# Chunghwa Telecom Certification Authority

# **Certification Practice Statement** (CHTCA CPS)

Version 1.2

Chunghwa Telecom Co., Ltd.

May 19, 2025

# Contents

# CPS Version Control

| Version | Date | Revision Summary |
|---|---|---|
| 0.95 | April 22, 2022 | (1) First Released.<br>(2) Combined version of CPS documents of four CAs, including eCA, PublicCA, eTSCA and CHT SMIME CA. |
| 1.0 | April 6, 2023 | The version approved by the competent authority, Ministry of Digital Affairs. This version is a CPS document that integrates eCA CPS version 1.75, eTSCA CPS version 1.01, PublicCA CPS version 2.06 and CHT SMIME CA CPS version 1.05. After the announcement of this document, the effectiveness of the aforementioned four CPS documents will be terminated and will be removed to the archive area simultaneously. |
| 1.05 | August 29, 2023 | Amendments are made on Sections 1.2, 2.3, 3.1.6, 3.2.2, 3.2.3, 3.2.5, 3.2.5.7, 4.1.1, 4.5.2, 4.9.10, 5.3.3, 6.1.2, 6.1.5, 6.1.6, 6.2.3, 6.2.6, 6.2.8, 6.2.9, 6.3.2.1, 6.4.1, 6.4.3, 6.6.1, 7.1.4.2, 7.2.2, 8.4, 8.7, 9.5 and 9.6.1. |
| 1.07 | May 06, 2024 | Incrementing the version number. |
| 1.1 | Aug. 27, 2024 | The version approved by the competent authority, Ministry of Digital Affairs. |
| 1.2 | May 19, 2025 | (1) Amendments are made on Sections 1.1.1, 1.2, 1.3.1, 1.3.2, 1.4.1, 1.4.2, 1.5.3, 2.1, 2.2, 2.3, 3.1.1, 3.1.2, 3.1.3, 3.1.5, 3.2.2, 3.2.4, 3.2.5, 3.2.7, 3.2.8, 3.3.1, 4.2.1, 4.2.2, 4.2.3, 4.3.1, 4.4.1, 4.4.2, 4.4.3, 4.5.2, 4.9.1.1, 4.9.10, 4.9.11, 4.9.13, 5.4.8, 6.1.2, 6.1.6, 6.1.7.1, 6.1.7.2, 6.2.5, 6.2.7, 6.3.2.1, 6.3.2.2, 6.6.1, 6.6.2, 7.1, 7.1.2, 7.1.4, 7.1.4.1, 7.1.4.2, 7.1.4.3, 7.2.2, 7.3.1, 8.2, 8.4, 8.6, 8.7, 9.2.2, 9.3.3, 9.6.1, 9.6.3, 9.12.3, 9.16.3, Appdendix 1, Appendix 2, Appendix 3, Appendix 3-1, and Appendix 3-2.<br>(2) In light of PublicCA's cessation of TLS certificate issuance as of December 10, 2024, all corresponding provisions related to TLS certificates have been formally removed from this CPS. |
| | | |

# 1. Introduction

## 1.1 Overview

According to the ePKI Certificate Policy (CP), ePKI Root Certification Authority (eCA) is a top-level CA and a trust anchor of ePKI. eCA must maintain a high level of credibility that relying parties can directly trust its certificates.

This Certification Practice Statement (CPS) uses the brand name of Chunghwa Telecom Certification Authority (CHTCA) to refer to the eCA and its subordinate CAs, including Public Certification Authority (PublicCA), ePKI Timestamping Certification Authority (eTSCA), and CHT SMIME Certification Authority (CHT SMIME CA), owned and operated by Chunghwa Telecom Co., Ltd. (CHT) in ePKI.

### 1.1.1 Certification Practice Statement

This CPS describes the practices used to comply with the ePKI CP, the R.O.C.

(1) Electronic Signatures Act and

(2) its sub-law “Regulations on Required Information for Certification Practice Statements”

and official versions of related international standards or regulations, including

(1) The Internet Engineering Task Force (IETF) request for comments (RFC) 3647, RFC 5280, RFC 6960, RFC 6962, RFC 5019, RFC 8659, RFC 3161, RFC 5816 and RFC 3628;

(2) ITU-T X.509;

(3) TS 102 023, EN 319 421 and EN 319 422 of (European Telecommunications Standards Institute, ETSI)

(4) Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (Baseline Requirements), Baseline Requirements for the Issuance and Management of Publicly-

Trusted S/MIME Certificates(S/MIME Baseline Requirements), and Network and Certificate System Security Requirements published by CA/Browser Forum (https://www.cabforum.org),

to provide guidance and requirements for what CHTCA should include in its CPS.

### 1.1.2 CPS Applicability

The practice statement stipulated in this CPS applies to CAs of CHTCA, registration authority (RA), subscribers, relying parties, repository, and other participants.

## 1.2 Document Name and Identification

This document is Chunghwa Telecom Certification Authority Certification Practice Statement. This CPS can be obtained at: https://chtca.hinet.net/repository.html.

The identity assurance level (IAL) and the CP object identifiers (OIDs) are listed in the Table below:

| IAL | OID Name | OID Value |
|---|---|---|
| Level 1 | id-cht-ePKI-certpolicy-class1Assurance | {id-cht-ePKI-certpolicy 1} |
| Level 2 | id-cht-ePKI-certpolicy-class2Assurance | {id-cht-ePKI-certpolicy 2} |
| Level 3 | id-cht-ePKI-certpolicy-class3Assurance | {id-cht-ePKI-certpolicy 3} |
| Level 4 | id-cht-ePKI-certpolicy-class4Assurance | {id-cht-ePKI-certpolicy 4} |

The eCA certificate is a self-signed certificate. According to international standards and practices, the eCA certificate does not indicate the CP OID to reflect its high credibility of root CA and was operated with IAL 4.

The above OIDs are gradually transferred to the id-pen-cht arc OID registered as private enterprise number (PEN) with the Internet Assigned Numbers Authority (IANA) from December 2014.

id-pen-cht ::= {1 3 6 1 4 1 23459}
id-pen-cht-ePKI ::= {1 3 6 1 4 1 23459 100}
id-pen-cht-ePKI-certpolicy::= {id-pen-cht-ePKI 0}

| IAL | OID Name | OID Value |
|---|---|---|
| Level 1 | id-pen-cht-ePKI-certpolicy-class1Assurance | {id-pen-cht-ePKI-certpolicy 1} |
| Level 2 | id-pen-cht-ePKI-certpolicy-class2Assurance | {id-pen-cht-ePKI-certpolicy 2} |
| Level 3 | id-pen-cht-ePKI-certpolicy-class3Assurance | {id-pen-cht-ePKI-certpolicy 3} |
| Level 4 | id-pen-cht-ePKI-certpolicy-class4Assurance | {id-pen-cht-ePKI-certpolicy 4} |

The CA certificate and PDF signing certificates (assurance level 2 or 3 certificates issued to organizations or individuals) issued by PublicCA may use the OID 1.3.6.1.4.1.23459.100.0.9, which is approved by the Adobe Approved Trust List (AATL).

With regard to S/MIME certificates, if there is any inconsistency between this CPS and the official version of the S/MIME Baseline Requirements, then the S/MIME Baseline Requirements takes precedence.

The following CP OIDs are reserved for use by subordinate CAs as a means of asserting compliance with the S/MIME Baseline Requirements as follows:

| Object Name | **CP OIDs** |
|---|---|
| CA/Browser Forum S/MIME Baseline Requirements | 2.23.140.1.5 |
| **Mailbox−validated** | |
| Mailbox-validated Legacy S/MIME Certificate | 2.23.140.1.5.1.1 |
| Mailbox-validated Multipurpose S/MIME Certificate | 2.23.140.1.5.1.2 |
| Mailbox-validated Strict S/MIME Certificate | 2.23.140.1.5.1.3 |
| **Organization−validated** | |
| Organization-validated Legacy S/MIME Certificate | 2.23.140.1.5.2.1 |
| Organization-validated Multipurpose S/MIME Certificate | 2.23.140.1.5.2.2 |

| Object Name | **CP OIDs** |
|---|---|
| Organization-validated Strict S/MIME Certificate | 2.23.140.1.5.2.3 |
| **Sponsor−validated** | |
| Sponsor-validated Legacy S/MIME Certificate | 2.23.140.1.5.3.1 |
| Sponsor-validated Multipurpose S/MIME Certificate | 2.23.140.1.5.3.2 |
| Sponsor-validated Strict S/MIME Certificate | 2.23.140.1.5.3.3 |
| **Individual−validated** | |
| Individual-validated Legacy S/MIME Certificate | 2.23.140.1.5.4.1 |
| Individual-validated Multipurpose S/MIME Certificate | 2.23.140.1.5.4.2 |
| Individual-validated Strict S/MIME Certificate | 2.23.140.1.5.4.3 |

For the types of S/MIME certificates listed in the table above, please refer to the descriptions in the table below.

| Types | Descriptions |
|---|---|
| Mailbox-Validated | Certificate Subject that is limited to (optional) subject:emailAddress and/or subject:serialNumber attributes. |
| Organization-Validated | Certificate Subject that includes only Organizational (Legal Entity) attributes. |
| Sponsor-validated | Certificate Subject which combines Individual (Natural Person) attributes in conjunction with an organization name attribute. Registration for Sponsor−validated certificates MAY be performed by an Enterprise RA where the organization name is either that of the delegated enterprise, or an Affiliate of the delegated enterprise, or that the delegated enterprise is an agent of the named Subject Organization. |
| Individual-Validated | Certificate Subject that includes only Individual (Natural Person) attributes. |

Generations (known as Legacy, Multipurpose, and Strict) are specified in the S/MIME Baseline Requirements for each of these Certificate Types, acknowledging both the current diversity of practice in issuing S/MIME Certificates as well as the desire to move towards more closely-defined practices over time.

The S/MIME Strict Generation profiles are the long-term target

profile for S/MIME certificates with extKeyUsage limited to id-kp-emailProtection, and stricter use of Subject DN attributes and other extensions. The S/MIME Multipurpose Generation profiles are aligned with the more defined Strict Profiles, but with additional options for extKeyUsage and other extensions. This is intended to allow flexibility for crossover use cases between document signing and secure email. The S/MIME Legacy Generation profiles provide flexibility for existing reasonable S/MIME certificate practices to become auditable under the S/MIME Baseline Requirements. This includes options for Subject DN attributes, extKeyUsage, and other extensions. The Legacy Profiles will be deprecated in a future version of the S/MIME Baseline Requirements.

For certificates issued on or after July 15th, 2025, CHTCA will not issue S/MIME subscriber certificates using the Legacy Generation profiles 2.23.140.1.5.1.1, 2.23.140.1.5.2.1, 2.23.140.1.5.3.1, or 2.23.140.1.5.4.1.

## 1.3 PKI Participants

The key members of CHTCA include:

(1) CHTCA

(2) RAs

(3) Subscribers

(4) Relying Parties

### 1.3.1 Certification Authorities

The following CAs of CHTCA are established and operated by Chunghwa Telecom Co., Ltd. (CHT), the relevant CPS shall be submitted to the Chunghwa Telecom Certificate Policy Management Authority (PMA) for review and approve.

| Certification Authority | Description |
|---|---|
| eCA | Root certificate authority, which has been implanted in major Root Certificate Programs. |

| | |
|---|---|
| PublicCA | Responsible for issuing publicly-trusted TLS certificates and natural person, organization, device, secure email (S/MIME), time-stamp or application software certificates. PublicCA will not issue TLS, time-stamp and S/MIME certificates since the 3rd generation. |
| eTSCA | CHT operates a time-stamping authority (TSA) and provides proof-of-existence for data at an instant in time. eTSCA is responsible for issuing a time-stamp certificate to the TSA. |
| CHT SMIME CA | In order to ensure the authentication, integrity, non-repudiation/content commitment and confidentiality of emails, CHT SMIME CA provides S/MIME certificates for natural person and organization. |

CHTCA's CA certificate information and applicable CP/CPS, external audit report and management statement are all published in the CA repository. PublicCA has ceased issuing TLS server certificates as of December 10, 2024.

### 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 CHTCA. Each RA counter has an RA officer (RAO) who is responsible for the review of certificate application, revocation, re-key, and renewal for different certificate groups and classes.

eCA directly accepts CA certificate registration and revocation requests and is responsible for collecting and verifying the identity and the certificate-related information of subordinate CAs and cross-certified CAs. There is no need to set up a RA.

The RA of the subordinate CA can be directly established and maintained by the subordinate CA (known as internal RA), or may be

established and maintained by the customer contracted by the CHT (known as external RA). RAs shall operate in accordance with this CPS, where internal RA may adopt stricter security control practices than this CPS.

### 1.3.3 Subscribers

A Subscriber refers to the subject who has applied for and obtained a certificate issued by CHTCA. The relationship between the subscriber and certificate subject is listed in the following Table:

| Certificate Subject | Subscriber |
|---|---|
| Natural person | himself |
| Organization | an authorized representative |
| Equipment | owner of the equipment |
| Application software | owner of the application software |
| TSA or Time-stamping Unit (TSU) | owner of TSA |

Generation of subscriber key pairs shall comply with Section 6.1.1 of this CPS. The subscriber must have the right and capability to control the private key that corresponds to its subscriber certificate. The Subscriber is not capable of issuing certificates to other parties.

In the ePKI, a Subordinate CA is not called the subscriber because the Subordinate CA is capable of issuing certificates.

### 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.

For S/MIME certificates, it may be used for the following purposes:

(1) Verify the identity of digital signature author within the email.

(2) Verify the integrity of the email protected with digital signatures.

(3) Encrypt email content.

For other certificates, it may be used for the following purposes:

(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

Other authorities include TSA and card management center (responsible for the production and management of tokens).

## 1.4 Certificate Usage

### 1.4.1 Appropriate Certificate Uses

eCA issues four kinds of certificates: self-signed certificates, self-issued certificates, subordinate CA certificates and cross-certificates. The types of certificates and their scope of application are shown as follows:

| Cert. Type | Scope of Applications |
|---|---|
| Self-signed certificates | A self-signed certificate is used to establish the trust anchor of the ePKI.<br>The issuance subject of the self-signed certificate is the eCA itself. The self-signed certificate contains the eCA public key which can be used to verify the digital signatures on subordinate CA certificates, cross-certificates, self-issued certificates and certification authority revocation lists (CARLs) issued by eCA. |
| Self-issued certificates | A self-issued certificate is used for the eCA re-key or as the path for certificate policy mutual trust. |
| Subordinate CA certificates | A subordinate CA certificate is used construct the trust path required for the interoperability of CAs.<br>The issuance subject of the subordinate CA certificate is subordinate CA established under the ePKI.<br>The subordinate CA certificate contains the subordinate CA public key which can be used to verify the digital signatures on certificates and CRLs issued by the subordinate CA. |
| cross- | A cross-certificate is used construct the trust path required for the |

| Cert. Type | Scope of Applications |
|---|---|
| certificates | interoperability of CAs under different PKIs.<br>The issuance subject of the cross-certificate is a root CA which is established under another PKI and cross-certifies with eCA.<br>The cross-certificate contains the cross-certified CA public key which can be used to verify the digital signatures on certificates and CARLs issued by that CA. |

The various types of subscriber certificates, defined in the ePKI CP, issued by the subordinate CAs are described below, along with their respective types and applicable scopes are shown as follows:

| Cert. Type | Scope of Applications |
|---|---|
| Level 1 subscriber certificates | Use email notification to verify that the applicant can control the email address. Suitable for use in network environments in which the risk of malicious activity is considered to be low or a higher assurance level cannot be provided. When used for digital signatures, it can identify that the subscriber originates from a certain email address 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 the symmetric key to guarantee the confidentiality of email content. Not suitable for online transactions that require identification and Non-Repudiation/ contentCommitment.<br>For example, information encryption and signatures required for emails. |
| Level 2 subscriber certificates | 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/emails (life essential and high value transaction documents).<br>For example, information encryption and identity authentication for small value e-commerce transactions. |
| Level 3 subscriber certificates | Suitable for use in network environments in which there are malicious users, who may intercept or tamper with information, and with risks greater than the environment of level 2. A signature shall be adopted to confirm its identity, which can be used for non-repudiation/content commitment online transactions.<br>Suitable for e-commerce application, Internet tax filing, e-government, email application, TLS encryption channel or identity identifying service. |
| Time-stamp certificates | • Provide evidence that an electronic document existed at or before a particular time.<br>• Proof of signature time of electronic documents. |

| Cert. Type | Scope of Applications |
|---|---|
| | • Electronic document storage and proof service.<br>• The recipient verifies the correctness of the time-stamp of the electronic document.<br>• Protection the evidence of digital asset generation time or issuance time.<br>• Scope of application includes (but not limited to): e-policy, e-contract, electronic bill, business secret protection, intellectual property protection, e-bidding, e-voting, e-documents, e-certificate letter and code signing, etc. |

If CHTCA can confirm that the token for storing the subscriber private key (e.g., the TSU private key is stored in a hardware cryptographic module), in addition to include the IAL, the authenticator assurance levels (AAL) defined in the ePKI CP can be included in the certificates. The AAL are described as follows:

| AAL | Descriptions |
|---|---|
| Level 1 | Providing only partial assurance as to whether or not the token controller truly binded the Subscribers' accounts. Its successful single-factor or multi-factor authentication via the use of any available verification technique shall, via a secure authentication protocol, be able to confirm that the subscriber truly have possession of and control over that token.<br>(1) Permitted token type: can use any one of the following types.<br>■ Memorable secret code, such as: password or personal identification number;<br>■ Single-factor encryption software;<br>■ Single-factor encryption equipment;<br>■ Multi-factor encryption software;<br>■ Multi-factor encryption equipment.<br>(2) Requirements of the token and validator:<br>■ The encryption token shall use the approved encryption technology. The software token can also try to detect the possible of malicious attack to the terminal equipment (such as: installed with malicious software). If it is found, the certification in question shall be terminated.<br>■ The token owner and validator shall communicate with each other via authorized and securely encrypted channel to avoid man-in-the-middle attack. |
| Level 2 | Providing reliable assurance as to whether or not the token controller truly binded the Subscribers' accounts. Its authentication carried out under the secure environment of authentication protocol via the use of two authentication factors shall include the approved encryption technology. |

| AAL | Descriptions |
|---|---|
| | (1) Permitted token type: The verify operation shall be performed via multi-factor authentication or two-factor authentication.<br>■ If multi-factor authentication is taken, the available types of token include:<br>➢ Multi-factor encryption software;<br>➢ Multi-factor encryption equipment.<br>■ If the authentication mechanism is only two-factor, it shall include a memorable secret code token and any one-time token described below:<br>➢ Single-factor encryption software;<br>➢ Single-factor encryption equipment.<br>(2) Requirements of the token and validator:<br>■ Encryption token shall use the approved encryption technology. The token for government procurement shall pass FIPS 140 level 1 certification. The software token can also try to detect the possible of malicious attack to the terminal equipment (such as: installed with malicious software). If it is found, the certification in question shall be terminated. In addition, at least one type of token with replay attacks prevention capacity, such as dynamic passwords, shall be used.<br>■ The token owner and validator shall communicate with each other via authorized and securely encrypted channel to avoid man-in-the-middle attack.<br>■ If equipment such as mobile device is used in the verification process, the equipment's original unlocking function (such as: fingerprint recognition or personal identification number verification) shall not be regarded as a verification factor. |
| Level 3 | Providing highly reliable assurance as to whether or not the token controller truly binded the Subscribers' accounts. It verifies ownership of the subscriber's key via encryption protocol. The verification operation requires hardware password token and token capable of blocking from hacked validator (can also simultaneously use equipment with the aforesaid functions) and shall be carried out under the secure environment of authentication protocol via the use of two authentication factors, which shall include the approved encryption technology.<br>(1) Permitted token type: can use a combination of any one of the following tokens.<br>■ Multi-factor encryption equipment;<br>■ A combination of single-factor encryption equipment and memorable secret code.<br>(2) Requirements of the token and validator:<br>■ The token owner and validator shall communicate with each other via authorized and securely encrypted channel to avoid man-in-the-middle attack. All encryption equipment token shall be equipped |

| AAL | Descriptions |
|---|---|
| | with validator capable of anti-hacking and replay attacks prevention.<br>■ The token shall be cryptographic module which passed FIPS 140 level 2 (or up) or is in compliance with Global Platform Trusted Execution Environment.<br>■ If equipment such as mobile device is used in the verification process, the equipment's original unlocking function (such as: fingerprint recognition or personal identification number verification) shall not be regarded as a verification factor. |

Below are the OIDs for each AAL defined in the ePKI CP:

| AAL | OID Name | OID Value |
|---|---|---|
| Level 1 | id-cht-ePKI-tokenAssurance 1 | 1.3.6.1.4.1.23459.100.4.1 |
| Level 2 | id-cht-ePKI-tokenAssurance 2 | 1.3.6.1.4.1.23459.100.4.2 |
| Level 3 | id-cht-ePKI-tokenAssurance 3 | 1.3.6.1.4.1.23459.100.4.3 |

Subscribers and relying parties must carefully read and comply with this CPS before using and trusting the certificate service provided by CHTCA, and pay attention to the update of this CPS.

### 1.4.2 Prohibited Certificate Uses

Certificates issued under this CPS are prohibited from being used in the scope of:

(1) Man-in-the-middle TLS traffic interception;

(2) applications or businesses that may result in bodily harm, psychological distress, or cause significant harm to social order and public interest; and

(3) applications or businesses explicitly prohibited or excluded by the Electronic Signatures Act, other relevant laws, or the competent authorities for specific business purposes.

Subscribers are expected to comply with all requirements of all applicable browser root policies, including revocation periods of 24 hours and 5 days as specified herein.

# 1.5 Policy Administration

## 1.5.1 Organization Administering the Document

Chunghwa Telecom Co., Ltd. (CHT).

## 1.5.2 Contact Person

### 1.5.2.1 CPS Related Issues

Any suggestions regarding this CPS, please contact us by the following information.

E-mail: caservice@cht.com.tw

Address: 10048 CHT Certification Authority (4F), Data Communication Building, No. 21, Sec.1, Hsinyi Rd., Taipei City, Taiwan (R.O.C.)

### 1.5.2.2 Certificate Problem Report

Subscribers, relying parties, application software suppliers, and other third parties may report private key lose, suspected private key compromise, certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to certificates by sending email to report_abuse@cht.com.tw.

CHTCA may or may not revoke in response to this request. See Sections 4.9.3 and 4.9.5 for detail of actions performed by CHTCA for making this decision.

## 1.5.3 Person Determining CPS Suitability for the Policy

CHTCA shall first check whether this CPS conforms to the ePKI CP regulations and then submit the CPS to the PMA for review and approval. After approval, CHTCA is able to officially reference the certificate policies of ePKI.

In addition, according to the Electronic Signatures Act, CAs can provide the service of certificate issuance after the CPS has been approved

by the competent authority, Ministry of Digital Affairs.

CHTCA conducts regular internal/external audits to demonstrate that it has operated with the assurance level under the ePKI CP. According to the regulations of the root certificate program, the audits of CHTCA are conducted annually and the latest CPS as well as the audit reports are submitted to the root certificate programs. CHTCA also publishes the audit seals to the CHTCA websites.

### 1.5.4 CPS Approval Procedures

This CPS is published by CHTCA following approval by the PMA or Ministry of Digital Affairs, the competent authority of the Electronic Signatures Act. This CPS must be revised in response to any revision of the ePKI CP, and the revised CPS must be submitted to the PMA and Ministry of Digital Affairs for approval.

After the revisions of this CPS take effect, if there is any inconsistency between the original CPS and the revised CPS, then the revised CPS takes precedence unless stipulated otherwise.

## 1.6 Definitions and Acronyms

See Appendix 1 for the abbreviations and definitions and Appendix 2 for the glossary.

# 2. Publication and Repository Responsibilities

## 2.1 Repositories

The CHTCA repository is responsible for the publication and storage of certificates and certificate revocation lists (CRLs) issued by CHTCA and this CPS. CHTCA provides availability of a repository inquiry service to subscribers and relying parties and the repository is available at: https://chtca.hinet.net/repository.html

The repository will resume normal operation within two working days if unable to operate normally for some reason.

## 2.2 Publication of Certification Information

CHTCA shall take responsibility for making the following information publicly accessible in its repository:

(1) This CPS and the ePKI CP.

(2) All CHTCA certificates, Cross-certificates, and CRLs

(3) Privacy protection policy.

(4) The latest external audit report (as specified in Section 8.6).

CAA (Certification Authority Authorization) issuer domain names (as specified in Section 4.2.1) of PublicCA include ‘pki.hinet.net’, ‘publicca.hinet.net’, ‘eca.hinet.net’ or ‘epki.com.tw’.

## 2.3 Time or Frequency of Publication

(1) This CPS is reviewed and updated at least once every 366 days, and a dated changelog is state in the “Document History” section even if no other changes are made to this document. New or modified version of this CPS is published in the repository as soon as possible upon receiving the approval letter from the competent authority,

(2) New or modified version of the ePKI CP complied with by CHTCA is published in the repository as soon as possible upon the approval of the PMA,

(3) CHTCA issues CRLs at least twice a day and publishes it in the repository, and

(4) CHTCA certificates are published in the repository within seven working days after accepting issuance by an upper-level CA.

## 2.4 Access Controls on Repositories

CHTCA implements access control where it provides read-only access to prevent anyone from unauthorized writing operation, which would put repository security in risk.

# 3. Identification and Authentication

## 3.1 Naming

### 3.1.1 Types of Names

CHTCA certificates are issued with the following types of names:

(1) The subject distinguished name (DN) shall comply with ITU-T X.500 standards.

(2) The subject alternative name extension for subscriber certificates must not be marked critical. When it contains a Mailbox address, the address must be store in the rfc822Name.

### 3.1.2 Need for Names to be Meaningful

The naming of the certificate subject should comply with the law of the country under the jurisdiction of the applicant.

The issuing CA and its RA may abridge the prefix or suffix of the organization name, e.g., change the official name “Company Name Incorporated” to its abbreviated version “Company Name, Inc.”, and the abbreviation must be made on the basis that the certificate subject is easily identifiable in the jurisdiction in which it is established or registered. If the organization name is longer than 64 characters, the issuing CA and its RA may abbreviate the organization name or delete the unimportant text in the organization name.

### 3.1.3 Anonymity or Psuedonymity of Subscribers

CHTCA may issue pseudonymous subscriber certificates if they are not prohibited by policy and any applicable name space uniqueness requirements are met.

### 3.1.4 Rules for Interpreting Various Name Forms

The rules for interpreting name forms follow the definition of name

attribute type documented in ITU-T X.520.

### 3.1.5 Uniqueness of Names

CHTCA shall use the X.520 standard to define the various naming attributes for assembly to ensure the uniqueness of the X.500 naming space recognized by CHTCA for name of the subscriber certificate subject name. The CHTCA subscriber certificate subject name permits (but not limited to) the use of the following naming attributes defined in the X.520 standard for assembly:

- countryName (abbreviated as C)
- stateOrProvinceName (abbreviated as S)
- localityName (abbreviated as L)
- organizationName (abbreviated as O)
- organizationalUnitName (abbreviated as OU)
- commonName (abbreviated as CN)
- serialNumber

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

The certificate subject name, including trademark or any name, business or company name or representation protected by law, provided by subscribers must comply with relevant regulations in our country's Trademark Act, Fair-Trade Act, and other relevant laws and regulations. CHTCA does not guarantee the recognition, verification, legality and uniqueness of the certificate subject name if it contains a trademark. Related disputes and arbitration shall not be the obligation of CHTCA, the subscriber shall apply to relevant competent authorities, courts or arbitration institutions.

CHTCA may reject any application or at its own discretion revoke certificates (refer to Section 4.9.1) that involves in a trademark dispute.

## 3.2 Initial Identity Validation

### 3.2.1 Method to Prove Possession of Private Key

CHTCA shall verify that the entity (Subordinate CA or individual) possesses the private key, which is paired with the public key to be contained in the certificate, with the following two methods:

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

(2) The card management center securely generates the subscriber's key pair inside the chip. During the issuance of the certificate, the RA delivers the subscriber's public key to CHTCA through a secure channel. In this way, the subscriber does not need to prove the possession of its private key when applying for the certificate.

### 3.2.2 Authentication of Organization Identity

The certification document required for organization identification and authentication, and the authentication and verification procedures whether need to be performed at the counter are determined based on various assurance levels as shown in the following Table.

| Assurance Level | Procedures for Authentication of Organization Identity |
|---|---|
| Level 1 | There is no requirement to link the applicant to a specific real-life identity. Any attributes provided in conjunction with the authentication process are self-asserted.<br>(1) No identity verification required.<br>(2) The applicant is required to demonstrate control of their email address or domain name to which the certificate relates.<br>(3) In-person identity proofing at counter is not required. |
| Level 2 | Evidence supports the real-world existence of the claimed |

| Assurance Level | Procedures for Authentication of Organization Identity |
|---|---|
| | identity and verifies that the applicant is appropriately associated with this real-world identity.<br>(1) No identity verification required.<br>(2) In-person identity proofing at counter is not required.<br>(3) The applicant is required to provide organization information such as organization ID number (i.e., withholding tax ID number) and organization name. CHTCA may additionally cross-check the information provided by the applicant for consistency with available government or third-party data sources. |
| Level 3 | CHTCA allows the following methods for authentication of organization identity:<br>(1) In-person (physically-present) identity proofing at counter, which can be one of the following means:<br>a. A certification document or official document issued by government agency in the jurisdiction of the applicant;<br>b. Public information obtained from a qualified government information source (QGIS) such as the MOEA industry and business registration database or a qualified government tax information source (QTIS) such as the Fiscal Information Agency of MOF; or<br>c. Organizations belonging to CHT apply for the certificate with written application.<br>(2) Remote identity proofing, which can be one of the following means and the detailed operating procedures are formulated in the internal control system of each RA:<br>a. Application through an identity assurance level 3 organization certificate issued by the GPKI or ePKI;<br>b. For those organization who has complete registration procedure with the competent authority, like (1)-a or (1)-b, mailing the copies of the certification documents is acceptable;<br>c. A letter attesting that subject information is correct written by an accountant, lawyer, or notary;<br>d. A site visit by CA personnel or a third party who is acting as an agent for the CA; or<br>e. Organizations belonging to CHT apply for the certificate with |

| Assurance Level | Procedures for Authentication of Organization Identity |
|---|---|
| | e-form. |
| Level 4 | (1) The identity authentication of a CA established by CHT is reviewed by a PMA meeting convened by CHT.<br>(2) For a CA not established by CHT, the CA shall submit a application of subordinate CA certificate or cross-certificate, and a PMA meeting shall conven by CHT to review the application. |
| S/MIME certificates | In compliance with the S/MIME Baseline Requirements and the provisions for assurance level 3 in this Section.. |

### 3.2.3 Authentication of Individual Identity

The certification document required for individual identification and authentication, and the authentication and verification procedures whether need to be performed at the counter are determined based on various assurance levels as shown in the following Table.

| Assurance Level | Procedures for Authentication of Individual Identity |
|---|---|
| Level 1 | There is no requirement to link the applicant to a specific real-life identity. Any attributes provided in conjunction with the authentication process are self-asserted.<br>(1) No identity verification required.<br>(2) No identity verification other than control of the email address listed in the certificate.<br>(3) In-person identity proofing at counter is not required. |
| Level 2 | Evidence supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity.<br>(1) No identity verification required.<br>(2) The applicant is required to provide a legible copy of a valid government issued national identity document or photo ID (such as National ID, passport or health insurance card), and CHTCA will verify the information through reliable communications.<br>(3) In-person identity proofing at counter is not required |

| Assurance Level | Procedures for Authentication of Individual Identity |
|---|---|
| Level 3 | CHTCA allows the following methods for authentication of individual identity:<br>(1) In-person (physically-present) identity proofing at counter, which can be one of the following means:<br>The applicant must in-person proofing his / her identity at the CA or RA counter, at least present a national government-issued photo ID (such as National ID card, passport or health insurance card) to the RAO to examine whether they are authentic and unexpired. If the applicant is unable to present the application in person at the counter, the applicant may submit a letter of appointment to appoint an agent to submit the application. When the applicant is not the citizen of Taiwan, the verification should be conducted according to the relevant regulations, where the detailed operating procedures are formulated in the internal control system of each RA.<br>If an applicant (such as minor under 18 years old) is unable to submit the above photo ID, government-issued credentials (such as household registration) sufficient to prove the identity of the applicant and one adult with legal capacity to guarantee the applicant's identity in writing may be used in its place. The identity of the adult providing the guarantee must pass through the above authentication.<br>(2) Remote identity proofing, which can be one of the following means and the detailed operating procedures are formulated in the internal control system of each RA:<br>a. Application through a Citizen Digital Certificate IC Card;<br>b. Delegate the duty of individual's identity examination to a financial institution who has business with the applicant;<br>c. A declaration of applicant's identity that is witnessed and signed by a notary, lawyer, accountant, or any entity certified by a State or National Government as authorized to confirm identities;<br>d. Other identity proofing mechanisms for remote account opening recognized by the competent authority of the relying party;<br>e. Application through an identity assurance level 3 individual certificate issued by ePKI;<br>f. A site visit by CA personnel or a third party who is acting as |

| Assurance Level | Procedures for Authentication of Individual Identity |
|---|---|
| | an agent for the CA; or<br>g. Application through a telecommunications authentication where the related information is obtained from a telecommunications service provider under the applicant's consent. This method, where Subscriber Identity Module (SIM) authentication is used, provides the witness that the applicant and the number hirer have the same National ID number and the applicant had made identity proofing at the counter of Regular Chain stores at the time of dealing telecommunications business. |
| S/MIME certificates | In compliance with the S/MIME Baseline Requirements and the provisions for assurance level 3 in this Section. |

### 3.2.4 Non-verified Subscriber Information

The common name of an assurance level 1 individual certificate is not verified as the legal name of the subscriber. The OU fields of other certificates are generally not validated unless required by industry standards.

### 3.2.5 Validation of Authority

When a certificate lifecycle activity such as a certificate application or revocation request is submitted by an individual (an authorized representative) related to the certificate subject, CHTCA or its RA shall perform a validation of authority in accordance with Section 3.2.6 of the S/MIME Baseline Requirements to verify that the individual can represent the certificate subject.

CHTCA verifies an individual's or organization's right to use or control an email address to be contained in a certificate that will have the "Secure Email" EKU by doing one of the following:

(1) CHTCA or RA, according to Section 3.2.2.2 of the S/MIME

Baseline Requirement, MAY confirm the Applicant's control over each Mailbox Field to be included in a Certificate by sending a Random Value via email and then receiving a confirming response utilizing the Random Value.

Control over each Mailbox Address SHALL be confirmed using a unique Random Value. The Random Value SHALL be sent only to the email address being validated and SHALL not be shared in any other way.

The Random Value SHALL be unique in each email. The Random Value SHALL remain valid for use in a confirming response for no more than 24 hours from its creation.

(2) CHTCA or RA, according to Section 3.2.2.1 of the S/MIME Baseline Requirement, MAY confirm the Applicant, such as an Enterprise RA, has been authorized by the email account holder to act on the account holder's behalf by verifying the entity's control over the domain portion of the Mailbox Address to be used in the certificate.

### 3.2.6 Criteria for Interoperation

CHTCA allows another root CA to interoperate with, see ePKI CP for details.

### 3.2.7 Data Source Accuracy

Prior to using any data source as a Reliable Data Source, CHTCA SHALL evaluate the source for its reliability, accuracy, and resistance to alteration or falsification. CHTCA SHOULD consider the following during its evaluation:

(1) The age of the information provided,
(2) The frequency of updates to the information source,
(3) The data provider and purpose of the data collection,
(4) The public accessibility of the data availability, and
(5) The relative difficulty in falsifying or altering the data.

Databases maintained by CHTCA, its owner, or its affiliated companies do not qualify as a Reliable Data Source, if the primary purpose of the database is to collect information for the purpose of fulfilling the validation requirements in Section 3.2 of the Baseline Requirements.

### 3.2.8 Multi-Perspective Issuance Corroboration

From March 15, 2025, CHTCA will perform Multi-Perspective Issuance Corroboration (MPIC), specified in Section 3.2.2.9 of the Baseline Requirements, for the required CAA record checks in accordance with Sections 4.2.2.1 and 4.2.2.2 of the S/MIME Baseline Requirements. MPIC can assist to corroborate the determinations (i.e., CAA permission/prohibition) made by the Primary Network Perspective from multiple remote Network Perspectives before certificate issuance.

## 3.3 Identification and Authentication for Re-key Requests

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

If the subscriber or CA's private key needs to be renewed upon expiry of the certificate period, certificate rekey work may be performed, and the subscriber may re-apply for certification. The RA may validate the subscriber's identity by using the subscriber's public key to verify the CSR or conduct an initial identity validation in accordance with Section 3.2. CHTCA shall re-validate the subscriber's identity through an initial registration process in accordance with Section 3.2 at least once every nine years from the time of initial registration.

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

If the subscriber or CA's private key needs to be re-keyed due to certificate revocation, the subscriber or CA shall re-apply for the certificate

with CHTCA. The RA shall conduct an initial identity validation in accordance with Section 3.2.

## 3.4 Identification and Authentication for Revocation Request

CHTCA or RA must perform authentication of the certificate revocation request to verify that the applicant has the right to submit the certificate revocation. The authentication procedure for certificate revocation request is the same as the regulations in Section 3.2.

# 4. Certificate Life-cycle Operational Requirements

## 4.1 Certificate Application

### 4.1.1 Who Can Submit a Certificate Application

Either the applicant or an individual authorized to request certificates on behalf of the applicant may submit certificate applications.

### 4.1.2 Enrollment Process and Responsibilities

The certificate application procedures are as follows:

(1) Use the appropriate secure platform to generate an appropriate key pair.

(2) Generate a PKCS#10 CSR using an appropriately tool.

(3) Fill out the information on the certificate application and agrees to a subscriber agreements or other applicable terms and conditions.

(4) Submit the certificate application request (including the CSR, the legal name of the organization or the website FQDN based on the type of the certificate applied for, etc.) and provide relevant identification documents to the RA, where the application information can be in electronic form.

The RA are responsible for ensuring the accuracy of the application request and performing the identification and authentication of the applicant before delivery the request to the issuing CA for issuance.

## 4.2 Certificate Application Processing

### 4.2.1 Performing Identification and Authentication Functions

Upon receipt of the certificate request, CHTCA and RAs shall verify the application information in accordance with Section 3.2. The certificate applicant shall submit correct and complete factual information. The

information required for the certificate application shall contain required and optional information. The information submitted by the certificate applicant and contact records kept by CHTCA and RA during the application process shall be properly kept in a secure, auditable manner in accordance with the ePKI CP and this CPS.

### 4.2.2 Approval or Rejection of Certificate Applications

The verification of the authorization domain name and the basic domain name must comply with the regulations as specified in Section 3.2.5. If all identity authentication work follows relevant regulations and best practices can be successfully implemented, CHTCA may approve the certificate application.

If the various identity authentication works cannot be successfully completed, CHTCA may reject the certificate application. In addition to this reason, CHTCA may refuse to issue certificates for other reasons. CHTCA and its RA may also reject certificate application from applicants who have previously been rejected or have previously violated the subscriber agreements.

A PMA meeting is convened when any CA submits a Subordinate CA certificate or cross-certificate application. The PMA will review the related documents provided by the CAs to evaluate the appropriateness for becoming a subordinate CA or Cross-certified CA of eCA. The PMA may decide that the application enters the next stage, supplemental information is required, or the application is rejected.

### 4.2.3 Time to Process Certificate Applications

CHTCA shall complete the certificate application within a reasonable period. Provided that the information submitted by the applicant is complete and complies with the ePKI CP, this CPS and other checking

requirements, the RAO shall quickly complete the certificate application review. The time needed by RA to process certificate applications and CHTCA to issue the certificates depends on the certificate group and type. These times may be disclosed in the subscriber agreements, contract or on the RA's websites.

Upon receiving the certificate application, the RAO will complete the review process, and the applicant will be asked to accept the certificate. The times when the issuing CA completes the issuance of the certificate are given as follows according to difference certificate types:

| Type of Certificates | Time required for processing and issuance the Certificate |
|---|---|
| Time-stamp Certificates | 5-10 working days |
| S/MIME Certificates | 2 working days |
| AATL Certificates | 2 working days |

Issuance time frames are greatly dependent on when the applicant provides the details and documentation necessary to complete validation or complates the certificate acceptance.

## 4.3 Certificate Issuance

### 4.3.1 CA Actions during Certificate Issuance

eCA cannot automatically issue certificates and shall follow the regulations in Section 5.2.2.

Upon CHTCA receive the certificate application, the relevant review procedures are enforced in accordance with Chapter 3 of this CPS to serve as a basis for determining whether approve the certificate issuance.

Certificate issuance steps are follows:

(1) The RA submits the certificate application passed the review procedures to the issuing CA.

(2) When the issuing CA receives the certificate application

submitted by the RA, the authorization status of the RA is first checked to confirm its authorized assurance level and scope, and then the certificate is issued according to the information of the certificate application submitted by the RA.

(3) If the authorized assurance level and scope of the RA does not comply with the certificate application, the issuing CA will response the error message to the RA and reject the request. If there are any questions, the RA may directly contact the issuing CA to understand where the problem is.

(4) Starting from March 15, 2025, the CA issuing S/MIME certificates provide the function of pre-issuance linting, which can check whether the format of the to-be-signed certificate complies with the requirements of the S/MIME Baseline Requirements. If it does not meet the requirements, it will be rejected to prevent mis-issuance or false of the certificate.

(5) In order to ensure the security, integrity and non-repudiability of the data transmitted between the issuing CA and its RAs, the data of the certificate application is signed with a digital signature and transmitted through the network encrypted by TLS protocol.

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

CHTCA shall notify the subscriber about the certificate issuance during the enrollment process by email or any other equivalent method. The email may contain the certificate itself or a link to download depending upon the workflow of the certificate requested.

## 4.4 Certificate Acceptance

### 4.4.1 Conduct Constituting Certificate Acceptance

Certificates are considered accepted if not revoked by the subscriber within 30 days of issuance. Acceptance of the certificate is deemed as the certificate applicant’s consent to comply with the rights and obligations in this CPS or related contracts.

### 4.4.2 Publication of the Certificate by the CA

CA Certificates are published in the CHTCA repository. End-entity certificates are published by delivering them to the subscriber.

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

RAs, partners, and other entities involved in the enrollment process may be informed of issuance.

## 4.5 Key Pair and Certificate Usage

### 4.5.1 Subscriber Private Key and Certificate Usage

Key pairs of subscribers shall be generated in compliance with Section 6.1.1 of this CPS. Subscribers must be able to control the private keys, which must not be used to issue certificates.

Subscribers shall protect their private keys from unauthorized use or disclosure and shall use their private keys only for the correct key usage (i.e., the policy for key usage specified in the extension of the certificates). Subscribers shall use their certificates in accordance with the ePKI CP and this CPS.

### 4.5.2 Relying Party Public Key and Certificate Usage

When relying parties use a certificate, they shall confirm its certificate usage and use it in accordance with this CPS. Relying parties may only use a tool or a method that is compliant with the ITU-T X.509, IETF RFCs, S/MIME Baseline Requirements or S/MIME Certificate Profile Requirements of Google.

Prior to a certificate’s use, the tool or method selected by relying parties must verify each certificate in the certificate chain, including the accuracy of the content of specific fields, the integrity of the signature, and the validity of the certificate status, where the certificate status may be

obtained from a CRL or an Online Certificate Status Protocol (OCSP) service.

In addition, relying parties shall check the content of the certificate policies extension of the issuing CA and subscriber certificates to confirm the assurance level of the certificates.

## 4.6 Certificate Renewal

CHTCA does not allow renewal of CAs, S/MIME, and time-stamp certificates, where which key pair generation and certificate request submission shall be conducted in the same manner as the initial registration. Only the other subscriber certificates can be renewed.

### 4.6.1 Circumstances for Certificate Renewal

Unrevoked certificates which are about to expire may be renewed under the following circumstances:

(1) The public key listed on the certificate has not reached the usage period stipulated in Section 6.3.2.2.

(2) The subscriber and its attribute information remain consistent.

(3) The private key corresponding to the public key listed on the certificate is still valid and has not been lost or compromised.

### 4.6.2 Who May Request Renewal

The subject of the certificate or an authorized representative whose certificates that are about to expired.

### 4.6.3 Processing Certificate Renewal Requests

The private key is used to sign a signature to the CSR when the subscriber makes a certificate renewal request, and the certificate application file is submitted to the RA. The RA uses the subscriber’s public key to verify the digital signature on the certificate application file to authenticate the subscriber’s identity.

### 4.6.4 Notification of New Certificate Issuance to Subscriber

According to Section 4.3.2, CHTCA shall issue a notification to the subscriber whose certificate has been renewed, to download the renewed certificate. If CHTCA denies the renewal, the reason of denial shall be communicated to the subscriber.

### 4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

As stated in Section 4.4.1.

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

As stated in Section 4.4.2.

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

No stipulation.

## 4.7 Certificate Re-Key

### 4.7.1 Circumstance for Certificate Re-key

Under the following circumstances, the Subordinate CA/Cross-certified CA will renew the key and ask eCA to issue a new subordinate CA/Cross-certified CA certificate:

(1) The lifecycle of currently used keys has ended.

(2) Security issues exist for currently used keys (such as suspected or confirmed key compromise).

Subscribers whose certificates have not expired may request a re-key, and CHTCA shall identify and authenticate them in accordance with Section 3.3.1. After the key pair is re-keyed, CHTCA may revoke the old certificate and does not allow the renewal, modification, or re-key of the old certificate.

### 4.7.2 Who May Request Certification of a New Public Key

The subject of the certificate or an authorized representative.

### 4.7.3 Processing Certificate Re-keying Requests

For subscriber certificate re-keying, CHTCA shall validate the request in accordance with Sections 3.1, 3.2, 3.3, 4.1 and 4.2 and may re-validate the subscriber subject with any previously validated data when needed.

### 4.7.4 Notification of New Certificate Issuance to Subscriber

As stated in Section 4.3.2.

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

As stated in Section 4.4.1.

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

As stated in Section 4.4.2.

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

No stipulation.

## 4.8 Certificate Modification

### 4.8.1 Circumstance for Certificate Modification

CHTCA does not allow modification of S/MIME and time-stamp certificates.

Certificate modification means creating a new certificate for the same subject, where authenticated information that slightly differs from the old certificate (e.g., changes to email address or other relatively attribute information). The new certificate has a new certificate serial number but with the same subject public key and ‘NotAfter’ date. After the certificate

is modified, the old certificate shall be revoked.

### 4.8.2 Who May Request Certificate Modification

The subject of the certificate or an authorized representative.

### 4.8.3 Processing Certificate Modification Requests

(1) The application procedure for certificate modification is as Section 4.2.

(2) If there is any change to the important identity information such as the organization name, individual name or national ID number, the original certificate must be revoked. The subscriber must submit a new certificate application with the modified organization name, individual name, or national ID number to obtain a new certificate.

### 4.8.4 Notification of New Certificate Issuance to Subscriber

As stated in Section 4.3.2.

### 4.8.5 Conduct Constituting Acceptance of Modified Certificate

As stated in Section 4.4.1.

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

As stated in Section 4.4.2.

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

No stipulation.

## 4.9 Certificate Revocation and Suspension

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

## 4.9.1 Circumstances for Revocation

### 4.9.1.1 Circumstances for Revoking a Subscriber Certificate

CHTCA shall revoke a certificate within 24 hours if one or more of the following occurs:

(1) The subscriber requests in writing to the CA that they wish to revoke the certificate;

(2) The subscriber notifies CHTCA that the original certificate request was not authorized and does not retroactively grant authorization;

(3) CHTCA obtains evidence that the subscriber's private key corresponding to the public key in the certificate suffered a key compromise;

(4) CHTCA is made aware of a demonstrated or proven method that can easily compute the subscriber's private key based on the public key in the certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys); or

(5) CHTCA obtains evidence that the validation of domain authorization or control for any FQDN or IP address in the certificate should not be relied upon.

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

(1) The certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6;

(2) CHTCA obtains evidence that the certificate was misused;

(3) CHTCA is made aware that a subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;

(4) CHTCA is made aware of any circumstance indicating that use of a FQDN or email address in the certificate is no longer legally permitted (e.g., a court or arbitrator has revoked a Domain Name

Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);

(5) CHTCA is made aware of a material change in the information contained in the certificate;

(6) CHTCA is made aware that the certificate was not issued in accordance with these requirements or the ePKI CP or this CPS;

(7) CHTCA determines or is made aware that any of the information appearing in the certificate is inaccurate;

(8) CHTCA's right to issue certificates under these requirements expires or is revoked or terminated, unless CHTCA has made arrangements to continue maintaining the CRL/OCSP Repository;

(9) Revocation is required by the ePKI CP and/or this CPS; or

(10) CHTCA is made aware of a demonstrated or proven method that exposes the subscriber's private key to compromise or if there is clear evidence that the specific method used to generate the private key was flawed.

#### 4.9.1.2 Circumstances for Revoking a Subordinate CA Certificate

eCA shall revoke a Subordinate CA certificate within seven (7) days if one or more of the following occurs:

(1) The Subordinate CA requests revocation in writing to eCA;

(2) The Subordinate CA notifies eCA that the original certificate request was not authorized and does not retroactively grant authorization;

(3) eCA obtains evidence that the Subordinate CA's private key corresponding to the public key in the certificate suffered a key compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6;

(4) eCA obtains evidence that the certificate was misused;

(5) eCA is made aware that the certificate was not issued in accordance with or that Subordinate CA has not complied with this document or the applicable CP/CPS;

(6) eCA determines that any of the information appearing in the certificate is inaccurate or misleading;

(7) eCA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the certificate;

(8) eCA's right to issue certificates under these Requirements expires or is revoked or terminated, unless eCA has made arrangements to continue maintaining the CRL/OCSP Repository; or

(9) Revocation is required by the ePKI CP and/or this CPS.

The issuing CA may at its own discretion revoke certificates, including subscriber certificates, Subordinate CA certificates or cross-certificates, under the aforementioned circumstances.

### 4.9.2 Who Can Request Revocation

Subscribers or legally authorized third party (such as judicial or prosecution authorities, the subject of the certificate or an authorized representative, and legal heirs of natural person) can request revocation.

In addition, a subscriber, relying party, application software suppliers or other third party may submit certificate problem report to advise CHTCA a reasonable reason to revoke the certificate. CHTCA shall take actions in accordance with Section 4.9.5 and confirm the validity of the certificate revocation request upon receiving the certificate problem report.

### 4.9.3 Procedure for Revocation Request

(1) The Applicant shall submit the certificate revocation request in accordance with the operation procedures 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 the Applicant's name and contact information, reason for revocation, and time and date of revocation to serve a basis for subsequent accountability;

(2) After the RA completes the review work, the certificate revocation request is sent to CHTCA;

(3) When CHTCA receives the certificate revocation request sent by the RA, CHTCA 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;

(4) If the above checking does not comply with the revocation request, CHTCA will response the error message to the RA and reject the request. If there are any questions, the RA may directly contact CHTCA to understand where the problem is;

(5) In order to ensure the security, integrity and non-repudiability of the data transmitted between CHTCA and its RA, the data of the certificate application is encrypted with a digital signature and transmitted through the network by TLS protocol;

(6) CHTCA uses the same 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; and

(7) CHTCA receives certificate problem reports and provides 24x7 availability of certificate problem response mechanism, as specified in Section 4.9.3.1.

#### 4.9.3.1 Mechanism for Responding the Certificate Problems

Under "the Announcement of CPS" at the repository, CHTCA provides the guidelines for certificate problem reports. Subscribers, relying parties, application software suppliers, and other third parties may submit certificate problem reports through the information specified in Section

1.5.2.2 under the circumstances of the private keys are cracked, the certificates are mis-issued, or the certificates are forged, cracked, abused, or used inappropriately.

### 4.9.4 Revocation Request Grace Period

The certificate revocation request grace period refers to the time to submit a revocation request when the subscriber has confirmed the certificate revocation circumstances. When the subscriber's private key is lost or suspect or known to be compromised, the subscriber shall promptly submit a revocation request to the RA. The revocation request grace period is two working days. CHTCA may extend the revocation grace period when deemed necessary.

If any of the circumstances described in Section 4.9.1 occurs, CAs or RAs shall submit the revocation request within 10 working days.

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

Within 24 hours after receiving a Certificate Problem Report, CHTCA shall investigate the facts and circumstances related to a Certificate Problem Report and provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report.

After reviewing the facts and circumstances, CHTCA shall work with the Subscriber and any entity reporting the Certificate Problem Report or other revocation-related notice to establish whether the certificate will be revoked, and if so, the period from receipt of the Certificate Problem Report or revocation-related notice to published revocation must not exceed the time frame set forth in Section 4.9.1. The date selected by CHTCA shall consider the following criteria:

(1) The nature of the alleged problem (scope, context, severity, magnitude, risk of harm);

(2) The consequences of revocation (direct and collateral impacts to

Subscribers and Relying Parties);

(3) The number of certificate problem reports received about a particular certificate or subscriber;

(4) The entity making the complaint; and

(5) Relevant legislation.

### 4.9.6 Revocation Checking Requirement for Relying Parties

Prior to relying on a certificate, relying parties must verify the accuracy and validity of each certificate in the certificate chain, including checking for the certificate validity, digital signature, issuer/subject name chaining, certificate policies, key usage, and certifciate status, where the certificate status may be checked through a CRL or an OCSP response.

Relying parties must also confirm the validity of the CRL or OCSP response prior to use it, such as verifying the digital signature, checking the validity period, and confirming the issuer/subject name chaining.

### 4.9.7 CRL Issuance Frequency

The CRL issuance frequency of CHTCA is at least twice per day. Issued CRL are valid for no more than 36 hours. Before the CRL expires, CHTCA may issue a new CRL. The new CRL validity period may overlap the validity period of the old CRL. Even though the old CRL has not yet expired, relying parties still may obtain the new CRL from the CHTCA repository to receive the updated certificate revocation information.

### 4.9.8 Maximum Latency for CRLs

Except for eCA has pre-signed of CRLs, after a CRL is produced by other CAs, it will be released immediately.

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

The status information for CHTCA cerificates is availabe via CRLs,

web-based certificate search/download function, and OCSP services.

CHTCA uses an OCSP responder to provide OCSP responses complying with RFC 6960 and RFC 5019, where the OCSP responses are signed by the OCSP responder using a 2048-bit or greater RSA key (that modulus size in bits is divisible by 8) and a hash algorithm at least as strong as SHA-256. In addition, the OCSP responder also provides OCSP responder certificates, which are issued by CHTCA and contain the extension of type id-pkix-ocsp-nocheck, as defined by RFC 6960.

### 4.9.10 On-line Revocation Checking Requirements

Relying parties must confirm the validity of a certificate in accordance with Section 4.9.6 before using it.

CHTCA provides an OCSP service that an OCSP responder operated under the service supports the HTTP-based POST and GET methods, as described in RFC 6960 and RFC 5019. The certificate status information provided by the service shall meet the following requirements:

(1) For status of subscriber certificates: an authoritative OCSP response MUST be available (i.e. the responder MUST NOT respond with the “unknown” status) starting no more than 15 minutes after the certificate is first published or otherwise made available. CHTCA updates an OCSP response prior to one-half of the validity period before the nextUpdate, and the validity interval of the OCSP response is greater than or equal to 8 hours and less than 16 hours.

(2) For status of self-issued certificates, subordinate CA certificates, and cross-certificates: CHTCA updates the information at least every twelve months and within 24 hours after any of these certificates is revoked.

A certificate serial number within an OCSP request is either:

(1) “assigned” if a certificate with that serial number has been issued

by CHTCA; or

(2) “unassigned” if neither of the previous conditions is met.

If the OCSP responder receives a request for the status of a certificate serial number that is “unassigned”, then the responder should not respond with a “good” status.

### 4.9.11 Other Forms of Revocation Advertisements Available

No Stipulation.

### 4.9.12 Special Requirements Related to Key Compromise

In case of a compromise of the subscriber’s private key, the subscriber must immediately notify CHTCA of the event. CHTCA will revoke the concerned certificate (choose the reason for the revocation as ‘key compromised’) according to the procedures set forth in Sections 4.9.1, 4.9.2 and 4.9.3 of this CPS, and publish a CRL to inform relying parties that the certificate can no longer be trusted.

The acceptable methods used by third parties as proof of key compromise are as follows:

(1) Confirming the third party’s possession of the private key by signing a challenge provided by CHTCA using the compromised private key; or

(2) Submitting the private key itself.

### 4.9.13 Circumstances for Suspension

CHTCA does not allow suspension of S/MIME and time-stamp certificates (i.e., Sections 4.9.13 to 4.9.17 are not applicable).

In addition, CHTCA may suspend the certificate under the following circumstances without advance permission from the subscriber:

(1) The subscriber is ordered to suspend operations.

(2) Notification in accordance with subscriber registered authority or the industry competent authority.

(3) Notification in accordance with judicial, supervisory or law enforcement agencies.

### 4.9.14 Who Can Request Suspension

The following two groups may apply for certificate suspension:

(1) The subscriber whose certificate is to be suspended.

(2) The subscriber registered authority or industry competent authority.

### 4.9.15 Procedure for Suspension Request

Subscribers submit the request. After the RA examines the application for accuracy and errors, a digital signature is affixed, and the information is transmitted to CHTCA. CHTCA then immediately suspends the certificate or may refuse the certificate suspension request if the review fail or for other reasons.

### 4.9.16 Limits on Suspension Period

After the subscriber submits the certificate suspension request, the RA shall promptly complete the review procedure within one working day. After passing review, CHTCA shall complete the certificate suspension within one working day.

When making a certificate suspension request, the subscriber does not need to state the suspension period required. The longest certificate suspension period set by CHTCA is the period from the request approval time to the expiry date of that certificate.

If the subscriber cancels the certificate suspension during the suspension period, the status of the certificate would become ‘valid’.

### 4.9.17 Procedure for Certificate Resumption

The subscriber submits the request. After the RA examines the application for accuracy and errors and the period of the suspended certificate has not expired, a digital signature is affixed, and the information is transmitted to CHTCA. CHTCA then immediately resumes use of the certificate or may refuse the certificate resume request if the review fail or for other reasons.

## 4.10 Certificate Status Services

### 4.10.1 Operational Characteristics

CHTCA provides CRLs and OCSP services. Revocation entries on a CRL or OCSP response must not be removed until after the expiry date of the revoked certificate. If a revocation entry contains the information of a suspended certificate, the entry can only be removed after the certificate has been resumed or expired.

### 4.10.2 Service Availability

CHTCA operates and maintains its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

CHTCA maintains an online 24x7 repository that application software can use to automatically check the current status of all unexpired certificates issued by CHTCA.

CHTCA maintains a continuous 24x7 ability to respond internally to a high-priority certificate problem report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a certificate that is the subject of such a complaint.

### 4.10.3 Optional Features

No stipulation.

## 4.11 End of Subscription

End of subscription signifies that subscriber stop using CHTCA's services. CHTCA allows subscribers to end their subscription to certificate services by having their certificate revoked or by allowing the certificate or applicable Subscriber Agreement to expire without renewal.

## 4.12 Key Escrow and Recovery

### 4.12.1 Key Escrow and Recovery Policy and Practices

CHTCA's private signing keys shall not be escrowed, but subscriber's private signing keys may be escrowed.

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

CHTCA does not currently support session key encapsulation and recovery.

# 5. Facility, Management, and Operation Controls

## 5.1 Physical Controls

### 5.1.1 Site Location and Construction

The CHTCA facility is located in the Chunghwa Telecom Information Technology Group. 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 CHTCA equipment.

### 5.1.2 Physical Access

CHTCA has established suitable measures to control connections to the hardware, software and hardware security module that serves to CHTCA.

The CHTCA 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 a card access control system. On the fourth level, a fingerprint recognition control system is used to control access for facility personnel. The fingerprint scanner uses 3D sampling technology which is capable of detecting whether the fingerprint is from a live object by fingerprint depth and color.

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 CHTCA system.

Non-CHTCA personnel entering the facility are required to sign the entry/exit log and must be accompanied throughout by CHTCA personnel.

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

(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 CHTCA facility is equipped with a generator (with enough fuel for six days of continuous operation) and an uninterrupted power system (UPS). 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 CHTCA facility has a constant temperature and humidity system to provide an optimal operation environment for the facility.

### 5.1.4 Water Exposures

The CHTCA 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 CHTCA 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 an off-site location.

### 5.1.7 Waste Disposal

When the documents of CHTCA detailed in Section 9.3.1 are no longer in use, it shall be shredded by the paper shredder. Any storage media that CHTCA used shall be formatted to erase the information stored on it before scrapping, and discs shall be physically destroyed.

### 5.1.8 Off-site Backup

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

## 5.2 Procedural Controls

In order to ensure that system procedures have a suitable assurance level, CHTCA uses procedural controls to specify the trusted roles of CHTCA 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 make appropriate segmentation and assignment of the responsibility for performing system-related operations, to prevent someone from maliciously using the CA system without being noticed, the trusted role authorized to perform each system access task is clearly defined in CHTCA.

The seven PKI personnel roles assigned by CHTCA are administrator, CA officer, internal auditor, system 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 CHTCA system
- Creation and maintenance of system user accounts
- Generation and backup of CHTCA keys
- Activation / deactivation of related keys of certificate manager
- System hardware and software updates
- System backup and recovery
- Website maintenance
- Patching the system vulnerabilities

The CA officer is responsible for:

- Generation and backup of CHTCA keys
- Activation / deactivation of keys for certificate issuance
- Activation / deactivation of keys for certificate revocation
- Activation / deactivation of keys for CRL issuance

The internal auditor is responsible for:

- Generation and backup of CHTCA keys
- Checking, maintenance and archiving of audit logs
- Conducting or supervising internal audits to ensure CHTCA is operating in accordance with this CPS
- Patching the anti-virus and vulnerabilities of audit system

The system operator is responsible for:

- Archiving of audit logs
- Daily operation and maintenance of system equipment
- Storage media updating
- Set up protection mechanisms for system security and threats of virus or malware

The physical security controller is responsible for:

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

The cyber security coordinator is responsible for:

- Maintenance of the network and network facilities
- Patches management for the vulnerabilities of the network facilities
- The network security of CHTCA
- The detection and report of the network security events

The anti-virus and anti-hacking coordinator is responsible for:

- Researching, applying, or providing the anti-virus, anti-hacking, 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 or the cyber security coordinator for patches management

### 5.2.2 Number of Persons Required per Task

In accordance with security requirements, the number of persons

required for each trusted role is as follows:

- Administrator

  At least 3 qualified individuals are needed.

- CA Officer

  At least 3 qualified individuals are needed.

- Internal Auditor

  At least 2 qualified individuals are needed.

- System Operator

  At least 2 qualified individuals are needed.

- Physical security controller

  At least 2 qualified individuals are needed.

- Cyber security coordinator

  At least 1 qualified individual.

- Anti-virus and anti-hacking coordinator

  At least 1 qualified individual.

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

| Assignments | Administrator | CA Officer | Internal Auditor | System Operator | Physical security controller | Cyber security coordinator | Anti-virus and anti-hacking coordinator |
|---|---|---|---|---|---|---|---|
| Installation, configuration, and maintenance of the CHTCA system | 2 | | | | 1 | | |
| Establishment and maintenance of system user accounts | 2 | | | | 1 | | |
| Generation and backup of CHTCA keys | 2 | 2 | 1 | | 1 | | |
| Activation / deactivation of certificate issuance, certificate revocation and CRL issuance | 2 | 2 | | | 1 | | |

| Assignments | Administrator | CA Officer | Internal Auditor | System Operator | Physical security controller | Cyber security coordinator | Anti-virus and anti-hacking coordinator |
|---|---|---|---|---|---|---|---|
| Checking, maintenance and archiving of audit logs | | | 1 | 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 CHTCA system | 1 | | | | 1 | | |
| Website maintenance | 1 | | | | 1 | | |
| Daily operation and maintenance of the network and network facilities | | | | 1 | 1 | 1 | |
| Patching the vulnerabilities of the network facilities | 1 | | | | 1 | 1 | |
| Reporting the threats and vulnerabilities of computer virus | | | | | | | 1 |
| Patching the anti-virus and vulnerabilities (audit system) | 1 | | 1 | 1 | 1 | | |
| Patching the anti-virus and vulnerabilities (systems other than the audit system) | 1 | | | 1 | 1 | | |

### 5.2.3 Identification and Authentication for Each Role

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

CHTCA utilizes user accounts, passwords, and groups for system account management and IC card to identify and authenticate administrator, CA officer, internal auditor and system operator. CHTCA utilizes the authority setting function of the central access control system to identify

and authenticate physical security controllers.

CHTCA utilizes user accounts, passwords, and groups for system account management, 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:

- Administrator, CA officer, internal auditor, and cyber security coordinator cannot assume any other roles among these four trust roles at the same time, but administrator, CA officer, and internal auditor can be system operator at the same time;
- Physical security controller shall not concurrently assume any role of administrator, CA officer, internal auditor, and system operator; and
- A person serving a trusted role is not allowed to perform self-audit.

## 5.3 Personnel Controls

### 5.3.1 Qualifications, Experience, and Clearance Requirements

(1) Security evaluation for personnel selection

Personnel selection includes the following items:

(a) Personality evaluation;

(b) Applicant experience evaluation;

(c) Academic and professional skills and qualifications evaluation;

(d) Personal identity check; and

(e) Evaluation of personnel conduct.

(2) Management of Personnel Evaluation

All CHTCA 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 CHTCA stating that personnel may not disclose business secrets verbally or by photocopy, loan, delivery, publishing or other methods.

### 5.3.2 Background Check Procedures

CHTCA shall check the related identify and qualification documents for authenticity for those personnel performing the trusted roles defined in Section 5.2 at the initial time of employment.

### 5.3.3 Training Requirements

| Trusted Role | Training Requirements |
|---|---|
| Administrator | (1) CHTCA security principles and mechanism.<br>(2) Installation, configuration, and maintenance of the CHTCA operation procedures.<br>(3) The use and operation procedures of CHTCA system software and hardware.<br>(4) Establishment and maintenance of system user accounts operation |

| Trusted Role | Training Requirements |
|---|---|
| | procedures.<br>(5) Audit parameter configuration setting procedures.<br>(6) CHTCA key generation and backup operation procedures.<br>(7) Disaster recovery and continuous operation procedure. |
| CA Officer | (1) CHTCA security principles and mechanism.<br>(2) CHTCA key generation and backup operation procedures.<br>(3) Activation/deactivation of certification issuance operation procedure.<br>(4) Activation/ deactivation of certification revocation operation procedure.<br>(5) Activation/ deactivation of certificate CRL issuance operation.<br>(6) Disaster recovery and continuous operation procedure. |
| Internal Auditor | (1) CHTCA security principles and mechanism.<br>(2) The use and operation procedures of CHTCA audit Server.<br>(3) CHTCA key generation and backup operation procedures.<br>(4) Audit log check, maintain and archiving procedures.<br>(5) Disaster recovery and continuous operation procedure. |
| System Operator | (1) Daily operation and maintenance procedures for system equipment.<br>(2) Upgrading of storage media procedure.<br>(3) Disaster recovery and continuous operation procedure.<br>(4) Network and website maintenance procedure. |
| Physical security controller | (1) Physical access authorization setting procedure.<br>(2) Disaster recovery and continuous operation procedure. |
| Cyber security coordinator | (1) Network and network facilities maintain procedure.<br>(2) Security mechanism for the network. |
| Anti-virus and anti-hacking coordinator | (1) Prevention to the threats and vulnerabilities of computer virus.<br>(2) Security mechanism for the operating system and the network. |

### 5.3.4 Retraining Frequency and Requirements

In case of software/hardware upgrades, working procedures changed, equipment replaced, or relevant regulations changed, relevant personnel will be arranged for retraining and the training situation will be recorded, so as to make the personnel understand the changes in relevant operating procedures and regulations.

### 5.3.5 Job Rotation Frequency and Sequence

(1) May not concurrently serve trusted roles. May not receive work reassignments.

(2) Personnel with a full two years of experience as a system operators, cyber security coordinator, or anti-virus and anti-hacking coordinator with the requisite training and review may be reassigned to the position of administrator, CA officer or internal auditor.

(3) Administrator, CA officer and internal auditor may be reassigned to the position of administrator, CA officer or internal auditor after they have been transferred from their original positions for one full year.

### 5.3.6 Sanctions for Unauthorized Actions

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

### 5.3.7 Independent Contractor Requirements

The duties, sanctions for unauthorized actions and required training documents of independent contractor serving a trusted role shall meet the requirements of Section 5.3 and the event logging and document retention shall meet the requirements of Section 5.4.1.

### 5.3.8 Documentation Supplied to Personnel

CHTCA shall make available to related personnel relevant documentation pertaining to the ePKI CP, this CPS, CHTCA system operation manuals, the Electronic Signatures Act and its enforcement rules.

## 5.4 Audit Logging Procedures

CHTCA shall keep security audit logs for all events related to CHTCA 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 in accordance with the archive retention regulations stated in Section 5.5.2.

### 5.4.1 Types of Events Recorded

(1) Key generation
- Key generation of CAs

(2) Private key loading and storage
- Loading the private key into a system component.
- All access to private keys kept by CHTCA for key recovery work.

(3) Certificate registration
- Certificate registration request process.

(4) Certificate revocation
- Certificate revocation request process.

(5) Account administration
- Add or delete roles and users.
- User account 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

CHTCA shall routinely review audit logs to prevent possible malicious activity, and any significant operations should be further reviewed. Review work includes examining all log entries and conducting a final complete check for any warnings or anomalies. Audit checking results shall be documented.

### 5.4.3 Retention Period for Audit Log

Audit logs shall be retained on-site for two months, and the log retention management system shall be operated in accordance with Sections 5.4.4, 5.4.5, 5.4.6 and 5.5.

If the retention period of the audit record file expires, the auditor is responsible for removing the data and cannot be behalfed by other personnel.

### 5.4.4 Protection of Audit Log

Signature and encryption technology shall be used to protect the current and archived audit logs. A CD-R or other media storage that cannot change the audit logs is used, and only authorized personnels can access.

CHTCA's audit system enforces resource control and identity identification security mechanisms, only authorized auditor has backup and read access to logs, and the system keeps a log file of access audit records to detect and prevent improper access.

### 5.4.5 Audit Log Backup Procedures

(1) CHTCA shall routinely archive event logs, and electronic audit logs are backed up at least once a month.
(2) At least one copy of the media for storing audit records shall be kept at an off-site location with proper security control measures.

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

Audit systems are built in the CHTCA system, and audit procedures are activated when the CHTCA system is activated and only stops when the CHTCA system is shut down.

If the automated audit system cannot operate normally, CHTCA shall suspend certificate issuance services until the issue is resolved before resuming service again to protect system information integrity and confidentiality when the security system is in a high-risk status.

### 5.4.7 Notification to Event-causing Subject

Where an event is logged by the audit system, the audit system does not need to notify the entity which caused the event.

### 5.4.8 Vulnerability Assessments

PublicCA should perform a vulnerability assessment when identifying significant changes to a network or system. PublicCA also must conduct penetration testing after it is determined that there is a significant upgrade or modification to the application program or infrastructure. CHTCA shall implement the enhancement and correction measures after the penetration testing and the vulnerability assessment. CHTCA shall record the skills, tools, followed ethics, competitive relations and independence guidelines for those personnel or groups capable of implementing reliable vulnerability scans, penetration testing, or information security diagnosis or security surveillance.

## 5.5 Records Archival

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

(1) Important tracking records regarding CHTCA's own key pair

generation, storage, backup, and re-key.

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

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 Records Archived

CHTCA retains the following information in its archives:

(1) CHTCA 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) CHTCA re-key records.
(11) Issued or announced CRLs.
(12) Audit logs.
(13) Other data or application programs used to verify and corroborate the archived content.
(14) Documents required by the auditor.

### 5.5.2 Retention Period for Archive

CHTCA retains archived data for at least 2 years. The application

programs used to process archived data are retained for 10 years.

### 5.5.3 Protection of Archive

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

(2) The archived data can be moved to another storage medium after pass through the CHTCA authorized procedures.

(3) The archived data is stored in a secure, protected location.

### 5.5.4 Archive Backup Procedures

CHTCA 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 authorized CHTCA personnel.

### 5.5.5 Requirements for Time-stamping of Records

All CHTCA 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 with calibrated system time. 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 Collection System (Internal or External)

There is currently no archive collection system.

### 5.5.7 Procedures to Obtain and Verify Archive Information

Only authorized CHTCA personnel are allowed to access the archive.

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

verified for written documents.

## 5.6 Key Changeover

CHTCA shall periodically change its private keys in accordance with Section 6.3.2 and shall change its key pair before the usage period of its private key issuing subscriber certificates has expired. After key changeover of Subordinate CAs, an application for a new CA certificate shall be submitted to eCA is required and the new CA certificate shall be published in the CHTCA repository.

After key changeover of eCA, eCA shall sign a new self-signed certificate (by using the new private key) and mutually sign a new self-issued certificate (by using the new and old private keys, separately). The new self-signed certificate shall be delivered to relying parties in accordance with Section 6.1.4 while the new self-issued certificates shall be published in the eCA repository.

CHTCA shall still maintain and protect its old private keys and shall make the old certificate available to verify CRL or OCSP until all of the subscriber certificates signed with the private key have expired.

If CHTCA's certificate has been revoked, CHTCA shall stop using its private keys and shall change its key pairs.

## 5.7 Compromise and Disaster Recovery

### 5.7.1 Incident and Compromise Handling Procedures

CHTCA establishes incident and compromise reporting and handling procedures and conducts drills annually.

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

CHTCA establishes recovery procedures in the event of computing

resource, software and data corruption and conducts annual drills.

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

### 5.7.3 Entity Private Key Compromise Procedures

CHTCA implements the following recovery procedure in the event of signature key compromise:

(1) Publish in the repository and notify subscribers and relying parties about the event of key compromise.
(2) Revoke the CHTCA signature key certificate and issued subscriber certificates.
(3) Generate new key pairs in accordance with the procedures in Section 5.6 and the new certificates are published in the CHTCA repository.

CHTCA shall conduct the drills of CA private key compromise at least once a year.

### 5.7.4 Business Continuity Capabilities after a Disaster

CHTCA has established a disaster recovery procedure and conducts drills each year. In the event of a disaster, the emergency response team shall initiate the disaster recovery procedure. Priority shall be given to restoring the CHTCA repository operations and quickly reestablishing certificate issuance and management capabilities.

## 5.8 CA or RA Termination

CHTCA shall follow CA service termination procedures in accordance with related regulations in the Electronic Signatures Act during

service termination. CHTCA shall follow the item below to ensure the rights of subscribers and relying parties:

(1) CHTCA shall notify the competent authority, Ministry of Digital Affairs, and subscribers 30 days prior to of the scheduled termination of service.

(2) CHTCA 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 CHTCA 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, CHTCA shall revoke the still valid certificates, publish the revoked certificates in the repository and notify all certificate-related persons 30 days prior to the scheduled termination of service. CHTCA will refund the certificate issuance and renewal fees based on the propotion of the certificate validity.
- The competent authorities, if necessary, may publish the certificates which are still valid at the time of revocation.

In case that the RA terminates the service, CHTCA shall stop its rights of review actions.

# 6. Technical Security Controls

This chapter describes the technical security controls implemented by PublicCA.

## 6.1 Key Pair Generation and Installation

### 6.1.1 Key Pair Generation

According to the regulations in Section 6.2.2, CHTCA generates key pairs within the hardware security module by using the algorithm and the procedures that meets NIST FIPS 140-2 standard. If the token used by the subscriber is an IC chip, the key pair is generated by the card management center on behalf of the subscriber; for other types of certificates, subscribers must generate their key pairs with the hardware security module set forth in Section 6.2.1.

CHTCA 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 PMA and/or the qualified auditors.

### 6.1.2 Private Keys Delivery to Subscriber

CHTCA should not generate key pairs of Subordinate CA certificates on behalf of the subscriber.

If the card management center generates a key pair for subscriber, the RA shall deliver the token (such as IC card) containing the subscriber key to the subscriber after certificate issuance by CHTCA.

### 6.1.3 Public Key Delivery to Certificate Issuer

If the card management center generates a key pair for a subscriber, the RA shall deliver the subscriber public key to CHTCA via secure channels.

If a subscriber self-generates a key pair, the subscriber shall deliver the public key to the RA via a CSR file with PKCS# 10 format. The RA shall delivery the public key to CHTCA 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 Chapter are the use of TLS or other equivalent or higher-level data encryption transmission protocols.

### 6.1.4 CA Public Key Delivery to Relying Parties

Commercial web browsers and platform operators are encouraged to embed Root Certificate Public Keys of CHTCA into their root stores and operating systems. CHTCA shall deliver the certificates containing the certificate chain of relevant CAs to the subscriber after certificate issuance. Relying parties can also download the public key certificates of the relevant CAs through the repository operated by CHTCA. Excepet for eCA, CHTCA notes the download location of the relevant public key certificates in the certificate chain through the Authority Information Access (AIA) extension of the issued certificate.

### 6.1.5 Key Sizes

CHTCA complies with the regulations of the ePKI CP in using key sizes, as described below:

(1) Root CAs shall use 4096-bit RSA keys with the SHA-256, SHA-384, or SHA-512 hash algorithm to issues certificates.

(2) Subordinate CAs and cross-certified CAs shall choose RSA keys with the modulus size of at least 2048 bits or ECDSA keys with a valid point on the NIST P-256/NIST P-384 elliptic curve. The hash algorithm required to issue certificates depends on the aforementioned CAs' key algorithm:

- RSA keys: SHA-256, SHA-384, or SHA-512.

- ECDSA keys: SHA-256 (with the P-256 curve) or SHA-384 (with the P-384 curve).

(3) Subscribers shall use RSA keys with the modulus size of at least 2048 bits or ECDSA keys with a valid point on the NIST P-256/NIST P-384 elliptic curve.

(4) The modulus size of the aforementioned RSA key (in bits) must be divisible by 8.

### 6.1.6 Public Key Parameters Generation and Quality Checking

The public key parameter of the RSA algorithm is null.

CHTCA shall use the ANSI X9.31 algorithm or the NIST FIPS 186-4 standard to generate the prime number needed for the RSA algorithm if a RSA key pair is selected and ensure that the prime number is a strong prime.

Cross-certified CAs must perform appropriate key parameter quality checking according to the selected algorithm.

There is no need to guarantee that the prime number, which is needed for the RSA algorithm, is a strong prime when a subscriber generates an RSA key pairs within the IC card or other software/hardware security modules. However, the key must pass a weak key check before it is allowed to be used for the certificate issuance.

According to Section 5.3.3 of NIST SP 800-89, CHTCA confirms that the value of the public exponent used by the RSA algorithm is an odd number greater than 3 and is in the range between $2^{16}+1$ and $2^{256}-1$. Furthermore, the modulus should also meet the following characteristics: an odd number, not the power of a prime, and have no factors smaller than 752.

In addition, CHTCA confirms the validity of all ECDSA keys using either the Elliptic Curve Cryptography (ECC) Full Public Key Validation Routine or the ECC Partial Public Key Validation Routine in accordance with NIST SP 800-56A Revision 3.

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

### 6.1.7.1 Key Usage Purposes of CAs

The private key corresponding to eCA's self-signed certificate can only be used for issuing self-signed certificates, self-issued certificates, subordinate CA certificates, cross-certificates, CRLs, OCSP responder certificates, or OCSP responses.

From the second generation of eCA, the self-signed certificates include a key usage extension. The content of the key usage and extended key usage extentions in the self-signed certificates and other certificates (including self-issued certificates, subordinate CA certificates, and cross-certificates) issued by eCA shall meet the requirements of Section 7.1.2.

### 6.1.7.2 Key Usage Purposes of Subscribers

The key usage purpose of subscribers is described as follows according to the type of certificates:

(1) S/MIME Certificates

The keyUsage extension of S/MIME certificates must have key usage bit(s) set: digitalSignature and/or nonRepudiation, where the dataEncipherment and/or keyEncipherment bit(s) may be set, and others must not be set. The extKeyUsage extension must include the value id-kp-emailProtection, where the values id-kp-serverAuth, id-kp-codeSigning, id-kp-timeStamping, and anyExtendedKeyUsage must not be set.

(2) Time-stamp Certificate

The keyUsage extension of time-stamp certificates has two key usage bits set: digitalSignature and contentCommitment. The extKeyUsage extension contains the value id-kp-timeStamping.

(3) Other Certificates

When the token used by the subscriber is an IC card or a USB token consolidating IC card and card reader, the token contains two certificates, where the key usage bit set in the key usage extension

of the two certificates are keyEncipherment and digitalSignature, respectively.

When the token used by the subscriber is not an IC card or a USB token, the keyUsage extension of a certificate included in the token may have two key usage bits set: keyEncipherment and digitalSignature.

For the dedicated server application software certificates, they can be further categorized into the following three types:

(1) E-mail type: The rule of the critical keyUsage extension shall be (digitalSignature | keyEncipherment | dataEncipherment), and the extKeyUsage extension shall only contain the value id-kp-emailProtection. Besides, the entry in the subjectAltName extension shall be stored using type rfc822Name.

(2) Other type: The rule of the critical keyUsage extension shall be (digitalSignature | keyEncipherment | dataEncipherment | nonRepudiation), and the extKeyUsage extension shall only contain the values id-kp-clientAuth and id-cht-ePKI-kp-dedicated (1.3.6.1.4.1.23459.100.1.1), where the latter is defined by CHTCA. In addition, it does not have a subjectAltName extension.

For PDF Signing certificates issued by subordinate CAs of CHTCA, the combination of keyUsage and extKeyUsage extensions complies with the AATL technical requirements.

## 6.2 Private Key Protection and Cryptographic Module Engineering Controls

### 6.2.1 Cryptographic Module Standards and Controls

CHTCA uses FIPS 140-2 Level 3 certified hardware security modules. Storage media for subscriber key pairs may be:

| Storage Media | Certified Standard |
|---|---|
| Chip | FIPS 140-2 Level 2, ISO 15408 or Common Criteria EAL 4+ (or higher) |

| | |
|---|---|
| Hardware Security Module (HSM) | FIPS 140-2 Level 3 or other level with equivalent security strength |
| Other Tokens (e.g. Software) | None |

Storage media for the private key corresponding to the Adobe PDF Signing certificate shall be a chip or a HSM validated by FIPS 140-2 Level 2 or equivalent security strength.

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

CHTCA's private keys are controlled in accordance with the multi-person control process specified in the ePKI CP, and this process can be used as the activation and deactivation methods for private keys as well as the backup and recovery methods for private key splitting.

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

### 6.2.3 Private Key Escrow

CHTCA does not escrow its private signing keys. CHTCA may provide private key escrow services for subscribers in order to provide the application of cloud signing.

### 6.2.4 Private Key Backup

Backups of CHTCA private keys are made according to private key multi-person control set forth in Section 6.2.2, and high-security IC cards are used as the storage media for secret sharing. CHTCA does not provide additional private key backup services.

### 6.2.5 Private Key Archival

The private signing keys of CHTCA shall not be archived, and CHTCA does not perform archival of subscribers' private signing keys.

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

Private keys are allowed to be exported from the cryptographic module into backup tokens or imported from backup tokens into the cryptographic module only during key backup/recovery or cryptographic module replacement. The private keys mentioned in the previous process are controlled complying with the requirements of Section 6.2.2. The private keys are encrypted or split when transferred out of the module or transported between cryptographic modules and never exist in plaintext form. After the private keys are imported, the related secret parameters generated during the transport process must be completely destroyed.

If CHTCA becomes aware that its subordinate CA's or cross-certified CA's private key has been communicated to an unauthorized person or an organization not affiliated with the subordinate CA or cross-certified CA, then eCA will revoke all certificates that include the public key corresponding to the communicated private key.

### 6.2.7 Private Key Storage on Cryptographic Module

As stated in Sections 6.1.1 and 6.2.1. When not in use, the hardware security module must be taken offline and stored in the location specified in Section 5.1.1.

### 6.2.8 Method of Activating Private Key

CHTCA private key activation is controlled by multi-person controls of the different usage IC cards kept by administrator and CA 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 follows:

(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 proxy mail server, the subscriber should self-trust and escrow its private key onto the server, and the activation method of the private key is controlled by the proxy mail server.

(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

When the private keys of CHTCA is not in use, an appropriate deactivation method will be selected to deactivate the private keys in compliance with ePKI CP. CHTCA does not provide the deactivate services of subscribe private keys.

### 6.2.10 Method of Destroying Private Key

In order to prevent the theft of CHTCA private keys which could endanger the authenticity of the entire certificate, the private key must be destroyed at the end of the CHTCA key lifecycle. Therefore, when CHTCA completes the key renewal and eCA issues a new CHTCA certificate, after no additional certificates or CRL are issued, zeroization is done on the old CHTCA private key stored inside the hardware security module to ensure that the old CHTCA private key is destroyed. In addition to destroying the old CHTCA private key in the hardware security module, physical destruction of the splitted IC cards with a backed-up key inside shall be done as well during the CHTCA key renewal.

If services are permanently not provided by a cryptographic module but it is still accessible, all private keys (already used or possibly used)

stored in that cryptographic module must be destroyed. After destroying the keys, the key management tools provided by this cryptographic module must be used to verify that the above keys no longer exist.

Subordinate CAs and cross-certified CAs must follow the ePKI CP regulations when choosing an appropriate private key destruction method. The destruction method for subscriber private keys is not stipulated.

### 6.2.11. Cryptographic Module Rating

See Section 6.2.1.

## 6.3 Other Aspects of Key Pair Management

### 6.3.1 Public Key Archival

CHTCA archives certificates issued by it in accordance with Section 5.5.

### 6.3.2 Certificate Operational Periods and Key Pair Usage Periods

#### 6.3.2.1 CA Certificate Operational Periods and Key Pair Usage Periods

Certificates and private keys of CHTCA's issuing CAs have maximum validity periods of:

| Type of CA | Private Key Usage | Certificate Term |
|---|---|---|
| Root CA | ■ Issuing self-signed certificates: 15 years<br>■ Issuing self-issued certificates: no stipulation<br>■ Issuing cross-certificates: no stipulation<br>■ Issuing subordinate CA certificates: 15 years<br>■ Issuing CRLs, OCSP responder certificates or OCSP responses: 30 years | 30 years |

| | | |
|---|---|---|
| Subordinate CA | ■ Issuing subscriber certificates: 10 years<br>■ Issuing CRLs, OCSP responder certificates or OCSP responses: 20 years | 20 years |

The expiry date of subordinate CA certificates or cross-certificates issued by eCA must not be greater than the end of eCA's self-signed certificate's validity period.

The expiry date of eCA's self-issued certificates cross-signed with old and new eCA keys shall be equal to the expiry date of eCA's self-signed certificate issued with the old eCA key.

After the expiration of the certificate issuance validity period of the issuing CA's private signing key, the issuing CA shall continue to provide CRLs, OCSP responder certificates, or OCSP responses until all issued certificates have expired.

The validity period for private keys and certificates of an OCSP responder is 36 hours. An OCSP response signed by the OCSP reponder's private key includes the signature and the OCSP responder certifcate that can be used by relying parties to verify the signature of the OCSP response.

#### 6.3.2.2 Subscriber Certificate Operational Periods and Key Pair Usage Periods

The maximum validity periods of the subscriber certificate and private key are:

| Type of Cert. | Private Key Usage Period | Maximum Validity Period |
|---|---|---|
| Strict & Multipurpose S/MIME Certificate | No stipulation | 825 days |
| Legacy S/MIME Certificate | No stipulation | 1185 days |
| S/MIME Certificate | No stipulation | Less than 27 months |
| Time-stamp Certificate | 15 months | 135 months |
| Other Certificate | 10 years | 10 years |

## 6.4 Activation Data

### 6.4.1 Activation Data Generation and Installation

The activation data of CHTCA's private key is randomly generated and written to the hardware cryptographic module after completing identity verification for administrators of n-out-of-m control IC cards based on the access control list set during the generation of the afforementioned private key. Administrators must insert their n-out-of-m control IC cards into the card reader built in the hardware cryptographic module and enter the correct personal identification number (PIN) of IC cards when performing identity verification as mentioned above.

### 6.4.2 Activation Data Protection

Activation data is protected by the n-out-of-m control IC cards. Administrators who hold the IC cards are responsible for the safekeeping of the card PIN, which shall not be stored in any media. If the administrator enters the wrong PIN for more than 3 consecutive times, the IC card is locked. During IC card handover, a new PIN is set by the new administrator.

### 6.4.3 Other Aspects of Activation Data

No stipulation.

## 6.5 Computer Security Controls

### 6.5.1 Specific Computer Security Technical Requirements

CHTCA 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, and

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

The CHTCA equipment is established on work platforms which have undergone a security assessment and the CA-related systems (hardware, software, operating system) must be operated with configurations which have undergone a security assessment. CHTCA enforces multi-factor authentication for all accounts capable of directly causing certificate issuance.

### 6.5.2 Computer Security Rating

CHTCA servers use Common Criteria EAL 3 or above certified computer operating systems.

## 6.6 Life Cycle Technical Controls

### 6.6.1 System Development Controls

CHTCA follows established software engineering methodologies for system development and quality control.

System development, test and production environments shall operate independently to prevent unauthorized access or changes. In addition, CHTCA may only use dedicated and authorized hardware and software.

For RA hardware and software, it must check for malicious code before the first use or version update and perform a security scan periodically.

For each product or program delivered to CHTCA, it is required to provide the delivery list, test report, and source code analysis report, as well as be under version control.

### 6.6.2 Security Management Controls

CHTCA shall not install software, hardware or components that are not related to its operation. When installing software onto a CA system, CHTCA shall first confirm the integrity and correctness of the version and check the integrity of CA software regularly or before each use. In addition, CHTCA documents and controls any change to the system as well as detecting unauthorized modifications to system software or configurations.

CHTCA references the methodologies and standards in the ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, ISO/IEC 31000, WebTrust Principles and Criteria for Certification Authorities, and Network and Certificate System Security Requirements for risk assessment, risk management, and security management and control measures.

### 6.6.3 Life Cycle Security Controls

CHTCA shall conduct a risk assessment at least once a year to determine if there is any risk of compromise for existing keys.

## 6.7 Network Security Controls

CHTCA implements network security control measures in compliance with the Network and Certificate System Security Requirements.

The CHTCA host and repository have firewalls and are connected to external networks. The repository is placed in the external service area of the firewall (de-militarized zone, DMZ) 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 CHTCA are digitally signed and transmitted to the repository. The CHTCA repository protects against

denial of service and intrusion attacks by system patch updates, system vulnerability scans, intrusion defending/detection systems, firewall systems and filtering routers.

CHTCA monitors the configuration of access control permissions, continuously monitors for system health and security events, and performs penetration test.

## 6.8 Time-stamping

CHTCA 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. Automatic or manual procedures may be used to adjust the system time, and system clock synchronizations shall be auditable events.

(1) Time of certificate issuance,

(2) Time of certificate revocation,

(3) Time of CRL issuance, and

(4) Time of system event occurrence.

# 7. Certificate, CRL, and OCSP Profiles

## 7.1 Certificate Profile

The certificates issued by CHTCA conform to the official versions of the ITU-T X.509, S/MIME Baseline Requirements and RFC 5280.

CHTCA generates non-sequential certificate serial numbers greater than zero (0) containing at least 64 bits of output from a cryptographically secure pseudorandom number generator (CSPRNG).

### 7.1.1 Version Number(s)

CHTCA issues certificates in compliance with RFC 5280 and ITU-T X.509 version 3.

### 7.1.2 Certificate Extensions

See Appendix 3, 3-1, and 3-2 for details.

### 7.1.3 Algorithm Object Identifiers

CHTCA uses the algorithms listed in the table below for signing certificates and generating key pairs.

| Purpose | Algorithm | OID |
|---|---|---|
| Signature | sha256WithRSAEncryption | {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)} |
| | sha384WithRSAEncryption | {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha384WithRSAEncryption(12)} |
| | sha512WithRSAEncryption | {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha512WithRSAEncryption(13)} |
| | ecdsaWithSHA256 | {iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2)} |
| | ecdsaWithSHA384 | {iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA384(3)} |
| | ecdsaWithSHA512 | {iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA512(4)} |

| | | |
|---|---|---|
| Key Generation | rsaEncryption | {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(1)} |
| | ecPublicKey | {iso(1) member-body(2) us(840) ansi-x962(10045) keyType(2) ecPublicKey(1)} |

During ECC algorithm is used for generarting ECDSA key pairs, the OIDs of the elliptic curve parameter is set as follows according to the key size:

| Key Size | Elliptic Curve Parameter | OID |
|---|---|---|
| P-256 | secp256r1 | {iso(1) member-body(2) us(840) ansi-x962(10045) curves(3) prime(1) prime256v1(7)} |
| P-384 | secp384r1 | {iso(1) identified-organization(3) certicom(132) curve(0) ansip384r1(34)} |

## 7.1.4 Name Forms

The subject DN and issuer DN fields of a certificate must use the X.500 distinguished name and the name attribute type shall comply with the official versions of the ITU-T X.509, S/MIME Baseline Requirements, S/MIME Certificate Profile Requirements of Google, RFC 8550, RFC 3161, RFC 3628 and RFC 5280.

### 7.1.4.1 Name Encoding

The encoded content of the issuer DN field of certificates issued by an issuing CA shall be byte-for-byte identical with the encoded form of the subject DN field of the issuing CA's certificate. If there are two or more CA certificates, including expired and revoked CA certificates, whose subject DNs can be compared as equal, the encoded content of the subject DN field of the aforementioned certificates shall be byte-for-byte identical.

### 7.1.4.2 Subject Information–CA Certificates

Certificates can be issued after issuing CAs followed the procedures

set forth in the ePKI CP and this CPS to verify that all of the subject information was accurate. For self-signed certificates issued since the second-generation of eCA and newly issued subordinate CA certificates, the subject field includes three attributes, namely “commonName”, “organizationName”, and “countryName”, described as follows:

(1) commonName

The name used to identify the issuing CA. It is the unique identifier of the certificate and can be used to distinguish the issuing CA’s certificate from other CA certificates.

(2) organizationName

The official name of the organization to which the issuing CA belongs. It can be adjusted according to the abbreviation method approved by our country. The authentication of this organization name shall be implemented in accordance with Section 3.2.2.

(3) countryName

The country where the place of business that the issuing CA locates. It shall be represented by the country codes specified in ISO 3166-1, which is “TW”.

#### 7.1.4.3 Subject Information–Subscriber Certificates

By issuing the subscriber certificates, CHTCA represents that they followed the procedures set forth in the ePKI CP and/or this CPS to verify that, as of the subscriber certificate’s issuance date, all of the subject information was accurate.

In addition, subject attributes MUST NOT contain only metadata such as ‘.’, ‘-’, and ‘ ’ (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.

For S/MIME certificates, the type of the entry contained in the subject alternative name extension must be rfc822Name, and must not be

dNSName, iPAddress, or uniformResourceIdentifier.

For the certificate application that the entry in the subject alternative name extension of subscriber certificates will contain an e-mail address, the RA officers shall validate the authorization or control of the email address in compliance with Section 3.2.5.

### 7.1.5 Name Constraints

Name constraints are not applied to CHTCA certificates. Self-signed certificates, self-issued certificates, subordinate CA certificates and cross-certificates, which are not technically constrained, will be disclosed publicly, such as being disclosed in the Common CA Database (CCADB) of Mozilla.

### 7.1.6 Certificate Policy Object Identifier

CHTCA certificates, excluding self-signed certificates of eCA, must include the certificate policies extension. In addition to the CP OID(s) defined in the ePKI CP, this extension may also contain the CA/Browser Forum-assigned OID(s) referenced in the ePKI CP according to the certificate purpose. With regard to the related statement of the CP OIDs, please refer to Section 1.2 of the ePKI CP.

### 7.1.7 Usage of Policy Constraints Extension

The policy constraints extension may be used as required for subordinate CA certificates and cross-certificates issued by eCA. Otherwise, certificates issued by CHTCA do not contain this extension.

### 7.1.8 Policy Qualifiers Syntax and Semantics

The policy qualifier field in the certificate policies extension of CHTCA certificates may be used as needed. When using this field, it may contain a CPS pointer qualifier that points to this CPS.

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

The certificate policies extension of the certificates issued by CHTCA are not marked critical.

## 7.2 CRL Profile

### 7.2.1 Version Number(s)

CHTCA issues CRLs complying with RFC 5280 and ITU-T X.509 version 2.

### 7.2.2 CRL and CRL Entry Extensions

The CRL and CRL entry extensions in the CRL issued by CHTCA comply with the official versions of the ITU-T X.509, S/MIME Baseline Requirements, S/MIME Certificate Profile Requirements of Google, RFC 8550, RFC 3161, RFC 3628 and RFC 5280. These extensions are described below.

(1) CRL Extensions

| Extension | Presence | Criticality | Description |
|---|---|---|---|
| Authority Key Identifier | MUST | N | The SHA-1 hash value of the CRL issuer's public key. |
| CRL Number | MUST | N | A monotonically increasing sequence number for a given CRL scope and CRL issuer. |
| Issuing Distribution Point | Optional | Y | This extension is only applicable to a partitioned CRL. It is used to identify the CRL distribution point, indicate whether the CRL covers revocation for end entity certificates only, CA certificates only, attribute certificates only, or a limited set of reason codes, and state whether or not it is an indirect CRL. The scope of the CRL only includes certificates issued by CHTCA, and thus the indirectCRL boolean must be set to FALSE. |

(2) CRL Entry Extensions

| Extension | Presence | Criticality | Description |
|---|---|---|---|
| Reason Code | Optional | N | If this CRL entry extension is used to identify the revocation reason of self-signed certificates, self-issued certificates, subordinate CA certificates and cross-certificates, the reasonCode value can be the follows:<br>➢ caCompromise(2)<br>➢ affiliationChanged(3)<br>➢ superseded(4)<br>➢ cessationOfOperation(5)<br>➢ privilegeWithdrawn(9)<br>If the CRL entry extension is used to identify the revocation reason of subscriber certificates, the reasonCode value is as follows.<br>➢ unspecified (0): If the use of this reason code is permitted, the extension field will be omitted.<br>➢ keyCompromise(1)<br>➢ affiliationChanged(3)<br>➢ superseded(4)<br>➢ cessationOfOperation(5)<br>➢ certificateHold(6)<br>➢ privilegeWithdrawn(9) |

## 7.3 OCSP Profile

CHTCA provides OCSP services in compliance with RFC 6960 and RFC 5019, and includes a HTTP URL of the issuing CA's OCSP responder in the authority Information access extension of CHTCA certificates (excluding self-signed certificates of eCA).

### 7.3.1 Version Number(s)

An OCSP request accepted by CHTCA shall contain the following information:

- Protocol version, and
- Target certificate identifier.

An OCSP response, issued by the OCSP responder, at a minimum consists of a responseStatus field indicating the processing status of the prior request. If the value of responseStatus is 'successful', the OCSP response must further include the other fields as follows:

| Field | Description |
|---|---|
| Version | v.1 (0x0) |
| OCSP Responder ID | The subject DN of OCSP responder |
| Produced Time | The time at which the OCSP response was signed |
| Target Certificate Identifier | The contents of this field include the hash algorithm, the hash of the issuer's DN, the hash of the issuer's public key and the serial number of the target certificate. |
| Certificate Status | The meaning of certificate status value is described below:<br>➢ 0: valid<br>➢ 1: revoked<br>When this status value is used, this field shall also contain the revocation time and reason of that certificate. The revocationReason field within the RevokedInfo of the CertStatus shall be identical to the CRLReason of the revoked certificate noted in the CRL (See Section 7.2.2).<br>2: unknown |
| Validity Period | Recommended validity period for this OCSP response, including ThisUpdate and NextUpdate |
| Signature Algorithm | OCSP response signature algorithm, which can be either:<br>■ sha256WithRSAEncryption, or<br>■ ecdsaWithsha384 |

| | |
|---|---|
| Signature | OCSP responder signature |
| Certificates | OCSP responder certificate |

### 7.3.2 OCSP Extensions

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

# 8. Compliance Audit and Other Assessments

## 8.1 Frequency or Circumstances of Assessment

CHTCA shall undergo routine external audits at least once per year (the audited period may not exceed 12 months) and non-routine internal audits to confirm that the security regulations and procedures of the ePKI CP and this CPS are being implemented and enforced.

## 8.2 Identity/Qualifications of Assessor

CHTCA entrusts external audit operations to qualified auditors, who is familiar with the operations of CHTCA and authorized by the WebTrust Principles and Criteria for Certification Authorities program management unit to implement relevant WebTrust Principles and Criteria for Certification Authorities audit criteria in R.O.C., to provide impartial and objective audit services. Audit personnel shall be a certified information system auditor or a person who has equivalent qualification; and shall at least possess the experience of conducting a WebTrust Principles and Criteria for Certification Authorities seal audit twice at 4 man-days or the experience of conducting a CA information security management audit twice at 8 man-days. CHTCA shall conduct identity identification of auditors during audits.

## 8.3 Assessor’s Relationship to Assessed Entity

CHT shall entrust an impartial third party to conduct audits of CHTCA operations.

## 8.4 Topics Covered by Assessment

CHTCA undergoes an audit in accordance with the scheme of

"WebTrust Principles and Criteria for Certification Authorities". For CAs issuing S/MIME certificates, they should also undergoe additional audit schemes of "WebTrust Principles and Criteria for Certification Authorities - SMIME" and "WebTrust Principles and Criteria for Certification Authorities - Network Security".

The assessment shall include the following topics:

(1) Whether CHTCA is operating in accordance with this CPS, including management and technical audit of the physical environment, personnel procedural controls, key control, certificate lifecycle control, and hardware cryptographic module control;
(2) Whether the RA of CHTCA complies with this CPS and related procedures; and
(3) Whether the requirements of this CPS are being implemented and enforced subject to the ePKI CP, and whether the requirements are suitable for the practical operations of CHTCA.

CHTCA has the right to conduct the review and examination of following (but not limited to) items to ensure its trustworthiness:

(1) If there is an event of computer emergency or key compromise that causes CHTCA to reasonably suspect the RA is unable to comply with the ePKI CP and this CPS;
(2) If the compliance audit has not been completed or there are special developments, CHTCA has the right to conduct a risk management review; or
(3) If action or inaction by the RA causes actual or potential security and integrity threat to the ePKI, CHTCA must conduct the related review or examination.

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

## 8.5 Actions Taken as a Result of Deficiency

If audit personnel find a discrepancy between the requirements of this CPS and the design, operation, or maintenance of CHTCA or its RA, the following actions shall be taken:

(1) Note the discrepancy,

(2) Notify CHTCA about the discrepancy, and

(3) CHTCA shall submit an improvement plan regarding the discrepancy items within 30 days and promptly implement it. The discrepancy items shall also be listed as follow-up audit tracking items. The RA is notified to make improvements to RA-related deficiencies.

## 8.6 Communications of Results

Except for any audit findings that could result in system attacks and the stipulations in Section 9.3, CHTCA shall make its audit report publicly available. Audit results are displayed with related WebTrust Principles and Criteria for Certification Authorities seals on CHTCA's homepage. The audit report and management's assertions may be viewed by clicking on the seals. CHTCA should make its audit report and management's assertions publicly available no later than three months after the end of the audit period. In the event of a delay greater than three months, CHTCA shall provide an explanatory letter signed by the qualified auditor.

## 8.7 Self audits

During the period in which it issues S/MIME certificates, CHTCA must strictly control its service quality by performing ongoing self audits against a randomly selected sample of at least three percent or thirty of the S/MIME certificates it has issued in the period beginning immediately after the last sample was taken in accordance with the S/MIME Baseline Requirements and WebTrust Principles and Criteria for Certification Authorities - S/MIME.

# 9. Other Business and Legal Matters

## 9.1 Fees

### 9.1.1 Certificate Issuance or Renewal Fees

The fee calculation framework for certificate application, issuance, and renewal between CHTCA and subscribers shall be stipulated in the related business contract terms and conditions and subscribers may directly connect to the repository to check related terms and conditions.

### 9.1.2 Certificate Access Fees

Certificate access fees are stipulated in related contract terms and conditions and subscribers may directly connect to the repository to check related terms and conditions.

### 9.1.3 Revocation or Status Information Access Fees

Fees may not be charged for subscriber CRL downloading or access. The fee calculation framework for OCSP service is stipulated in related contract terms and conditions. Subscribers may directly connect to the repository for inquiry.

### 9.1.4 Fees for Other Services

No stipulation.

### 9.1.5 Refund Policy

With regard to the certificate issuance and renewal fees charged by CHTCA, if a subscriber is unable to use a certificate due to oversight by CHTCA, CHTCA shall issue a new certificate after conducting an investigation. If the subscriber does not accept the newly issued certificate, CHTCA 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

CHTCA is owned and operated by CHT. Its financial responsibilities are the responsibilities of CHT. CHTCA has taken out a Commercial General Liability insurance of USD 5 million in coverage, and eCA and PublicCA have taken out an additional Professional Liability/Errors & Omissions insurance of USD 10 million in coverage.

### 9.2.2 Other Assets

CHTCA finances are a part of the overall finances of CHT. CHT is a publicly listed company. In accordance with Article 36 of the Securities and Exchange Act, annual financial reports duly audited and attested by a certified public accountant, approved by the board of directors and recognized by the supervisors are publically announced and registered with the competent authority within three months after the close of each fiscal year. Financial reports duly reviewed by a certified public accountant and reported to the board of directors are publicly announced and registered within 45 days after the end of the first, second and third quarters of each fiscal year. The operating status for the preceding month is publicly announced and registered within the first 10 days of each month. CHTCA can provide self-insured asset prices based on CHT's financial reports.

### 9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

## 9.3 Confidentiality of Business Information

### 9.3.1 Scope of Confidential Information

The following information generated, received and kept by CHTCA

or its RA is deemed 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 or kept by CHTCA,

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

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

Current and departed personnel in CHTCA and RA and audit personnel shall keep secrets for the aforementioned confidential information.

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

(1) Identification information and information listed in the certificate are not deemed confidential information unless stipulated otherwise, and

(2) Issued certificates, revoked certificates, suspended information and CRLs published in the CHTCA repository are not deemed confidential information.

### 9.3.3 Responsibility to Protect Confidential Information

CHTCA shall handle subscriber application information in accordance with the Electronic Signatures Act, WebTrust Principles and Criteria for Certification Authorities related audit criteria, and Personal Information Protection Act and its related sub-laws.

## 9.4 Privacy of Personal Information

### 9.4.1 Privacy Plan

CHTCA has posted its personal information statement and privacy

declaration on its website. CHTCA conducts privacy impact analysis and personal information risk assessments and has established a privacy protection plan.

### 9.4.2 Information Treated as Private

Private information includes:

(1) The personal information listed on certificate applications should not be disclosed without the subscriber's consent or in accordance with related laws,

(2) Subscriber information that cannot be obtained through certificates, CRLs or certificate catalog service,

(3) Personnel identifiable information in CHTCA such as names together with palmprint or fingerprint biometrics, and

(4) Personal information on confidentiality agreements or contracts.

CHTCA and its RAs implement security control measures to prevent personally identifiable information from unauthorized disclosure, leakage, or damage.

### 9.4.3 Information Not Deemed Private

The following information not deem as private:

(1) Identification information, information listed in certificates, and certificates are not deemed private information unless stipulated otherwise, and

(2) Issued certificates, revoked certificates or suspension information and CRLs published in the CHTCA repository are not private information.

### 9.4.4 Responsibility to Protect Private Information

The personal information required for the operation of CHTCA, in either paper or digital form, must be handled in accordance with Personal

Information Protection Act and its related sub-laws and privacy rights declaration posted on the website. CHTCA shall negotiate the liability of protecting private information with its RA.

### 9.4.5 Notice and Consent to Use Private Information

Pursuant to the Personal Information Protection Act and its related sub-laws, personal information shall not be used for other purposes without the consent of subscriber or unless stipulated otherwise in Personal Information Protection Act, privacy rights declaration or this CPS. Subscribers may inquire their application information specified in Section 9.3.1 paragraph (3); however, CHTCA reserves the right to charge reasonable fees from subscribers applying for access to this information.

### 9.4.6 Disclosure Pursuant to Judicial or Administrative Process

If judicial, supervisory or law enforcement authorities need to check private information under Section 9.3.1 due to one of the following conditions, the matter shall be handled in accordance with law or regulation:

(1) The provisions of government decrees and the legal authorization of the competent authority; or
(2) The court handles disputes arising from the use of certificates and legal application needs for arbitration.

Otherwise, the registered personal information and identification-related information of subscribers will never be arbitrarily provided to the competent authority or any other person.

### 9.4.7 Other Information Disclosure Circumstances

Subscriber personal information obtained during CHTCA operations is handled in accordance with related laws and may not be disclosed externally, unless stipulated otherwise under the law.

## 9.5 Intellectual Property Rights

The following is the intellectual property of CHTCA:

(1) Related documents or system development for certificate management of CHTCA;

(2) Certificates and CRLs issued by CHTCA; and

(3) This CPS.

This CPS is available for free download from the repository or reasonable use according to the relevant provisions in the Copyright Act of R.O.C. This CPS can be used reasonably and no fee will be charged. CHTCA reserves the right to pursue legal action for any violation of the use or dissemination of this CPS.

## 9.6 Representations and Warranties

### 9.6.1 CA Representations and Warranties

CHTCA represents and warrants to the Certificate Beneficiaries including Subscribers, Relying Parties, and Application Software Suppliers that, during the period when the Certificate is valid, CHTCA complies with the ePKI CP and this CPS in issuing and managing the Certificate.

The Certificate Warranties specifically include, but not limited to, the following:

(1) **Right to Use Domain Name or Mailbox Address**: That, at the time of issuance, CHTCA (i) implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the Domain Name(s) or Mailbox Addresses listed in the Certificate's subject field and subjectAltName extension (or, only in the case of Domain Names, was delegated such right or control by someone who had such right to use or control); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CPS (see Section 3.2);

(2) **Authorization for Certificate**: That, at the time of issuance, CHTCA (i) implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CPS (see Section 3.2.5);

(3) **Accuracy of Information**: That, at the time of issuance, CHTCA (i) implemented a procedure for verifying the accuracy of all of the information contained in the Certificate; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CPS (see Sections 3.2.2, 3.2.3 and 3.2.7);

(4) **No Misleading Information**: That, at the time of issuance, CHTCA (i) implemented a procedure for reducing the likelihood that the information contained in the Certificate's subject:organizationalUnitName attribute would be misleading; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CPS (see Sections 3.2.2, 3.2.3 and 3.2.7);

(5) **Identity of Applicant**: That, if the Certificate contains Subject Identity Information, CHTCA (i) implemented a procedure to verify the identity of the Applicant in accordance with Sections 3.2.2 and 3.2.3; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CPS;

(6) **Subscriber Agreement**: That, if CHTCA and Subscriber are not Affiliated, the Subscriber and CHTCA are parties to a legally valid and enforceable Subscriber Agreement that satisfies the S/MIME Baseline Requirements, or, if CHTCA and Subscriber are the same entity or are Affiliated, the Applicant Representative acknowledged the Terms of Use;

(7) **Status**: That CHTCA maintains a 24 x 7 publicly-accessible

Repository with current information regarding the status (valid or revoked) of all unexpired Certificates (see Section 4.10.2); and

(8) **Revocation**: That CHTCA will revoke the Certificate for any of the reasons specified in the S/MIME Baseline Requirements (see Section 4.9.1).

### 9.6.2 RA Representations and Warranties

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

RAs shall represent and warrant that:

(1) Certificate verification is performed in compliance with the ePKI CP and this CPS;

(2) All information provided to the issuing CA does not contain any false or misleading information;

(3) Translations performed by the RA are an accurate translation of the original information;

(4) All Certificates requested by the RA meet the requirements of this CPS;

(5) Identification and authentication procedures for RAO are implemented; and

(6) RA private keys are securely managed.

### 9.6.3 Subscriber Representations and Warranties

For the express benefit of CHTCA and the Certificate Beneficiaries, the Applicant shall warrant that, prior to the issuance of a certificate, CHTCA will obtain, either:

(1) The Applicant’s agreement to the Subscriber Agreement with CHTCA, or

(2) The Applicant’s acknowledgement of the Terms of Use.

Applicant (or human sponsor for device certificates or agent under a subcontractor or hosting service relationship) shall represent and warrant to CHTCA that it will:

(1) Securely generate its private keys and prevent its private keys from compromise,

(2) Provide accurate and complete information to CHTCA and RA,

(3) Comply with the stipulations and procedures in Chapters 3 and 4,

(4) Confirm the accuracy of certificate data prior to using the certificate,

(5) Promptly notify CHTCA, cease using a certificate, and request revocation of the certificate, if

  (i) any information in the certificate is or becomes incorrect or inaccurate, or

  (ii) there is any actual or suspected misuse or compromise of the Subscriber's private key associated with the public key included in the certificate (and cease using the private key),

(6) Use the certificate only for legal and authorized purposes, consistent with the ePKI CP, this CPS and Subscriber Agreement, and

(7) Promptly cease using the certificate and related private key after the certificate's expiration.

### 9.6.4 Relying Party Representations and Warranties

Each relying party represents and warrants to:

(1) Comply with the provisions of this CPS when using a certificate or querying the CHTCA repository;

(2) Check the certificate assurance level before using it;

(3) Check the keyUsage field listed in the certificate prior to the use of certificates;

(4) Validate a certificate (issued by CHTCA) by using a CRL or OCSP published by CHTCA to confirm the validity;

(5) Carefully select secure computer environments and reliable

application systems. If the rights of subscribers and relying parties are infringed due to the use of an untrusted computer environment or application system, relying parties shall bear the responsibility solely;

(6) Seek other ways for completion of legal acts as soon as possible if CHTCA is unable to operate normally for some reason. It may not be a cause of defending others that CHTCA is not function properly; and

(7) Have understood and agreed to the legal liability clauses of CHTCA and will use the certificate in accordance with Section 1.4.1 when accepting the certificate.

If there is a violation, relying parties shall bear liability for damages in accordance with the Civil Code and related laws and regulations.

### 9.6.5 Representations and Warranties of Other Participants

No stipulation.

## 9.7 Disclaimers of Warranties

Except to the extent prohibited by law or as otherwise provided herein, CHTCA disclaims all express and implied warranties including all warranties of merchantability or fitness for a particular purpose.

## 9.8 Limitations of Liability

Except to the extent CHTCA has issued and managed the certificate in accordance with the Baseline Requirements and this CPS, CHTCA shall not be liable to the subscribers or relying parties for any losses suffered as a result of use or reliance on such certificate. Otherwise, CHTCA will assume the compensation liability no more than the amount stipulated in Section 9.9 of this CPS.

# 9.9 Indemnities

## 9.9.1 Indemnification by CHTCA

If subscribers or relying parties suffer damages due to the intentional or unintentional failure of CHTCA to follow the ePKI CP, this CPS, relevant laws or the provisions of contracts signed between CHTCA and subscribers/relying parties when processing subscriber certificate-related work, CHTCA shall be held liable. Subscribers may claim compensation for damages based on the related provisions of the contract set down between CHTCA (or its RA) and subscribers. Relying parties shall request compensation in accordance with laws and regulations. The total compensation limit of CHTCA for each subscriber or relying party is shown in the Table below. If the subscriber or relying party has signed a contract with CHTCA, the certificate scope of use and transaction compensation limit shall be determined separately.

| Certificate Assurance Level | Compensation Limit (NTD) |
|---|---|
| Level 1 | 3,000 |
| Level 2 | 100,000 |
| Level 3 | 3,000,000 |
| Level 4 | 5,000,000 |

These compensation limits are the maximum compensation amounts. The actual compensation amounts are based on the actual damages incurred by the subscribers or relying parties.

## 9.9.2 Indemnification by RA

If subscribers or relying parties suffer damages due to the RA intentional or unintentional failure to follow this CPS, related laws or the provisions of contracts signed between the RA and subscribers/relying parties when processing subscriber certification registrations, CHTCA is

only responsible for compensation for the RA established by CHTCA, and the compensation limits are detailed in Section 9.9.1. For other RA not established by CHTCA, the RA takes the responsible of compensation. If the RA and subscribers or relying parties have a contract determing the usage of certificates and transaction compensation amounts, then the contract takes precedence. Compensation claims by subscribers shall be made in accordance with related provisions in the contract set down with the RA. Compensation claims by relying parties shall be made in accordance with relevant laws and regulations.

## 9.10 Term and Termination

### 9.10.1 Term

This CPS is effective when approved by the Electronic Signatures Act competent authority and published to CHTCA's repository.

### 9.10.2 Termination

The new version of this CPS is announced after being approved by the Electronic Signatures Act competent authority, and the current version is terminated.

### 9.10.3 Effect of Termination and Survival

The effect of this CPS remains valid until the expiration or revocation of the last certificate issued according to this CPS.

## 9.11 Individual Notices and Communications with Participants

CHTCA, RAs, subscribers, relying parties shall adopt suitable methods for establishing mutual notification and communication channels including but not limited to official document, letter, telephone, fax, email or secure email.

## 9.12 Amendments

### 9.12.1 Procedure for Amendment

This CPS is reviewed annually, and an assessment is made to determine if the CPS needs to be amended to maintain its assurance level. This CPS shall be amended accordingly if the ePKI CP is amended or the OID is changed, and if so, changes to this CPS are indicated by appropriate numbering. The new version of this CPS will publish according to the regulations stated in Section 2.3.

### 9.12.2 Notification Mechanism and Period

CHTCA will post appropriate notice on its websites of any major or significant changes to this CPS as well as any appropriate period by when the revised CPS becomes effective. If subscribers or relying parties have any comment on the change items, they can submit the comment within the comment period. Reassess to the changes and response may or may not be made by CHTCA according to these comments.

No further notice will be given in case of typesetting of this CPS.

### 9.12.3 Circumstances under which OID Must Be Changed

If modifications to ePKI CP do not affect the stated certificate usage purposes or assurance levels, the CP OID does not need to be changed. However, if the CP OID is changed, changes shall be made to this CPS accordingly.

## 9.13 Dispute Resolution Provisions

In the event of a dispute between subscribers/RA and CHTCA, the parties shall resolve the dispute under the principle of good faith. In the event of litigation, the parties agree that Taiwan Taipei District Court shall be the court of first instance.

## 9.14 Governing Law

For disputes involving CHTCA issued certificates, the applicable ROC laws shall govern.

## 9.15 Compliance with Applicable Law

Related ROC laws must be followed regarding the interpretation of any agreement signed based on this CPS.

## 9.16 Miscellaneous Provisions

### 9.16.1 Entire Agreement

The commitments set forth in this CPS constitute the entire agreement between the participants (CHTCA, RAs, subscribers and relying parties).

### 9.16.2 Assignment

The participants describe in this CPS may not assign or delegate their rights or obligations under this CPS to other parties in any form without prior notice to CHTCA.

### 9.16.3 Severability

If any chapter of this CPS is held invalid or unenforceable by a competent court or tribunal, the remainder of this CPS will remain valid and enforceable.

### 9.16.4 Enforcement (Attorney's Fees and Waiver of Rights)

In the event that CHTCA suffers damages attributable to an intentional or unintentional violation of this CPS by a subscriber or relying party, CHTCA may seek compensation for damages and indemnification and attorneys' fees related to the dispute or litigation from the responsible party.

CHTCA's failure to assert rights with regard to the violation of this CPS to the party does not waive CHTCA's right to pursue the violation of this CPS later or in the future.

### 9.16.5 Force Majeure

CHTCA is not liable for any delay or failure to perform an obligation under this CPS to the extent that the delay or failure is caused by a force majeure or other circumstances not attributable to CHTCA, including natural disasters, wars, or terrorism which may cause the interruption of telecommunications network. CHTCA has set clear limitations for certificate usage and is not bear any legal responsibility for damages caused by exceeding these usage limitations.

## 9.17 Other Provisions

No stipulation.

# Appendix 1: Acronyms and Definitions

| Acronyms | Full Name | Definition |
|---|---|---|
| AATL | Adobe Approved Trust Lis | |
| AIA | Authority Information Access | See Appendix 2. |
| CA | Certification Authority | See Appendix 2. |
| CAA | Certification Authority Authorization | See Appendix 2. |
| CARL | Certification Authority Revocation List | See Appendix 2. |
| CMMI | Capability Maturity Model Integration | See Appendix 2. |
| CP | Certificate Policy | See Appendix 2. |
| CPA | Chartered Professional Accountants Canada | See Appendix 2. |
| CP OID | CP Object Identifier | |
| CPS | Certification Practice Statement | See Appendix 2. |
| CRL | Certificate Revocation List | See Appendix 2. |
| DN | Distinguished Name | |
| DNS | Domain Name System | See Appendix 2. |
| eCA | ePKI Root Certification Authority | See Appendix 2. |
| EE | End Entities | See Appendix 2. |
| ePKI | Chunghwa Telecom ecommerce Public Key Infrastructure | See Appendix 2. |
| FIPS | (US Government) Federal Information Processing Standard | See Appendix 2. |
| FQDN | Fully Qualified Domain Name | See Appendix 2. |
| IANA | Internet Assigned Numbers Authority, IANA | See Appendix 2. |

| Acronyms | Full Name | Definition |
|---|---|---|
| IDN | Internationalized Domain Name | See Appendix 2. |
| IETF | Internet Engineering Task Force | See Appendix 2. |
| NIST | (US Government) National Institute of Standards and Technology | See Appendix 2. |
| OCSP | Online Certificate Status Protocol | See Appendix 2. |
| OID | Object Identifier | See Appendix 2. |
| PIN | Personal Identification Number | |
| PKCS | Public-Key Cryptography Standard | See Appendix 2. |
| PKI | Public Key Infrastructure | See Appendix 2. |
| QGIS | Qualified Government Information Source | See Appendix 2. |
| QTIS | Qualified Government Tax Information Source | See Appendix 2. |
| RA | Registration Authority | See Appendix 2. |
| RFC | Request for Comments | See Appendix 2. |
| TLS | Transport Layer Security | See Appendix 2. |
| UPS | Uninterrupted Power System | See Appendix 2. |

# Appendix 2: Glossary

| | |
|---|---|
| Access | Use the information processing capabilities of system resources |
| Access Control | Authorization procedure for access to information system resources given to subscribers, programs, procedures and other systems. |
| Activation Data | Private data, other than keys, that are required to access cryptographic modules and that need to be protected (i.e., unlock private keys for signing or decryption events). |
| Applicant | Subscribers who request certificates from a CA and have not yet completed the certificate procedure. |
| Archive | A physically separate storage site for long-term information (storage site for important information) which can be used to support audit, usage and integrity services. |
| Assurance | A basis that the trusted entity has complied with certain security requirements. [Article 2-1, Chapter 1, Regulations on Required Information for Certification Practice Statements] |
| Assurance Level | A certain level in a relative assurance tier. [Article 2-2, Chapter 1, Regulations on Required Information for Certification Practice Statements] |
| Audit | Assessment of whether system controls are adequate and ensure conformance with existing policy and operation procedures, and independent checking and review of recommended required improvements to existing controls, policies and procedures. |
| Audit Data | Activity logs of a system organized in the order of time of occurrence that can be used to reconstruct or investigate the time sequence or changes that occurred during a certain event. |
| Authenticate | (1) Authentication is the process by which a claimed identity is verified. [A Guide to Understanding Identification and Authentication in Trusted Systems, National Computer Security Center] |

| | |
|---|---|
| | (2) Determination of identity authenticity when an identity of a certain entity is shown. |
| Authentication | (1) The process of establishing confidence in user identities electronically presented to an information system. [NIST.SP.800-63-2 Electronic Authentication Guideline]<br>(2) Safety measures used to secure data transmission or ways to authorize the privilege of individuals upon receiving certain types of information.<br>(3) Authentication is the process by which a claimed identity is verified. [A Guide to Understanding Identification and Authentication in Trusted Systems]<br>Mutual authentication means that the authentication is performed between two parties during communication. |
| Authority Information Access (AIA) | Records extensions related to certificate authority information access. The content may include: OCSP service sites and certificate issuance authority certificate verification path downloading site. |
| Authorization Domain Name | The Domain Name used to obtain authorization for certificate issuance for a given FQDN. The CA may use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. If the FQDN contains a wildcard character, then the CA MUST remove all wildcard labels from the left most portion of requested FQDN. The CA may prune zero or more labels from left to right until encountering a Base Domain Name and may use any one of the intermediate values for the purpose of domain validation. |
| Backup | Information or program copying that can be used for recovery purposes when needed. |
| Base Domain Name | The portion of an applied-for FQDN that is the first domain name node left of a registry controlled or public suffix plus the registry-controlled or public suffix (e.g. "example.co.uk" or "example.com"). For FQDNs where the right-most domain name node is a gTLD having ICANN Specification 13 in its registry agreement, the gTLD itself may be used as the Base Domain Name. |

| | |
|---|---|
| Baseline Requirements | "The Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" issued by CA/Browser Forum, and all the amendments. |
| Binding | The process for binding (connecting) two related information elements. |
| Biometric | The physical or behavioral attributes of a person. |
| CA Certificate | Certificates issued by CAs. |
| CA Key Pair | A Key Pair where the Public Key appears as the Subject Public Key Info in one or more Root CA Certificate(s) and/or Subordinate CA Certificate(s). |
| Capability Maturity Model Integration (CMMI) | CMMI is the successor of the Capability Maturity Model (CMM) and was developed by the Software Engineering Institute at Carnegie Mellon University. CMMI models provide guidance for developing or improving processes that meet the business goals of an organization. Its purpose is to help improve organizational performance. |
| Certificate | (1) Refers to verification information carrying a digital signature used to verify the identity and qualifications of the signer in electronic form [Article 2-6, Electronic Signatures Act]<br>(2) Digital presentation of information. The contents include:<br>A. Issuing certificate authority<br>B. Subscriber name or identity<br>C. Subscriber public key<br>D. Certificate validity period<br>E. Certification authority digital signature<br>The term 'certificate' referred to this CPS specifically refers to ITU-T X.509 v.3 format certificates which states the certificate policy object identifier in the 'certificate policy' field. |
| Certification Authority (CA) | (1) The agency or natural person that issues certificate [Article 2-5, Electronic Signatures Act]<br>(2) The competent body trusted by the subscriber. Its functions are the issuance and administration of ITU-T X.509 format public key certificates, CARLs and CRLs. |

| | |
|---|---|
| Certification Authority Authorization (CAA) | The certification authority authorization (CAA) DNS resource record allows a DNS domain name holder to specify one or more certification authorities (CAs) authorized to issue certificates for that domain. CAA resource records allow a public CA to implement additional controls to reduce the risk of unintended certificate mis-issue. [RFC 8659] |
| 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 [Article 2-3, Chapter 1, Regulations on Required Information for Certification Practice Statements]<br>(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. |
| Certification Practice Statement (CPS) | (1) External notification by the certificate authority used to describe the practice statement of the certificate authority governing certificate issuance and processing of other certification work. [Article 2-7, Electronic Signatures Act]<br>(2) Announcement of a statement that certain procedures of the certificate authority for certificate work (including issuance, suspension, revocation, renewal and access) comply with certain requirements (listed in the certificate policy or other service contracts). |
| Certificate Profile | A set of documents or files that defines requirements for Certificate content and Certificate extensions in accordance with Section 7 of the Baseline Requirements. e.g. a Section in a CA's CPS or a |

| | |
|---|---|
| | certificate template file used by CA software. |
| Certificate Problem Reports | The complaints regarding suspected cracking of keys, certificate misused, or other types of fraud, cracks, abuse, or inappropriate behaviors related to certificates. |
| Certificate Renewal | The procedure for issuing a new certificate to renew the validity of information bound together with the public key. |
| Certificate Revocation | Termination of a certificate prior to its expiry date. |
| Certificate Revocation List (CRL) | (1) The certificate revocation list digitally signed by the certification authority provided for relying party use. [Article 2-8, Chapter 1, Regulations on Required Information for Certification Practice Statements]<br>(2) List maintained by the certificate authority. The expiry dates of the above revoked certificates issued by the certification authority are recorded on the list. |
| Chartered Professional Accountants Canada (CPA) | Institution which jointly drafted The Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy system standards with the American Institute of Certified Public Accountants (AICPA) and the management organization for WebTrust for CA and SSL Baseline Requirement & Network Security mark. Canadian Institute of Chartered Accountants is abbreviated as CICA. |
| Compromise | Information disclosed to unauthorized persons or unauthorized intentional or unintentional disclosure, modification, destruction or loss of objects which constitutes a violation of information security policy. |
| Confidentiality | Information which will not be known or be accessed by unauthorized entities or programs. |
| Cross-Certificate | A certificate used to establish a trust relationship between two root CA. This certificate is a type of CA certificate and not a subscriber certificate. |
| Cryptographic | A set of hardware, software, firmware or combination |

| | |
|---|---|
| Module | of the above used to run cryptologic or programs (including crypto algorithms) and included within the cryptographic boundaries of the module. |
| Data Integrity | Information that has been subjected to unauthorized access or accidental modification, damage or loss. |
| Digital Signature | An electronic signature generated by use of mathematic algorithm or other means to create a certain length of digital data encrypted by the signatory's private key and capable of being verified by the public key. [Article 2-3, Electronic Signatures Act] |
| Domain Contact | The Domain Name Registrant, technical contact, or administrative contract (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record. |
| Domain Name | A node label assigned by the domain name system. Converts the IP address into a text name that is easily remembered by humans. |
| Domain Name Registrant | Sometimes referred to as the domain name owner, but it is more appropriate to say a certain individual or entity who have registered with the Domain Name Registrar to have the right to use a domain name and the Domain Name Registrant or WHOIS has listed the 'registrant' as a natural person or legal person. |
| Domain Name Registrar | A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns). |
| Domain Name System (DNS) | A distributed database used to automatically convert the IP address to domain name. |
| DNS CAA Email Contact | The email address defined in BR Section A.1.1. |
| DNS TXT Record Email Contact | The email address defined in BR Section A.2.1. |
| Duration | A certificate field made up of two subfields "start time |

| | |
|---|---|
| | of the validity period" (notBefore) and "end time of the validity period" (notAfter). |
| E-commerce | Provision of goods for sale and other services through the use of network technology (specifically the Internet). |
| End Entity | The PKI includes the following two types of entities:<br>(1) Those responsible for the safeguarding and use of certificate public keys.<br>(2) Third parties who trust the certificates issued by the PKI (not holders of private keys and not a certificate authority). The end entities are subscribers and relying parties including personnel, organizations, accounts, devices and sites. |
| End-Entity Certificate | Certificates issued to end-entities. |
| Chunghwa Telecom ecommerce Public Key Infrastructure (ePKI) | A hierarchical PKI established by CHT in compliance with ITU-T X.509 to promote electronic services. It can be used within various applications in e-commerce and e-government. |
| Chunghwa Telecom Certificate Policy Management Authority (PMA) | An organization which was established for electronic certificate management matters, such as (i) discussion and review of the CP and the electronic certificate framework of the PKI owned by CHT and (ii) review of interoperation requests submitted by subordinate CAs and cross-certified CAs and that of CPS. |
| ePKI Root CA (eCA) | The Root CA and top-level CA in ePKI, and its public key is the trust anchor of ePKI. |
| Federal Information Processing Standard (FIPS) | Except for military organizations in the US Federal Government System, information processing standard for all government organizations and government subcontractors. The security requirement standard for the cryptographic module is FIPS no. 140 standard (FIPS 140). FIPS 140-2 divides the cryptographic module into 11 types of security requirements. Each security requirement type is then divided into 4 security levels. |

| | |
|---|---|
| Firewall | An access restriction gateway between networks which complies with near-end (local area) security policy. |
| Fully Qualified Domain Name (FQDN) | An unambiguous domain name that specifies the exact location of a computer within the domain's hierarchy. The fully qualified domain name consists of two parts: the host name (service name) and domain name. For example, ourserver.ourdomain.com.tw, ourserver is the host name and ourdomain.com.tw is the domain name. In this name, ourdomain is the third-level domain, com is the second-level domain name and tw is the country code top-level domain (ccTLD). A fully qualified domain name always starts with a host name. For example, www.ourdomain.com，www is the host name. Ourdomain is the the second-level domain name. com is Generic Top-Level Domain, gTLD. |
| High Risk Certificate Request | The CA marks the request to be referred to the internal standards maintained by the CA and other database for reviewing. They may include the high-risk names used for phishing or other wrongful purposes, Miller Smiles phishing list, Google Safe Browsing list, or the names identified by the CA with the risk-reducing standards. |
| Identification | A statement of who the user is. [A Guide to Understanding Identification and Authentication in Trusted Systems]<br><br>A way that can be used to describe or claim the identity of an individual or entity, e.g., user account, name or email. |
| Integrity | Protecting information so that it is not subject to unauthorized modification or damage. Preserve information in an untampered state during transmission and storage following generation at its source until receipt by the final recipient. |
| Internationalized Domain Name (IDN) | A kind of internet domain name, including at least one script or alphabetic character of one specific language, and then encoded with Punycode, and used for the domain name service only accepting ASCII codes. |
| Internet Assigned Numbers Authority | An organization that oversees the allocation of global IP address, domain names and many other parameters |

| | |
|---|---|
| (IANA) | used for Internet. |
| Internet Engineering Task Force (IETF) | Responsible for the development and promotion of Internet standards. Official website is at: https://www.ietf.org/. Its vision is the generation of high quality technical documents affects how man designs, uses and manages the Internet and allows the Internet to operate smoothly. |
| Issuing CA | For a particular certificate, the CA that issues the certificate is the issuing CA. |
| Key Escrow | Storage of related information using the subscriber's private key and according to the terms of the mandatory subscriber escrow agreement (or similar contract). The terms of this escrow agreement requires that one or more than one agencies have possession of the subscriber key provided it is beneficial to the subscriber, employer or another party in accordance with the provisions of the agreement. |
| Key Exchange | Mutual exchange of keys to establish a secure communication processing procedure. |
| Key Pair | Two mathematically related keys having the following properties:<br>(1) One (public) key can be used to encrypt a message that can only be decrypted by using the other (private) key, and<br>(2) It is computationally infeasible to determine one key from another. |
| Linting | A process in which the content of digitally signed data such as a Precertificate [RFC 6962], Certificate, Certificate Revocation List, or OCSP response, or data-to-be-signed object such as a tbsCertificate (as described in RFC 5280, Section 4.1.1.1) is checked for conformance with the profiles and requirements defined in these Requirements. |
| Non-Repudiation | Provide proof of delivery to the information sender and proof of sender identity to the receiver so neither party may repudiate the processing of this information after the fact. Technically speaking, non-repudiation refers to the guarantee that this signature must be signed by the corresponding private key if a certain public key |

| | |
|---|---|
| | can be used to verify a certain digital signature for a trusted party. Legally speaking, non-repudiation refers to the establishment of a possession and control system for private signature keys. |
| Object Identifier (OID) | (1) One type of unique alphanumeric / numeric identified registered under the International Standard Organization registration standard which could be used to identify the uniquely corresponding certificate policy; where the certificate policy is modified, the OID is not changed accordingly. [Article 2-4, Chapter 1, Regulations on Required Information for Certification Practice Statements]<br>(2) When a special form of code, object or object type is registered with the International Standard Organization (ISO), the unique code may be used as an identified. For example, this code can be used in the public key infrastructure to indicate what certificate policy and cryptographic algorithms are used. |
| Online Certificate Status Protocol (OCSP) | The Online Certificate Status Protocol is a type of online certificate checking protocol which lets the application software of relying parties to determine the status (such as revoked or valid) of a certain certificate. |
| OCSP Responder | The online server that is authorized, maintained, and operated by the CA, and connects to the repository to process the certificate status request. |
| Out-of-Band | Delivery method other than ordinary information delivery channels. If the delivery method is by electric cable, a special secure channel may be the use of physical registered mail. |
| Private Key | (1) The key in the signature key pair used to generate digital signatures.<br>(2) The key in the encryption key pair used to decrypt secret information.<br>This key must be kept secret under these two circumstances. |
| Public Key | (1) The key in the signature key pair used to verify the validity of the digital signature. |

| | |
|---|---|
| | (2) The key in the encryption key pair used for encrypting secret information.<br><br>These keys must be made public (usually in a digital certificate form) under these two circumstances. |
| Public-Key Cryptography Standard (PKCS) | In order to promote the use of public key technology, the RSA laboratory under the RSA Information Security Company has developed a series of public key cryptography standards that are widely used by the industry. |
| Public Key Infrastructure (PKI) | A set of law, policy, standards, personnel, equipment, facilities, technology, processes, audits and services developed on a broad scale and management of asymmetric cryptography and public key certificates. |
| Qualified Auditor | Accountant firms, entities, or individuals that satisfy the auditor qualification requirements specified in Section 8.2 of the Baseline Requirements, as well as independent from the audited parties. |
| Qualified Government Information Source (QGIS) | A regularly-updated and current, publicly available, database designed for the purpose of accurately providing the information for which it is consulted, and which is generally recognized as a dependable source of such information provided that it is maintained by a Government Entity, such as Ministry of Economic Affairs Bussiness & Factory Registration Database, the reporting of data is required by law, and false or misleading reporting is punishable with criminal or civil penalties.<br><br>Nothing in the EV SSL Certificate Guidelines shall prohibit the use of third-party vendors to obtain the information from the Government Entity provided that the third party obtains the information directly from the Government Entity. |
| Qualified Government Tax Information Source (QTIS) | A Qualified Governmental Information Source that specifically contains tax information relating to Private Organizations, Business Entities, or Individuals. Such as Fiscal Information Agency, Ministry of Finance in Taiwan and IFS in USA. |
| Random Value | A value specified by a CA to the Applicant that exhibits at least 112 bits of entropy. |

| | |
|---|---|
| Registration Authority (RA) | (1) Responsible for checking the identity and other attributes of the certificate applicant but does not issue or administer certificates. The nature and scope of obligations borne by the registration authority are set down in the applicable certificate policy or agreement.<br>(2) An entity responsible for the identity identification and authentication of the certificate subject which does not issue certificates. |
| Re-key | Changing the key values used in the cryptographic system application program. It is commonly achieved by issuing a new certificate for the new public key. |
| Relying Party | (1) Recipient of a certificate who acts in reliance of that certificate or a digital signature to verify the public key listed in the certificate, or the counterpart to identify (or its attributes) of the subject named in a trusted certificate and public key listed in the certificate. [Article 2-6, Chapter 1, Regulations on Required Information for Certification Practice Statements]<br>(2) The individual or agency which receives information including a certificate and digital signature (the public key listed on the certificate may be used to verify the digital signature) and may rely on this information. |
| Repository | (1) A system for storing and retrieving certificates or other information relevant to certificates. [Article 2-7, Chapter 1, Regulations on Required Information for Certificate Practice Statements]<br>(2) A database that contains information and data relating to certificates as specified in the CP/CPS. |
| Request Token | A value derived in a method specified by the CA which binds this demonstration of control to the certificate request.<br>The Request Token SHALL incorporate the key used in the certificate request.<br>A Request Token MAY include a timestamp to indicate when it was created.<br>A Request Token MAY include other information to |

| | |
|---|---|
| | ensure its uniqueness.<br>A Request Token that includes a timestamp SHALL remain valid for no more than 30 days from the time of creation.<br>A Request Token that includes a timestamp SHALL be treated as invalid if its timestamp is in the future.<br>A Request Token that does not include a timestamp is valid for a single use and the CA SHALL NOT re-use it for a subsequent validation.<br>The binding SHALL use a digital signature algorithm or a cryptographic hash algorithm at least as strong as that to be used in signing the certificate request. |
| Required Website Content | Either a Random Value or a Request Token, together with additional information that uniquely identifies the Subscriber, as specified by the CA. |
| Reserved IP Addresses | IPv4 and IPv6 addresses reserved in the IANA setting. See:<br>http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml and http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml |
| Request for Comments (RFC) | A series of memos issued by the Internet Engineer Task Force that include Internet, UNIX and Internet community standards, protocols and procedures for number assignment. |
| Secure Sockets Layer | Protocol issued by Netscape through introduction of their web browser which can encrypt network communication in the transport layer and ensure the integrity of transmitted information and perform identity authentication on the server and client.<br>The advantage of the secure socket layer protocol is it is independent and separate from the application layer protocol. High level application layer protocol (such as: HTTP, FTP and Telnet) may be established on top of SSL. The SSL protocol completes encryption algorithm, communication secret key agreement and server authentication work before the application layer protocol communication. This protocol is a successor to the Transport Layer Security (TLS) protocol. |

| | |
|---|---|
| Signature Certificate | Public key certificates which contains a digital signature public key used for verification purposes (not used for data encryption or other cryptographic uses). |
| Subordinate CA | In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA. |
| Subscriber | An entity that<br>(1) is the subject named or identified in a certificate issued to that entity,<br>(2) holds a private key that corresponds to the public key listed in the certificate, and<br>(3) does not itself issue certificates to another party.<br><br>This includes, but is not limited to, an individual, an organization, an application or network device. |
| Technical Non-Repudiation | Technical evidence provided by the public key system to support non-repudiation security service. |
| Threat | Any status or event which may cause damage (including destruction, disclosure, malicious tampering or denial of service) to information systems. Can be divided into internal threats and outside threats. Internal threats are use of authorization to employ information destruction, disclosure, tampering or denial of service methods to damage the information system. Outside threats are an outside unauthorized entity which has the potential to damage the information system (including information destruction, tampering, disclosure and interruption of service). |
| Time-stamp | A digitally signed assertion by a trusted authority that a specific digital object existed at a certain time. |
| Transport Layer Security (TLS) | TLS 1.0 was first defined in RFC 2246 by the IETF based on the SSL 3.0 and updated in RFC 5246 and RFC 6176 as TLS 1.2. The current version is TLS 1.3 defined in RFC 8446 by the IETF in 2018. |
| Trust List | List of trusted certificates used by relying parties to authenticate certificates. |

| | |
|---|---|
| Trusted Certificate | Certificate trusted by relying party obtained through a secure and reliable transmission method. The public key contained in this type of certificate comes from a trusted path. Also called a trust anchor. |
| Trustworthy System | Computer hardware, software and programs which possess the following attributes:<br>(1) Functions that protect again intrusion and misuse.<br>(2) Provides reasonably accessible, reliable and accurate operations.<br>(3) Appropriate implementation of preset function.<br>(4) Security procedures uniformly accepted by the general public. |
| Uninterrupted Power System (UPS) | Provide uninterrupted backup power to loading equipment in the event of abnormal power conditions (such as power outage, interference or power surge) to allow uninterrupted operation of servers, switches and other critical equipment and precision instruments to prevent loss of calculation data, communication network interruption and loss of instrument control. |
| Validation | The process of identification of certificate applicants. Validation is a subset of identification and refers to identification in the context of establishment of the identity of certificate applicants. [RFC 3647] |
| WHOIS | Information retrieved directly from the Domain Name Registrar or registry operator via the protocol defined in RFC 3912, the Registry Data Access Protocol defined in RFC 7482, or an HTTPS website. |
| Zeroize | Method to delete electronically stored information. Storage of changed information to prevent information recovery. |

# Appendix 3: Certificate Extensions

The extensions of certificates issued by CHTCA are set in compliance with the official versions of the ITU-T X.509, S/MIME Baseline Requirements, S/MIME Certificate Profile Requirements of Google, RFC 8550, RFC 3161, RFC 3628 and RFC 5280.

CHTCA shall not issue a certificate with:

(1) Extensions that do not apply in the context of the public internet; and

(2) Semantics that will mislead a relying party about the certificate information verified by CHTCA.

# Appendix 3-1: CA Certificates

CA certificates issued by CHTCA include the self-signed certificate and self-issued certificate of root CA, subordinate CA certificate and cross-certificate. The certificate extensions are described below. Other optional extensions may be used as applicable, and the methods comply with the regulations in Appendix 3.

(1) Self-signed Certificate

| Extension | Presence | Criticality | Description |
|---|---|---|---|
| Authority Key Identifier | Optional | N | Only the keyIdentifier field is present in this extension, and its value must be identical to the subjectKeyIdentifier extension. |
| Subject Key Identifier | MUST | N | The SHA-1 hash value of the root CA's public key. |
| Basic Constraints | MUST | Y | Subject Type=CA<br>Path Length Constraint=None |
| Key Usage | MUST | Y | Bits contained in this extension are as follows:<br>➢ keyCertSign (required)<br>➢ cRLSign (required)<br>➢ digitalSignature (optional) |

(2) Self-issued Certificate

| Extension | Presence | Criticality | Description |
|---|---|---|---|
| Authority Key Identifier | MUST | N | Only the keyIdentifier field, used to contain the SHA-1 hash value of the new (old) root CA's public key, is present in this extension. Its value must be identical to the subjectKeyIdentifier extension of the self-signed certificate issued by the new (old) root CA. |
| Subject Key Identifier | MUST | N | The SHA-1 hash value of the old (new) root CA's public key. |
| CRL Distribution Points | MUST | N | The HTTP URL of the new (old) root CA's CRL service. |
| Authority Information Access | MUST | N | This extension shall contain at least one of the following:<br>➢ The HTTP URL of the new (old) root |

| Extension | Presence | Criticality | Description |
|---|---|---|---|
| | | | CA's self-signed certificate (optional)<br>➢ The HTTP URL of the new (old) root CA's OCSP responder (optional) |
| Certificate Policies | MUST | N | This extension must contain the following information. The policy qualifier field in this extension may be used as needed. When using this field, it may contain a CPS pointer qualifier that points to this CPS.<br>➢ All the CA/Browser Forum-assigned OID(s) referenced in the ePKI CP.<br>➢ All CP OIDs defined in the ePKI CP. |
| Key Usage | MUST | Y | The content in this extension shall be identical to the content of the key usage extension in the old (new) root CA's self-signed certificate. |
| Basic Constraints | MUST | Y | Subject Type=CA<br>Path Length Constraint=None |

(3) Subordinate CA Certificate

| Extension | Presence | Criticality | Description |
|---|---|---|---|
| Authority Key Identifier | MUST | N | Only the keyIdentifier field, used to contain the SHA-1 hash value of the root CA's public key, is present in this extension. Its value must be identical to the subjectKeyIdentifier extension of the self-signed certificate issued by the root CA. |
| Subject Key Identifier | MUST | N | The SHA-1 hash value of the subordinate CA's public key. |
| CRL Distribution Points | MUST | N | The HTTP URL of the root CA's CRL service. |
| Authority Information Access | MUST | N | This extension shall contain at least one of the following:<br>➢ The HTTP URL of the root CA's self-signed certificate (optional)<br>➢ The HTTP URL of the root CA's OCSP responder (optional) |
| Certificate Policies | MUST | N | This extension is used to indicate the one or more CP OIDs that the root CA approved and permitted the subordinate CA to use. The policy qualifier field in this extension may be used as needed. When using this field, it may contain a CPS pointer qualifier that points to this CPS. The following CP OIDs may be contained |

| Extension | Presence | Criticality | Description |
|---|---|---|---|
| | | | in this extension:<br>➢ The CA/Browser Forum-assigned OID(s) referenced in the ePKI CP.<br>➢ CP OIDs defined in the ePKI CP. |
| Extended Key Usage (EKU) | MUST | N | This extension specifies the extended key usages intended for use by the subordinate CA. The rules that must be followed are as follows:<br>■ If subordinate CA certificates will be used to issue S/MIME certificates, the following requirements shall be met in this extension:<br>➢ The value id-kp-emailProtection must be present.<br>➢ The value listed below must not be present.<br>✓ id-kp-serverAuth<br>✓ id-kp-codeSigning<br>✓ id-kp-timeStamping<br>✓ anyExtendedKeyUsage<br>■ If subordinate CA certificate will be used to issue time-stamp certificates, the following requirements shall be met in this extension:<br>➢ The value id-kp-timeStamping must be present.<br>➢ The value id-kp-serverAuth must not be present.<br>■ If subordinate CA certificate will not be used to issue S/MIME certificates or time-stamp certificates, the following requirements shall be met in this extension:<br>➢ The value id-kp-serverAuth must not be present.<br>➢ Other values may be present, but should not combine multiple independent key purposes (e.g. including id-kp-timeStamping with id-kp-codeSigning) |
| Key Usage | MUST | Y | Bits contained in this extension are as follows:<br>➢ keyCertSign (required)<br>➢ cRLSign (required)<br>➢ digitalSignature (optional) |
| Basic Constraints | MUST | Y | Subject Type=CA |

| Extension | Presence | Criticality | Description |
|---|---|---|---|
| | | | Path Length Constraint=0 |

(4) Cross-Certificate

| Extension | Presence | Criticality | Description |
|---|---|---|---|
| Authority Key Identifier | MUST | N | Only the keyIdentifier field, used to contain the SHA-1 hash value of the root CA's public key, is present in this extension. Its value must be identical to the subjectKeyIdentifier extension of the self-signed certificate issued by the root CA. |
| Subject Key Identifier | MUST | N | The SHA-1 hash value of the cross-certified CA's public key. |
| CRL Distribution Points | MUST | N | The HTTP URL of the root CA's CRL service. |
| Authority Information Access | MUST | N | This extension shall contain at least one of the following:<br>➢ The HTTP URL of the root CA's self-signed certificate (optional)<br>➢ The HTTP URL of the root CA's OCSP responder (optional) |
| Certificate Policies | MUST | N | This extension is used to indicate the one or more CP OIDs that the root CA approved and permitted the cross-certified CA to use. The policy qualifier field in this extension may be used as needed. When using this field, it may contain a CPS pointer qualifier that points to this CPS. One or more of the following CP OIDs may be contained in this extension:<br>➢ The CA/Browser Forum-assigned OID(s) referenced in the ePKI CP.<br>➢ CP OIDs defined in the ePKI CP. |
| Policy Mappings | Optional | N | This extension is used to indicate the correspondences between the certificate policies of the cross-certified CA and the ones of the root CA. It lists one or more pairs of CP OIDs. The pairing indicates the root CA considers its CP OID equivalent to the cross-certified CA's CP OID. |
| Key Usage | MUST | Y | Bits contained in this extension are as follows:<br>➢ keyCertSign (required)<br>➢ cRLSign (required) |

| Extension | Presence | Criticality | Description |
|---|---|---|---|
| | | | ➢ digitalSignature (optional) |
| Basic Constraints | MUST | Y | Subject Type=CA<br>Path Length Constraint= Set according to the needed certificate path length of the cross-certified CA. It may not be present as well. |

# Appendix 3-2: Subscriber Certificates

For subscriber certificates issued by subordinate CAs of CHTCA, the certificate extensions are described as follows according to the certificate type. The usage of extensions not mentioned in this appendix shall be handled in accordance with the provisions of Appendix 3.

(1) S/MIME Certificate

| Extension | Presence | Criticality | Description |
|---|---|---|---|
| Certificate Policies | MUST | N | The policy qualifier field in this extension may be used as needed. When using this field, it may contain a CPS pointer qualifier that points to this CPS. |
| CRL Distribution Points | MUST | N | The HTTP URL of the subordinate CA's CRL service. |
| Authority Information Access | MUST | N | Two items of information included in this extension:<br>➢ The HTTP URL of the subordinate CA's OCSP responder.<br>➢ The HTTP URL of the subordinate CA's certificate. |
| Basic Constraints | Optional | N | Subject Type=EE<br>Path Length Constraint= None |
| Key Usage | MUST | Y | Bit positions for digitalSignature and/or nonRepudiation must be set, and the dataEncipherment and/or keyEncipherment may be set. Other bits must not be set. |
| Extended Key Usage | MUST | N | ➢ The value id-kp-emailProtection must be present.<br>➢ The value listed below must not be present.<br>✓ id-kp-serverAuth<br>✓ id-kp-codeSigning<br>✓ id-kp-timeStamping<br>✓ anyExtendedKeyUsage |

(2) Time-stamp Certificate

| Extension | Presence | Criticality | Description |
|---|---|---|---|
| Certificate Policies | MUST | N | The policy qualifier field in this extension may be used as needed. When using this |

| Extension | Presence | Criticality | Description |
|---|---|---|---|
| | | | field, it may contain a CPS pointer qualifier that points to this CPS. |
| CRL Distribution Points | MUST | N | The HTTP URL of the subordinate CA's CRL service. |
| Authority Information Access | MUST | N | Two items of information included in this extension:<br>➢ The HTTP URL of the subordinate CA's OCSP responder.<br>➢ The HTTP URL of the subordinate CA's certificate. |
| Basic Constraints | Optional | N | Subject Type=EE<br>Path Length Constraint= None |
| Key Usage | Optional | Y | Bit positions for keyCertSign and cRLSign must not be set, but the digitalSignature and contentCommitment may be set. |
| Extended Key Usage | Required | Y | The value id-kp-timeStamping must be present. |

(3) Other Certificate

| Extension | Presence | Criticality | Description |
|---|---|---|---|
| Certificate Policies | MUST | N | The policy qualifier field in this extension may be used as needed. When using this field, it may contain a CPS pointer qualifier that points to this CPS. |
| CRL Distribution Points | MUST | N | The HTTP URL of the subordinate CA's CRL service. |
| Authority Information Access | MUST | N | Two items of information included in this extension:<br>➢ The HTTP URL of the subordinate CA's OCSP responder.<br>➢ The HTTP URL of the subordinate CA's certificate. |
| Basic Constraints | Optional | N | Subject Type=EE<br>Path Length Constraint= None |
| Key Usage | Optional | Y | Bit positions for keyCertSign and cRLSign must not be set. Please refer to Section 6.1.7 for the key usage of each type of certifcates. |
| Extended Key Usage | Optional | N | The value anyExtendedKeyUsage must not be present. |
| Authority Key Identifier | MUST | N | It must contain a keyIdentifier field and it |

| Extension | Presence | Criticality | Description |
|---|---|---|---|
| | | | must not contain an authorityCertIssuer or authorityCertSerialNumber field. |