4.1.2 Add Supporting evidence<br>(2) Update 4.2.4 Add Inspection method CAA Record | 05/03/2021 |
| 1.7 | Published | 31/03/2023 | TDID PCA | (1) Deleted 4.1.2 SSL Certificate for Personal Domain Name | 07/04/2023 |
| 2.0 | Published | 30/11/2023 | TDID PCA | (1) Revise 1.1 Overview<br>(2) Revise 1.2 OID (Object Identifier)<br>(3) Add 1.3.1 Thailand NRCA<br>(4) Revise 1.3.2 TDID CA<br>(5) Revise 1.4 Categories of Corticated<br>(6) Revise 1.4.1. Appropriate Certificate Uses<br>(7) Revise 1.6.1 Definitions<br>(8) Add 1.6.2 Acronyms<br>(9) Revise 2.2 Publication of Information<br>(10) Revise 2.8.3 Time or Frequency of Publication<br>(11) Revise 3.1.3 Anonymity or Pseudonymity of Subscribers<br>(12) Revise 3.1.4 Rules for Interpreting Various Name Forms<br>(13) Revise 3.1.6 Recognition, Authentication, and Role of Trademarks<br>(14) Revise 3.2.1 Method to Prove Possession of Private Key<br>(15) Revise 3.2.2 Authentication of Organization Identity<br>(16) Add Sub clause 3.2.2.1-3.2.2.8<br>(17) Add 3.2.3.1 In-person Verification<br>(18) Revise 4.1.2 Enrollment Process and Responsibilities<br>(19) Remove 4.2.4 Certificate Authority Authorization from the Subscriber's CAA Record- to be 3.2.2.8<br>(20) Revise 4.5.1 Subscriber Private Key and Certificate Usage<br>(21) Revise 4.9.1 Circumstances for Revocation<br>(22) Revise 4.9.3 Procedure for Revocation Request<br>(23) Revise 4.9.4 Revocation Request | 30/11/2023 |

| | | | | | |
|---|---|---|---|---|---|
| | | | | Grace Period<br>(24) Revise 4.9.6 Revocation Checking Requirements for Relying Parties<br>(25) Revise the name of 4.9.12 Special Requirements Key Compromise<br>(26) Revise 4.11 End of Subscription<br>(27) Revise 5.3.7 Independent Contractor Requirements<br>(28) Revise 5.5.5 Requirements for Time-Stamping of Records<br>(29) Revise 5.6 Key Changeover<br>(30) Revise 5.7.1 Incident and compromise handling procedures<br>(31) Revise 6.1.1. Key Pair Generation<br>(32) Revise 6.1.5 Key Sizes<br>(33) Revise 6.2.5 Private Key Archival<br>(34) Revise 6.2.7 Private Key storage on cryptographic module<br>(35) Revise 6.2.10 Method of destroying private key<br>(36) Revise 6.3.2 Certificate operational periods and key pair usage periods<br>(37) Revise 6.6.1 System Development Controls<br>(38) Revise 6.7 Network Security Controls<br>(39) Revise 6.8 Timestamping<br>(40) Revise 7.1.3 Algorithm object identifiers<br>(41) Revise 7.1.8 Policy Qualifiers Syntax and Semantics<br>(42) Revise 7.2.2 CRL and CRL entry extensions<br>(43) Revise 7.2.3 OCSP extensions<br>(44) Revise 8. Compliance Audit and Other Assessment<br>(45) Revise 9.4.1 Privacy Plan<br>(46) Revise 9.4.2 Information Treated as Private<br>(47) Revise 9.5 Intellectual Property Rights<br>(48) Revise 9.6.4 Relying party representations and warranties<br>(49) Revise 9.9 Indemnities<br>(50) Revised 9.10 Term and Termination<br>(51) Revise 9.13 Dispute Resolution Procedures | |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | |

**หมายเหตุ :**

TDID PCA = TDID Policy Creation Authority

## Table of Contents

# 1. Introduction

## 1.1 Overview

Thai Digital ID Co., Ltd. ("TDID CA") is a leading Certificate Authority established in 2000 with a mission to provide comprehensive certificate services, foster IT security, and build confidence in the Thai e-commerce group. Applying advanced Public Key Infrastructure (PKI) technology, TDID CA is an expert in the development and distribution of IT security systems in both hardware and software forms, which enabling the digital signatures solution. Additionally, TDID CA offers services for the design, development, and implementation of customer CA systems by utilizing industry-standard CA hardware and software to deliver its services. Striving for excellence, TDID provides CA system service in accordance with the WebTrust for CA and ISO 27001 safety standards, contributing to elevating Thailand's IT security level to international benchmarks.

This document is titled "Certificate Policy/Certification Practice Statement" or "CP/CPS" in compliance with the Internet Engineering Task Force Public Key Infrastructure X.509 (IETF PKIX) Certificate Policy and Certification Practices Framework [RFC3647] and meant to inform all relying parties related to the electronic certificates by Thai Digital ID Certification Authority: TDID CA.

TDID CA adheres to the latest Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published on http://www.cabforum.org. The baseline requirement shall supersede if any conflict arises.

The Certificate Authority Common Name (CN) for TDID is "Thai Digital ID CA G3", which includes issuing Personal Certificate, Enterprise Certificate, Enterprise User Certificate, Computer/Equipment Certificate, and Web Server Certificate (SSL Certificate).

TDID CA is the Subordinate CA under Thailand National Root Certificate Authority (NRCA). Relying parties can directly trust the root certificates of the Thailand National Root Certificate Authority (NRCA) because Thailand National Root Certificate Authority (NRCA) is the highest-level CA and trust anchor.

The CP/CPS applies to Thai Digital ID Company Limited 's all subordinate certification authorities under Thailand National Root Certificate Authority (NRCA) and thereby provides assurances of uniform trust throughout the Thailand National Root Certificate Authority (NRCA).

## 1.2 Document Name and Identification

This document is titled "Certificate Policy/Certification Practice Statement", or "CP/CPS" owned by the certificate authority and meant to inform all parties related to the electronic certificates of and clarify the statements in the certificate policy.

The Object Identifier (OID) for TDID CA and sub -value arc of joint-iso-itu-t- (2) country (16) TH (764) ETDA (1) NRCA (1) TDID CA (2),

TDID CA organizes its OID as follows:

| OID Types | TDID OIDs | CA/B Forum OIDs |
|---|---|---|
| TDID OID | 2.16.764.1.1.2.1 | |
| TDID CP/CPS Document Class | 2.16.764.1.1.2.1.0 | |

| | | |
|---|---|---|
| TDID CP/CPS Verion 2.0 | 2.16.764.1.1.2.1.0.2.0 | |
| TDID Certificate Specification Class | 2.16.764.1.1.2.1.1 | |
| Personal Certificate | 2.16.764.1.1.2.1.1.20001.1 | |
| Juristic Person Certificate | 2.16.764.1.1.2.1.1.10001.1 | |
| Enterprise User Certificate | 2.16.764.1.1.2.1.1.10002.1 | |
| Machine Certificate | 2.16.764.1.1.2.1.1.40001.1 | |
| TLS/SSL Certificate – Organization Validation | 2.16.764.1.1.2.1.1.30001.1 | 2.23.140.1.2.2 |

## 1.3 PKI Participants

### 1.3.1 Thailand National Root Certification Authority (Thailand NRCA):

Thailand NRCA is the highest-level certification authority, trust anchor, of the PKI domain in Thailand. Thailand NRCA is responsible for managing Subordinate CAs.

### 1.3.2 Thai Digital ID Certification Authorities: TDID CA

Certification authority responsible issuance of a digital certificate to a person or legal entity by using a collection of hardware, software, personnel, and operating procedures that create, sign, and issue certication of public key for Subscribers and for publication of Certificate Revocation List, also known as CRL.

In this CP/CPS, CAs refers to those established and owned by Thai Digital ID Company Limited and they are subordinate CAs under NRCA.

### 1.3.3 Thai Digital ID Registration Authorities: TDID RA

Registration authority for requests of Certificate Issuance, Revocation, and Renewal, responsible for verification of Subscriber's information entered in the Certification Authorities' form.

### 1.3.4 Subscribers

Individuals, companies, or other entities with Certificates from the Certificate Authorities.

### 1.3.5 Relying Parties

Individuals, companies, or other entities who recognize any Digital Signature Trust or Certificate. A Relying Parties may or may not be a Subscriber of the Certificate Authorities who engages in actions or inaction due to the recognition of such Digital Signature Trust or Certificate to verify the identity of the Subscriber whose name appears on the Certificate5

### 1.3.6 Other Participants

Individuals, companies, or other entities apart from those mentioned above such as Providers of Repository Service or Outsourced Certificate Authorities, etc.

## 1.4 Certificate Usage

Certificates issued by Certificate Authorities consist of 5 categories of Certificates, namely:

(1) Personal Certificates are issued to individuals or generic civilians for security of electronic transactions. Valid for 1 or 2 years.

(2) Juristic Person Certificates are issued to legal persons including governmental or private organizations or companies for security of electronic transactions. Valid for 1 or 2 years.

(3) Enterprise User Certificates are issued to officials of an organization including governmental or private organizations or companies for security of electronic transactions. Valid for 1 or 2 years.

(4) Machine Certificates are issued to computers or Equipment that utilize network communicate, such as routers. The main purpose of Machine Certificate is to ensure the security of online transactions. This type of certificate has a validity period of 1 or 2 years.

(5) TLS/SSL Certificate are used for Web Server Authentication. Valid for 1 year.

### 1.4.1 Appropriate Certificate Uses

This CP/CPS covers several different types of Certificates. The following table provides a brief description of the appropriate uses of each. The descriptions are for guidance only and are not binding.

| Type of Certificate | Appropriate Use |
|---|---|
| Personal Certificate<br>Juristic Person Certificate<br>Enterprise User Certificate | Used in the process of digitally signing a document, this ensures that the portion of the document signed by the signer remains unmodified. |
| Machine Certificate | Used to authenticate and secure communication between servers in a network, ensuring the integrity and authenticity of data transfers.<br>Device-to-Device<br><br>Used in scenarios where devices need to communicate securely with each other. |
| TLS/SSL Certificate | Use to secure web server communication. TLS/SSL Certificate provide encryption and authentication for data transmitted between a web server and a web browser. |

### 1.4.2 Prohibited Certificate Uses

Certificates issued to Individuals or Legal Persons by the Certificate Authorities must only be used as described usages under item 1.4. Other uses are strictly prohibited.

## 1.5 Policy Administration

The details of Policy Creation Authority (also known as PCA) of the Certificate Authority responsible for this CP/CPS are described below.

| | |
|---|---|
| **Name:** | Thai Digital ID CA |
| **Company Registration No.:** | 0105543112679 |
| **Trading as:** | TDID CA |
| **Postal Address:** | 319, 25th Floor, Room 10-11, Chamchuri Square Building, Phayathai Road, Pathumwan, Bangkok, 10330 Thailand. |
| **Phone:** | +66-2029-0312 |
| **Domain Name:** | www.thaidigitalid.com |
| **Email Address:** | support@thaidigitalid.com |
| **Contact:** | Policy Creation Authority, Thai Digital ID Co., Ltd.<br>319, 25th Floor, Room 10-11, Chamchuri Square Building, Phayathai Road, Pathumwan, Bangkok, 10330 |

### 1.5.1 Organization Administering the CP/CPS Document

Policy Creation Authority of the Certificate Authority

### 1.5.2 Contact Person

Policy Creation Authority of the Certificate Authority

### 1.5.3 Person Determining CPS Suitability for Policy

Policy Creation Authority of the Certificate Authority, including internal auditors and external auditors.

### 1.5.4 CPS Approval Procedures

Any change to this CP/CPS must be approved by the PCA of the Certificate Authority before the change is made.

If the change is approved by the PCA, the change will be applied through the Change Control Procedure by the PCA to the Managing Director. Once approved by the MD, the Version of the CP/CPS shall be revised in the Change Log section before it is published on the Company's website.

The CP/CPS document is normally reviewed once yearly by the PCA and the revision will be submitted for the Managing Director's approval through Change Control Procedure and recorded in the Change Log section before it is published on the Company's website: www. thaidigitalid. com.

## 1.6 Definitions and Acronyms

### 1.6.1 Definitions

| Terms | Definitions |
|---|---|
| Certification Authority/TDID CA | Thai Digital ID Company Limited under TDID CA Service, responsible for issuance of Certificates, approval of Public Keys for Subscribers, and publication of Certificate Revocation List. |
| Registration Authority/TDID RA | Certificate Registrar responsible for accepting Application for Certificate Issuance, Suspension, and Revocation by reviewing and verifying the information given by the Subscriber. |
| Digital Certificate | An electronic document that forms the Public Key infrastructure of the Subscribers that may be individuals, legal persons, or devices. Such electronic document must be compliant with the standards of X.509 Version 3 Certificate and comprise at least the following:<br>— Electronic Certificate Version<br>— Electronic Certificate Identification Number<br>— The Procedure used to create the Digital Signature of the Electronic Certificate Holders.<br>— Name of the Certificate Authority<br>— Start and end date of Certificate usage<br>— Name of the Certificate holder<br>— The Certificate holder's Public Key and Creation Algorithm |
| Subscriber | An individual or legal person that subscribe to the Certificate with the Certificate Authority. The issued Certificate will bear the name of the Subscriber on it. |
| Key | Symbol, series of symbols, or electronic signal related to the symbols used for encryption or decryption of data. |
| Private Key | Key used to generate Digital Signature that can be used to decrypt an encrypted electronic data in order to understand the encrypted data. The Private Key will be used to generate the Digital Signature. |
| Public Key | The Key used to verify the Digital Signature and encrypt electronic data in order to secure the confidentiality of the encrypted data. The Public Key will be used to verify the Digital Signature. |
| Key Pair | Private Key and Public Key used for asymmetric encryption where the Private Key is generated with mathematical relationship to the Public Key and the Public Key can be used to verify whether the Private Key is used to create a certain Digital Signature. The Public Key can be used to encrypt electronic data to maintain confidentiality except to |

| Terms | Definitions |
|---|---|
| | individuals with Private Key that can be used to decrypt the electronic data. |
| Digital Signature | A type of electronic signature that consists of numbers generated with electronic data to be used with Key Pair. The Signature holder's Public Key can be used to verify whether the Signature is generated with their Private Key and whether the signed electronic data has been altered after it is digitally signed. |
| Certificate Revocation | Termination of Electronic Certificate's usage that revoke the function of the Subscriber's Private Key in creating Digital Signature and electronic data decryption. Certificate revocations do not affect the Public Key or Certificate, which can still be used to verify the Digital Signature generated before the Revocation. |
| Certificate Revocation List | The list of rovoked Electronic Certificate |
| Relying Party | Persons who engage in or abstain from certain actions relying the trust in Electronic Certificate or Digital Signature by utilizing the Public Key available in the Certificate to verify the identity of the subscriber who digitally signed and whose name appears on the Certificate. |
| Directory | The data repository properly managed for search capability that is quick and compliant with the directorial standards (X.500 or LDAP) |
| Database | The data repository that allows convenient and fast access, management, and edit by computer programs. |

### 1.6.2 Acronyms

| Acronyms | Term |
|---|---|
| CRL | Certificate Revocation List |
| FQDN | Fully-Qualified Domain Name |
| DNS | DNS Domain Name System |
| NRCA | National Root Certification Authority |
| OCSP | Online Certificate Status Protocol |
| PA | Policy Authority |
| RAO | Registration Authority Officer |

## 2. Publication and Repository Responsibilities

### 2.1 Repositories

All data related to Electronic Certificate request will be recorded in the database and signed the Registration Authority while the Electronic Certificate will be stored in X.500 Directory.

### 2.2 Publication of Information

This CP/CPS publicly available and publication of certificates and related information online on the following URL: https://www.thaidigitalid.com/downloads/

### 2.3 Time or Frequency of Publication

The Certificate will be published on the X.500 Directory immediately on issuance within seven calendar days after accepting issuance by an upper level CA.

The Certificate Authority will keep the Certificate Policy/Certificate Practice Statement up to date and published on their website (www.thaidigitalid.com) as reference for all Subscribers and general public within three working day of the approval of changes.

The latest versions of CRLs are published within 3 days after updating and of their approval (See section 4.9.7 and 4.9.9. for additional details.)

### 2.4 Access Controls on Repositories

Electronic Certificates can be accessed through LDAP Protocol. Certificate Policy/Certification Practice Statement document can be downloaded from www.thaidigitalid.com.

## 3. Identificatiomn and Authentication (I&A)

### 3.1 Naming

#### 3.1.1 Type of Names

The name that appears on each Subscriber's Certificates will be unique and Distinguished Name (DN) to ensure that Certificates can refer to a Subscriber, Certificate Authority, or a Service Device, according to ISO/IEC 9594-1/ITU-T Recommendation X.500 The Directory: Overview of Concepts, Models and Services

#### 3.1.2 Need for Names to be Meaningful

The name that appears on each Certificate will have meanings that refer to the owner of such Certificate for identification of the owner of such Certificate.

#### 3.1.3 Anonymity or Pseudonymity of Subscribers

The Common Name (CN) may be designated according to the Subscriber's preference.

The TDID CA does not issue anonymous or pseudonymous certificates.

#### 3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting distinguished name forms are specified in X.501. Rules for interpreting e-mail addresses are specified in RFC 2822. RFC 2253 and RFC 2616 are interpreted as Uniform Resource Identifiers.

#### 3.1.5 Uniqueness of Names

The names that appear on Certificates must be unique for each Certificate issued by the same CA to allow identification of the Certificate owners.

#### 3.1.6 Recognition, Authentication, and Role of Trademarks

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

### 3.2 Initial Identity Validation

Identity validation or authentication for certification is a responsibility of the Registration Authority. The Subscriber must fill the Electronic Certificate request form to apply as well as provide the evidence required for the Registration Authority. The details are described in item 4.1: Identity Validation for New Certificate Applications.

#### 3.2.1 Method to Prove Possession of Private Key

The Subscriber self-generates the key pairs and creates the PKCS#10 Certificate Signing Request and signs it with the private key. When applying for a certification, the Certificate Signing Request is submitted to the RA. The RA shall use the Subscriber's public key to verify the signature on the Certificate Signing Request to prove that the Subscriber is in possession of the corresponding private key.

#### 3.2.2 Authentication of Organization Identity

The Certificate Authority will verify the juristic person certificate issued within 3 months by the Department of Business Development, Ministry of Commerce before application and signed by an authorized director or corporate formation act.

For other processes, TDID CA shall conform to Authentication of Organization and Domain Identity Section in CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates with the latest version.

##### 3.2.2.1 Identity

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

1. A government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;
2. A third party database that is periodically updated and considered a Reliable Data Source;
3. A site visit by the CA or a third party who is acting as an agent for the CA; or
4. An Attestation Letter.

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

The certification documents shall be affixed with the seal of the organization and responsible person The RAO shall check the authenticity of the application information submitted by the organization and representative identity and verify that the representative has the right to apply for the certificate in the organization's name, the organization must submit the correct certification documents which have been approved by the competent authority or a legally authorized body (such as a court) to the RAO.

##### 3.2.2.2 DBA/Tradename

TDID CA verifies DBA/tradename when the Subject Identity Information included.
Verification the Applicant's right to use the DBA/tradename using at least one of the following:

1. Documentation provided by, or communication with, a government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;

2. A Reliable Data Source;

3. Communication with a government agency responsible for the management of such DBAs or tradenames;

4. An Attestation Letter accompanied by documentary support; or

5. A utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that the CA determines to be reliable.

#### 3.2.2.3 Verification of Country

TDID CA follows Section 3.2.2.2 of CA/B Forum Baseline Requirements.

#### 3.2.2.4 Validation of Domain Authorization or Control

TIDID CA employs the approved methods to confirm that the Subscriber requesting a certificate possesses the proper authority or control over the domain.

The Subscriber is required to demonstrate control over the domain (DNS-Based Validation) by either creating a DNS record with a unique value provided by TDID CA, which can be validated by querying the DNS record from the Internet, or by following the instructions in a message sent to the email address of the domain's Subscriber, technical, or administrative contact as listed in the domain's WHOIS record.

#### 3.2.2.5 Authentication for an IP Address

Not Applicable

#### 3.2.2.6 Wildcard Domain Validation

TIDID CA employs the approved methods to confirm that the Subscriber requesting a certificate possesses the proper authority or control over the wildcard domains.

The Subscriber is required to demonstrate authority or operational control over the entire domain, encompassing all subdomains covered by the wildcard certificate. This verification can be accomplished through the same methods outlined in standard domain validation (section 3.2.2.4). However, additional validation checks are necessary to ensure control over the wildcard domain. These additional validation methods include, but are not limited to: Performing DNS-based validation not only for the primary domain but also for a representative sample of subdomains, thereby confirming control across the entire wildcard scope.

Obtaining explicit documented approval from individuals or groups responsible for the domain's administration, especially when different subdomains have distinct administrative contacts.

These measures are essential to ensure comprehensive control over the wildcard domain.

#### 3.2.2.7 Data Source Accuracy

Not Applicable

#### 3.2.2.8 CAA Records

The Certificate Authority provides certificate authority authorization service from the Subscriber's CAA record, provided the CAA record is set to "thaidigitalid.com".

The authorization process consists of confirmation whether the SSL Certificate uses thaidigital.com as the CAA record. If not, the RA will not issue an SSL certificate. The CAA record can be accessed via https://dnschecker.org/#CAA/google.com.

The Subscriber must be set DNS Values follow the table

| SSL Brand | Record Type | Flags | Tag | Value/Answer/Destination |
|---|---|---|---|---|
| TDID | CAA | 0 | issue | thaidigitalid.com |

### 3.2.3 Authentication of Individual Identity

The Certificate Authority will verify the trustworthiness from signature on the application and the copy of national ID or passport enclosed to authenticate the Subscriber.

#### 3.2.3.1 In-person Verification

The applicant must verify his / her identity in person at Thaidigital ID Company Limited.

The RA must check written documentation:

The applicant shall provide information which includes name, ID number and at least present at least one original approved photo ID (such as national ID card) during certificate application to the RAO to authenticate the applicant's identity.

If an applicant (such as minor under 18 years old) is unable to submit the above photo ID, government issued written documentation (such as household registration) sufficient to prove the identity of the applicant and one adult with legal capacity to guarantee the applicant's identity in writing may be used in its place. The identity of the adult providing the written guarantee must pass through the above authentication.

### 3.2.4 Non-verified Subscriber Information

Issued Certificates must be confirmed and verified with the documents listed in the application. Application without complete proofs will not be approved.

### 3.2.5 Validation of Authority

The Certificate Authority will verify and retain the power of attorney attached with the application as the proof that the Subscriber is authorized by the directors and may apply on behalf of the company.

### 3.2.6 Criteria for Interoperation

Not applicable.

## 3.3 Identification and Authentification for Re-Key Requests

### 3.3.1 Identification and Authentication for Routine Re-key

The Subscriber must submit a new Certificate Application with required evidence to a Registration Authority as detailed in item 4.1 and 4.3.

### 3.3.2 Identification and Authentication for Re-key after Revocation

The Certificate Authority will verify the Key owner's information from the application form and submitted evidence that comprise the applicant's name, national ID card or passport number, and the applicant's own signature.

### 3.4 Identification and Authentication for Revocation Requests

Subscriber who wishes to revoke their Certificate must directly contact the Certificate Authority. When the Certificate Authority has been informed of the revocation request and has completed the procedural verification, the Certificate Authority will revoke the Certification and publish on the Certificate Revocation List as described in item 4.9.

## 4. Certificate Life-Cycle Operational Requirements

### 4.1 Certificate Application

#### 4.1.1 Who Can Submit a Certificate Application?

Applicants may be individuals applying for Individual Certificates or individuals authorized to apply for Enterprise Certificates on behalf of their company to maintain the security of their electronic transactions. They may apply for Certificates listed under item 1.4.

#### 4.1.2 Enrollment Process and Responsibilities

Subscribers should follow the process described below:

**Personal Certificate Application**

Process

1. Fill the Electronic Certificate application
2. Submit the application form to:
   Registration Authority, Thai Digital ID Co., Ltd.
   319 25 th Floor, Room 10-11, Chamchuri Square Building, Phayathai Road, Pathumwan, Bangkok, 10330
   Tel. 02-029-0290 Ext.4
3. The registration officer verifies the application form and submitted evidence.
4. The registration officer delivers the Electronic Certificate to the Subscriber.
5. The Subscriber pays service fee.

**Required Evidence**

1. Signed photocopy of the Subscriber's national ID (or signed photocopy of passport in cases of non-Thai residents).
2. Signed photocopy of the Subscriber's house registration (or signed photocopy of work permit in cases of non-Thai residents).

**Juristic Person Certificate Application**

Process

1. Fill the Electronic Certificate application
2. Submit the application form to:
   Registration Authority, Thai Digital ID Co., Ltd.
   319 25 th Floor, Room 10-11, Chamchuri Square Building, Phayathai Road, Pathumwan, Bangkok, 10330
   Tel. 02-029-0290 Ext.4
3. The registration officer verifies the application form and submitted evidence.
4. The registration officer delivers the Electronic Certificate to the Subscriber.
5. The Subscriber pays service fee.

**Supporting Evidence**

1. Copy of business registration certificate not older than 90 days (3 months) signed by an authorized director and sealed with Company's seal (if any).

2. Signed photocopy of the authorized director's national ID (or signed photocopy of passport in cases of non-Thai residents).
3. If the authorized director delegated the registration to another person, additional document to be submitted are:
    3.1 Power of attorney, affixed with 30-baht revenue stamps for each delegate.
    3.2 Signed photocopy of each delegate's national ID (or signed photocopy of passport in cases of non-Thai residents).

**TLS/SSL Certificate Application**

Process

1. Fill the Electronic Certificate application
2. Submit the application form to:
   Registration Authority, Thai Digital ID Co., Ltd.
   319 25 th Floor, Room 10-11, Chamchuri Square Building, Phayathai Road, Pathumwan, Bangkok, 10330
   Tel. 02-029-0290 Ext.4
3. The registration officer verifies the application form and submitted evidence.
4. The registration officer delivers the Electronic Certificate to the Subscriber.
5. The Subscriber pays service fee.

**Supporting Evidence**

**For enterprise domain name registration:**

1. Copy of business registration certificate not older than 90 days (3 months) signed by an authorized director and sealed with Company's seal (if any).
2. Copy of domain name registration certificate, signed by an authorized director.
3. Signed photocopy of the authorized director's national ID (or signed photocopy of passport in cases of non-Thai residents).
4. If the authorized director delegated the registration to another person, additional document to be submitted are:
    4.1 Power of attorney, affixed with 30-baht revenue stamps for each delegate.
    4.2 Signed photocopy of each delegate's national ID.
5. CAA Record on the DNS Server of the domain host must be updated to thaidigitalid.com

## 4.2 Certificate Application Processing

### 4.2.1 Performing Identification and Authentication Functions

The Certificate Authority will verify the application and supporting evidence before issuing the certificate and will notify the Subscriber for any incorrect information on the application or incomplete supporting evidence.

### 4.2.2 Approval or Rejection of Certificate Applications

The Registration Authority will review the registration from electronic certificate application and supporting evidence for completeness and authenticity before issuing the certificate. In cases where some part or entirety of the electronic certificate application is either incorrect or incomplete, the document will be returned to the Subscirber with explanation about the issue.

#### 4.2.3 Time to Process Certificate Applications

After receiving the application, the Registration Authority will verify the supporting evidence. If the supporting evidence is complete, the electronic certificate will be issued within the next operating day.

### 4.3 Certificate Issuance

#### 4.3.1 CA Actions During Certificate Issuance

- The Certificate Authority will verify the supporting evidence and CSR file (if any) from the Subscriber for congruence and notify the Subscriber if any discrepancy is found.
- Once verified, the Registration Authority will record the registrar will record the information from the electronic certificate application and issue the certificate.
- The registrar will verify the issued certificate and information on the issued certificate.
- The registrar delivers the electronic certificate to the Subscriber by appropriate means.

#### 4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

Once the registrar has issued the certificate, the system will deliver the information and certificate acceptance form to the Subscriber by email simultaneously with the OTP (One-Time Password) sent to the Subscriber's mobile phone for the next step.

### 4.4 Certificate Acceptance

#### 4.4.1 Conduct Constituting Certificate Acceptance

The Certificate Authority will only recognize the Subscriber's Certificate Acceptance when the Subscriber has completed the following 2 steps:

1. The Subscriber uses the OTP to activate the certificate through the website.
2. The Subscriber signs and sends the certificate acceptance form to the CA.

The CA will not activate the certificate unless the Subscriber has used the OTP to activate the certificate and the Subscriber has sent the signed certificate acceptance form back to the CA.

#### 4.4.2 Publication of the Certificate by the CA

The certificate accepted by the Subscriber will be published on X.500 Directory of the Certificate Authority.

#### 4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Once the registrar has issued the certificate, the system will deliver the certificate information and certificate acceptance form to the Subscriber by email simultaneously with the OTP (One-Time Password) sent to the Subscriber's mobile phone.

### 4.5 Key Pair and Certificate Usage

#### 4.5.1 Subscriber Private Key and Certificate Usage

The Private keys shall only be used for correct keyUsages (key usages are listed in the keyUsages extension of the certificate) such as Digital Signature or Data Encryption usage for applications.

The Subscriber may not use expired or revoked certificates.

#### 4.5.2 Relying Party Public Key and Certificate Usage

Responsibilities of parties in using the public key or certificate shall follow the regulations and conditions for each certificate category issued by the CA. Relying parties, however, must refer to and must verify the certificate status as described on the Certificate Policy/Certification Practice Statement.

### 4.6 Certificate Renewal

#### 4.6.1 Circumstance for Certificate Renewal

Currently, the Certificate Authority does not issue new certificates to Subscribers without changing the public key or information that appears on the certificate.

Everyday, the system will notify the Subscribers whose certificates will expire within 60 or 30 days as a reminder for certificate renewal as described in item 4.1.

#### 4.6.2 Who may Request Renewal

Not applicable

#### 4.6.3 Processing Certificate Renewal Request

Not applicable

#### 4.6.4 Notification of New Certificate Issuance to Subscriber

Not applicable

#### 4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Not applicable

#### 4.6.6 Publication of the Renewal Certificate by the CA

Not applicable

#### 4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable

### 4.7 Certificate Re-key

#### 4.7.1 Circumstance for Certificate Re-Key

Subscribers may submit the certificate and supporting document to request new certificate with the same process described in item 4.1.

#### 4.7.2 Who may Request Certificate of a New Public Key

Refer to item 4.1.

#### 4.7.3 Processing Certificate Re-Keying Requests

Refer to item 4.1.

#### 4.7.4 Notification of New Certificate Issuance to Subscriber

Refer to item 4.3 and 4.4.

#### 4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

Refer to item 4.3 and 4.4.

#### 4.7.6 Publication of the Re-Keyed Certificate by the CA

Refer to item 4.3 and 4.4.

#### 4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Refer to item 4.3 and 4.4.

### 4.8 Certificate Modification

#### 4.8.1 Circumstances for Certificate Modification

If cases where the Subscriber wishes to modify an issued certificate, the Subscriber must submit document for a certificate revocation and document for new application.

#### 4.8.2 Who may Request Certificate Modification

Refer to item 4.1.

#### 4.8.3 Processing Certificate Modification Request

Refer to item 4.1.

#### 4.8.4 Notification of New Certificate Issuance to Subscriber

Refer to item 4.3 and 4.4.

#### 4.8.5 Conduct Constituting Acceptance of Modified Certificate

Refer to item 4.3 and 4.4.

#### 4.8.6 Publication of the Modified Certificate by the CA

Refer to item 4.3 and 4.4.

#### 4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Refer to item 4.3 and 4.4.

### 4.9 Certificate Revocation and Suspension

#### 4.9.1 Circumstances for Revocation

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

- The Subscriber requests revocation in writing;
- The private key becomes known, accessed, or used by a third party.
- The private key lost, modified, disclosed without authorization or has been subject to other damage or misuse.
- The password used to access the private key becomes known by a third party.
- The device used to store private key becomes lost or unusable.
- The Subscriber’s company has ceased its operation.

- The subscriber wishes to modify information on the certificate such as names.
- The Subscriber does not comply with the CA's terms and conditions of certificate use, Certificate Policy/Certificate Practice Statement, or service agreement.
- Following a court order or prosecution.
- The Certificate Authority's pricate key becomes known by a third party.
- The Certificate Authority has suspended or ceased its operation.
- The Certificate Authority has receveied an incident report from a security vendor about a malicious certificate.
- Other circumstances where the Certificate Authority has deemed to impact the security of certificate providing service

### 4.9.2 Who Can Request Revocation

- Certificate Authority
- Registration Authority
- Certificate Owner

### 4.9.3 Procedure for Revocation Request

TDID CA processes a revocation request as follows:

1. TDID CA logs the request or incident report and the reason for requesting revocation based on the list in section 4.9.1 TDID CA may also include its own reasons for revocation in the log
2. If the request from the Subscriber, TDD CA revokes the Certificate based on the reason for revocation listed in 4.9.1 and the Subscriber processs as follows;

   2.1 The certificate revocation applicant fills and signs the certificate revocation request.

   2.2 Submit the revocation request and supporting document to the registration authority staff. The supporting document consists of:

   - For personal certificate, a signed photocopy of the Subscriber's national ID (or signed photocopy of passport in cases of non-Thai residents).
   - For enterprise certificate, a copy of business registration certificate not older than 90 days (3 months) signed by an authorized director and sealed with Company's seal (if any) and a signed photocopy of the authorized director's national ID (or signed photocopy of passport in cases of non-Thai residents).
     - If the authorized director delegated the registration to another person
     - Power of attorney, affixed with 30-baht revenue stamps for each delegate.
     - Signed photocopy of each delegate's national ID.

   2.3 The Registration Authority officer verifies the revocation request and supporting evidence.

   2.4 The Registration Authority officer will only revoke the certificate after verifying the certificate revocation request and supporting evidence.

3. In the event of receiving a report from a third party, TDID shall investigate such report and decide whether revocation is appropriate based on thefollowing criteria:
   a. the nature of the alleged problem,
   b. the number of reports received about a particular Certificate orwebsite,
   c. the identity of the complainants (for example, complaints from a law enforcement official that a web site is engaged in illegal activities have more weight than a complaint from a consumer alleging they never received the goods they ordered), and
   d. relevant legislation

**Remark**

Certificate revocation does not only remove the certification from the database. The revoked certificate will be permanently terminated, published on the CA system.

#### 4.9.4 Revocation Request Grace Period

The Certificate Authority will normally revoke the certificate within one business day after receiving revocation request and verifying the revocation request and supporting document.

#### 4.9.5 Time within Which CA Must Process the Revocation Request

Refer to item 4.9.4

#### 4.9.6 Revocation Checking Requirements for Relying Parties

Relying parties can access CRL published on the URL: http://www.thaidigitalid.com/tdidcag3crl/

#### 4.9.7 CRL Issuance Frequency

The Certificate Authority will update the CRL every 20 minutes. Any certificate revoked in between will be updated in the next CRL.

#### 4.9.8 Maximum Latency for CRLs

The Certificate Authority will publish CRL on its website within 1 hour.

#### 4.9.9 On-line Revocation/Status Checking Availability

Relying parties can access the OCSP on the following URL:
http://www.thaidigitalid.com/tdidcag3ocsp

#### 4.9.10 On-Line Revocation Checking Requirements

Refer to item 4.9.9

#### 4.9.11 Other Form of Revocation Publishing Available

The Certificate Authority does not have other revocation publication other than CRL and OCSP.

#### 4.9.12 Special Requirements Key Compromise

The Certificate Authority has policies for handling of crucial data leakage and continuity of service. Any leakage of data regarding the Subscriber's private key will be informed to the Subscriber and the affected certificate will be revoked.

#### 4.9.13 Circumstances for Suspension

Certificate Suspension refers to a temporary suspension that makes the certificate temporarily unusable. The Certificate Authority or Subscriber may suspend a certificate in the following circumstances:

- The private key is suspected to be known, accessed, or used by a third party.
- The password is suspected to be used to access the private key becomes known by a third party.
- The Subscriber does not comply with the CA's terms and conditions of certificate use, Certificate Policy/Certificate Practice Statement, or service agreement.
- Following a court order or prosecution.

#### 4.9.14 Who Can Request Suspension

- Certificate Authority
- Registration Authority
- Certificate Owner

#### 4.9.15 Procedure for Suspension Request

There are 2 methods for suspension requests:

- The owner makes a telephone call to the registration authority officer, requesting suspension who will then verify the authority of the Subscriber then immediately proceed to suspend the certificate.

- If the owner submits electronic certificate suspension request to the registration authority officer, the officer will proceed to suspend the certificate within 1 operating day after verifying the authority of the Subscriber.

#### 4.9.16 Limits on Suspension Period

Each suspension may last for up to 45 days.

### 4.10 Certificate Status Services

The Subscriber and/or Relying Parties can check the certificate statuses on the CA's website or by calling the RA office.

#### 4.10.1 Operational Characteristics

Relying parties can access the CRL on the following URL: http://www.thaidigitalid.com/tdidcag3crl/ and the OCSP on the following URL: http://www.thaidigitalid.com/tdidcag3ocsp

#### 4.10.2 Service Availability

The Certificate Authority provides 24-hour certificate status reporting service on its website.

#### 4.10.3 Optional Features

Not Applicable.

### 4.11 End of Subscription

Subscribers may end the use of certificate by following procedures described under item 4.9.3: Procedure for Revocation Request

The Subscriber may end a subscription by allowing its certificate to expire without requesting a new certificate

### 4.12 Key Escrow and Recovery

The CA does not provide escrow service for personal keys. Subscribers are responsible for secure retention of personal key. Personal keys issued to the Subscribers must only be appropriately used according to the category.

#### 4.12.1 Key Escrow and Recovery Policy and Practices

Refer to item 4.12.

#### 4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Refer to item 4.12.

## 5. Facility, Management, and Operational Controls

### 5.1 Physical Security Controls

#### 5.1.1 Site Location and Construction

The office of the Certificate Authority is at building number 319, Chamchuri Square Building, 25th floor, Room 10-11, Phayathai Road, Pathumwan, Bangkok, 10330 that is compliant with ISO27001 (Information Security Management System: ISMS) and WebTrust (Trust Service Principles and Criteria for Certification Authorities) standards for CA. The CA has additionally equipped the following equipment at the site of the CA system for safety and security.

1) CCTV for record of event images at the site.

2) Door Hold Open Sounder that will alarm when the door is held open for the safety of the site.

4) Smoke Detector System for fire prevention.

5) FM-200 Fire Extinguisher (gas) that does not harm the computer system.

6) Added metal sheets on each wall, ceiling, and floor of the server room to prevent all kinds of breach.

#### 5.1.2 Physical Access

Only authorized personnels and visitors supervised by authorized personnels can access the operation area of the certificating process. Authorization requires password, RFID Staff ID card, and fingerprint scan. The number of authorized personnels is minimized and all access to the operation area will be logged.

The CA site is access-controlled and zoned according to security levels only accessible by authorized personnels and visitors supervised by authorized personnels.

#### 5.1.3 Power and Air Conditioning

All service systems are supplied with standard electrical output with uninterruptible power supply (UPS) to ensure continuity. The temperature and humidity within the service systems are controlled by air conditioning system independent from the building's air conditioning system.

### 5.1.4 Water Exposures

The operation area is protected from water exposure by elevation and is located in a non-flood area. The building is designed to be 6 inches higher than surrounding area.

### 5.1.5 Fire Prevention and Protection

The fire prevention system utilizes FM-200 type agent that does not damage electronics or computers. The system includes smoke detectors.

### 5.1.6 Media Storage

All media will be stored in multiple safe rooms.

### 5.1.7 Waste disposal

All waste and unused equipment will be disposed. Unused data disposal will be controlled in compliance with ISO 27001 standard.

### 5.1.8 Off-site Backup

Data from the main operation center will be automatically backed up to the secondary operation site everyday.

## 5.2 Procedural Controls

### 5.2.1 Trusted Roles

Combination of access control and key management does not allow any single individual to access the entire system. The roles in operation are divided for security and must at least consist of the following roles:

**5.2.1.1** Trusted Roles for Certification Authority

Consist of:

- CA Operation Manager, responsible for
  - Management of the Subscribers' Private Keys
  - Making and supervision the security policies regarding certificating service system
  - Reviewing the operation of System Support and System Administrator officers
- System Support Officers, responsible for
  - Defining important parameters for systems relating to the certificating service system
  - Operation and management of computer network devices relating to the certificating service system
  - Defining important parameters for computer network devices relating to the certificating service system
- System Administrator Officers, responsible for
  - Performance tuning and security hardening for the computers
  - Management of Subscribers' private keys
  - Making and supervision the security policies regarding certificating service system
  - Reviewing the operation of System Support officers and CA operators

- CA Operators, responsible for
  - Operation and management of computers for the certificating service system
  - Maintenance of the computer operating system
  - Operation and management of data storage for the certificating service system

**5.2.1.2** Trusted Roles for Registration Authority

Can be divided as following:

- RA Operators, responsible for
  - Reception of electronic certificate applications
  - Identification and verification of Subscribers
  - Issuance of certificates
  - Reception of certificate revocation requests
  - Revocation of certificates as requested by the Subscribers
  - Publishing certificate revocation lists
- RA Auditors, responsible for
  - Auditing RA Operator

### 5.2.2 Number of Persons Required Per Task

Operational tasks are divided as described above, allowing a balanced, secure, and accountable operation. The key principles for task sharing are:

1. CA Operator must be separated from System Administrator to ensure separation from the audit log
2. Any task that involves using CA system or database access must require at least 2 operators. One of which will be the operator and the other an inspector.

### 5.2.3 Identification and Authentication for each Role

Personnel assigned for operation must be officially selected by standard process to ensure "trustworthiness".

### 5.2.4 Roles Requiring Separation of Duties

The duties of CA and RA officers are separated.

- CA Officers' main tasks are operation and management of certificate service systems, related softwares (Database, firewall, and LDAP), and system backup.
- RA Officers' main tasks are review of electronic certificate applications, verification of supporting evidence, issuance, suspension, and revocation of certificates.

## 5.3 Personnel Controls

The CA will select trustworthy officers based on knowledge and skills required in operation. The selection process will include criminal background check. The criminal background check will be reconducted every 5 years.

### 5.3.1 Qualifications, Experience, and Clearance Requirements

Must have at least a bachelor's degree in computer science, Information Technology, Computer Engineering, or related majors.

### 5.3.2 Background Check Procedures

The CA will submit the candidates who have passed preliminary recruitment process to the National Police Bureau for background check. After receiving the police clearance, the CA will consider appointing the candidate after 3 months of probation.

### 5.3.3 Training Requirements

Training subjects for new recruits include:

- Basic PKI Concept
- Job responsibilities
- Operational policies and procedures
- ISO27001 Standard
- WebTrust Standard for CA
- BCP and DRP plans

### 5.3.4 Retraining Frequency and Requirements

Officers will be provided with training for their duties and responsibilities on a yearly basis as well as additional training when a new technology is introduced to the operating environment.

### 5.3.5 Job Rotation Frequency and Sequence

Officers' performance will be assessed every 2 years, where job rotation and promotion will also be considered.

### 5.3.6 Sanctions for Unauthorized Actions

Sanctions will be according to the regulations of the certificate authority.

### 5.3.7 Independent Contractor Requirements

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

### 5.3.8 Documentation Supplied to Personnel

CA and RA Officers will be supplied with CA Operation Manual and RA Operation Manual.

## 5.4 Audit Logging Procedures

### 5.4.1 Types of Events Recorded

The following events will be logged in the system:

CA Events Recorded

- CA key life cycle management events
- Key Generation, Backup, Storage,
- CA and Subscriber certificate life cycle management
- Certificate application, Renewal, Revocation
- Successful or unsuccessful processing of request

RA Events Recored

- RA Operation log

- Method used to validate identification document

Environment Events Recored

- Security-related events including
- Security profile changes
- System crashes, hardware failures
- Firewall and router activity
- Facility visitor entry/exit

### 5.4.2 Frequency of Log Processing

Audit Log will be reviewed by the officers on a daily basis and will be thoroughly inspected in cases suspicious occurrences arise.

The log reviewing will include the log and all document related to the event logged.

### 5.4.3 Retention Period for Audit Log

Audit log will be retained for 10 years.

### 5.4.4 Protection of Audit Log

Audit log records can only be accessed by authorized personnel.

### 5.4.5 Audit Log Backup Procedures

Audit log will be automatically backed up to the Log Server everyday.

### 5.4.6 Audit Collection System (Internal vs. External)

The service provider keeps the log of the OS, Application, and Firewall at the local machine and keeps the backup at the secondary operation center.

### 5.4.7 Notification to Event-Causing Subject

When an issue concerning Audit Log occurs, the responsible officer will diagnose, analyze, and notify responsible officers related to the issue.

### 5.4.8 Vulnerability Assessments & Penetration Testing

The CA will regularly conduct vulnerability assessment every 3 months and penetration testing every year.

## 5.5 Records Archival

### 5.5.1 Types of Records to be Archived

The following events will be recorded:

CA Events Recorded

- CA key life cycle management events
- Key Generation, Backup, Storage,
- CA and Subscriber certificate life cycle management
- Certificate application, Renewal, Revocation
- Successful or unsuccessful processing of request

RA Events Recored

- RA Operation log
- Method used to validate identification document

Environment Events Recored

- Security-related events including
- Security profile changes
- System crashes, hardware failures
- Firewall and router activity
- Facility visitor entry/exit

#### 5.5.2 Retention Period for Archive

The CA will retain the information related to the certificate for 10 years and will retain the information related to the certificating system as required by the Computer Crimes Act B.E. 2550 (2007)

#### 5.5.3 Protection of Archive

The archive must only be accessible to authorized personnel.

#### 5.5.4 Archive Backup Procedures

Data from the main operation center will be automatically backed up to the secondary operation site everyday.

#### 5.5.5 Requirements for Time-Stamping of Records

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

#### 5.5.6 Archive collection system (internal or external)

The information mentioned in item 5.5.1 will be kept both as hard copy and soft file both at the main operation center and secondary operation center.

#### 5.5.7 Procedures to obtain and verify archive information

Only authorized persons may access the archive. The archive information will be verified in cases where the information is used.

### 5.6 Key Changeover

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

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

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

### 5.7 Compromise and Disaster Recovery

#### 5.7.1 Incident and compromise handling procedures

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

In case that there is an event that affects the security of TDID CA system, the corresponding TDID CA officers shall notify the PA if any of the following occur:

1) Suspected or detected compromise of any TDID CA system or subsystem.

2) Physical intrusion or electronic penetration of any TDID CA system or subsystem.

3) Successful denial of service attacks or disruption on any TDID CA system or subsystem.

4) Any incident preventing TDID CA from issuing and publishing a CRL or online status checking prior to the time indicated in the nextUpdate field in the currently published CRL, or the certificate for online status checking suspected or detected compromise

#### 5.7.2 Computing resources, software, and/or data are corrupted

Resource management shall include Maintenance Plan (MA Plan) and usage cycle life check. If any resource whether hardware, software, or data appear corrupted, they must be disposed and managed according to the safety policy of the CA.

#### 5.7.3 Entity private key compromise procedures

The CA provides procedures for continuity and management in cases of compromises of key information. If the private key of the CA or Subscriber is compromised, NRCA and all related Subscribers will be notified. All affected private keys and certificates will be revoked immediately once the compromise is confirmed.

#### 5.7.4 Business continuity capabilities after a disaster

The CA has the business continuity plan and disaster recovery plan to alleviate the situations when an issue or occurrence has caused to system to halt.

### 5.8 Certificate Authority or Registration Authority Termination

In the cases where the Certificate Authority or the Registration Authority has to terminate its operation, the CA will notify the NRCA and the Subscriber at least 60 days in advance and the CA will arrange for the transfer to another system, a replacement system, or another appropriate measure to correct the impact that might arise from the termination.

## 6. Technical Security Controls

### 6.1 Key Pair Generation and Installation

#### 6.1.1 Key Pair Generation

Cryptographic keying material used by Thailand NRCA to sign certificates, CRLs or status information are generated in FIPS 140-2 Level 3 or equivalent standard validated cryptographic modules. Multi-party control is required for Thailand NRCA key pair generation, as specified in Section 6.2.2. Thailand NRCA key pair generation created a verifiable audit trail demonstrating that the security requirements for procedures were followed. The documentation of the procedure has shown that appropriate role separation was used. An independent third party has validated the execution of the key generation procedures by witnessing the key generation, as well as by examining the signed and documented record of the key generation. Subordinate CA key pair generation shall be performed by the Subordinate CA. The Subordinate CA is required to generate the signature key pairs for the purpose of digital signature by FIPS 140 FIPS 140-2 Level 3 validated hardware cryptographic modules to support source authentication. The subordinate CA shall not generate keys for SSL certificates.

1. The generated key pair shall be explicitly used as a Subordinate CA key pair, under the hierarchy of the "Thailand NRCA".

2. The private key shall be used exclusively for CA signing operations, including the issuance of end-entity certificates and CRL generation.

3. The public key shall be included in the Subordinate CA's certificate signed by the "Thailand NRCA".

6.1.1.1 CA Key Pair Generation

For CA Key Pairs that are used as a CA Key Pair for a Root Certificate.

The CA SHALL:

1) prepare and follow a Key Generation Script,

2) have a Qualified Auditor witness the CA Key Pair generation process or record a video of the entire CA Key Pair generation process, and

3) have a Qualified Auditor issue a report opining that the CA followed its key ceremony during its Key and Certificate generation process and the controls used to ensure the integrity and confidentiality of the Key Pair. For other CA Key Pairs that are for the operator of the Root CA or an Affiliate of the Root CA, the CA SHOULD:

1) prepare and follow a Key Generation Script and

2) have a Qualified Auditor witness the CA Key Pair generation process or record a video of the entire CA Key Pair generation process.

In all cases, the CA SHALL:

1) generate the CA Key Pair in a physically secured environment as described in this CP/CPS;

2) generate the CA Key Pair using personnel in Trusted Roles under the principles of multiple person control and split knowledge;

3) generate the CA Key Pair within cryptographic modules meeting the applicable technical and business requirements as disclosed in this CP/CPS;

4) log its CA Key Pair generation activities; and

5) maintain effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in its CP/CPS and (if applicable) its Key Generation Script.

6.1.1.2 RA Key Pair Generation

No stipulations

6.1.1.3 Subscriber Key Pair Generation

The CA 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) The CA is aware of a demonstrated or proven method that exposes the Applicant’s Private Key to compromise;

4) The CA 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) The CA 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-kpserverAuth [RFC 5280] or anyExtendedKeyUsage [RFC 5280], the Subordinate CA SHALL NOT generate a Key - 49 - Pair on behalf of a Subscriber, and SHALL NOT accept a certificate request using a Key Pair previously generated by the CA.

### 6.1.2 Private Key Delivery to Subscribers

The Subscribers' key pair will be generated and stored in electronic media Smartcard, USB Token, or Hardware Security Module (HSM), a high-security personal key storage device that does not allow the Subscribers' private key or other information to be exported. Such electronic media will be stored with the Subscriber. In the cases where private keys are stored as files, they must be password-protected.

### 6.1.3 Public Key Delivery to Certificate Issuer

Public key delivered to the certificate authority will be formatted as PKCS#10 Certificate Signing Request (CSR) or sent through website certified with Secure Sockets Layer (SSL) standards.

### 6.1.4 CA Public Key Delivery to Relying Parties

The CA's public key will be delivered to the relying parties either attached with the Subscriber's certificate or downloadable at the CA's website.

### 6.1.5 Key Sizes

The CA's key size will be RSA 4096-bit. The Subscribers' key size will be a RSA-2048-bit.
TDID CA use the SHA-256, SHA-512 hash algorithm when issuing certificates and CRLs and generating digital signatures.

### 6.1.6 Public Key Parameters Generation & Quality Checking

The CA will generate public key parameters according to the X.509 Version 3 standards. The quality checking will be automatically done with the certificating system.

### 6.1.7 Key Usage Purposes

The key usage purposes have been described under item 1.4: Certificate Usage.

## 6.2 Private Key Protection and Cryptographic Module Engineering Controls

### 6.2.1 Cryptographic Module Standards and controls

The cryptographic module is certified with Federal Information Processing Standard (FIPS) 140-2 Level 3, an international standard for generation and security of private key for certificating system.

### 6.2.2 Certificate Authority's Private Key (n out of m) Multi-Person Control

The CA's private key has multi-person control in place.

### 6.2.3 Private Key Escrow

The CA does not provide escrow service for private keys.

### 6.2.4 Private Key Backup

Only CA's private keys are backed up.

### 6.2.5 Private Key Archival

The CA private keys beyond the validity period will be kept at least 1 0 years and stored in Cryptographic Module with FIPS 140-2 Level 3 standards

### 6.2.6 Private Key Transfer into or from a Cryptographic Module

The CA's private key is generated in cryptographic module certified with Federal Information Processing Standard (FIPS) 140-2 Level 3 and will only be decrypted by authorization process through hardware with the same level security and only with correct password from the certificate authority's CA.

### 6.2.7 Private Key storage on cryptographic module

TDID CA shall store their Private Keys on a cryptographic module which complies with FIPS 140-2 Level 3 or above standard.

### 6.2.8 Method of Activating Private Key

Private keys of the CA and Subscribers will be activated by authorization process through hardware with the same level security and only with correct password.

### 6.2.9 Method of Deactivating Private Key

The private key can only be deactivated upon a revocation request from the Subscriber.

### 6.2.10 Method of destroying private key

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

### 6.2.11 Cryptographic Module Rating

Private keys of the CA and Subscribers are generated with standardized softwares.

## 6.3 Other Aspects of Key Pair Management

### 6.3.1 Public Key Archival

The public key will be on the certificate and the certificate will be retained in the CA's database throughout its operational period.

### 6.3.2 Certificate operational periods and key pair usage periods

The usage periods of the certificate and key pair of the CA is 20 years.

The validity period of a certificate issued under this CP/CPS shall not exceed the maximum validity periods as below

| Type of Certificate | Maximum Validity Periods |
|---|---|
| Personal Certificate | 2 years |
| Juristic Person Certificate | 2 years |

| | |
|---|---|
| Enterprise User Certificate | 2 years |
| Machine Certificate | 2 years |
| TLS/SSL Certificate | 825 days (Certificates issued after 1 March 2018 but prior to 1 September 2020) |
| TLS/SSL Certificate | 398 days (Certificates issued on or after 1 September 2020) |

## 6.4 Activation Data for Installation of the Certificate

### 6.4.1 Activation Data Generation and Installation

The activation data of the Subscribers are securely generated and kept. To activate the certificate, the Subscriber must contact the CA to verify the authority of the certificate Subscriber. Then, the certificate will be activated through the CA's software system and the certificate status on X.500 Directory will be updated.

### 6.4.2 Activation Data Protection

The Subscribers' activation data will be protected by the protection system of HSM device according to the FIPS 140-2 Level 2 or 3 standards such as password or other authorization process for certificate installation.

### 6.4.3 Other Aspects of Activation Data

There is no other information other than key information used for certificate application.

## 6.5 Computer Security Controls

### 6.5.1 Specific Computer Security Technical Requirements

The CA has arranged a system security plan that incorporates the computer security technical requirements for certificating according to the ISO 27001 ( Information Security Management System: ISMS) and WebTrust for CA ( Trust Service Principles and Criteria for Certification Authorities) Standards.

### 6.5.2 Computer Security Rating

The CA has arranged a system security plan that incorporates computer security rating for certificating according to the ISO 27001 (Information Security Management System: ISMS) and WebTrust for CA (Trust Service Principles and Criteria for Certification Authorities) Standards.

## 6.6 Life Cycle Security Controls

### 6.6.1 System Development Controls

The software of the certificating system is developed under appropriate quality controls according to the Information Technology Security Evaluation Criteria Level E3 (ITSEC E3).

The software must be performed in a test environment before deployment in a production environment. Any change to the CA systems must go through the Change-Advisory Board review and approval.

### 6.6.2 Security Management Controls

The security management controls are controlled and managed under the ISO 27001 (Information Security Management System: ISMS) WebTrust for CA (Trust Service Principles and Criteria for Certification Authorities) systems with the details regarding the tools, procedures, and trusted personnel described under item 5.2.1: Trusted Roles.

### 6.6.3 Life Cycle Security Ratings

The CA has created risk assessment document that identifies and mitigate the life cycle security risks rated as 'high risk' and 'very high risk' in certificating system.

## 6.7 Network Security Controls

The network control for certificating system has been designed to only use related computers and devices. TDID CA system is connected *to one internal network* and is protected by firewalls and Network Address Translation for all internal IP addresses.

Both hardware and software firewalls (only configurable by IT Security Manager) are utilized to prevent intrusion from external source. The system also includes Intrusion Protection System (IPS) and Anti-Virus.

The certificate public services (i.e CRLs, OCSP) are allowed to access through public internet.

## 6.8 Timestamping

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

# 7. Certificate, Certificate Revocation List, and OCSP Profiles

## 7.1 Certificate Profile

### 7.1.1 Version number(s)

Certificates issued by the CA conforms with X.509 Version 3 Certificate Standard and has the following information:

- Version 3
- Serial Number
- Signature Algorithm: Algorithm TDID CA uses for signature generation
- Issuer: The name of certificate issuer
- Validity: The start and end date of certificate validity
- Subject: National ID number or tax ID of enterprise
- Subject Public Key Information: Public key and generating algorithm

### 7.1.2 Certificate Extension

Additional information of the certificate issued by the CA following the X.509 V.3 certificate extensions standards that contains at least the following information:

- Authority Key Identifier: Public key of the CA
- Key Usage: Intended usage for the key
- Extended Key Usage: Extended usage for the key
- CRL Distribution Points: Location of the CRL for status check

- Basic Constraints: Categories of the certificate whether it belongs to the CA or Subscribers and the maximum number of certificate chain.
- Certificate Policies: Reference to the Certificate Policy in the form of Object Identifier (OID)

### 7.1.3 Algorithm object identifiers

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

| Algorithm | Object Identifier |
|---|---|
| SHA256 withRSAEncryption | 1.2.840.113549.1.1.11 |
| SHA512withRSAEncryption | 1.2.840.113549.1.1.13 |
| RSAEncryption | 1.2.840.113549.1.1.1 |

### 7.1.4 Name Forms

Names in Certificate Issuer and Certificate Subject fields of the certificate are distinguished names according to X.500 standard.

The Distinguished Name (DN) of TDID CA will use the following information:

| | | |
|---|---|---|
| C | = | TH |
| S | = | <State> |
| L | = | <Locality> |
| O | = | <Customer Corporate name in English> |
| organizationIdentifier | = | <Customer Corporate tax ID> |
| OU | = | <Department Name in English > |
| Title | = | <Position in organization> |
| Serial Number | = | <identification ID> |
| Givenname | = | <Customer First Name in Thai> |
| SN | = | <Customer Last Name in Thai> |
| CN | = | <Customer Name in English> |
| E | = | <Email> |

The information that appears as the DN also depends on the Certificate Policy, viewable on TDID Website (https://www.thaidigitalid.com).

### 7.1.5 Name Constraints

Comma (,) may not be used as TDID uses comma (,) as a divider between each Distinguished Name (DN)

### 7.1.6 Certificate Policy Object Identifier

2.16.764.1.1.2.1.10001.1 Enterprise Certificate
2.16.764.1.1.2.1.10002.1 Enterprise User ID Certificate
2.16.764.1.1.2.1.20001.1 Personal Certificate
2.16.764.1.1.2.1.30001.1 SSL Certificate

### 7.1.7 Usage of Policy Constraints Extension

The policies must display the following extension fields:

- Authority Key Identifier
- Key Usage
- CRL Distribution Points
- Basic Constraints
- Certificate Policies
- Subject Alternative Name
- Authority Info Access
- Enhanced Key Usage

The information that appears on the extension field also depends on the Certificate Policy, viewable on TDID Website (https://www.thaidigitalid.com).

### 7.1.8 Policy Qualifiers Syntax and Semantics

The CA has described its policies qualifiers syntax and semantics under Certificate Policy on TDID Website ( URL: https://www.thaidigitalid.com/downloads/).

### 7.1.9 Processing Semantics for the Critical Certificate Policies Extension

2 fields of critical extensions are identified: Basic Constrains and Key Usage.

## 7.2 Certificate Revocation List Profile

### 7.2.1 Version

CRL published by the CA uses X.509 CRL Version 2 standard comprising:

- Signature Algorithm: Algorithm that TDIT CA used to generate the signature on the CRL
- Issuer: Name of the CRL Issuer
- Effective date: Date and time the CRL is published
- Next update: Date and time the next CRL is due for publication
- CRL Number: Number of the CRL
- Revocation List: The list of certificates revoked

### 7.2.2 CRL and CRL entry extensions

The information on certificate revocation lists issued by the Certification Authority complies with the ISO / IEC 9594-8:2012 standard and contains at least the following:

| Extension | Value |
|---|---|
| Authority Key Identifier | Subject Key Identifier of the CRL issuer certificat |
| CRL Number | Never repeated monotonically increasing integer |

## 7.3 OCSP profile

The Online Certificate Status Protocol is an online mean to check the status of a certificate.

### 7.3.1 Version number(s)

The CA's OCSP uses X.509 OCSP Version 1 standard according to the rfc2 5 6 0 standard (https://www.ietf.org/rfc/rfc2560.txt).

### 7.3.2 OCSP extensions

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

## 8. Compliance Audit and Other Assessment

The Certificate Authority under the name of TDID CA G3 adheres to the ISO 27001 (Information Security Management System: ISMS) standard for policies regarding risk assessment and security and has arranged for internal and external audits with the latest WebTrust for CA (Trust Service Principles and Criteria for Certification Authorities) and WebTrust for CA - SSL Baseline (WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security) standards published on http://www.cabforum.org for its certificating and management for trustworthiness.

TDID CA has a compliance audit mechanism in place to ensure that the requirements of its CP/CPS are being implemented and audited for complying with the following standards: .

o Adobe Approved Trust List – Technical Requirements (if applicable).

o Electronic Transactions Act, B.E. 2544 (2001)

and related version.

o The NRCA CP.

### 8.1 Frequency or Circumstances of Assessment

The CA will be assessed for the following standards at least once a year:

1. ISO 27001 Standard
2. Webtrust for CA Standard
3. Webtrust for CA - SSL Baseline Standard

### 8.2 Identity/Qualifications of Assessor

Assessor for ISO 27001, Webtrust for CA, and Webtrust for CA - SSL Baseline standards must be qualified to certify the associated standards.

### 8.3 Assessor's Relationship to Assessed Entity

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

### 8.4 Topics Covered by Assessment

The purpose of compliance audit is to verify that a CA and its RAs comply with all the requirements of the current version of the CP and the CA's CPS. The audit meets the requirements of the audit schemes highlighted in Section 8 under which the assessment is being made. These requirements may vary as audit schemes are updated. An audit scheme is applicable to CAs in the year following the adoption of the updated scheme.

### 8.5 Actions Taken as a Result of Deficiency

Any deficiency within the system reported must be corrected by the CA within the period set by the assessor.

The plan will be submitted to auditors and Thailand NRCA to ensure that sufficient security of the system is still in place.

### 8.6 Communication of Results

After the assessment is completed, the audit compliance report and identification of corrective measures (if any) must be sent to the PA within 30 days of completion. However, the audit compliance report must be sent to the PA and made publicly available within three months after the end of the audit period. In the case of delay, the CA shall provide an official letter signed by the qualified auditor.

### 8.7 Self-Audits

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

## 9. Other Business and Legal Matters

### 9.1 Fees

The CA will collect fees for the following instances:

1. Certificate Issuance
2. Certificate Renewal

Applicable fees can be viewed on the CA's website.

#### 9.1.1 Certificate Issuance or Renewal Fees

The certificate issuance or renewal fees will be displayed on the certificated issued from the system.

#### 9.1.2 Certificate Access Fees

The CA does not collect fees for Subscriber's access to the certificate.

#### 9.1.3 Revocation or Status Information Access Fees

The CA does not collect fees for Subscriber's access to the CRL published on the CA's website.

#### 9.1.4 Fees for Other Services

The CA does not collect fees for downloading the CP/CPS document.

#### 9.1.5 Refund Policy

The CA will not charge for certificate issuance if the Subscriber request for revocation of such certificate within 15 days from issuance.

### 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

The CA is a legal entity registered in accordance with Thai law with asset information available in the financial statement on Department of Business Development's (Ministry of Commerce) website.

#### 9.2.3 Insurance or warranty coverage for end-entities

The CA guarantees the accuracy of information present on the certificate. In cases there is any mistake associated with the RA or CA, the Subscriber must notify the CA within 15 days after issuance. The CA will then issue a new certificate free of charges.

### 9.3 Confidentiality of Business Information

Electronic certification service providers have defined the scope of confidentiality of business information, including business plans, sales information, trade secrets, and information obtained from third parties in pursuit of service agreement, contract, or other service document.

#### 9.3.1 Scope of Confidential Information

Confidential information that must not be disclosed includes:

- Certificate issuance list
- Subscribers' Private Key
- Audit record
- Audit report
- Business continuity plan

#### 9.3.2 Information Not Within the Scope of Confidential Information

The certificates, revoked certificates, and certificate statuses are not confidential information that may be disclosed. Other information not interpreted as confidential or non-confidential will be considered in accordance with the appropriate laws.

#### 9.3.3 Responsibility to Protect Confidential Information

The CA will not disclose confidential information to unrelated entities in any circumstance.

### 9.4 Privacy of Personal Information

Any processing of personal information must be consented by the Subscriber before personal data can be disclosed except for instances of lawful enforcement or court order to disclose personal information.

#### 9.4.1 Privacy Plan

The CA has a defined privacy plan and will keep the Subscribers' private information confidential.

#### 9.4.2 Information Treated as Private

Private information in this document means related information of Subscribers that is not included in the certificate or directory.

#### 9.4.3 Information Not Deemed Private

The CA and Subscribers acknowledge and agree that information on the certificates is not confidential.

#### 9.4.4 Responsibility to Protect Private Information

The CA is strictly responsible for protection of private information.

#### 9.4.5 Notice and Consent to Use Private Information

In cases there are reasonable grounds for disclosing the Subscribers' private information, the CA must priorly acquire a written consent from the Subscriber.

### 9.4.6 Disclosure Pursuant to Judicial or Administrative Process

The CA reserves the right to disclose its Subscribers' private information in cases of court requests for judicial or administrative process under Thai law.

### 9.4.7 Other Information Disclosure Circumstances

Any case that requires disclosure other than in item 9.4.6 must also be priorly consented by the Subscriber in writing.

## 9.5 Intellectual Property Rights

TDID CA is the sole owner of intellectual properties within and arising from this Certificate Policy/ Certification Practice Statement. TDID authorizes to copy the CP/CPS may be copied in the CCADB and Trust Store archives, and posted on the public Bugzilla.

## 9.6 Representations and Warranties

### 9.6.1 CA representations and warranties

The CA guarantees that

- Approvals of certificate issuance are processed under strict supervision of the CA against all errors.
- Certificate issued by the system complies with this Certificate Policy/ Certification Practice Statement.
- Certificate status report via the LDAP repository complies with this Certificate Policy/ Certification Practice Statement.

### 9.6.2 RA representations and warranties

The RA guarantees that

- Information in certificate application and supporting document will be thoroughly and carefully reviewed. There will be no alteration to the information provided in the certificate application form.
- Information on the certificate application will be delivered to the CA under strict supervision by the RA to prevent errors.
- Certificate issued by the system complies with this Certificate Policy/ Certification Practice Statement.

### 9.6.3 Subscriber representations and warranties

The Subscriber guarantees that

- Certificate issued by the CA will be appropriately used within the scope and according to this Certificate Policy/Certification Practice Statement.
- Private key will be securely kept and not usable by others.
- Information on the certificate application form is accurate and true.
- Information on the certificate is extract from the application form and is accurate and true.
- The Subscriber is an individual, organization, or company that does not operate as a CA Provider.

#### 9.6.4 Relying party representations and warranties

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

#### 9.6.5 Representations and warranties of other participants

Not applicable

### 9.7 Disclaimers of Warranties

The CA makes no warranties, whether express or implied, other than those appearing on this Certificate Policy/Certification Practice Statement, nor does it guarantee commercial performance or any specific purpose.

### 9.8 Limitations of Liability

Any liability relating to the certificate will be limited to no more than 30 times the fees of the certificate for each case of damage.

The CA shall not be held liable for any damage due to the use of certificate that is either illegal or outside of scope of appropriate use according to this Certificate Policy/ Certification Practice Statement or violation of the terms and conditions of the CA. Additionally, the CA shall not be held liable for indirect and consequential damages, damages caused by special circumstances, and loss of revenue or commercial profits.

The first paragraph shall not apply if there is other existing limitation of liability for each type of certificates in the related terms or contracts.

### 9.9 Indemnities

Indemnity claims shall be agreed between the CA and Subscribers. However, in cases where relying parties use the certificate without checking the CRL, the CA reserves its right to deny any indemnity claims for any damage to arise. In case the damage occurs to the CA from the actions of Subscribers or relying parties, the CA reserves the right to claim damages.

### 9.10 Term and Termination

#### 9.10.1 Term

This CP/CPS of TDID CA takes effect from the date of publication upon the approval of the PA.

#### 9.10.2 Termination

This CP/CPS of TDID CA takes effect until it is terminated.

#### 9.10.3 Effect of termination and survival

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

### 9.11 Individual notices and communications with participants

The CA provides means of communications for Subscribers including telephone and email as shown on the CA's website. TDID CA will communicate to those participants using a reliable channel as soon as possible in accordance with the importance of information.

### 9.12 Amendments

The CA reserves the right to modify, add, cancel, or change any terms of service within this document.

#### 9.12.1 Procedure for amendment

In cases where the CA wishes to modify, add, cancel, or change any term in this document, the CA will notify its Subscriber or the RA at least 90 days before the effective date of change. The notice may be a letter, email, or announcement on CA website: www.thaidigitalid.com.

#### 9.12.2 Notification mechanism and period

If the CA or its Subscriber deem that the modification, addition, cancellation, or change of the terms will decrease their legitimate right, the RA or Subscriber may request termination of the service according to this document by notifying the CA not less than 30 days prior to the effective date of termination, except for modification, addition, cancellation, or change of the terms required by law.

#### 9.12.3 Circumstances under which OID must be changed

The CA does not specify the circumstances when OID must be changed.

### 9.13 Dispute Resolution Procedures

#### 9.13.1 Disputes between Issuer and Subscriber

Incases of dispute regarding the certificate issuance, all parties will first try to negotiate. In cases the dispute cannot be settled in 60 days after the dispute arises, the parties shall resolve such dispute by judicial proceedings in Bangkok, Thailand in accordance with the Arbitration Rules of the Institute of Arbitration of Thailand under the Arbitration Act B.E. 2545 (2002). The parties require 3 arbitrators shom selection shall be governed by the Office of the Judiciary Regulations for arbitration.

The arbitral award of dispute in the first paragraph shall be in accordance with the Institute of Arbitration of Thailand regularion, Dispute Resolution Bureau, the Office of the Judiciary, and the current laws in force. The CA and the Subscriber agree to be responsible for.

#### 9.13.2 Disputes between Issuer and Relying Parties

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

### 9.14 Governing Law

Any agreement in this document shall be interpreted and enforced in accordance with the laws of Thailand.

### 9.15 Compliance with Applicable Law

The CA agrees to comply with Thai laws relating to the electronic certificate issuance.

### 9.16 Miscellaneous Provisions

#### 9.16.1 Entire agreement

This document in combination with the certificate application, and terms of certificate use shall be considered important information provided by the CA to the Subscribers regarding terms for the

management of certificate and shall be equivalent to an agreement between the CA and Subscribers to process and comply with such document.

### 9.16.2 Assignment

The CA agrees not to transfer the rights or duties described in this document whether partially or its entirety to a third party unless prior written consent is obtained from the Subscriber.

Such consent pursuant to paragraph one does not clear the CA off the liabilities accrued as results of this agreement and thus, the CA shall share the liabilities for damages caused by the recipient whether willfully or by negligence.

### 9.16.3 Severability

In circumstances where any part of this document becomes void, incomplete, or unenforceable by law, the affected clause or clauses shall not affect the applicability of other clauses within this agreement which are complete and enforceable.

### 9.16.4 Enforcement (attorneys' fees and waiver of rights)

The party that violates the agreement will be liable for all costs accrued including attornes' fees arising out of non-compliance with this document and/or related document.

Any waiver or extension made by any party pursuant to this document shall be deemed situational that only applies to that instance and does not imply waiver for the rights in accordance with this document.

### 9.16.5 Force Majeure

Each party shall not be held liable to the damages resulting from inability or delay to act according to this document due to force majeure.

In circumstances where one party cannot act according to this document due to force majeure, the affected party must immediately notify other party in writing, describing the nature of the force majeure, action taken to mitigate or negate the impact of such force majeure, and estimation of possibility of the force majeure to subside.

Force majeure may refer to events beyond the control of each party that result in the inability or impossibility to perform their duties described in this document. Force majeure may include natural disasters, earthquakes, fires, explosions, strikes, labor disputes, protests, accidents, epidemics, storms, floods, wars, revolutions, civil unrests, and shortage or resources such as water, electricity, fuel, or labour, etc.

In the circumstances that force majeure persists for longer than 30 days, both parties may agree to terminate the service or certificate issuance according to this contract.

## 9.17 Other provisions

Not applicable