บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน)
Internet Thailand Public Company Limited

One Certification Authority

Certification Practice Statement

(Certification Policy Identifier (OID): 2.16.764.1.1.3.1.11001.1.1)

Document Revision History

Date	Revision	Description
30/10/2018	00	First baseline

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

Table of Contents

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

1. Introduction

1.1 Overview

1.1.1 Certification Practice Statement

The name of this document is the One Certification Authority (One CA) Certification Practice Statement (CPS). The CPS is stipulated to follow the Certification Policy (CP) for Internet Thailand Public Company Limited and complies with the Electronic Transactions Act and related international standards such as the Internet Engineering Task Force (IETF) RFC 3647, ITU-T X.509 and IETF PKIX Working Group RFC 5280.

The One CA is the Level 1 Subordinate CA under the Thailand National Root Certification Authority (NRCA) and is responsible for issuance and administration of individual and juristic person certificates. The Thailand NRCA is the highest-level CA and trust anchor. Relying parties can directly trust the root certificates of the Thailand NRCA.

1.1.2 CPS Applicability

The practice statement stipulated in this CPS applies to the One CA, RAs, subscribers, relying parties and the repository.

1.2 Document Name and Identification

This version is 1.0 and the issue date of this version is August 27, 2018. The latest version of this CPS can be obtained from:

https://ca.inet.co.th/

The CPS object identifiers (OIDs) are listed in the Table below:

OID Name	OID Value
iso-itu-t-country-th-etda-nrca-One CA	2.16.764.1.1.3

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

1.3 PKI Participants

The key members of the One CA include:

(1) One CA

(2) RAs

(3) Subscribers

(4) Relying Parties

(5) Other Participants

(6) Third Parties

1.3.1 Certification Authorities

The One CA is established by INET and operate on INET's infrastructure by One Authen. Co Ltd. and issues individual and juristic person in accordance with CP/CPS regulations.

1.3.2 Registration Authorities

The RA is responsible for collection and authentication of subscriber identity and certificate-related information. The RA is comprised of one or more RA counters authorized under the organization approved by the One CA. Each RA counter has an RA officer (RAO) who is responsible for performing certification application, revocation, rekey, renewal work for different groups and classes.

1.3.3 Subscribers

Subscribers refer to the subject who has applied for and obtained a certificate issued by the One CA. The relationship between the subscriber and certificate subject is listed in the Table below:

Certification entity	Subscriber
Natural person	Whomself
Enterprise	Trustee of authorized organization

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

Generation of subscriber key pairs shall conform to the regulations in section 6.1.1 of the CPS. The subscriber must solely possess the right and capability to control the private key that corresponds to the certificate. Subscribers may not issue certificates themselves to other parties.

1.3.4 Relying Parties

The relying party refers to a third party that acts in reliance of the relationship between the certificate subject name and the public key. The relying party must verify the validity of the certificate used based on the corresponding CA certificate and certificate status information. The certificate may be used for the following work after checking the validity of the certificate:

(1) Verify the integrity of a digitally signed electronic document.

(2) Identify the creator of a digitally signed electronic document.

(3) Establish a secure communication channel with the subscriber.

1.3.5 Other Participants

The One CA selects other authorities, which provide related trust services, such as time stamp authority (TSA) and card management center as the collaborative partners, the related information shall be disclosed on the website and the collaboration mechanism and mutual rights and obligations shall be set down in the CPS.

1.3.6 Third parties

One CA's Data Center host at INET's Data Center, they were maintain between One Authen and INET with 3rd party contract.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The One CA issues certificates for individual and juristic person as defined in the CP.

The appropriate certificate uses are as follows:

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

Applicable Type of Certificates	Verification	Applicable Scope
individual, juristic person	Applicant needs to apply in person at counter. Applicant provides legal and proper documentation proving individual or juristic person identity. The registration authority officer checks the accuracy of application information. The system may automatically compare the applicant's information with a reliable database to verify its accuracy. Verify that the applicant can operate the e-mail account, if the e-mail address in certificate subject alternative name is use for Secure-Email.	Verify that the applicant can operate the e-mail account. When used for digital signatures, it can identify that the subscriber originates from a certain e-mail account or guarantee the integrity of the signed document. When used for encryption, the relying party can use the subscriber's certificate public key to encrypt and transmit the message or the symmetric key to guarantee its confidentiality. Suitable for use with information which may be tampered with, but the network environment has no malicious tampering (data interception is possible, but likelihood is not high). Not suitable for the signing of important documents (life essential and high value transaction documents). For example, Internet tax filing, secure e-mail, information encryption and identity authentication for small value e-commerce transactions.

Subscribers must carefully read the CPS and watch for CPS updates before using and trusting the certificate services provided by the One CA.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

1.4.2 Prohibited Certificate Uses

It is prohibited to use the certificates issued by the One CA for the following purposes:

- Crime
- Control of military orders and war situations as well as nuclear, biological and chemical weapons
- Operation of nuclear equipment
- Aviation flight and control systems
- Scope of prohibitions announced under the law

1.5 Policy Administration

1.5.1 Organization Administering the Document

Policy Authority (PA) of Internet Thailand Public Company Limited

1.5.2 Contact Person

If you have any questions regarding this CPS or a subscriber wishes to report a missing key, you may directly contact the One CA.

Address: 1768 Thai Summit Tower, 16th Floor and IT Floor

New Petchaburi Road, Khwaeng Bang Kapi,

Khet Huay Khwang, Bangkok 10310

Phone: +66-2257-7000

E-mail: ra@inet.co.th

Website: https://ca.inet.co.th

If there is any other contact information or changes to the contact information, please check the following website: https://ca.inet.co.th

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

1.5.3 Person Determining CPS Suitability for the Policy

The One CA shall first check whether the CPS conforms to relevant CP regulations and then submit the CPS to the Policy Authority for review and approval. After approval, One CA shall officially use the CP.

In accordance with the regulations defined in the Electronic Transactions Act, the CPS established by the CA must be approved by the competent authority, before it is provided externally for certificate issuance service.

1.5.4 CPS Approval Procedure

The CPS is published by the One CA following approval by the INET PA

After the CPS revisions take effect, the revised CPS content shall take precedence in the event of a discrepancy between the revised and original content. If the revisions are made by attached document, the attached documents shall take precedence in the event of discrepancy between the attached documents and the original CPS.

1.6 Definitions and Acronyms

1.6.1 Definitions

Table 1 Terms and Definitions

Term	Definition
Certificate	A form of electronic documents used for verifying the relationship between entities and public key. A certificate is issued in compliance with ITU-T Recommendation X.509 (11/08): Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks and ISO/IEC 9594-8:2008 Information technology -- Open Systems Interconnection -- The Directory: Public-key and attribute certificate frameworks.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

Certificate Policy (CP)	1. Refers to a named set of rules that indicates the applicability to a certain community or class of application with common security requirements (RFC 3647) 2. Certificate policy refers to the dedicated profile administration policy established for the electronic transactions performed through certificate administration. Certificate policy covers a variety of issues including the formation, generation, delivery, auditing, administration and restoration after compromise. Certificate policy indirectly controls the use and operation of certificate security systems to protect the transactions performed by the communication systems. The security services required for certain application are provided through control of the certificate extension methods, certificate policy and related technology.
Certificate Repository	Source for storage and publication of certificates and certificate revocation lists.
Certificate Revocation	A certificate may be revoked prior to its expiration date. Once revoked, it can no longer be used.
Certification Authority (CA)	An entity authorized to issue, manage, revoke, and renew certificates.
Certification Practice Statement (CPS)	A statement of the practices that a certification authority employs in issuing, managing, revoking, and renewing or re-keying certificates.
Cryptographic Module	Specialized equipment used to maintain, manage and operate the key pair.
Digital Signature	A Digital Signature is a mathematical scheme for demonstrating the authenticity and integrity of a digital message or document.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

Entity	Individual, Server, Operating Unit/Site, or any Device that is under the control of the individual.
Key Pair	A Key Pair refers to two separate keys of the asymmetric cryptographic system, one of which is secret (Private Key) and another is public (Public Key). The two parts of the key pair are mathematically linked in the ways that one key locks or encrypts the plaintext, and the other unlocks or decrypts the cipher text. Neither key can perform both functions by itself. The Key Pair can be used to authenticate the digital signature as well as maintain confidentiality of information.
OCSP (Online Certificate Status Protocol)	A protocol used for verifying status of a certificate.
Private Key	The key used to create a digital signature and can be used to decrypt the message that is encrypted with its pair of public key, to obtain the original message.
Public Key	The key used to verify a digital signature to ensure the integrity of electronic message and also to encrypt message to maintain its confidentiality.

1.6.2 Acronyms

Table 2 Acronyms

Acronym	Term
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
NRCA	National Root Certification Authority
PA	Policy Authority
PIN	Personal Identification Number

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

PKI	Public Key Infrastructure
RA	Registration Authority
ETDA	Electronic Transactions Development Agency (Public Organization)

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

2. Publishing and Repository Responsibilities

2.1 Repositories

The repository, under the management of the One CA, publishes and stores the One CA issued certificates, certificate revocation lists (CRL) and the CPS and provides inquiry services to subscribers and relying parties. The repository provides 24-hour round-the-clock service. The Internet address of the One CA repository is https://repository.inet.co.th The repository will resume normal operation within 24 hours if unable to operate normally for some reason.

The responsibility of the repository includes:

(1) Regularly publish issued certificates, and revoked certificates and CRL in accordance with section 2.2.

(2) Publish the latest CPS and CP information.

(3) Access control of the repository shall comply with the provisions in Section 2.4.

(4) Publish external audit results specified in section 8.6.

(5) Guarantee the accessibility status and availability of the repository information.

2.2 Publication of Certification Information

(1) This CPS and the CP of Internet Thailand Public Company Limited

(2) CRLs.

(3) Certificates of the One CA itself (until the expiry of all certificates issued with private key corresponding to that certificate's public key).

(4) Issued certificates.

(5) Privacy protection policy.

(6) The latest One CA-related news.

(7) Subscriber agreements.

(8) The latest external audit results specified in section 8.6.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

2.3 Time or Frequency of Publication

(1) One CA is follow CP/CPS from NRCA, that we need to update and publish our CP/CPS after NRCA's publish.

(2) The CP and/or CPS shall be published in the One CA repository within 3 working days upon receiving the competent authority's approval document.

(3) CRLs are issued by the One CA at least twice a day and published in the repository.

(4) The One CA's own certificates are published in the repository within seven calendar days after accepting issuance by an upper level CA.

2.4 Access Controls on Repositories

The One CA host is installed inside the firewall with no direct external connection. The repository is linked to the One CA certificate administration database via its internal firewall to access certificate information or download certificates. Only authorized personnel of the One CA are permitted to administer the repository host.

The information published by the One CA under section 2.2 is primarily provided for browser inquiries by subscribers and relying parties. As a result, access control should be implemented when providing access for viewing to guarantee repository security and maintain accessibility and availability.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

The One CA uses the X.501 Distinguished Names (DN) for the certificate subject name of issued certificates. The Distinguished Names consist of the components specified in Table 3 below.

Attribute Name	Value
Country (C) =	TH
Organization (O) =	Internet Thailand Public Company Limited
Common Name (CN) =	INET CA - G1

Table 3 Distinguished Name Attributes in certificates

The Subject Alternative extension for non-SSL certificates is optional. If present, the entry in this extension may be an email address for certificate application.

3.1.2 Need for Names to be Meaningful

The names contained in a certificate must be in English or Thai with commonly understood semantics permitting the determination of the identity of the individual or juristic person that is the Subject and Issuer of the certificate, for example, through the verification of Jurisdiction of Incorporation and/or Certificate of Registration issued by the Department of Business Development, Ministry of Commerce.

3.1.3 Anonymity or Psuedonymity of Subscribers

The One 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.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

3.1.5 Uniqueness of Names

The distinguished names of subscriber must be unique within the domain of The One CA

3.1.6 Recognition, Authentication and Role of Trademarks

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

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

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

Subscribers will submit their applications for certificates with the its name, business address in Thailand, and the Certificate of Corporate Registration issued by the Department of Business Development, Ministry of Commerce. Copies of official documents require certified true copy from authorized representative.

3.2.2.1 Identity

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

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

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

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

3.2.2.2 DBA/Tradename

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

3.2.2.3 Verification of Country

One CA follows Section 3.2.2.3 of CA/B Forum Baseline Requirements.

3.2.2.4 Validation of Domain Authorization or Control

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

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

3.2.2.4.1 Validating the Applicant as a Domain Contact

One CA follows Section 3.2.2.4.1 of CA/B Forum Baseline Requirements.

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

One CA follows Section 3.2.2.4.2 of CA/B Forum Baseline Requirements.

3.2.2.4.3 Phone Contact with Domain Contact

One CA follows Section 3.2.2.4.3 of CA/B Forum Baseline Requirements.

3.2.2.4.4 Constructed Email to Domain Contact

One CA follows Section 3.2.2.4.4 of CA/B Forum Baseline Requirements.

3.2.2.4.5 Domain Authorization Document

One CA follows Section 3.2.2.4.5 of CA/B Forum Baseline Requirements.

3.2.2.4.6 Agreed-Upon Change to Website

One CA follows Section 3.2.2.4.6 of CA/B Forum Baseline Requirements.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

3.2.2.4.7 DNS Change

One CA follows Section 3.2.2.4.7 of CA/B Forum Baseline Requirements.

3.2.2.4.8 IP Address

One CA follows Section 3.2.2.4.8 of CA/B Forum Baseline Requirements.

3.2.2.4.9 Test Certificate

One CA follows Section 3.2.2.4.9 of CA/B Forum Baseline Requirements.

3.2.2.4.10 TLS Using a Random Number

One CA follows Section 3.2.2.4.10 of CA/B Forum Baseline Requirements.

3.2.2.5 Authentication for an IP Address

One CA follows Section 3.2.2.5 of CA/B Forum Baseline Requirements.

3.2.2.6 Wildcard Domain Validation

One CA follows Section 3.2.2.6 of CA/B Forum Baseline Requirements.

3.2.2.7 Data Source Accuracy

One CA follows Section 3.2.2.7 of CA/B Forum Baseline Requirements.

3.2.2.8 CAA Records

Not Applicable

3.2.3 Authentication of Individual Identity

There are regulations regarding identification documents, checking procedure as shown below:

The applicant must verify his / her identity in person at the CA or RA counter.

Check written documentation:

The applicant shall provide information which includes name, ID number and birthdate 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

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

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-Validated Subscriber Information

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

3.2.5 Validation of Authority

When there is a connection between a certain individual and the certificate subject name when performing a certificate lifecycle activity such as a certificate application or revocation request, the One CA or the RA shall perform a validation of authority to verify that the individual can represent the certificate subject such as:

1. Authorized Representative Appointment Letter from the relevant juristic person or other document of the same kind, corporate sealed and signed by the authorized representative of the juristic person, as specified under the Certificate of Corporate Registration issued by the Department of Business Development, Ministry of Commerce, with a certified true copy of identification card or passport of the authorized director of such juristic person.
2. A certified true copy of identification card or passport of the authorized representative of the juristic person. The RA verifies and endorses the integrity of documents.

For certificates issued by the One CA to organizations and individuals, if the e-mail address is recorded in the certificate subject name field for secure e-mail use, the RA shall use the following method to verify the certificate applicant is able to control the e-mail account recorded on the certificate:

Use the RA system to send e-mails requesting the subscriber to click on reply or input a certification code during certificate application to verify that the e-mail address is owned by that person.

3.2.6 Criteria for Interoperation

One CA is the Level 1 subordinate CA under the Thailand National Root Certification Authority (NRCA) and is responsible for issuance and administration of individual and juristic person certificate. The Thailand NRCA is the highest-level CA and trust anchor

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

3.3 Identification and Authentication for Re-key Request

3.3.1 Identification and Authentication for Routine Re-key

Identification and authentication procedures are specified in Section 3.2.

3.3.2 Identification and Authentication for Re-key after Revocation

Identification and authentication procedures are specified in Section 3.2.

3.4 Identification and Authentication for Certificate Revocation Request

Identification and authentication procedures are specified in Section 3.2.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

4. Certificate Lifecycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Organizations and individuals may submit certificate applications.

4.1.2 Enrollment Process and Responsibilities

The One CA and the RA are responsible for ensuring that the certificate applicant identity is verified in compliance with the CP and CPS provisions before certificate issuance. The certificate applicant is responsible for providing sufficient and accurate information (such as filling out the organization legal name or code, certificate applicant name or website fully qualified domain name based on the type of the certificate applied for) and identification documents are given to the RA. The One CA shall perform the necessary identity identification and authentication work before certificate issuance. The subscriber shall bear the following responsibilities:

(1) The subscriber shall follow the relevant application regulations in the CPS and verify the accuracy of the information submitted for the application.

(2) The subscriber shall accept the certificate in accordance with the regulations in section 4.4 after the One CA approves the certificate application and issues the certificate.

(3) After obtaining the certificate issued by the One CA, the subscriber shall check the accuracy of the information contained on the certificate and use the certification in accordance with the regulations in section 1.4.1. If there is an error in the certificate information, the subscriber shall notify the RA and refrain from using the certificate.

(4) The subscriber shall properly safeguard and use their private key.

(5) If a subscriber certificate must be suspended, restored, revoked or reissued, the subscriber shall follow the regulations in Chapter 4. If a certificate needs to be revoked due to the leakage or loss of private key information, the subscriber shall promptly notify the RA, but the subscriber shall still bear the legal responsibility for use of that certificate before the change.

(6) The subscriber shall carefully select computer environments and trustworthy application systems. If the rights of relying parties are infringed upon due to factors such as the computer environment or application system, the subscriber shall bear sole responsibility.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

(7) If the One CA is unable to operate normally for some reason, the subscriber shall speedily seek other ways for completion of legal acts and may not be used as a defense to others.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

The One CA and the RA shall ensure that the system and procedure are sufficient to verify that the subscriber identity complies with CP and CPS regulations. The initial registration procedure is implemented in accordance with the regulations in section 3.2 of the CPS. The certificate applicant shall submit correct and complete factual information. The information required for the certificate application shall contain required and optional information. Only the information listed on the certificate profile is recorded on the certificate. The information submitted by the certificate applicant and contact records kept by the CA and RA during the application process shall be properly kept in a secure, auditable manner in accordance with CP and CPS regulations.

4.2.2 Approval or Rejection of Certificate Applications

If all identity authentication work follows relevant regulations and best practices can be successfully implemented, the One CA and the RA may approve the certificate application.

If the various identity authentication works cannot be successfully completed, the One CA may reject the certificate application. Except for applicant identity identification and authentication reasons, the One CA and RAs may refuse to use the certificate for other reasons. The One CA and RAs may also reject certificate application from applicants who have previously been rejected or have previously violated the subscriber agreements.

4.2.3 Time to Process Certificate Applications

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

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

After the One CA and its RAs accept the certificate application information, the relevant review procedures are followed in accordance with the regulations of Chapter 3 in the CPS to serve as a basis for determining whether approve the certificate issuance or not.

Certificate issuance steps are follows:

1) The RA submits the certificate application information from the review process to the One CA.
2) When the One CA receives the certificate application information submitted by the RA, the authorization status of the relevant RA is first checked, the authorized scope is verified and then the certificate is issued based of the certificate application information submitted by the RA.
3) If the RA authorized scope does not comply with the certificate application, the One CA sends back the related erroneous message to the RA and refuse to perform related subsequent work. If there are any questions, the RA may directly contact the One CA to understand where the problem is.
4) In order to ensure the security, integrity and non-repudiability of the information transmitted by the One CA and the RA, the certificate application information is encrypted with a digital signature and transmitted through the network by transport layer security (TLS) protocols.
5) The One CA reserves the right to refuse certificate issuance to any entity. The One CA shall not bear any liability for damages to certificate applicants.

4.3.2 Notification to subscriber by the CA of issuance of certificate

After the One CA completes certificate issuance, the subscriber is notified to pick up the certificate or the RA is used to notify the subscriber to pick up the certificate via email.

If the One CA or the RA does not approve the certificate issuance, the certificate applicant is notified by e-mail or telephone and shall be informed of the reasons for the refusal. Besides applicant identity identification and authentication reason, certificate issuance may be refused due to other reasons.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

4.4 Certificate Acceptance

After the One CA completes certificate issuance, the certificate applicant shall be notified to pick up the certificate. The certificate applicant reviews the information recorded on the certificate for accuracy and provides consistent information for the application. After indicating acceptance of the issued certificate, that certificate may be published in the repository. If the certificate applicant refuses to accept the issued certificate after reviewing the content of the issued certificate, the One CA shall revoke the certificate.

The certificate field is reviewed by above certificate applicant before deciding whether or not to accept the certificate; the review shall at least include the certificate subject name. If the organization or individual e-mail address is submitted for secure e-mail use, the organization or individual certificate applicant shall review e-mail address recorded in the certificate subject name field and submit consistent information for the application before certificate acceptance.

Acceptance of the certificate is deemed as the certificate applicant consent to follow the CPS and the rights and obligations in related contracts.

If there is fee collection or refund problems involved with certificate refusal, the certificate applicant shall handle the matter in accordance with the contract established in compliance with the Law of Information Technology.

4.4.1 Conduct Constituting Certificate Acceptance

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

4.4.2 Publication of the Certificate by the CA

The One CA repository service regularly publishes the issued certificates information within one business day after certificate acceptance by the subscriber.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

RA will notify the subscriber whenever a certificate is issued via email.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers refer to the entities who request and obtain certificates approved by the One CA. Their relationship with the certificate subject is shown in section 1.3.3. Usage of certificates is stipulated in section 1.4.1. Subscriber key pair generation shall comply with the regulations in section 6.1.1. Subscribers must independently possess and control the right and capability to the private key corresponding to the certificate. Subscribers themselves do not issue certificates to others. Subscribers shall protect the private key from unauthorized use or disclosure. Private keys shall only be used for correct keyUsages (key usages are listed in the keyUsages extension of the certificate) such as digitalSignature or keyEncipherment. Subscribers must correctly use certificates according to the certificatePolicies extension listed on the certificates.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties refer to third parties who trust the connecting relationship between the certificate subject name and public key. Relying parties shall use software that is compliant with ITU-T X.509 and related Internet Engineering Task Force (IETF) RFCs.

Relying parties shall verify the validity if the certificate used based on the related One CA certificate and certificate status information. After verifying the validity of the certificate, the certificate may be used for the following purposes:

- Verify the integrity of the electronic documents with digital signatures.
- Verify the identity of the document signature author.
- Establish secure communication channels with the subscriber.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

The above certificate status information may be obtained from CRL or OCSP inquiry services. The CRL information can be obtained from the cRLDistributionPoints extension of the certificate. In addition, the relying parties shall check the CA issuer and subscriber certificate CP to verify the assurance level of the certificate.

For example, relying parties may only trust digital signatures that conform to the following conditions:

- Digital signature is generated through the corresponding valid certificate and the certificate accuracy can be verified through the certificate chain.
- Related CRL or OCSP response messages are checked for certificate and unrevoked certificates used by relying parties.
- Certificates are used according their CPS regulations and certificate usage.

4.6 Certificate Renewal

4.6.1 Circumstances for Certificate Renewal

Not Applicable.

4.6.2 Who May Request Renewal

Not Applicable.

4.6.3 Processing Certificate Renewal Requests

Not Applicable.

4.6.4 Notification of New certificate Issuance to Subscriber

Not Applicable.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Not Applicable.

4.6.6 Publication of the Renewal Certificate by the CA

Not Applicable.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

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

Not Applicable.

4.7 Certificate Re-Key

4.7.1 Circumstances for Certificate Re-Key

The CA requires subscribers to re-key the certificate in the following cases:

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

4.7.2 Who May Request Certificate Re-Key

A subscriber or legally authorized third party (representative authorized by the organization) may submit a subscriber certificate application with the One CA.

4.7.3 Processing certificate re-keying requests

When the One CA certificate is re-keyed, a new certificate application is submitted to the Thailand NRCA. See the regulations in sections 3.1, 3.2, 3.3, 4.1 and 4.2 of the Thailand NRCA CPS.

For subscriber certificate re-key, a new certificate application is submitted to the One CA. See the regulations in sections 3.1, 3.2, 3.3, 4.1 and 4.2 of the CPS.

4.7.4 Notification of new certificate issuance to subscriber

For notification to issue subscriber certificate re-key, see the regulations in section 4.3.2.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

4.7.5 Circumstances Constituting Acceptance of Certificate Re-Key

For circumstances constituting acceptance of the CA certificate re-key by the One CA, see section 4.7.5 in the Thailand NRCA CPS.

The certificate applicant previews the content of issued subscriber certificate or reviews the subscriber certificate content for errors. The subscriber certificate is published by the CA on the repository or delivered to the certificate applicant.

4.7.6 Publication of the Re-Key by the CA

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

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

The One CA notifies the result of certificate issuance to other entities according to the procedure in Section 4.4.3.

4.8 Certificate Modification

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

4.8.1 Circumstances for Certificate Modification

Since the interpretation of modifying certificate contents are sometimes complex, One CA does not offer certificate modification. If a circumstance for certificate modification is deemed to arise, re-certification will be followed, that means the initial registration process as described in section 3.2 will be gone through again. The new certificate shall have a different subject public key.

4.8.2 Who May Request Certificate Modification

Not Applicable.

4.8.3 Processing Certificate Modification Requests

Not Applicable.

4.8.4 Notification of New Certificate Issuance to Subscriber

Not Applicable.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not Applicable.

4.8.6 Publication of the Modified Certificate by the CA

Not Applicable.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not Applicable.

4.9 Certificate Revocation and Suspension

This section mainly describes under what circumstances a certificate may (or must) be suspended or revoked and explain the certificate suspension and revocation procedures.

4.9.1 Circumstances for Revocation

4.9.1.1 Reasons for Revoking a Subscriber Certificate

The issuing CA shall revoke a subscriber's certificate within 24 hours of the following circumstances:

1. Private key lost, stolen, modified, disclosed without authorization or has been subject to other damage or misuse.
2. The information listed on the certificate is sufficient to have a significant effect on subscriber trust.
3. Certificate is no longer needed for use.
4. The original certificate request is not authorized by the subscriber, and the subscriber is not willing to grant authorization retroactively.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

Not Applicable.

4.9.2 Who Can Request Certificate Revocation

Subscribers, the One CA, RAs or legally authorized third party (such as judicial or prosecution authorities, agents authorized by the organization, and legal heirs of natural person).

In addition, a subscriber, relying party, application software provider or other third party may submit certificate problem report to advise the One CA a reasonable basis to revoke the certificate.

4.9.3 Certificate Revocation Procedure

1. The certificate revocation applicant shall submit the certificate revocation request in accordance with the guidelines established by the RA. After the RA receives the certificate revocation request, the relevant review procedures are implemented, and records of all certificate revocation requests are kept including applicant name, contact information, reason for revocation, time and date of revocation to serve a basis for subsequent accountability.
2. After the RA completes the review work, the certificate revocation application information is sent to the One CA.
3. When the One CA receives the certificate revocation application information sent by the RA, the One CA first checks the authorization status of the relevant RA to verify that its authorized assurance level and scope. Afterward, the certificate is revoked based on the certificate revocation request sent by the RA.
4. If the application does not pass the above checking, the One CA shall send the related erroneous message to the RA and refuse to handle subsequent related work. If the RA has any questions, the RA may directly contact the One CA to understand the source of the problem.
5. In order to ensure the security, integrity and non-repudiability of the information transmitted by the One CA and RA, the certificate application information is affixed with a digital signature, encrypted and transmitted through the network by transport layer security (TLS) protocols.
6. The One CA uses the same One CA private key issuing the certificate to publish the revoked certificate serial number and the reason for revocation to the CRL by the digital signature.
7. Provide a timelier OCSP inquiry service (e.g. the status of being revoked, the status of being applied, or the status is valid).

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

8. The One CA receives certificate problem reports and provides the certificate problem response mechanism 24x7, as specified in section 4.9.3.1.

4.9.3.1 Mechanism for Responding the Certificate Problems

In the repository, the One CA will provide the guidelines for certificate problem reports, for the subscribers, the application software providers, the relying parties, and other third-party organizations to report the certificate problem reports when they observe the possible events of the private keys are cracked, the certificates are mis-issued, or the certificates are forged, cracked, abused, or used inappropriately.

4.9.4 Certificate Revocation Request Grace Period

There is no grace period for revocation under this CPS.

4.9.5 Time Period for the CA to Process Certificate Revocation Requests

After the subscriber submits a certificate revocation application, the RA shall promptly complete the review procedure within one working day. If the revocation application information is free of errors and passes the review, the One CA shall complete the certificate revocation work within one working day.

The One CA shall investigate and confirm if the request of certificate revocation is accepted by the following principles in 24 hours upon receiving the certificate problem reports. If the request of certificate revocation is accepted after the confirmation, the operation of certificate revocation will be proceeded by the regulations of Section 4.9.3.

(1) The claimed problematic content.

(2) The quantity of the certificate problem reports of the certificate or the subscriber.

(3) The entity submits the certificate problem report.

(4) The related laws and regulations.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

4.9.6 Certificate Revocation Checking Requirements for Relying Parties

Before using certificates issued by the One CA, the relying parties shall first check the CRL or OCSP responses published by the One CA to verify the validity of certificates. The relying parties shall verify the revoking time of certificates, the validity of signatures of the CRL or OCSP responses, and certificate chains with their validity.

The One CA publishes suspended and revoked certification information on the repository for checking purposes. There are no restrictions for the checking of CRL by relying parties. The website is as follows: https://ca.inet.co.th/

4.9.7 CRL Issuance Frequency

The One CA will issue a CRL within the following circumstances:

1. Issuing a CRL whenever a certificate is revoked.

2.Issuing a CRL for certificates every six months whether or not the CRL has any changes.

4.9.8 Maximum Latency for CRL Publishing

The One CA shall publish the CRL at the latest before the nextUpdate listed on the CRL within one hour after generation.

4.9.9 Availability of On-line Revocation/ Status Inspection

On-line status checking is provided by One CA. Where on-line status checking is supported, status information is updated and available to relying parties within 2 hours of CRL publication.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

The One CA uses OCSP Responder to provide the OCSP responses complying with RFC 6960 and RFC 5019 standards. The key for signatures of the One CA uses RSA 4096 w/ SHA-512 hash function algorithm to issue OCSP Responder certificates, for the relying parties to verify the digital signatures of the OCSP responses and the integrity of the information sources.

The One CA updates information provided via an OCSP regularly as specified in Section 4.9.10.

4.9.10 On-Line Revocation Checking Requirements

If relying parties are unable to check the CRL in accordance with the regulations in section 4.9.6, relying parties shall use the OCSP service stipulated in section 4.9.9 to check if the certificates used are valid or not.

The One CA uses SHA-512 hash function algorithm to issue OCSP responses.

The One CA supports the relying parties of the OCSP inquiry service to use HTTP POST and HTTP GET to execute the OCSP inquiry service.

Regarding the subscriber certificates, the updating frequency of OCSP shall be at least one update every four days; the maximum effective period of OCSP responses is 10 calendars days.

In case the OCSP responders receive the status request of the un-issued certificates, the status shall not be replied as “Good,” and the One CA shall supervise if the OCSP responders reply such request complying with the above-mentioned secure responding procedures.

4.9.11 Other forms of revocation advertisements available

Not Applicable.

4.9.12 Other Special Requirements Related to Key Compromise

There are no other requirements different from the regulations in sections 4.9.1, 4.9.2 and 4.9.3.

4.9.13 Circumstances for Suspension

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

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

4.9.14 Who Can Request Certificate Suspension

Not Applicable.

4.9.15 Procedure for Certificate Suspension

Not Applicable.

4.9.16 Limits on Suspension Period

Not Applicable.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The One CA provides CRLs and OCSP inquiry services. The URLs of CRLs and OCSP service are recorded on the cRLDistributionPoints and authorityInfoAccess extensions of the subscriber certificate.

The revocation record of a certificate in CRL or OCSP response will only be removed once that revoked certificate expires.

4.10.2 Service Availability

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

4.10.3 Optional Features

Not Applicable.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

4.11 End of Subscription

End of subscription refers to the termination of One CA services to certificate subscribers including termination of One CA services provided to subscribers upon certification expiry or service termination upon subscriber certification revocation.

The CA shall allow the subscriber not to renew or cancel the purchase of certificate services in the event of invalidation of the subscriber agreements.

4.12 Private Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

Private keys used for signatures may not be escrowed.

4.12.2 Session Key Encapsulation and Recovery Policy and Practice

The One CA does not currently support session key encapsulation and recovery.

No stipulation

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

5. Facility, Management and Operation Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

The One CA facility is located in the OneAuthen Data Communication Branch. The construction of the facility housing is consistent with facilities used to house high value, sensitive information. Combined with other physical security mechanisms including access control, security, intrusion detection and video monitoring, it provides robust protection against unauthorized access to related One CA equipment.

5.1.2 Physical Access

The One CA has established suitable measures to control connections to One CA service hardware, software and hardware security module.

The One CA facility has a total of four levels of security control. On the first and second levels, there are year-round entrance and building security controls in place. On the third level, access is controlled to this floor using 2FA (at the main site used card and fingerprint, at the backup site used card and passwords) for entering data center room. On the fourth level, One CA service hardware and hardware security module are stored in a secure rack where physical access to such system requires dual-control and two-factor authentication.

The access control system is able to protect the facilities against unauthorized access. There is also a monitoring system in place to control cabinet access which prevents unauthorized access to any hardware, software or hardware security module.

Portable storage devices that are brought into the facility housing are checked for computer viruses or other types of software that could damage the One CA system.

Persons who are not personnel of the One CA entering the facility are required to sign the entry/exit log and must be accompanied throughout by at least one personnel of the One CA.

The following checks and records need to be made when the One CA personnel leave the facility to prevent unauthorized personnel from entering the facility:

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

(1) Check if system equipment is operating normally.

(2) Check if the computer racks are locked.

(3) Check if the access control system is operating normally.

5.1.3 Power and Air Conditioning

In addition to municipal power, The power system at the One CA facility is equipped with an uninterrupted power system (UPS) and power generators, which can last at least six days when a long period of the main power outage occurs. The system is capable of automatically switching between municipal power and generator power. At least six hours of power can be supplied for repository backup work.

The One CA facility has a constant temperature and humidity system to provide an optimal operation environment for the facility.

5.1.4 Water Exposures

The One CA facility is located at the third or higher floor of a raised foundation building. This building has water gate and water pump protection and no history of major damage caused by flooding.

5.1.5 Fire Prevention and Protection

The One CA facility has an automatic fire detection, alarm and protection system with self-activating extinguishing equipment. Switches are installed at every major entrance / exit of the facility to allow manual activation by personnel on-site during emergencies.

5.1.6 Media Storage

Audit records, archives and backups are kept in storage media at the facility described in section 5.1.1. In addition, one copy shall be kept at a secure location.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

5.1.7 Waste Disposal

When information and documents of the One CA detailed in section 9.3.1 are no longer in use, all shredded paper, magnetic tapes, hard disks, floppy disks, MO and other forms of memory shall be formatted to erase the information stored on them. Optical disks shall be physically destroyed.

5.1.8 Off-site Backup

The off-site backup location shall be over 30 km away from the One CA facility. The backup content shall include information and system programs.

5.2 Procedural Controls

In order to ensure that system procedures have a suitable assurance level, the One CA uses procedural controls to specify the trusted roles of One CA system operations, the number of people required for each task and how each role is identified and authenticated.

5.2.1 Trusted Roles

In order to ensure that assignments of key functions of the One CA are properly distinguished to prevent undetected malicious use of the system, the trusted role authorized to perform each system access task is clearly defined.

The seven PKI personnel roles assigned by the One CA are administrator, officer, auditor, operator, physical security controller, cyber security coordinator and anti-virus and anti-hacking coordinator to prevent potential internal attacks. Each trusted role may be performed by multiple persons but one person in each group shall be assigned the chief role to lead group work. The tasks performed by the seven roles are as follows:

The administrator is responsible for:

- Installation, configuration and maintenance of the One CA system.
- Creation and maintenance of system user accounts.
- Generation and backup of keys of the One CA.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

The officer is responsible for:

- Activation / deactivation of certificate issuance services.
- Activation / deactivation of certificate revocation services.
- Activation / deactivation of CRL issuance services.

The auditor is responsible for:

- Checking, maintenance and archiving of audit logs.
- Conducting or supervising internal audits to ensure the One CA is operating in accordance with CPS regulations.

The operator is responsible for:

- Daily operation and maintenance of system equipment.
- System backup and recovery.
- Storage media updating.
- System hardware and software updates.
- Website maintenance.
- Set up protection mechanisms for system security and threats of virus or malware.
- Maintenance of the network and network facilities.
- Patches management for the vulnerabilities of the network facilities
- Providing the anti-virus and anti-malicious software technologies or measures to ensure the security of the system and the network.
- Reporting the collected threats or vulnerabilities of computer virus to the administrator

The physical security controller is responsible for:

- System physical security controls (such as facility access controls, fire prevention, flood prevention and air conditioning systems).

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

5.2.2 Number of Persons Required per Task

In accordance with security requirements, the number of people needed for each trusted role is as follows:

- Administrator

At least 3 qualified individuals are needed.

- Officer

At least 2 qualified individuals are needed.

- Auditor

At least 2 qualified individuals are needed.

- Operator

At least 2 qualified individuals are needed.

- Physical security controller

At least 2 qualified individuals are needed.

The number of people assigned to perform each task is as follows:

Assignments	Administrator	Officer	Auditor	Operator	Physical security controller
Installation, configuration, and maintenance of the One CA system	2				1
Establishment and maintenance of system user accounts	2				1
Generation and backup of One CA keys	2		1		1
Activation / deactivation of certificate issuance services		2			1

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

Assignments	Administrator	Officer	Auditor	Operator	Physical security controller
Activation / deactivation of certificate revocation services		2			1
Activate/deactivate the issuance services of CRL		2			1
Checking, maintenance and archiving of audit logs			1		1
Daily operation and maintenance of system equipment				1	1
System backup and recovery				1	1
Storage media updating				1	1
Hardware and software updates outside the One CA certificate management system				1	1
Website maintenance				1	1
Daily operation and maintenance of the network and network facilities				1	1
Patching the vulnerabilities of the network facilities	1				1
Reporting the threats and vulnerabilities of computer virus					

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

Assignments	Administrator	Officer	Auditor	Operator	Physical security controller
keep the antivirus system's signatures update and patches for the vulnerabilities				1	1

5.2.3 Identification and Authentication for Each Role

Use IC cards to identify and authenticate administrator, officer, auditor and operator roles as well as central access system to determine the authority to identify and authenticate physical security controller role.

When the RA officers log in the RA system and conduct the related review actions, they shall use IC cards to verify their identities and execute digital signatures.

Operating system account management by the One CA host uses login account numbers, passwords and groups to identify and authenticate administrator, officer, auditor and operator roles. The One CA uses the user's account, password, and system account administration functions, or other security mechanisms to identify the role of the cyber security coordinator.

5.2.4 Roles Requiring Separation of Duties

The seven trusted roles are defined in section 5.2.1. Personnel and trusted roles must conform to the following regulations:

- The administrator, the officer, the auditor cannot assume any other roles among these four trust roles at the same time, but the administrator, the officer, and the auditor can be the operator as well.
- The physical security controller shall not concurrently assume any role of the administrator, the officer, the auditor, and the operator.
- A person serving a trusted role is not allowed to perform self-audit.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

5.3 Personnel Controls

5.3.1 Background, Qualifications, Experience and Clearance Requirements

1. Security evaluation for personnel selection

   Personnel selection includes the following items:

   (1) Personality evaluation.

   (2) Applicant experience evaluation.

   (3) Academic and professional skills and qualifications evaluation.

   (4) Personal identity check.

   (5) Trustworthiness.

2. Management of Personnel Evaluation

   All One CA personnel performing certificate work shall have their qualifications reviewed at the initial time of employment to verify their reliability and work capabilities. After formal employment, personnel shall receive appropriate training and sign a document accepting responsibility to perform certain duties. All personnel shall have their qualifications rechecked each year to reconfirm their reliability and work ability. If personnel do not pass the qualification check, that person shall be reassigned to another position and a qualified person shall be assigned to serve in that position.

3. Appointment, Dismissal and Transfer

   If there are changes to the employment terms or contract especially personnel severance and termination of temporary worker contracts, personnel are still required to fulfill their duty of confidentiality.

4. Duty of Confidentiality Agreement

   Work personnel shall fulfill their duty of confidentiality in accordance with relevant regulations and sign a business secret agreement drafted by the One CA stating that personnel may not disclose business secrets verbally or by photocopy, loan, delivery, publishing or other methods.

5.3.2 Background Check Procedures

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

- Identification card
- House registration

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

- Certification of the highest education
- Criminal records
- Professional certificate (if any)
- Confirmation letter of previous employment
- Background Check (Recheck at least every three years)

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

5.3.3 Training Requirements

Trusted Role	Training Requirements
Administrator	1. One CA security principles and mechanism. 2. Installation, configuration, and maintenance of the One CA operation procedures. 3. Establishment and maintenance of system user accounts operation procedures. 4. Audit parameter configuration setting procedures. 5. One CA key generation and backup operation procedures. 6. Disaster recovery and continuous operation procedure. 7. Prevention and control to the threats and vulnerabilities of computer virus. 8. Security mechanism for the operating system and the network.
Officer	1. One CA security principles and mechanism. 2. One CA system software and hardware use and operation procedures. 3. Activation/deactivation of certification issuance operation procedure. 4. Activation/deactivation of certification revocation operation procedure. 5. Activation/deactivation of certificate CRL issuance service operation. 6. Disaster recovery and continuous operation procedure.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

Trusted Role	Training Requirements
Auditor	1. One CA security principles and mechanism. 2. One CA system software and hardware use and operation procedures. 3. One CA key generation and backup operation procedures. 4. Audit log check, upkeep and archiving procedures. 5. Disaster recovery and continuous operation procedure.
Operator	1. Daily operation and maintenance procedures for system equipment. 2. System backup and recovery procedure. 3. Upgrading of storage media procedure. 4. Disaster recovery and continuous operation procedure. 5. Network and website maintenance procedure.
Physical security controller	1. Physical access authorization setting procedure. 2. Disaster recovery and continuous operation procedure.

5.3.4 Retraining Frequency and Requirements

All related personnel at the One CA shall be familiar with any changes to One CA and related work procedures, laws and regulations. One CA provides its officers with appropriate training at least once a year on the topics related to Information Security Awareness. Additional training may be considered if there is a change in hardware and software related to CA operations and the training status shall be recorded to ensure that work procedures and regulatory changes are understood.

5.3.5 Job Rotation Frequency and Sequence

1. May not concurrently serve trust roles. May not receive work reassignments.
2. Operators with the requisite training and clearance may be reassigned to the position of administrator, officer or auditor after two years.
3. Administrator, officer and auditor personnel who have not concurrently served in the position of operator may be reassigned to the position of administrator, officer or auditor after serving one full year as operator.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

4. Only personnel with a full two years of experience as a cyber security coordinator as well as the requisite training and clearance may be reassigned to the position of, administrator, officer, or auditor.
5. Only personnel with a full two years of experience as an anti-virus and anti-hacking coordinator as well as the requisite training and clearance may be reassigned to the position of administrator, officer, or auditor.

5.3.6 Sanctions for Unauthorized Actions

The One CA related personnel shall be subject to appropriate administrative and disciplinary actions for violations of the CP, CPS or other procedures announced by One CA. In the event of serious cases that result in damages, appropriate legal action shall be taken.

5.3.7 Independent Contractor Requirement

Section 5.3 shall be followed for the security requirements of personnel employed by the One CA.

5.3.8 Documentation Supplied to Personnel

The One CA shall make available to related personnel relevant documentation pertaining to the CP, CPS, One CA system operation manuals, the Electronic Transactions Act and its enforcement rules.

5.4 Audit Logging Procedure

The One CA shall keep security audit logs for all events related to One CA security. Security audit logs shall be collected by automatic system generation, logbook or paper. All security audit logs shall be retained and made available during compliance audits. Auditable security audit logs are kept in accordance with the archive retention regulations in section 5.5.2.

5.4.1 Types of Events Records

(1) Key generation

■ One CA key generation times (not mandated for single use or single session keys).

(2) Private key loading and storage

■ Loading the private key into a system component.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

- All access to private keys kept by the One CA for key recovery work.

(3) Certificate registration

- Certificate registration request procedure.

(4) Certificate revocation

- Certificate revocation request procedure.

(5) Account administration

- Add or delete roles and users.
- User account number or role access authority revisions.

(6) Certificate profile management

- Certificate profile changes.

(7) CRL profile management

- CRL profile changes.

(8) Physical access / site security

- Known or suspect violation of physical security regulations.

(9) Anomalies

- Software defect.
- CPS violation.
- Reset system clock.

5.4.2 Frequency of Processing Log

The One CA shall routinely review audit logs and explain major events. Review work includes examining all log entries and conducting a final complete check for any warnings or anomalies at least a weekly.

Audit checking results shall be documented at least biannually.

5.4.3 Retention Period for Audit Logs

Audit logs shall be retained on-site for three months and the log retention management system shall be operated in accordance with the regulations in sections 5.4.4, 5.4.5 and 5.4.6.

When the retention period for audit information ends, audit personnel are responsible for removing the information. Other personnel may not perform this work upon their behalf.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

5.4.4 Protection of Audit Log

Current and archived automatic event logs shall be kept in secure manner with digital signature to ensure the integrity of the audit log file. Audit log files shall only be viewed by authorized personnel.

5.4.5 Audit Log Backup Procedures

Electronic audit logs are backed up at least once a month. The One CA shall store the event logs in a secure protected site.

5.4.6 Audit Collection System (Internal vs. External)

Audit logs shall be kept on all One CA security-related events. Security audit logs shall be collected by automatic system generation, logbook or paper. All security audit logs shall be retained and made available during compliance audits.

5.4.7 Notification to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

One CA assesses security vulnerability at least on a quarterly.

5.4.9 Penetration Test Assessments

One CA assesses security Penetration Test at least on yearly.

5.5 Records Archival

A reliable mechanism shall be adopted by the One CA to accurately and completely save certificate-related records as computer data or in written form including:

(1) Important tracking records regarding the One CA's own key pair generation, storage, backup and re-key.

(2) Important tracking records regarding certificate application, issuance, revocation and reissuance.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

In addition to being provided for tracking and audits, these records may also serve as evidence, if necessary, for dispute resolution. In order to follow the above regulations, RAs may ask applicants or their representatives to submit related certification documents when deemed necessary.

5.5.1 Types of Recorded Archived

The One CA retains the following information in its archives:

(1) One CA accreditation information from competent authorities.

(2) CPS.

(3) Major contracts.

(4) System and equipment configuration settings.

(5) System and configuration setting modifications and updates.

(6) Certificate application information.

(7) Revocation request information.

(8) Subscriber identity identification information stipulated in section 3.2.

(9) Issued and published certificates.

(10) One CA re-key records.

(11) Issued or announced CRLs.

(12) Audit logs.

(13) Used to verify and validate the content of files and other information or application programs.

(14) Audit personnel requirement documents.

5.5.2 Retention Period for Archive

The retention period for One CA file information is 10 years. The application programs used to process file data are kept for 10 years.

5.5.3 Protection of Archive

(1) Amendments, modifications and deletion of archived information not allowed by any user.

(2) Transfer of archived information to another storage media which has passed through the One CA authorization procedure.

(3) Archived information stored in a secure, protected location.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

5.5.4 Archive Backup Procedures

One CA electronic records shall be regularly backed up and saved in storage media in accordance with backup procedures. Paper records shall be regularly sorted and filed by the One CA.

5.5.5 Requirements for Time-stamping of Records

All One CA computer systems are regularly calibrated to ensure the accuracy and trustworthiness of the date and time information on electronic records. For archived electronic records (such as certificates, CRLs and audit logs), the timestamping information on each record shall include the date and time information and accurate times following system calibration shall be used. These records shall have appropriate digital signature protection which can be used to check the date and time information on the records for alteration.

5.5.6 Archive Information Collection System

Archive Collection System is internal to One CA only.

5.5.7 Procedures to Obtain and Verify Archive Information

Archive information may be obtained by relevant personnel after formal authorization is received.

Audit personal shall follow verification procedures when verifying archive information. The authenticity of signatures and dates on written documents must be verified.

5.6 Key Changeover

The One CA private keys shall be regularly renewed in accordance with the regulations in section 6.3.2. After the key pair is renewed, an application for a new certificate shall be submitted to the One CA. The new certificate shall be published in the repository for subscriber downloading.

Certificate subscriber private keys shall be regularly renewed in accordance with the certificate subscriber private key usage period regulations in section 6.3.2.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

If compromise of the One 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.

The One CA establishes handling procedures in the event of emergencies or system compromise and conducts annual drills.

5.7.2 Computing Resources, Software and/or Data Are Corrupted

The One CA establishes recovery procedures in the event of computing resource, software and data corruption and conducts annual drills.

If the One CA's computer equipment is damaged or unable to operate, but the One CA signature key has not been destroyed, priority shall be given to restoring operation of the One CA repository and quickly reestablishing certificate issuance and management capabilities.

5.7.3 Entity Private Key Compromise Procedure

The One CA implements the following recovery procedure in the event of signature key compromise:

(1) Publish in the repository, notify subscribers and relying parties.

(2) Revoke the One CA signature key certificate and issued subscriber certificates.

(3) Generate new key pairs in accordance with the procedures in section 5.6. New certificates are published in the repository for subscriber and relying party downloading.

The One CA shall conduct at least one One CA signature key compromise drill each year.

5.7.4 Business Continuity Capabilities after a Disaster

The One CA has prepared a disaster recovery plan which have been tested, verified and continually updated. A full restoration of services will be done within 24 hours in case of disaster.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

5.8 CA or RA Termination

The One CA shall follow CA service termination procedures in accordance with related regulations in the Electronic Signatures Act during service termination. The One CA shall follow the item below to ensure the rights of subscribers and relying parties:

(1) The One CA shall notify the competent authority and subscribers of the service termination 30 days in advance.

(2) The One CA shall take the following measures when terminating their service:

- For certificates which are valid at the time of termination, arrangements shall be made for other CA to take over the service. Matters regarding service termination and service acceptance by other CAs shall be published in the repository and subscribers with valid certificates stall be notified. This shall not apply if notification cannot be made.
- All records and files during the operation period shall be handed over to the other CA that is taking over this service.
- If there is no CA willing to take over the One CA service, a report shall be submitted to the competent authority to arrange for other CA to take over this service.
- If the competent authority arranges for other CA to take over the service but no other CA takes over the service, the One CA shall revoke the still valid certificates, publish the revoked certificates in the repository and notify all certificate-related persons 30 days prior to service termination. The One CA shall refund the certificate issuance and renewal fees based on the certificate validity.
- The competent authorities, if necessary, may publish the certificates which are still valid at the time of revocation.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

6. Technical Security Controls

This chapter describes the technical security controls implemented by the One CA.

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The One CA and subscribers generate pseudo random numbers and public key pairs within the hardware security module in accordance with the regulations in section 6.2.1.

According to the regulations in section 6.2.1, the One CA generates key pairs within the hardware security module using the NIST FIPS 140-2 algorithm and procedures. The private keys are imported and exported in accordance with the regulations in sections 6.2.2 and 6.2.6.

One CA key generation is witnessed and videotaped by those related personnel who have signed key initiation witness document (the public key of the generated key pair is listed on it). The related personnel shall include the members of the One CA Policy Management Committee, One CA and the qualified auditors.

6.1.2 Private Keys Delivery to Subscriber

The subscriber must generate the key pair by themselves.

6.1.3 Delivery of Subscriber Public Keys to the CA

After the subscriber generate the key pair , the subscriber shall deliver the public key by PKCS# 10 certificate application file format to the RA. The RA shall delivery the public key to the CA via secure channels after it is verified that the subscriber is in possession of the corresponding private key in accordance with the regulations in section 3.2.1.

Secure channels referred in this section means the use of transport layer security (TLS) or other equivalent or more secure data encryption transmission protocols.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

6.1.4 CA Public Keys Delivery to Relying Parties

The public-key certificate of the One CA is issued by the Thailand NRCA and published in the repository of the Thailand NRCA the repository of the One CA for direct downloading and installation by subscribers and relying parties. Relying parties shall obtain the public key or the self-signed certificate of the Thailand NRCA via secure channels before using the public key of the One CA. The public key or the self-signed certificate of the Thailand NRCA shall then be used to check the signature on the certificate of the One CA to ensure the trustworthiness of the public key of the One CA.

6.1.5 Key Sizes

The One CA uses 4096-bit RSA keys and SHA-512 hash function algorithm to issue certificates and CRLs.

Subscribers must use at least 2048-bit RSA keys or other key types of equivalent security strength on and before December 31, 2030.

Subscribers shall use at least 3072-bit RSA keys or other key types of equivalent security strength after December 31, 2030.

6.1.6 Public Key Parameters Generation and Quality Checking

The public key parameter of the RSA algorithm shall be null.

For the signing key pair, The One CA follows the NIST FIPS 186-4 standard to generate the prime numbers needed for the RSA algorithm and ensure that the prime number is a strong prime.

For the subscriber key pair, the subscriber generates the prime numbers needed for the RSA algorithm in its own environment, therefore there is no guarantee that the prime number is a strong prime.

In according tosection 5.3.3 of NIST SP 800-89, the One CA confirms that the value of the public exponent shall be in the range between 216+1 and 2256-1. The modulus exponent should also have the following characteristics: an odd number, not the power of a prime, and have no factors smaller than 752.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

6.1.7 KeyUsage Purposes (as per X.509 v3 key usage field)

The One CA's signature private key is used to issue certificates and CRLs. The One CA's own public key certificate is issued by the NRCA. The key usage bits used for the keyUsage extension setting are key CertSign and CRLSign.

When the token used by the subscriber is software token, keyUsage extension may contain key Encipherment and digitalSignature at the same time.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The One CA uses hardware cryptographic modules that pass FIPS 140-2 Level 3 or higher-level certification requirements.

Subscribers may use software tokens for all cryptographic operations.

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

The One CA key splitting multi-person control uses n-out-of-m LaGrange Polynomial Interpolation. It is a perfect secret sharing method which can used for private key splitting and recovery. Besides, n and m must be values greater than or equal to 2, and n must be less than or equal to m. Use of this method can provide the highest security level for the One CA private key multi-person control. Therefore, it can be used as the activation method for private keys (see section 6.2.8).

There are no further regulations for multi-person control of subscriber private key.

6.2.3 Private Key Escrow

The signing private key of the One CA is not escrowed. The One CA shall never keep subscriber's private keys.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

6.2.4 Private Key Backup

Backups of One CA private keys are made according to the key splitting multi-person control methods in section 6.2.2, and IC cards verified with FIPS 140-2 Level 2 or above standards may serve as the private key splitting storage media.

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

6.2.5 Private Key Archival

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

6.2.6 Private Key Transfer Into or From a Cryptographic Module

The One CA transfers the private key into the cryptographic modules under the following circumstances:

1) Key generation or cryptographic module replacement.
2) For key splitting backup recovery, the secret sharing (n-out-of-m control) method is used in the circumstance to recover the One CA private key. Once the private key secret sharing IC card is recovered, the complete private key is written into the hardware cryptographic module.
3) When the cryptographic module is replaced, encryption is used for the private key importation method to ensure that key plain code is not exposed outside the cryptographic module during the importation process and the related confidential parameters generated during the importation process are completely destroyed after the private key importation is completed.

6.2.7 Private Key Storage on Cryptographic Modules

The private key of the One CA is stored in a hardware cryptographic module and backed up in another hardware cryptographic module.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

6.2.8 Method of Activating Private Key

The private key activation of the One CA is controlled by multi-person controls of the different usage IC cards kept by administrator and officer.

Subscribers shall choose a secure computer environment and a trustworthy application system carefully and keep and use the private keys properly. The methods to activate the private keys of subscribers are categorized by the private key storage media as the following:

1) If it is an IC card, the private keys shall be activated by the subscribers' (whose identity is validated) configuration and the PINs only known to the subscribers.
2) If it is a hardware security module, the private keys are activated by the IC cards controlled by multiple people. The controlling IC cards for different purposes are maintained by different people.
3) For other private key tokens, subscribers shall use strong passwords or other identification with the same level to activate the private keys, in order to prevent the unauthorized access or use of the private keys.

6.2.9 Method of Deactivating Private Key

The multi-person control methods in section 6.2.2 are used to deactivate One CA private keys.

The One CA does not provide subscriber private key deactivation service.

6.2.10 Method of Destroying Private Key

In order to prevent the theft of the private keys of the One CA which could endanger the authenticity of the all issued certificate, the private key must be destroyed at the end of the One CA key lifecycle. Therefore, after the One CA completes the key renewal and the Thailand NRCA issued a new One CA certificate and no additional certificates or CRLs need to be issued by the old private key of the One CA (see section 4.7), zeroization is done on the old private key inside the hardware security module to ensure that the old private key is destroyed. In addition, physical destruction of the private key secret sharing IC card will be done.

6.2.11 Cryptographic Module Rating

The One CA used hardware cryptographic modules comply with FIPS 140-2 Level 3 standard.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The One CA performs subscriber certificate archival and securely controls the archival system in accordance with the regulations in section 5.5.

6.3.2 Certificate Operational Periods and Key Pair Usage Period

The certificate validity period and key pair associated with the certificate can be used up to the expiry date specified in the certificate. Public key can be used to verify the digital signature even if the certificate is expired but the digital signature to be verified must be created before expiry date of the certificate. For the private key, it can be used to decrypt even if certificate is expired.

The certificate period and key pair usage validity period of the One CA are not more than 20 years, and the certificate period and key pair usage validity period of the subscriber are not more than 10 years.

Certificate operational periods and key pair usage periods shall be assessed by PA at least once a year or as necessary especially in an incident that is believed to significantly impact trustworthiness of the One CA.

(Due to the technical limitations on UTC Time, the certificate issued by the One CA will last no longer than the year 2580 (AD 2037)).

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The One CA activation data, such as Personal Identification Number (PIN) and passwords for accessing the CA systems, are user-selected and protected under multi-person control by each of whom holding that activation data.

6.4.2 Activation Data Protection

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

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

6.4.3 Other Aspects of Activation Data

Not Applicable.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The One CA and related auxiliary systems provide the following security control functions through the operating systems, combined operating systems, software and physical protection measures:

(1) Trusted role or identity authentication login.

(2) Provide discretionary access control.

(3) Provide security audit capability.

(4) Access control restrictions for certificate services and PKI trusted roles.

6.5.2 Computer Security Rating

The One CA applies ISO/IEC 27001 (Information Security Management System) and WebTrust Principles and Criteria for Certification Authorities.

6.6 Lifecycle Technical Controls

6.6.1 System Development Controls

For both commercial-off-the-shelf (COTS) software and in-house developed software by the One CA that are used in certificate management, the software shall be checked to ensure it is genuine and fully tested in non-production environment before deployment in production environment. Any change to One CA systems or components must go through the Change Management Control review and approval process.

6.6.2 Security Management Controls

When software is installed for the first time, the One CA shall check if the provider has supplied the correct and unmodified version.

The One CA may only use components which have received security authorization. Unrelated hardware devices, network connections or component software may not be installed.

The One CA records and controls system configuration and any modification or function upgrades as well as detect unauthorized modifications to system software and configuration.

The One CA adopts the methodologies and standards in ISO/IEC 27001 and CPA WebTrust Principles and Criteria for Certification Authorities for risk assessment, risk management, and security management and control measures.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 Network Security Controls

The One CA servers and repository have firewalls and are connected to external networks. The repository is placed on the Demilitarized Zone (DMZ) inside the firewall and connected to the Internet. Except during required maintenance or backup, the repository provides uninterrupted certificate and CRL inquiry services.

The certificates and CRLs issued by the One CA have digital signature protection and are manually delivered from the One CA server to the repository.

The One CA external repository protects against denial of service and intrusion attacks by system patch updates, system vulnerability scanning, intrusion defending/detection systems, firewall systems and filtering routers.

6.8 Time Stamping

The One CA regularly conducts system clock synchronization with a reliable time source to maintain the correctness of system time and ensure the accuracy of the following times:

(1) Certificate issuance times.

(2) Certificate revocation times.

(3) CRL issuance times.

(4) System event occurrence times.

Automatic or manual procedures may be used to adjust the system time. System clock synchronizations are auditable events.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

7. Certificate, CRL and OCSP Profiles

7.1 Certificate Profile

Certificates issued by the One CA comply with the current versions of the ITU-T X.509 and PKIX Working Group RFC 5280.

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

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

Table 4 Fields in the Certificate

The One CA uses Cryptographically Secure Pseudorandom Number Generator (CSPRNG) to generate the certificate serial numbers which are larger than zero, non-sequential, and containing at least 64-bit entropy.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

7.1.1 Version Number(s)

The One CA issues X.509 V3 version certificates.

7.1.2 Certificate Extensions

The certificate extensions of the certificates issued by the One CA conform to the current versions of the ITU-T X.509 and PKIX Working Group RFC 5280.

7.1.2.1 CA Certificate of the One CA

The certificate extensions of One CA are described as the following:

A. certificatePolicies

This certificate extension is a required extension, marking the non-critical fields. The content is used to mark policyIdentifier.

B. cRLDistributionPoints

This certificate extension is a required extension, marking the non-critical fields. The content is used to mark the HTTP URL of the CRL service of the NRCA.

C. authorityInfoAccess

This certificate extension is a required extension, marking the non-critical fields. The content is used to mark the HTTP URL of the OCSP responder of the NRCA, as well as the HTTP URL of the self-signed certificate of the NRCA.

D. basicConstraints

This certificate extension is a required extension, marking the critical fields. The content is used to mark the value of CA field as true. As the One CA does not sign the subordinate CA certificates downwards, the pathLenConstraint is set to 0.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

E. keyUsage

This certificate extension is a required extension, marking the critical fields. The content is used to mark keyUsage bits as keyCertSign and cRLSign. The One CA does not sign the OCSP response with the signature private key, but issues the OCSP responder certificate, and the OCSP responder issues OCSP responses, and thus the configuration does not use digitalSignature.

F. nameConstraints

The subordinate CA certificate issued to the One CA by the NRCA does not have the certificate extension.

G. extKeyUsage

The subordinate CA certificate issued to the One CA by the NRCA does not have the certificate extension.

7.1.2.2 Subscriber Certificate

A. certificatePolicies

This certificate extension is a required extension, marking the non-critical fields. The content is used to mark policyIdentifier.

B. cRLDistributionPoints

This certificate extension is a required extension, marking the non-critical fields. The content is used to mark the HTTP URL of the CRL service of the One CA.

C. authorityInfoAccess

This certificate extension is a required extension, marking the non-critical fields. The content is used to mark the HTTP URL of the OCSP responder of the One CA, as well as the HTTP URL of the certificate of the One CA.

D. basicConstraints

The subscriber certificate issued by the One CA does not have the certificate extension.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

E. keyUsage

This certificate extension is an optional extension and marking the critical fields if any. The content shall not mark the used keyUsage bits as keyCertSign and cRLSign. For the keyUsages for different categories of certificates, please refer to section 6.1.7.

F. extKeyUsage

The subscriber certificate issued by the One CA does not have the certificate extension.

7.1.3 Algorithm Object Identifiers

The algorithm OIDs used for signatures on One CA issued certificates is:

sha512WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13}

(OID： 1.2.840.113549.1.1.13)

The algorithm OID used during One CA issued certificate generation of subject keys is:

RsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}

(OID: 1.2.840.113549.1.1.1)

7.1.4 Name Forms

The subject and issuer fields of the certificate must use the X.501 Distinguished Names, and the name attribute type shall comply with the current version of the ITU-T X.509 and IETF PKIX Working Group RFC 5280.

The CA certificates of the One CA Subject information shall contain countryName (OID 2.5.4.6) field, the value of which is the double alphabet country code specified in ISO 3166-1 for the country where the One CA locates. Besides, the organizationName (OID 2.5.4.10) field must be included, and the value of which is the identifier including the name able to identify the One CA, trademark, or their meaningful name, for the purpose of identifying the One CA more precisely; it is not allowed to contain the commonName only. Please refer to section 3.1.5 for the X.500 distinguished name of the CA certificate of the One CA.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

7.1.4.1 Issuer Information

According to RFC 5280 “Name Chaining”, the content of Issuer DN for the certificate issuer, shall be identical to the Subject DN of the CA issuing the certificate. Therefore, for the subscriber certificate issued by the One CA, the Issuer DN shall be identical to the content of the Subject DN of the One CA.

7.1.4.2 Subject Information–Subscriber Certificates

By issuing the subscriber certificates, the One CA and RAs have complied with the procedures specified in the CP and/or the CPS, to ensure all the values recorded in the Subject of these certificates are accurate.

7.1.4.2.1 Subject Alternative Name Extension

The Subject Alternative Name Extensions for none SSL certificates are as follows:

Certificate Extension	Required/Optional Extension
extension:subjectAltName	Optional

The Subject Alternative Name Extension will mark the e-mail account certificate application. The RA officers shall validate the ownership or control of the email account as specified in section 3.2.5.

7.1.4.2.2 Subject Distinguished Name Fields

The Subject Distinguished Name Fields of various subscriber certificates issued by the One CA are described as the following:

Certificate field	Juristic certificate	Individual certificate
subject:commonName (OID 2.5.4.3)	Δ	Δ
subject:organizationName (OID 2.5.4.10)	O	Δ
subject:givenName (OID 2.5.4.42) and subject:surname (OID 2.5.4.4)	X	Δ
subject:streetAddress (OID 2.5.4.9)	Δ	Δ
subject:localityName	Δ	Δ

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

(OID 2.5.4.7)		
subject:stateOrProvinceName (OID 2.5.4.8)	Δ	Δ
subject:postalCode (OID 2.5.4.17)	Δ	Δ
subject:countryName (OID 2.5.4.6)	○	○
subject:organizationUnitName (OID 2.5.4.11)	Δ	Δ

Symbols' meaning:

Optional: Δ

Required: ○

Prohibited: X

7.1.4.3 Subject Information–CA Certificates

The CA certificate of the One CA is validated and issued by the NRCA based on the procedures specified in the CP and/or the CPS. The Subject Distinguished Name Fields are as the following:

7.1.4.3.1 Subject Distinguished Name Field

Certificate Field	Required/Optional Field
subject:commonName (OID 2.5.4.3)	Required
subject:organizationName (OID 2.5.4.10)	Required
subject:countryName (OID 2.5.4.6)	Required

7.1.5 Name Constraints

Name constraints are not used.

7.1.6 Certificate Policy Object Identifier

Not Applicable.

7.1.7 Usage of Policy Constraints Extension

Not Applicable.

7.1.8 Policy Qualifiers Syntax and Semantics

Not Applicable.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Not Applicable.

7.2 CRL Profile

The One CA's certificate revocation list complies with ITU-T X.509 v2 has following details as in Table 7.

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

Table 5 Item list in Certificate Revocation

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

7.2.1 Version Number(s)

The One CA issues ITU-T X.509 v2 version CRLs.

7.2.2 CRL and CRL Entry Extensions

The One CA issued CRL, CRL extensions, and CRL entry extensions conform with the current version of the ITU-T X.509 and IETF PKIX Working Group RFC 5280.

The information on certificate revocation lists issued by Certification Authority is complied with ITU-T X.509 v2 contains at least the following:

7.2.2.1 authorityKeyIdentifier

This attribute indicates information associated with the public key of the certificate which is digitally signed by subscribers. The signing uses SHA-512 hashing algorithm of public key of Certificate Authority.

7.2.2.2 BaseCRLNumber

This attribute indicates the sequence number that Certificate Authority assigns to each revoked certificate to order the certificate revocation list.

7.2.2.3 reasonCode

This attribute indicates the Reason Code (0-9) of revoked certificate.

7.2.2.4 invalidityDate

This attribution indicates start time when using the pair of private key and the revoked certificate is insecure. It is defined in Greenwich Mean Time (GMT) format.

7.2.2.5 issuingDistributionPoint

This attribution is used to locate the certificate revocation list (Distribution Point) and indicates that the certificate revocation list is for a Certification Authority or subscribers including the reasons of revocation (Reason Code).

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

7.3 OCSP Profile

The One CA provides OCSP inquiry services complies with IETF PKIX Working Group RFC 6960 and RFC 5019 standards, and the One CA OCSP service website is contained in the authorityInfoAccess extension.

7.3.1 Version Number(s)

The OCSP inquiry packets accepted by the One CA include the following information:

- Version number
- Target certificate identifier

The target certificate identified includes: Hash function algorithm, hash value of CA issuer name, hash value of CA issuer key and the certificate number of the target certificate.

One CA OCSP service response packets contain the following basic fields:

Field	Description
Status	Response status, includes success, request format error, internal error, try again later, request no signature or request no certificate authorization, the following items must be included when status is successful
Version number	v.1 (0x0)
OCSP responding server ID (Responder ID)	OCSP responder subject DN
Produced Time	Response packet sign time
Target certificate identifier	Includes: Hash algorithm, hash value of certificate issuer name, hash value of certificate issuer key, and the certificate number of the target certificate
Certificate Status	Certificate status code (0: valid /1: revoked /2: unknown)
ThisUpdate/NextUpdate	Recommended validity region for this response packet includes: ThisUpdate and NextUpdate
Signature Algorithm	Response packet signature algorithm, can be RSA 4096 w/ SHA-512
Signature	OCSP responder signature
Certificates	OCSP responder certificate

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

7.3.2 OCSP Extensions

No stipulation.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

8. Compliance Audit and Other Assessment

8.1 Frequency or circumstances of assessment

The One CA received one annual external audit and one non-routine internal audit with an audit period of no more than 12 months to ensure that One CA operations are in compliance with the security regulations and procedures in the CP and CPS. The standards used for the audit are WebTrust Principles and Criteria for Certification Authorities.

8.2 Identity / Qualifications of Assessor

The auditor must demonstrate competence in the field of compliance audits and must be thoroughly familiar with the CP and the CPS of the One CA. The One CA will retain a qualified auditor to perform the One CA compliance audit work who is familiar with One CA operations and has been authorized by CPA as a licensed WebTrust practitioner to perform WebTrust Principles and Criteria for Certification Authorities to provide fair and impartial audit services. Audit personnel shall be a qualified and authorized Certified Information Systems Auditor (CISA) or have equivalent qualifications and shall at least possess the experience of conducting a WebTrust for CA signature audit twice at 4 man-days or the experience of conducting a CA information security management audit twice at 8 man-days. The One CA shall conduct identity identification of audit personnel during audits.

8.3 Assessor's Relationship to Assessed Entity

The One CA will retain an impartial third party to conduct audits of One CA operations.

8.4 Topics covered by assessment

The scope of audit is stipulated as follows:

(1) Whether or not the One CA operations comply with the CPS including administrative and technical audit of the physical environment, personnel procedural controls, key control, certificate lifecycle control, hardware security module.

(2) Whether or not the RA operations comply with the CPS and related procedures.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

(3) Whether or not the content disclosed from the CPS comply with the corresponding CP and suitable with respect to One CA practices.

The RA shall undergo one external audit every year noting any CP / CPS non-compliance or exceptions and the actions taken to correct the deficiencies.

Before a dedicated RA establishes an interface with general RA, the One Certification Authority assigns personnel to conduct a site survey to check the implementation status of related security measures.

If an organization or business under a dedicated RA is unable to undergo the above external audit due to regulations or other factors, the RA may state their exclusion from the scope of audit for that year in an audit report or management's assertions but the Company reserves the rights to conduct a compliance audit on whether or not the above RA is in compliance with the CP and CPS to reduce any risk derived from any non-conformity with the CP or CPS. The One CA has the right the conduct the following (but not limited to) review and examination items to ensure the trustworthiness of the One CA:

(1) If there is an event that causes the One CA to reasonably suspect the external RA is unable to comply CP and CPS in the event of a computer emergency event or key compromise.

(2) If the compliance audit has not been completed or there are special developments, the One CA has the right to conduct a risk management review.

(3) If action or inaction by the RA causes actual or potential security and integrity threat to the One CA, the Company must conduct the related review or examination.

The One CA has the right to retain a third-party auditor to perform audit and examination functions. The audited external RA shall provide full and reasonable cooperation to the One CA and the personnel conducting the audit and examination.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

8.5 Action Taken as a Result of Deficiency

If audit personnel find that the establishment and operation One CA or an RA does not conform with CPS regulations, the following actions shall be taken:

(1) Record non-conformities.

(2) Notify the One CA about the non-conformities.

(3) With regard to the non-conformities, the One CA shall submit an improvement plan within 30 days, promptly implement the plan and record the tracking items for subsequent audits. RAs are notified to make improvements to RA-related deficiencies.

8.6 Communications of Results

Except for systems that could possibly be attacked, and the scope specified in section 9.3, One CA shall announce the information which should be publicly stated by the qualified auditor. The audit results are displayed on the One CA website's front page using WebTrust ®for Certification Authorities seals. The compliance audit and management's assertions may be viewed by clicking on the seals. The most recent compliance audit and management's assertions shall be made publicly available in the repository within three months after the end of the audit period. If the posting of the latest audit results needs to be postponed for some reason, the CA shall provide a letter of explanation signed by the qualified auditor. After the assessment is completed, the audit compliance report and identification of corrective measures will be sent to PA within 30 days of completion.

8.7 Self-Audits

Not Applicable.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

The certificate issuance and renewal fees will be agreed between the One CA and subscribers will in the related business contract terms and conditions.

9.1.2 Certificate Access Fees

No stipulation.

9.1.3 Certificate Revocation or Status Information Access Fees

Certificate Revocation or Status Information Access is free for all relying-parties.

9.1.4 Fees for Other Services

No stipulation.

9.1.5 Refund Policy

With regard to the certificate issuance and renewal fees collected by the One CA, if a subscriber is unable to use a certificate due to oversight by the One CA, the One CA shall issue a new certificate after conducting an investigation. If the subscriber does not accept the newly issued certificate, the One CA shall refund the fee to the subscriber. Except for the above circumstances and circumstances in section 4.9, other fees shall not be refunded.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

The One CA is responsible to the damage only if the damage is caused by intention acts or gross negligence. Entities acting as relying parties, shall determine what financial limits, if any, they wish to impose for certificates used to consummate a transaction.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

9.2.2 Other Assets

Not Applicable

9.2.3 Insurance or Warranty Coverage for End-Entities

Not Applicable

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The generation, receipt and safekeeping of information by the One CA or RAs shall be deemed to be confidential information.

(1) Private keys and passphrases used for operations.

(2) Key splitting safekeeping information.

(3) Subscriber application information.

(4) Audit and tracking logs generated and kept by the One CA.

(5) Audit logs and reports made by audit personnel during the audit process.

(6) Operation-related documents listed as confidential level operations.

Current and departed One CA and RA personnel and various audit personnel shall keep confidential information in strict confidence.

9.3.2 Information not Within the Scope of Confidential Information

(1) Certificate Practice Policy of certification authority

(2) Certificate uses policy

(3) Information inside certificate

(4) Certificate revocation

(5) Information without impact on security and reliability of One CA such as articles and news

9.3.3 Responsibility to Protect Confidential Information

The One CA has security measure in place to protect confidential information.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

9.4 Privacy of Personal Information

9.4.1 Privacy Protection Plan

The One CA has posted its personal information protection statement and privacy declaration on its website. The One CA conducts privacy impact analysis and personal information risk assessments and also has established a privacy protection plan.

9.4.2 Information Treated as Private

Any personal information listed on any certificate application is deemed private information and only may be disclosed with the consent of the subscriber or in accordance with related laws and regulations. Information that cannot be obtained through the certificate and CRL or subscriber information obtained through certificate catalog service and personally identifiable information to maintain the operation of CA trusted roles such as names together with palm print or fingerprint characteristics, personal information on confidentiality agreements or contracts are deemed private information which requires protection. The One CA and RAs implement security control measures to prevent personally identifiable information from unauthorized disclosure, leakage and damage.

9.4.3 Information Not Deemed Private

Identification information or information listed on certificates, unless stipulated otherwise, is not deemed to be confidential and private information.

Issued certificates, revoked certificates, suspension information and CRLs published in the repository is deemed to be confidential and private information.

9.4.4 Responsibility to Protect Private Information

The personal information required for the operation of the One CA, in either paper or digital form, must be security stored and protected in accordance with the personal information protection and privacy rights declaration posted on the website and comply with WebTrust Principles and Criteria for Certification Authorities Audit Criteria, CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security. The One CA shall negotiate protection of private information with RAs.

9.4.5 Notice and Consent to Use Private Information

Personal information shall not be used for other purposes without the consent of subscriber or unless stipulated otherwise in the personal information protection and privacy rights declaration and CPS. The subscriber may check the subscriber's own application information specified in section 9.3.1 paragraph (3). However, the One CA shall reserve the right to collect reasonable fees from subscribers applying for access to this information.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

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

9.4.7 Other Information Disclosure Circumstances

None

9.5 Intellectual Property Rights

The following is the intellectual property of the One CA:

(1) One CA and RA key pair and secret share of the keys.

(2) Writing of related documents or system development for certificate management work performed by the One CA.

(3) Certificates and CRLs issued by the One CA.

(4) This CPS.

The Company agrees that the CPS may be freely downloaded from the One CA repository. Copying and distribution may be done in accordance with relevant copyright regulations, but it must be copied in full and copyright noted as being owned by Internet Thailand Public Co., Ltd. Fees may not be collected from others for the copying and distribution of CPS. The Company shall prosecute improper use or distribution which violates the CPS in accordance with the law.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

One CA shall follow the procedures in Chapter 4 of the CPS to perform related certificate management work. One CA obligations include:

(1) Comply with CP and CPS in operations.

(2) Perform certificate application identification and authentication.

(3) Provide certificate issuance and publication services.

(4) Revoke, suspend or resume use of certificates.

(5) Issue and publish CRLs.

(6) Issue and provide OCSP response messages.

(7) Securely generate One CA and RA private keys.

(8) Secure management of private keys.

(9) Use private keys in accordance with section 6.1.7 regulations

(10) Support related certificate registration work performed by RAs.

(11) Identification and authentication of CA and RA personnel.

9.6.2 Registration Authority Representations and Warranties

RAs shall follow the procedures in CPS regulations and are responsible for registration work including the collection or verification of certificate subscriber identity and certification related information. The legal responsibility arising from registration work performed by RAs shall be borne by the RAs.

Certificate subject identity check is done for certificates issued by the One CA. Its checking level is the review results of the RAO at that time, but no guarantee is provided for the credit status, financial capability, technical capability or reliability of the subscriber.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

RA obligations include:

(1) Provide certificate application services.

(2) Perform certificate application identification and authentication.

(3) Notify subscribers and relying parties of the obligations and responsibility with regard to the One CA and RA.

(4) Notify subscribers and relying parties to follow CPS related regulations when obtaining and using the certificates issued by the One CA.

(5) Implement identification and authentication procedures for RAO.

(6) Manage RA private keys.

9.6.3 Subscriber Representations and Warranties

Subscribers shall bear the following obligations. If there is a violation, subscribers shall be solely liable for damages to other parties in accordance with the Civil Code and related regulations:

(1) Subscribers shall comply with related application regulations in the CPS and ensure that the application information provided is accurate.

(2) Subscribers shall accept the certificate in accordance with the regulations in section 4.4 after the One CA approves the certificate application and issues the certificate.

(3) Subscribers shall check the information contained on the certificate after obtaining the certificate issued from the One CA and use the certificate in accordance with the regulations in section 1.4.1. If the certificate information contains errors, subscribers shall notify the RA and may not use that certificate.

(4) Subscribers shall properly safeguard and use their private keys.

(5) Subscribers shall follow the regulations in Chapter 4 if certificates need to be suspended, restored, revoked or reissued. If private key information is leaked or lost and the certificate must be revoked, the RA should be promptly notified. However, subscribers shall still bear legal responsibility for the use of the certificate before the change.

(6) Subscribers shall select secure computer environments and reliable application systems. If the rights of relying parties are infringed upon due to the use of computer environments and application systems, the subscribers shall bear sole responsibility.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

(7) If the One CA is unable to operate normally for some reason, the subscribers shall speedily seek other ways for completion of legal acts and the inability for the One CA to operate normally shall not be used as a defense to others.

9.6.4 Relying Parties Representations and Warranties

Relying parties using certificates issued by the One CA shall bear the following obligations: If there is a violation, relying parties shall be solely liable for damages to other parties in accordance with the Civil Code and related regulations:

(1) Relying parties shall follow relevant CPS regulations when using the certificates issued by the One CA or checking the One CA repository.

(2) Relying parties shall first check CP OID of end entities's certificates and One CA's CA certificate to protect their rights during use of certificates issued by the One CA.

(3) Relying parties shall check the certificate and keyUsage listed on the certificate during use of the certificate issued by the One CA.

(4) Relying parties shall first check the CRL or OCSP response message to determine if the certificate is valid during use of certificates issued by the One CA.

(5) Relying parties shall first check the digital signature to determine if the certificate, CRL or OCSP response message is correct when using certificates, CRL or OCSP response message issued by the One CA.

(6) Relying parties shall select secure computer environments and reliable application systems. If the rights of relying parties are infringed upon due to the use of computer environments and application systems, the relying parties shall bear sole responsibility.

(7) If the One CA is unable to operate normally for some reason, the relying parties shall speedily seek other ways for completion of legal acts and the inability for the One CA to operate normally shall not be used as a defense to others.

(8) Relying party acceptance of a certificate issued by the One CA indicates understanding and agreement of the One CA legal liability clauses in accordance with the scope of certificate use outlined in section 1.4.1.

9.6.5 Representations and Warranties of Other Participant

Not Applicable.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

9.7 Disclaimer of Warranties

In the event that damages are suffered by subscribers and relying parties due to failure to use the certificates according to the scope of use stipulated in section 1.4.1 or failure to follow the CPS, related laws and regulations and subscriber and related relying party contract provisions or any damages occur which are not attributable to the One CA, subscribers or relying parties shall be held liable.

In the event that relying parties suffer damages due to reasons attributable to the subscriber or damages occur which are not attributable to the RA, subscribers or relying parties shall be held liable.

In the event that damages are suffered by subscribers and relying parties due to failure to follow the CPS, related laws and regulations or related relying party contract provisions or damages occur which are not attributable to the RA, subscribers or relying parties shall be held liable.

9.8 Limitations of Liability

If there are One CA maintenance, conversion or expansion requirements, notification shall be posted in the repository three days in advance. Subscribers and relying parties may not use temporary suspension of some certificate services as a reason to claim compensation from the One CA.

If the subscriber submits a certificate revocation request is submitted due the reasons for certification revocation stipulated in section 4.9.1, the One CA shall complete the certificate revocation work within one working day, and issue and post the CRL on the repository after the certification revocation request is approved. Before the certificate revocation status is published, subscribers shall take appropriate action to reduce the effect on relying parties and bear responsibility arising from use of the certificates.

9.9 Indemnities

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

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

9.10 Term and Termination

9.10.1 Term

The CPS and any attachments take effect when published on the One CA website and repository and remain in effect until replaced with a newer version.

9.10.2 Termination

The CPS and any attachments remain in effect until replaced by a newer version. The old version is terminated.

9.10.3 Effect of Termination and Survival

The conditions and effect of the CPS termination shall be communicated via the One CA website and repository. This communication shall emphasize which provisions survive CPS termination. At the minimum, the responsibilities related to protecting confidential information shall survive CPS termination.

9.11 Individual Notices and Communication with Participants

The Company accepts comments about the CPS by digitally signed e-mail or written notice at the address in section 2.2 of the CPS. It is deemed valid only after sender receives a valid reply slip with a digital signature. If the reply slip is not received in 5 days, the comments may be sent in writing by express or registered mail. The One CA, RAs, subscribers, relying parties shall take respective actions to establish notification and communication channels including but not limited to: official document, letters, telephone, fax, e-mail or secure e-mail.

9.12 Amendments

9.12.1 Procedure for Amendment

A regular annual assessment is made to determine if the CPS needs to be amended to maintain its assurance level. Amendments are made by attaching documents or directly revising the CPS content. The CPS shall be amended accordingly if the CP is amended or the OID is changed.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

Every year, the One CA regularly review the terms and conditions in the official version of Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates issued by CA/Browser Forum: http://www.cabforum.org, to assess if the CPS shall be modified. Shall the CPS be contradictory to the regulation of the forum in the description of SSL certificate issuance management, the terms and conditions issued by CA/Browser Forum shall prevail, and the CPS is modified accordingly.

9.12.2 Notification Mechanism and Period

The One CA conducts annual reviews of the terms specified in the official version of Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates issued by CA/Browser Forum (http://www.cabforum.org), to evaluate if the CPS needs any amendment. If there is any contradiction regarding the SSL certificate issuance between the CPS and the regulations of that Forum, the regulations of the Forum prevail, and the CPS is amended accordingly.

9.12.2.1 Notification Mechanism

All change items are posted in the One CA repository. No additional notification is made for non-material changes to the CPS.

9.12.2.2 Modification Items

Assess the level on impact of change items on subscribers and relying parties:

(1) Significant impact: Post 30 calendar days in the One CA repository before making the revision.

(2) Less significant impact: Post 15 calendar days in the One CA repository before making the revision.

9.12.2.3 Comment Reply Period

The reply period for comments on change items is:

Where the impact of section 9.12.2.2 (1) is significant, the reply period is within 15 calendar days of the posting date.

Where the impact of section 9.12.2.2 (2) is less significant, the reply period is within 7 calendar days of the posting date.

9.12.2.4 Comment Handling Mechanism

For comments on change items, the reply method posted in the One CA repository is transmitted to the One CA prior to the end of the comment reply period. The One CA shall consider related comments when evaluating the change items.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

9.12.2.5 Final Notification Period

The change items announced by the CPS shall be revised in accordance with sections 9.12.1 and 9.12.2. The notification period shall be at least 15 calendar days in accordance with the section 9.12.2.3 until the CPS revisions take effect.

9.12.3 Circumstances under which the OID Must Be Changed

If CP revisions do not affect the certificate usage and assurance level stated in the CP, the CP OID does not require modification. Corresponding changes shall be made to CPS in response to the changes made to the CP OID.

9.13 Dispute Resolution Provisions

9.13.1 Disputes between Issuer and subscriber

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

Internet Thailand Public Company Limited
1768 Thai Summit Tower, 10th -12th Floor and IT Floor
New Petchaburi Road, Khwaeng Bang Kapi,
Khet Huay Khwang, Bangkok 10310

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

In the event of undefined, PA has jurisdiction over the dispute.

9.13.2 Disputes between Issuer and Relying Parties

Same procedure as stated in section 9.13.1. In the event of undefined, PA has jurisdiction over the dispute.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

9.14 Governing Law

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

9.15 Compliance with Applicable Law

One CA is required to comply with the laws of the Kingdom of Thailand.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

An entire agreement clause, which typically identifies the document or documents comprising the entire agreement between the key participants (One CA, RA, Subscribers and relying parties) and states that such agreements supersede all prior and contemporaneous written or oral understandings relating to the same subject matter and the CPS entire agreement shall be the final agreement mutually agreed upon for the CPS.

9.16.2 Assignment

Entities described in the CPS may not assign their rights or obligations without the prior written consent of the Company. The Company does not provide advance notice of rights and obligations assignment. The rights and obligations of key participants (One CA, RA, subscribers and relying parties) described in the CPS may not be assigned in any form to other parties without notifying the One CA.

9.16.3 Severability

If any chapter of the CPS is deemed incorrect or invalid, the remaining chapters of the CPS will remain valid until revisions are made to the CPS.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222

Regarding the issuance of SSL certificates, the CPS complies with the requirements in the official version of Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates issued by CA/Browser Forum (http://www.cabforum.org); however, if the related requirements of the Baseline Requirements conflict with the related domestic laws and regulations complied by the CPS, the CPS may be adjusted to satisfy the requirements of the laws and regulations and notify CA/Browser Forum about the changed contents of the CPS. If the domestic laws and regulations are not applicable anymore, or the Baseline Requirements are revised their contents to be compatible with the domestic laws and regulations, the CPS will delete and amend the adjusted contents. The aforesaid actions shall be completed in 90 calendar days.

9.16.4 Enforcement

In the event that the One CA suffers damages attributable to an intentional or unintentional violation of related CPS regulations by a subscriber or relying party, the One CA may seek compensation for damages from the responsible party related to the dispute or litigation.

The One CA's failure to assert rights with regard to the violation of the CPS regulations does not waive the One CA's right to pursue the violation of the CPS subsequently or in the future.

9.16.5 Force Majeure

In the event that a subscriber or a relying party suffers damages due to a force majeure or other circumstances not attributable to the One CA including but not limited to natural disasters, war or terrorist attack, the One CA shall not bear any legal liability. The One CA shall set clear limitations for certificate usage and shall not bear any legal responsibility for damages caused by exceeding these usage limitations.

9.17 Other Provisions

Not Applicable.

www.inet.co.th
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) สำนักงานใหญ่ เลขประจำตัวผู้เสียภาษี 0107544000094
1768 อาคารไทยซัมมิท ทาวเวอร์ ชั้น 10-12 และชั้น IT ถ.เพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310
Internet Thailand Public Company Limited Head Office TAX ID 0107544000094
1768 Thai Summit Tower, 10th-12th Floor and IT Floor, New Petchaburi Road, Bangkapi, Huay Khwang, Bangkok 10310
Tel. (662) 257-7000 Fax. (662) 257-7222