Certificate Policy for the Chunghwa Telecom ecommerce Public Key Infrastructure

Version 2.4

Chunghwa Telecom Co., Ltd.

August 11, 2026

Contents

CP Version Control

Version	Date	Revision Summary
1.0	Oct. 2004	First Release.
1.1	Dec. 22, 2014	RFC 3647 Version of CP released. Add OV/DV CP OID.
1.2	Oct. 5, 2015	Revised identification of Certificate Policy and added CABF EV/IV CP OID, assurance level, publication scope of audited result, acronyms and definitions, glossary, etc.
1.3	Jan. 27, 2016	(1) Revised Section 1.4.1 SSL Certificate Applicability and description. (2) Revised Chapter 8 Compliance Audit and other assessments, Section 8.1 Frequency and circusmstances of assessment and Section 8.6 Publication of Audited Results, and deleted version number of the cited auditing criteria. (3) Revised Section 3.2.2 and 3.2.3 Identification procedures for organizations and individuals.
1.4	Sep. 9, 2016	Revised CP identification, assurance level, abbreviations and definitions, and glossary, etc.
1.5	Dec. 1, 2017	(1) Added subordinate CA's description to Section 1.3.2.2. (2) Added items to Section 2.2 Publication of certificate information.. (3) Revised Section 1.4.1 SSL Certificate Applicability for minimizing risk in accordance with the review comments by CPS reviewers of the Ministry of Economic Affairs. (4) In Section 4.9.11, stating that all ePKI CAs support OCSP Stapling. (5) In accordance with CA/Browser Forum Baseline Requirements, revised by adding SSL certificates must not temporarily suspend and Certificate Resumption in Section 4.9.13 and Section 4.9.17. (6) In Section 4.2.1 changed RAO inquiry of CAA DNS records to mandatory. (7) Revised Chapter 5 about Trusted Roles. (8) In Section 6.3.2.2 Usage Period of Subscriber Public Key and Private Key, effective from March 1, 2018 to shorten the OV, DV, IV SSL certificate validity period to 825 days. (9) In Section 7.1.4 Name Form, added related

Version	Date	Revision Summary
		Name Chaining requirement.
1.6	May 28, 2018	(1) Amended Section 1.3.1 about reorganizaiton of Policy Management Committee. (2) Based on the audit criteria information announced in CPA Canada's website (http://www.webtrust.org) to amend Abstract, Section 5.4.8, Section 6.6.2, Section 8.2, Section 8.6, and section 9.4.4. (3) Add the information of CAA issuer Domain Names of ePKI into Section 1.3.2.2 and Section 4.2.1 based on Baseline Requirements.
1.7	Apr. 30, 2019	(1) Section title revision to meet RFC 3647. (2) Add the information of self-signed certificate of the third-generation eCA and that of CA certificate of the third-generation PublicCA in Section 1.3.2. (3) Add token assurance level definitions to Section 1.4.1. (4) Amendments are made in Sections 1.5.2 and 4.9 in compliant with the Baseline Requirements. (5) Revision of Sections 3.2.6, 4.7.1, 6.1.7, 6.2.6, 6.3.2, 7.1.3, 9.9, 9.11 and 9.12.2.
1.75	Aug. 12, 2019	Add the information of CA certificate of the first-generation GTLSCA in Section 1.3.2.
1.8	Nov. 18, 2019	(1) Add the information of CA certificate of the first-generation eTSCA in Section 1.3.2. (2) Amendments is made in Section 6.3.2.2 about the validity of subscriber certificates.
1.9	Nov. 17, 2020	(1) Max validity of SSL certificates set to 398 days in compliant with the Baseline Requirements. (2) Revision of Sections 3.3, 3.4, 4.5.2, 4.9.10, 4.10.2, 5.7.3, 6.2, 6.3.2, 6.4.1, 6.6.2, 7.1 and 7.2.2.
1.95	Apr. 22, 2021	(1) Add the information of CA certificate of the first-generation CHT SMIME CA in Section 1.3.2. (2) Revision of Sections 1, 1.2, 1.3.1, 1.3.2, 1.3.4, 1.4.1, 1.4.2, 2.3, 3.1.6, 3.2.1, 3.2.2, 3.2.3,

Version	Date	Revision Summary
		3.2.5, 3.3.1, 4.2.2, 4.5.2, 4.9.12, 5.5.2, 6.2.6, 6.3.2.1, 6.3.2.2, 6.6.1, 6.6.2, 7.1.4, 8, 8.2, 8.6, 9.2.1, 9.4.2, 9.10.1, 9.10.2, 9.10.3, 9.16.1, 9.16.3 and 9.16.5.
2.0	Apr. 22, 2022	Revision of Sections 1.2, 3.1.1, 4.5.1, 4.5.2, 4.9.6, 4.9.10, 6.1.5-6.1.7, 6.2.1, 6.2.4, 6.2.6, 6.3, 6.3.1, 6.3.2.1, 6.3.2.2, 6.4.1, 6.4.2, 6.6.1-6.6.3, 7.1.2-7.1.4, 7.2.1, 7.2.2 and 7.3.
2.05	Dec. 7, 2022	Amendments are made on Sections 1.2, 1.3.1, 1.3.2, 1.5.3, 4.12.1 and 6.2.3.
2.1	Aug. 29, 2023	Amendments are made on Sections 1, 1.2, 1.5.3, 1.5.4, 3.2, 3.2.5, 4.9.3, 6.3.2.2, 8 and 8.7.
2.2	Aug. 26, 2024	Amendments are made on Sections 1.2, 1.3.2.1, 2.1, 2.2, 3.1.1, 3.1.4, 4.5.2, 4.9, 4.9.6, 4.9.7, 4.9.8, 4.9.9, 4.9.12, 4.10.1, 4.10.2, 5.4.1, 5.5.1, 5.5.2, 5.6, 6.1.7, 6.2.1, 6.2.3, 6.2.4, 6.2.5, 6.2.6, 6.2.7, 6.3.2.1, 6.3.2.2, 6.3.2.3, 6.6.1, 6.6.2, 6.7, 6.8, 7.1.2, 7.1.4, 7.1.9, 7.2.1, 7.2.2, 7.3, 7.3.1, 7.3.2 and 9.6.4.
2.3	Aug. 18, 2025	Annual review and only version number is updated.
2.4	Aug. 11, 2026	(1) Amendments are made on Sections 1, 1.2, 1.3.1, 1.3.2, 1.4.1, 1.4.2, 1.5.2.1, 2.2, 3.1.2, 3.2, 3.2.2, 3.2.5, 3.2.6, 3.2.7, 3.3.1, 4.1.1, 4.2.1, 4.4.1, 4.5.1, 4.5.2, 4.9.1.1, 4.9.6, 4.9.9, 4.9.10, 4.9.11, 4.9.13, 4.9.14, 4.9.15, 4.9.16, 4.10.1, 4.10.2, 5.3.3, 5.4.8, 6.1.1, 6.1.6, 6.1.7, 6.2, 6.2.1, 6.2.2, 6.2.5, 6.2.6, 6.3.2.1, 6.3.2.2, 6.6.1, 6.8, 7.1, 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.1.9, 7.2, 7.2.1, 7.2.2, 7.3, 7.3.1, 7.3.2, 8, 8.2, 8.6, 9.6.3, 9.16.3, Appendix 1 & Appendix 2. (2) Removed all TLS and S/MIME-related business content from the document and deleted Section 8.7.

1. Introduction

The Chunghwa Telecom ecommerce Public Key Infrastructure (ePKI) was established in conjunction with Chunghwa Telecom Co., Ltd. (CHT) to promote electronic policy and create a sound e-commerce infrastructure environment in order to provide comprehensive electronic certification services.

This Certificate Policy (CP) is a policy document drafted in accordance with the official versions of the Electronic Signatures Act of R.O.C. and related international standards such as Internet Engineering Task Force (IETF) Request for Comments (RFC) 3647, ITU-T X.509, RFC 5280 and CA/Browser Forum (http://www.cabforum.org) Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (Baseline Requirements) to provide guidance and requirements for what a CA in ePKI should include in its certification practice statement (CPS).

This certificate policy is subject to the latest version of the following policy document:

(1) Common CA Database (CCADB) Policy;

(2) Microsoft Trusted Root Program Requirements; and

(3) Apple Root Certificate Program Policy

There are five identity assurance levels defined under this CP: level 1, level 2, level 3, level 4 and test level. The higher the number, the higher the assurance level. According to ITU-T X.509 standards, the assurance level must be indicated with the CP Object Identifier (OID, see Section 1.2) and these CP OID are recorded in the certificatePolicies extension of the certificate.

The assurance level refers to the trust level of the relying party to following items:

(1) The certificates issued by CAs can be divided into two types. If a certificate is issued to an end entity (EE, see Section 1.3.7), the CP OID represents what assurance level is followed for identity authentication and issuance. If a certificate is issued to a CA, there may one or more CP OIDs in the CA certificate which means the

CA may issue certificates which comply with the CP OID assurance level to EEs.

(2) The CA-related system work procedures including certificate issuance and administration and private key delivery.

(3) The ability of the subscriber or subject in the certificate information to effectively control the private key stored in the software or hardware used by the subscriber which corresponds to the public key recorded in the certificate. In other words, the ability of the relying party to trust the binding relationship between the subject and the public key recorded on the certificate.

CAs in the ePKI shall use appropriate CP OIDs so that interoperability can be performed between CAs within the ePKI and further increase cross-field interoperability between the ePKI and domestic and international PKI fields. The five assurance levels established in this CP are only used for the administration and interoperability of the ePKI. Only other PKI fields which have equivalent approved policy are allowed to use the ePKI CP OID in the policyMappings extension of the certificate.

When a CA in the ePKI issues certificates, an appropriate CP OID may be selected to be recorded in the certificatePolicies extension of the certificate, relying parties may use the CP OID recorded in the certificate to check the scope of usage of that certificate. Relying parties may use CP OID pairs to check the corresponding CP relationship between the issuing CA and subject CA.

The items and clauses in the CP are stipulated in accordance with related laws and regulations. The term “certificate authority” in the CP refers to all certificate authorities in the ePKI. Based upon the interoperability principle between the ePKI and other domestic or foreign PKI, after being approved by CHT, eCA may perform cross-certification together with a root certification authority (root CA) outside the ePKI. If any problems result from the use of this CP by other CA outside the ePKI, that CA shall bear sole responsibility.

1.1 Overview

1.1.1 Certificate Policy

Certificate policy (CP) is one form of network certification information technology guidelines. CP refers to one set of rules listed for a certain subject or circumstance for which certificates are used. The subject or circumstance may be a certain community or joint security requirement application. The CP OID for five assurance levels has been registered in the ePKI for use by the CA to indicate the assurance level when a certificate is issued for a certain purpose. The CA can directly use the registered CP OID and relying parties may use the CP OID to check whether the applicability of the issued certificates is correct.

eCA certificates are self-signed certificates which are also a trust anchor of the ePKI. Relying parties should directly trust eCA certificates. In accordance with international standards and practices, there are no CP OID listed on eCA certificates because the eCA must possess a high level of credibility to operate at assurance level 4.

1.1.2 Relationship between the CP and the CPS

CAs must state what criteria are used for each CP assurance level in the CPS.

1.1.3 Certificate Policy Object Identifiers cited by Certification Authority

ePKI CAs shall follow the CP. CP may not be established independently. The ePKI CP OID used by CAs must be approved by CHT. Contact CHT if there are any suggestions regarding the CP.

1.2 Document Name and Identification

This document is the Certificate Policy for the Chunghwa Telecom e-commerce Public Key Infrastructure. The latest version of this CP can be obtained at: https://chtca.hinet.net/repository.html. The CP of certificates issued by the CA (not including self-signed certificates) must be recorded in the certificatePolicies extension of the certificate. The CP OIDs are registered in the id-cht arc as follows:

id-cht ::= {2 16 886 1}

id-cht-ePKI ::= {2 16 886 1 100}

id-cht-ePKI-certpolicy::= {id-cht-ePKI 0}

Assurance Level	OID Name	OID Value
Test Level	id-cht-ePKI-certpolicy-testAssurance	{id-cht-ePKI-certpolicy 0}
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 above OIDs will be gradually transferred to the id-pen-cht arc CP OIDs 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}

Assurance Level	OID Name	OID Value
Test Level	id-pen-cht-ePKI-certpolicy-testAssurance	{id-pen-cht-ePKI-certpolicy 0}
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 subordinate CA certificates and the subscriber certificates applied to PDF document signatures (certificates that are issued to organizations and/or individuals with assurance Level 1, 2, or 3) may use OID 1.3.6.1.4.1.23459.100.0.9. This OID is trusted by Adobe Approved Trust List (AATL).

1.3 PKI Participants

1.3.1 Policy Management Authority

To ensure the compliant operation and continuous business development of each PKI operated by Chunghwa Telecom, the Chunghwa Telecom Certificate Policy Management Authority (PMA) is established to be responsible for the management of this PKI. The composition of the PMA complies with the Establishment Guidelines of the PMA, wherein the President of the Information Technology Group appoints one Vice President or equivalent level to serve as the Chair, along with 6 to 9 appointed members. The tasks of the authority include:

(1) Witnessing the key generation of CA within the Chunghwa Telecom Public Key Infrastructure.

(2) Reviewing the CP, CPS or combined CP/CPS.

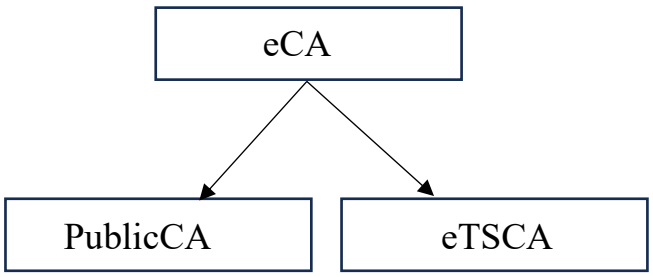
(3) Reviewing interoperability applications from cross-certified CA and their CPS.

(4) Reviewing and approving the certificate policies for cross-certified CA with the Chunghwa Telecom Public Key Infrastructure.

(5) Supervising the compliance of cross-certified CA with allowed certificate policies to facilitate the continuous operation of interoperability mechanisms.

1.3.2 Certificate Authorities

ePKI is a hierarchical PKI established in compliance with ITU-T X.509. The infrastructure includes a trust anchor, namely ePKI Root Certification Authority (eCA), and two Subordinate CAs, Public Certification Authority (PublicCA) and ePKI Timestamping Certification Authority (eTSCA). The architecture of ePKI is as follows:



1.3.2.1 ePKI Root Certification Authority

eCA is the root CA in ePKI and represents the principal CA in the ePKI. The primary duty is as follows:

(1) Responsible for issuance and administration of certificates issued by eCA, including self-signed certificates, self-issued certificates and subordinate CA certificates.

(2) Establishes cross-certification procedure between eCA and CA outside the ePKI including issuance and administration of cross-certificates outside the ePKI.

(3) Publishes issued certificates and certification revocation lists (CRLs) in the repository and ensures normal operation of the repository.

eCA shall establish subordinate CA identification and authentication procedures and cross-certification procedures for external CA in the CPS.

The certificates of the eCA, CP, and CPS shall be published in the CA repository and disclosed in the external audit report and management statement. Below is the imporatnt information for each generation of eCA certificates:

(1) Self-signed certificate of the first-generation eCA

ePKI Root Certification Authority

Cartificate Serial Number: 15 c8 bd 65 47 5c af b8 97 00 5e e4 06 d2 bc 9d

SHA-1 Certificate Fingerprints: 67 65 0d f1 7e 8e 7e 5b 82 40 a4 f4 56 4b cf e2 3d 69 c6 f0

SHA-256 Certificate Fingerprints: C0 A6 F4 DC 63 A2 4B FD CF 54 EF 2A 6A 08 2A 0A 72 DE 35 80 3E 2F F5 FF 52 7A E5 D8 72 06 DF D5

Valid Period: December 20th, 2004 to December 20th, 2034

Key Type / Key Size: RSA 4096 with SHA-1

(2) Self-signed certificate of the second-generation eCA

ePKI Root Certification Authority - G2

Certificate Serial Number: 00 d6 96 2e c1 0a 15 93 12 af 8f 63 bc d4 44 c9 5b

SHA-1 Certificate Fingerprints: d9 9b 10 42 98 59 47 63 f0 b9 a9 27 b7 92 69 cb 47 dd 15 8b

SHA-256 Certificate Fingerprints: 1E 51 94 2B 84 FD 46 7B F7 7D 1C 89 DA 24 1C 04 25 4D C8 F3 EF 4C 22 45 1F E7 A8 99 78 BD CD 4F

Valid Period: November 17th, 2015 to December 31st, 2037

Key Type / Key Size: RSA 4096 with SHA-256

(3) Self-signed certificate of the third-generation eCA

ePKI Root Certification Authority - G3

Certificate Serial Number: 62 37 e0 1b 9a ae 4e 4d f8 62 29 bb 44 49 7b 01

SHA-1 Certificate Fingerprints: cf 5f 43 17 b8 e5 55 3f 65 8e 18 02 ff 80 63 44 7a c1 76 15

SHA-256 Certificate Fingerprints: 55 8F AB 7F 4B 5D FF 16 B6 8B A4 E4 0D 1D 3E 94 0E FA 9B 01 33 50 61 7D 6F 37 7C 17 24 D9 D4 21

Valid Period: April 30th, 2019 to December 31st, 2037

Key Type / Key Size: RSA 4096 with SHA-256

(4) Self-signed certificate of the fourth-generation eCA

ePKI Root Certification Authority - G4

Certificate Serial Number:：

00 f6 70 f9 59 88 f4 52 05 8e 31 e1 68 86 3e fa 7a

SHA-1 Certificate Fingerprints:：

85 a6 69 3e d1 2c 4a ad 8d b6 9c 88 60 b5 80 13 4e bf 2c 77

SHA-256 Certificate Fingerprints:：

19 a2 fa 09 33 2c 6d 8e ac 13 93 d5 f3 03 71 dd 8b 4d d6 87

b0 e1 e5 0a 6b 48 ae 76 2c ab a2 b5

Valid Period:：November 3, 2022 to November 3, 2047

Key Type / Key Size:：RSA 4096 with SHA-256

1.3.2.2 Subordinate CA

The subordinate CA, another type of CA in the ePKI, is mainly responsible for the issuance and administration of EE certificates. When necessary, the PKI hierarchy can be followed. A level 1 subordinate CA issues certificates to a level 2 subordinate CA, or a level 2 subordinate CA issues certificates to a level 3 subordinate CA and so on to establish a multi-level hierarchy of PKI. However, the subordinate CA cannot directly cross-certify with CA outside the ePKI.

A contact window which is responsible for the interoperability work with the eCA and other subordinate CAs shall be established by the subordinate CA in accordance with CP regulations.

Currently, ePKI has two Subordinate CAs, including PublicCA and eTSCA. The subordinate CA certificates shall be disclosed in the external audit reports and management statements and registered in the Common CA Database (CCADB).

There may be multiple Subordinate CA certificates sharing the same subject name, public key, and validity period due to updates in certificate extensions. These certificates are distinguished by different serial numbers. The valid subordinate CA certificates are listed below:

(1) CA certificate of the second-generation PublicCA

A1. Public Certification Authority - G2

Certificate Serial Number:

14 35 96 f2 44 1a 71 67 98 3f fc 95 97 41 9b 53

SHA-1 Certificate Fingerprints:

78 62 ca ba b6 3a c7 a7 4e 07 56 a8 f8 6a 2c 02 1a 9f 69 b3

SHA-256 Certificate Fingerprints:

DA E3 43 4F 69 6F C9 F0 F6 52 E1 B2 A6 F6 9B 5E 92 73 D0 9F 43 BD 3B DD 47 17 D6 14 1F 8C D2 C2

Valid Period: December 11th, 2014 to December 11th, 2034

Key Type / Key Size: RSA 2048 with SHA-256

A2. Public Certification Authority - G2

Certificate Serial Number:

00 ce 60 97 fd 33 e1 2d a0 75 ce dc 96 5d c0 c4 a3

SHA-1 Certificate Fingerprints:

dd b1 3c 36 50 3d ba d9 4a b0 b2 e3 89 e3 bb f4 91 31 3e 5f

SHA-256 Certificate Fingerprints:

F5 FB 67 C8 45 3E DA 34 DB EC 8A 76 65 74 F0 7A 03 54 8C 08 4A F2 F5 E6 45 5E A7 69 60 8D 9A D5

Valid Period: December 11th, 2014 to December 11th, 2034

Key Type / Key Size: RSA 2048 with SHA-256

A3. Public Certification Authority - G2

Certificate Serial Number:

00 C4 23 D2 21 91 86 8F AC 4E E2 FC E4 A0 11 D1 A7

SHA-1 Certificate Fingerprints:

A0 28 DF 21 DB 93 AF 1E BD 97 0E 0E 68 1C F9 02 C2 0B 21 85

SHA-256 Certificate Fingerprints:

60 99 30 EB 80 7A D4 20 AF DA 2A 8A A6 1B 67 48 30 39 16 8C D7 66 E0 99 42 A4 8B FE 7F 3B DC 10

Valid Period: December 11, 2014 to December 11, 2034

Key Type / Key Size: RSA 2048 with SHA-256

(2) CA certificate of the third-generation PublicCA

Public Certification Authority - G3

Certificate Serial Number:

00 88 c1 80 7b a0 ab b6 2e 1f 49 a4 2a 02 8b e4 3e

SHA-1 Certificate Fingerprints:

74 fb 76 84 87 88 37 53 3d f7 d9 19 81 66 4b 3c 6d 67 ab 8d

SHA-256 Certificate Fingerprints:

B0 F1 F7 C7 DF 83 7B DF 88 82 5A 44 44 44 E4 81 5D A7 E0 89 97 28 A0 7A E8 76 7D 5F 65 B5 09 95

Valid Period: April 30th, 2019 to December 31th, 2037

Key Type / Key Size: RSA 2048 with SHA-256

(3) CA certificate of the first-generation eTSCA

ePKI Timestamping Certification Authority - G1

Certificate Serial Number:

00 b2 14 37 d0 d6 7c 63 87 48 44 f8 46 1c 5f 4b 54

SHA-1 Certificate Fingerprints:

29 7e 0d 74 47 74 35 6e c8 09 04 d6 57 7d 14 c5 40 e4 9c be

SHA-256 Certificate Fingerprints:

DA 31 29 3D 65 97 81 C6 9E 00 85 C7 32 A2 81 1D B5 0E 5C C5 76 90 91 49 B8 0A 98 A9 B0 F9 3F D9

Valid Period: October 18th, 2019 to December 30th, 2037

Key Type / Key Size: RSA 4096 with SHA-256

1.3.2.3 Cross-Certified CA

Currently the eCA does not cross certify with any CA other than the CAs under the ePKI.

1.3.3 Registration Authorities

Registration Authority (RA) is mainly responsible for collection and authentication of subscribers' identities, attributes and contact information to facilitate CA's certificate issuance, certificate revocation and certificate administration work including re-key, modification, renewal, suspension and resumption.

The eCA itself serves the role of RA and performs RA work in accordance with the CPS approved by the PMA.

Subordinate CA may establish separate RA and outline its work in the CPS. The RA of the subordinate CA may be divided into RA directly established and operated by the subordinate CA or RA independently established and operated by customers who have signed contracts with CHT. RAs, regardless of type, must be operated in accordance in the CP and their respective CPS. RAs independently established and operated by customers who have signed contracts with CHT may adopt security control practices which are stricter than the CP or CA CPS to which it is subordinate in accordance with its internal requirements and regulations.

1.3.4 Subscribers

Subscribers refer to the certificate subject who is unablie to issue certificate and the entity in possession of the private key that corresponds with the certificate's public key. In this CP, the root CA, subordinate CA or cross-certified CA are not referred to as subscribers because they are able to issue certificates.

1.3.5 Relying Parties

The relying party refers to a third party who trusts the relationship between the certificate subject name and the public key. The relying party must verify the validity of the certificate received based on the certificate status information of the CA.

The relying party may use the certificate to verify the integrity of the digitally signed message, confirm the identity of the message sender and establish a secret communication channel between relying parties and subscribers. In addition, the relying party may use the certificate information (such as CP OIDs) to check the appropriateness of certificate use.

1.3.6 Other Participants

If the CA selects other authorities, which provide related trust services, such as an audit authority, attribute authority, time stamp authority, data archiving service authority or card management center as collaborative partners, the collaboration mechanism and mutual rights and obligations shall be set down in the CPS to ensure the efficiency and reliability of the CA service quality.

1.3.7 End Entities

The EEs in the ePKI include the following two types of entities:

(1) Private key holders responsible for the safeguarding and use of certificates.

(2) A third party (not a private key holder or a CA) which trusts certificates issued by the CA in the ePKI.

1.4 Certificate Usage

Five types of assurance levels based on different security requirements have been established by the CP in response to various different application requirements. When deciding the assurance level for issued certificates, CAs shall select an appropriate method that conforms to the security assurance level for CA operation and certificate issuance and administration by careful evaluation of the various risks, potential dangers in the environment, possible vulnerability and certificate usage / application importance within the scope of application.

1.4.1 Appropriate Certificate Uses

There are no mandatory regulations in the CP regarding the scope of certificate usage for each assurance level. There are also not restrictions concerning which communities may use certain assurance levels. The recommended scope of use is as follows:

Assurance Level	Scope of Applications
Test Level	Only provided by test use. No legal liability borne for the transmitted data.
Level 1	Use e-mail notification to verify that the applicant can operate the e-mail

Assurance Level	Scope of Applications
	account. Suitable for use in an Internet environment in which the risk of malicious activity is considered to be low or unable to provide a higher assurance level. When used for a digital signature, can be used to determine if a subscriber comes from a certain e-mail account and ensure the integrity of the signed document. When used for encryption, relying parties can use the subscriber's certificate public key to encrypt and transmit messages or symmetric key to ensure its confidentiality but is not suitable for online transactions when identity authentication and non-repudiation is required.
Level 2	Suitable for use in Internet environment where information may be tampered with but malicious tampering is not present (information interception is possible but the probability is not high). Not suitable for the signing of importance documents (life-related or high value transaction documents). Suitable for data encryption and identity verification of small value e-commerce transactions.
Level 3	Suitable for use in Internet environments in which there are malicious users, which intercept or tamper with information, and risks, which are greater than the environment of Level 2. Transmitted information includes on-line cash or property transactions.
Level 4	Suitable for use in Internet environments where potential threats to data are high or the cost to restore tampered data is high. Transmitted information includes high value on-line transactions or highly confidential documents.

This CP provides 3 authenticator assurance levels for each CA and relying party described as follows:

Authenticator Assurance Level	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. (1) Permitted token type: can use any one of the following types. ■ Memorable secret code, such as: password or personal identification number (PIN);

Authenticator Assurance Level	Descriptions
	■ Single-factor encryption software; ■ Single-factor encryption equipment; ■ Multi-factor encryption software; ■ Multi-factor encryption equipment. (2) Requirements of the token and validator: ■ 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. ■ 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. (1) Permitted token type: The verify operation shall be performed via multi-factor authentication or two-factor authentication. ■ If multi-factor authentication is taken, the available types of token include: ➢ Multi-factor encryption software; ➢ Multi-factor encryption equipment. ■ If the authentication mechanism is only two-factor, it shall include a memorable secret code token and any one-time token described below: ➢ Single-factor encryption software; ➢ Single-factor encryption equipment. (2) Requirements of the token and validator: ■ Encryption token shall use the approved encryption

Authenticator Assurance Level	Descriptions
	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. ■ The token owner and validator shall communicate with each other via authorized and securely encrypted channel to avoid man-in-the-middle attack. ■ 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. (1) Permitted token type: can use a combination of any one of the following tokens. ■ Multi-factor encryption equipment; ■ A combination of single-factor encryption equipment and memorable secret code. (2) Requirements of the token and validator: ■ The token owner and validator shall communicate with each

Authenticator Assurance Level	Descriptions
	other via authorized and securely encrypted channel to avoid man-in-the-middle attack. All encryption equipment token shall be equipped with validator capable of anti-hacking and replay attacks prevention. ■ The token shall be cryptographic module which passed FIPS 140 level 2 (or up) or is in compliance with Global Platform Trusted Execution Environment. ■ 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 authenticator assurance level defined in this CP:

Authenticator Assurance Level	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 shall choose suitable assurance level and type of certificates based on actual requirements and applications. Different certificates are applicable for different cases. When using a private key, subscribers shall choose a secure and trusted computer environment and application systems to prevent theft of the private key which could harm one's interests.

Relying parties must use the keys in compliance with Section 6.1.7 and use the certificate validation methods in accordance with international standards (such as ITU-T X.509 or RFC 5280) to verify the validity of certificates.

1.4.2 Prohibited Certificate Uses

Certificates issued by CAs under the ePKI are prohibited from being used in the scope of :

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

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

1.5 Policy Administration

1.5.1 Organization Administering the Document

Chunghwa Telecom Co., Ltd.

1.5.2 Contact Person

1.5.2.1 CP Related Issues

Any suggestion regarding this CP, please contact us by the following information.

Tel: +886 800-080-123

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

E-mail: caservice@cht.com.tw

Other information can be found at https://chtca.hinet.net/repository.html.

1.5.2.2 Certificate Problem Report

CAs shall provide the information of their contact window that is responsible for certificate problem report in their CPS.

1.5.3 Person Determining CPS Suitability for the Policy

The CA first individually checks if the CPS conforms to relevant CP regulations and then submits the CP to the PMA for review and approval. After approval, the CA may then formally introduce the ePKI CP.

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

CHT has the right to audit (in accordance with Chapter 8 regulations) CA compliance of certificate policy. The CA shall conduct regular self-audits to prove that CP assurance levels have been introduced for operation.

In order to allow the certificates issued in the ePKI to smoothly operate in various operating systems, browsers and software platforms, the ePKI has already applied to participate in the root certificate programs for operating systems, browsers and software platforms so that the eCA self-issued certificates are broadly deployed in CA trust lists of various software platforms. In conformance with root certificate program regulations and the external audit principle of uninterrupted coverage of the entire ePKI, ePKI CAs must submit the latest CPS and external audit results each year.

1.5.4 CPS Approval Procedures

The CA CPS must follow relevant laws, comply with this CP and obtain approval from CHT and the Ministry of Digital Affairs, the competent authority of the Electronic Signatures Act. If the CPS must be revised together with the posted CP revisions, the CPS is submitted to the PMA and Ministry of Digital Affairs for approval.

1.6 Definitions and Acronyms

See Appendices 1 and 2.

2. Publishing and Repository Responsibilities

2.1 Repositories

Repositories provide information inquiry and downloading services for certificates, CRL and status of certificates issued by the CA and publish certificate issuance and administrative-related information from the CP and CPS.

Repositories may be operated by CA or other authorities. One CA is not limited to having one repository, but it must have at least one primary repository for external operations. CAs shall state the repository website in the CPS and ensure the availability of the repository, suitability of access controls and information integrity. Related repository information shall be stated in the CA's CPS.

CA repository services shall be responsible for the following obligations:

(1) Publish the signed certificates, revoked certificates, or suspended certificates (if any, please refer to Section 4.9.13) according to Section 2.2.

(2) Regularly publish issued certificates.

(3) Publish the latest CP and CPS information.

(4) Repository access controls must follow the regulations in section 2.4.

(5) Ensure the accessibility and availability of the repository's data.

(6) Publish the result of the external audit.

2.2 Publication of Certificate Information

CA shall routinely publish in the repository:

(1) This ePKI CP and its CPS.

(2) CRL, including CRL issuance time and validity, certificate revocation time.

(3) Online Certificate Status Protocol (OCSP) service

(4) For the CAs' own certificates, until the expiry date of all certificates issued by their corresponding private keys.

(5) All issued certificates (including certificates issued to other CAs).

(6) Issued CRL (such as CA issued certificates given to other CAs).

(7) Privacy protection policy.

(8) The latest result of the external audit.

(9) Related latest news.

In addition to the above information, the CA shall publish information required to verify digital signatures.

CA CPS shall state the repository service suspension time limits. The CA shall state the publication and notification regulations in the CPS.

2.3 Timing or Frequency of Publication

Publication requirements for CRLs are provided in Sections 4.9.7. New or modified version of this CP is published in the eCA repository as soon as possible upon the approval of the PMA. CAs shall publish their new or modified CPS to their repositories as soon as possible upon receiving the approval letter from the competent authority.

2.4 Access Controls on Repositories

(1) Access controls are not required for CP and CA CPS.

(2) CA shall decide independently whether or not to set up access controls for certificates.

(3) CA shall protect repository information to prevent malicious open dissemination or modification. The public key and certificate status information shall be made publicly accessible via the Internet.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

CAs shall issue certificates with a non-null subject distinguished name (DN) that complies with ITU-T X.500 standards.

For certificate applications, the CA has the right to determine whether the subject alternative name provided by the subscriber will be included in the certificate. If the subject alternative name is included in the certificate, the extension shall be marked as non-critical.

3.1.2 Need for Names to be Meaningful

The certificate subject names of organizations and individuals must conform to the subject naming regulations under ROC law and use the official registered name.

The organization name of certificate subject name of the equipment or server shall be the name of the equipment or server software administrator and its common name shall be used for easy understanding, for instance, the module name, serial name or application program.

3.1.3 Anonymity or Pseudonymity of Subscribers

Certificates with anonymous names and pseudonyms can be issued to end entities by level 1 subordinate CA. If the certificates are not prohibited by the policy used (such as the type of certificate, assurance level and certificate profile) and the uniqueness of the name space can be ensured.

3.1.4 Rules for Interpreting Various Name Forms

CAs shall specify the rules for interpreting name forms in their CPS.

3.1.5 Uniqueness of Names

The certificate subject name must be unique in the PKI. CHT is responsible for establishing X.500 name space related guidelines used by CA to ensure the uniqueness of names. The CA states how to use X.500 name space in the CPS and ensures the uniqueness of the certificate subject name when naming the certificate subject with the same name.

3.1.6 Recognition, Authentication, and Role of Trademarks

If the subject name contains a trademark, its naming shall conform to relevant ROC trademark laws and regulations.

3.1.7 Dispute Resolution of Naming

Name ownership is handled in accordance the naming rules in relevant ROC laws and regulations (for example the Company Act, Name Act and Civil Education Act). CAs shall detail the name claim dispute resolution procedure in the CPS. CAs do not need to establish regulations for test assurance level operations.

CHT is the arbitration authority for PKI name claim disputes.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

When the CA applied for a certificate, it is checked if the applicant's private key and the public key listed on the certificate form a pair.

Different methods shall be used by those who generate different keys to prove possession of the private key. The following two methods to prove possession are stipulated in the CP:

(1) Trusted third party (i.e. card issuance authority) generates the key pair for the subscriber:
The CA or RA must obtain the subscriber's public key via secure channels from a trusted third party in accordance with the regulations in section 6.1.3. The subscriber does not need to prove possession of the corresponding private key but must undergo identity identification in accordance with the regulations in sections 3.2.2 and 3.2.3 to obtain the private key and activation data. The regulations in section 6.1.2 are followed to deliver the private key to the subscriber.

(2) Key pair self-generated by subscriber:
The private key used by the subscriber can be used to create a signature and this signature is provided to the CA or RA in

accordance with the regulations in section 6.1.3. The CA or RA uses the subscriber's public key to verify the signature and prove subscriber possession of the private key. The CP allows use of other methods (such as the methods listed in RFC 2510 and RFC 2511) in equivalent security levels to prove possession of the private key.

3.2.2 Authentication of Organization Identity

There are different regulations for different assurance levels regarding the number of documents needed for organization identity authentication, identification and authentication procedure and whether in-person application is required as listed in the table below:

Assurance Level	Organization Identity Identification and Authentication
Test level	No stipulation
Level 1	(1) Document checking is not required. (2) Applicant only needs to have e-mail address to apply for certificate. Identification and authentication procedure does not need to be performed. (3) In-person application at counter is not required.
Level 2	(1) Document checking is not required. (2) Subscriber submits organization information such as organization identity ID number (i.e. withholding tax ID number), organization name shall be checked against CA approval information. (3) In-person application at counter is not required.
Level 3	CAs are allowed to use the following methods for authentication of organization identity: (1) In-person (physically-present) identity proofing at counter, which can be one of the following means: a. A certification document or official document issued by government agency in the jurisdiction of the applicant; b. Public information obtained from a qualified government information source (QGIS) such as the MOEA industry and business registration

Assurance Level	Organization Identity Identification and Authentication
	database or a qualified government tax information source (QTIS) such as the Fiscal Information Agency of MOF; or c. Organizations belonging to CHT apply for the certificate with written application. (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: a. Application through an identity assurance level 3 organization certificate issued by the GPKI or ePKI; 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; c. A letter attesting that subject information is correct written by an accountant, lawyer, or notary; d. A site visit by CA personnel or a third party who is acting as an agent for the CA; or e. Organizations belonging to CHT apply for the certificate with e-form.
Level 4	Organization identity authentication can be divided into the following two types: (1) Private organization identity authentication Application information includes the organization name, location and representative name which is sufficient to identify the organization. In addition to verifying the authenticity of the application information and representative identity, the CA or RA shall verify that the representation has the right to apply for certificate using the name of the organization. The representative shall present the application in person at the counter with the CA or RA. The above mentioned private organization refers to the corporate bodies, non-corporate bodies

Assurance Level	Organization Identity Identification and Authentication
	or the organizations belonging to the previous two. (2) Identity authentication for organizations belonging to CHT Organizations belonging to CHT who must apply for the certificate shall appoint an individual by official document who can be authenticated by the CA or RA. The representative of the agency or authority shall apply for the certificate with the CA or RA in person. The CA or RA shall verify that the agency or authority really exists and the authenticity of the public document. The identity of the individual representing the agency or authority shall be authenticated in accordance with the assurance level 4 regulations under section 3.2.3.

3.2.3 Authentication of Individual Identity

There are different regulations regarding the number of documents required for individual identity authentication at different assurance levels as shown in the Table below:

Assurance Level	Authentication of Individual Identity Procedure
Test level	No stipulation
Level 1	(1) Documentation check is not required. (2) Applicant only needs to have an e-mail address to apply for certificate. Identification and authentication procedure does not need to be performed. (3) In-person application at counter is not required.
Level 2	(1) Documentation checking is not required. (2) Subscriber submits personal information including personal identification code (such as ID card number) and name which is checked against CA recognized information. (3) In-person application at counter is not required.

Assurance Level	Authentication of Individual Identity Procedure
Level 3	(1) Check documentation: The subscriber shall present at least one original approved photo ID (such as National ID, passport or health insurance card) during certificate application to the CA or RA to authenticate the subscriber's identity. 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. (2) Personal information submitted by the subscriber such as personal identification code (ID card number), name and address (household registration address) shall be checked against the information registered with the competent authority (such as household registration information) or other information registered with a trusted third party recognized by the competent authority. (3) Counter application: The subscriber must verify his / her identity in person at the CA or RA. If the subscriber is unable to present the application in person, the subscriber may submit a letter of appointment to appoint an agent to submit the application in person on their behalf but the CA or RA must verify the authenticity of the letter of appointment (such as the subscriber's seal on the letter of appointment or verify the identity of the agent by means of communication provided by a trusted source) and authenticate the identity of the agent in accordance with the above regulations.

Assurance Level	Authentication of Individual Identity Procedure
	If an individual has previously passed through the CA, RA or CA trusted authority or individual (such as household registration office, notary or personnel authorized by the Company) counter identification and authentication procedure which conforms to the above regulations and supporting identification and authentication information (such as seal certification) has been submitted, the individual does not need to apply in person. The CA or RA needs to verify the supporting information. (4) Use MOICA certificates to apply for certificate When a digital signature with an assurance level 3 certificate issued by the MOICA is applied for certificate, the subscriber does not need to verify his / her identity in person at the CA or RA but the CA or RA shall verify that the digital signature is valid. (5) When a digital signature with an assurance level 3 personal certificate issued through the ePKI for hardware devices or server software certificates, the representative does not need to apply in person at the counter but the CA or RA shall verify the digital signature for the certificate application information.
Level 4	(1) Checking documentation: The subscriber shall at least present one original approved photo ID (such as national ID card) during certificate application for authentication of the subscriber identity by the CA and RA. (2) Subscriber submits personal information including personal identification code (such as ID card number), name and address (such as household registration address) which is checked against the information registered with competent authorities (such as household

Assurance Level	Authentication of Individual Identity Procedure
	registration agency). (3) The subscriber must verify his identity with the CA or RA when applying in person.

3.2.4 Non-verified Subscriber Information

The CA does not need to check if the common name of assurance level 1 and test level personal certificates is the legal name of the applicant.

3.2.5 Validation of Authority

When there is a connection between a certain individual (certificate applicant) and certificate subject name and there are certificate lifecycle activities such as a certificate application or revocation request, the CA shall state how the CA and its RA perform validation of authority in the CPS to verify that the individual can represent the certificate subject.

3.2.6 Criteria for Interoperation

CAs shall review at least the CP, CPS, and certificate types issued of the PKI that a Root CA wishing to interoperate with belongs to. In addition, all CAs under that PKI shall undergo routine external audits of WebTrust for CA standards.

3.2.7 Data Source Accuracy

Prior to using any data source as a Reliable Data Source, the CA SHALL evaluate the source for its reliability, accuracy, and resistance to alteration or falsification. The CA SHALL consider the followings 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.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

Certificate re-key is the issuance of a new certificate possessing the same characteristics and assurance level as the old certificate. Besides the different public key (corresponding with the new and different private key) and different serial number, the new certificate may also be assigned a different validity period.

When a subordinate CA renews the key pair, identification and authentication of the CA to which the subordinate CA certificate is issued shall be performed in accordance with Section 3.2 before the new certificates are issued to the subordinate CA.

Subscribers of the subordinate CAs must comply with the following authentication requirements when renewing a key:

Assurance Level	Authentication Requirements for Re-key of Subscriber Certificates
Test level	No stipulation
Level 1	A subscriber's identity shall be validated through use of current signature key or follow the same procedures as initial registration processes in Section 3.2.
Level 2	A subscriber's identity shall be validated through use of current signature key or follow the same procedures as initial registration processes in Section 3.2. However, each subscriber shall re-establish its identity using the initial registration processes of Section 3.2 if the identity has been validated for 15 years from the time of initial registration.
Level 3	A subscriber's identity shall be validated through use of current signature key or follow the same procedures as initial registration processes in Section 3.2. However, each subscriber shall re-establish its identity using the initial registration processes of Section 3.2 if the identity has been validated for 9 years from the time of initial registration.
Level 4	A subscriber's identity shall be validated through use of current signature key or follow the same procedures as initial registration processes in Section 3.2. However, each

Assurance Level	Authentication Requirements for Re-key of Subscriber Certificates
	subscriber shall re-establish its identity using the initial registration processes of Section 3.2 if the identity has been validated for 3 years from the time of initial registration.

3.3.2 Identification and Authentication for Re-key After Revocation

The subscriber whose certificate has been revoked shall re-establish its identity using the initial registration processes of Section 3.2.

3.4 Identification and Authentication for Revocation Request

CAs or RAs shall conduct identification and authentication for certificate revocation request. CAs shall specify the methods for validating the identities of applicants in their CPS that comply with Section 4.9 to ensure that the applicants have the rights to submit the revocation request.

Requests to revoke a certificate may be authenticated using that certificate's public key, regardless of whether the associated private key has been compromised.

4. Certificate Life-cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

eCA certificate applicants include eCA, subordinate CA established by CHT or root CA outside the PKI.

Subordinate CA certificate applicants include organizations or individuals.

Computer and communications equipment (such as routers, firewalls and load balancers) do not have the capacity to act under the law so the organization or individual who administers the equipment must submit the certificate application.

4.1.2 Enrollment Process and Responsibilities

The CA is responsible for ensuring that the identity of the certificate applicant is authenticated prior to certificate issuance in accordance with the CP and CPS regulations. The certificate applicant is responsible for providing sufficient and correct information and the identity certification documents to the CA or its RA so the necessary identity identification and authentication can be conducted prior to certificate issuance. Subscribers who accept CA issued certificates shall have the following obligations:

(1) Follow the regulations and procedures in Chapters 3 and 4.

(2) Use the certificate in a correct manner.

(3) Properly safeguard and use the private keys (not required for certificates issued at the test assurance level).

(4) Notify the CA immediately in the event of private key compromise (not required for certificates issued at the test assurance level).

4.2 Certificate Application Processing

The CA shall state the initial registration, certificate renewal and certificate re-key application procedures, application processing locations and websites in the CPS.

The eCA may accept certificate applications from CA established by CHT to become a level 1 subordinate CA in the PKI. The application

procedure shall be determined separately by the PMA.

The cross-certificate procedure for Root CA outside the PKI applications to the eCA shall be determined separately by the PMA.

Subordinate CA at each level in the PKI shall not accept other CA applications to become subordinate CA unless permission is given by a higher-level CA.

A negotiation between the PMA and eCA shall be conducted prior to the issuance of a cross-certificate issued by eCA to a Root CA outside ePKI.

4.2.1 Performing Identification and Authentication Functions

The CA shall ensure that the system and procedures for authenticating subscriber identity conform to CP and CPS regulations. The initial registration procedures shall be implemented in accordance with section 3.2 of the CP. The certificate applicant shall verify that the information is correct and complete. The information required for certificate applications includes both required and optional information. Only the information listed on the certificate profile is recorded on the certificate. The information provided from contact during the application process and in the certificate application by the applicant shall be kept by the CA or RA in accordance with the CP and CPS regulations in a secure and auditable manner.

4.2.2 Approval or Rejection of Certificate Applications

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

If the identify authentication cannot be successfully completed, the CA may refuse the certificate application. In addition to applicant identity identification and authentication reasons, the CA may refuse to issue the certificate for other reasons. The CA may refuse the certificate application for reasons such as previous certificate application rejection or violation of subscriber terms and conditions.

4.2.3 Time to Process Certificate Applications

Provided that the applicant submits the information in full which conforms to CP and CPS requirements, the CA and RA shall complete the certification application processing within a reasonable period of time. The

time to process certificate applications may be stated in the CPS, subscriber terms and conditions or the certificate applicant contract.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

Certificate issuance by CA shall follow the regulations in section 5.2 and the CPS. Suitable personnel shall perform the tasks related to certificate issuance. After certificate issuance, the CA or RA shall notify the applicant in a suitable manner.

eCA shall issue one self-signed certificate for each key lifecycle to establish a trust anchor. Several self-issued certificates shall also be issued in response to the changes in the key and certificate policy. The PMA must check the content of the eCA self-signed certificates and self-issued certificates. Newly issued self-issued certificates are delivered to relying parties in accordance with the regulations in section 6.1.4 and the self-issued certificates are published in the repository to allow downloading by relying parties.

When cross certificates are issued, the eCA shall state the path length constraint in the basicConstraints extension field to ensure that the certificate interoperable path is permitted, and the defined value of the certificate path length constraint is set in the permitted certificate interoperable path length.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

CAs operating at assurance levels 1, 2, 3 and 4 shall state application notification method after certificate issuance in the CPS.

If the CA or RA does not approve the certificate issuance, the certificate application shall be notified in a suitable manner and the reason for refusing to issue the certificate shall be clearly stated. In addition to applicant identity identification and authentication reasons, the CA may refuse to issue the certificate for other reasons. CAs operating at assurance levels 1, 2, 3 and 4 shall state the notification methods for certificate issuance refusal in the CPS.

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 repository service shall routinely publish the issued certificates. The RA shall delivery the certificate to the subscriber as stipulated in the CA.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

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 CP. Subscribers must have control of their private keys, which must not be used to issue certificates.

Subscribers shall protect their private keys from unauthorized use or disclosure and shall ensure that their private keys are used in accordance with the key usages specified in the certificate extensions. Subscribers shall use their certificates in accordance with this CP, the CPS of the issuing CA, and the Subscriber Agreement.

4.5.2 Relying Party Public Key and Certificate Usage

Prior to relying on a certificate, relying parties shall confirm its certificate usage and use it in accordance with this CP and the CPS of the issuing CA. Relying parties shall use tools or methods that are appropriate for the intended certificate usage and compliant with applicable international standards and specifications, such as ITU-T X.509 and relevant IETF RFCs.

Prior to the use of a certificate, the tools or methods selected by relying parties must verify all certificates in the certificate path, including the

correctness of the field contents, the integrity of the signatures, and the validity of the certificate status. Certificate status information may be obtained from CRLs or OCSP services. After certificate validation is completed, the subscriber certificate in the certificate path may be used to perform the following operations:

(1) Verify the integrity of digital signatures of electronic documents,

(2) Verify the identity of the document signer, or

(3) Establish secure communication channels with subscribers.

Relying parties shall also verify the certificate policies extension in both the issuing CA certificate and the subscriber certificate to determine the assurance levels of the certificates.

4.6 Certificate Renewal

Renewal of CA certificates is not allowed. Only subscriber certificates can be renewed. The expired, suspended, revoked certificates shall not be renewal; The maximum term of the renewal shall not exceed the upper limit of the period of public keys specified in Section 6.3.2.2, to protect the security of the keys.

4.6.1 Circumstance for Certificate Renewal

When the subscriber's certificate is about to expire, non-suspended, non-revoked certificates may be renewed under the following circumstances:

(1) Public keys listed on the certificate have not reached their usage period stipulated in section 6.3.2.2.

(2) The subscriber and identity attribute information are consistent.

(3) The private key that corresponds to the public key listed on the certificate is still valid, and is not lost or compromised.

4.6.2 Who May Request Renewal

The certificate is about to expire and the applicant is the subscriber subject or authorized representative of the original certificate.

4.6.3 Processing Certificate Renewal Requests

When the subscriber applies for certification renewal, the private key is

used to sign the certificate application file 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 identity.

4.6.4 Notification of New Certificate Issuance to Subscriber

As stated in Section 4.3.2.

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

(1) CA private keys shall be regularly renewed in accordance with Section 6.3.2.

(2) Certificate re-key is required under the following cases (but not limited to):

(a) A certificate is revoked for reasons of key compromise, and

(b) A certificate has expired and the usage period of the key pair has also expired.

For subscribers which hold assurance level 1, 2 and 3 certificates, if the certificate has not been revoked, the Subordinate CA or its RA may start to process the re-key and new certificate application two months before the expiry of the subscriber private key usage period. The procedure for applying a new certificate is performed in accordance with Section 4.2.

For the CA that issues assurance level 2, 3 and 4 certificates, if its certificate has not been revoked, eCA may start to process the re-key and new CA certificate application one month before the expiry of the CA private key usage period. The procedure for applying a new CA certificate is performed in accordance with Section 4.2.

4.7.2 Who May Request Certification of a New Public Key

CAs may accept a re-key request provided that it is authorized by either the original subscriber, or an authorized representative who retains responsibility for the private key on behalf of a subscriber through a suitable certificate lifecycle account challenge response. A certificate signing request file for certificate re-key is mandatory with any new public key.

4.7.3 Processing Certificate Re-keying Requests

When processing re-keys, the CA shall request the certificate applicant to provide extra information or reverify the subscriber identity including suitable challenge and response system identity authentication. The related procedures must be implemented in accordance with the regulations in sections 3.1, 3.2, 3.3, 4.1 and 4.2.

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

Certificate modification means creating a new certificate for the same subject, where authenticated information that slightly differs from the old certificate. The new certificate has a new certificate serial number but with the same subject public key and 'NotAfter' date.

4.8.2 Who May Request Certificate Modification

The subscriber certificate subject or an authorized representative of the certificate subject may request modification of the certificates.

4.8.3 Processing Certificate Modification Requests

As stated in Section 4.2.

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

All CAs except for those CAs operating at a test assurance level shall provide certificate revocation services. CAs shall specify the mechanism to accept and respond to revocation requests and certificate problem reports in their CPS, and CAs shall decide whether to provide certificate suspension services depending on certificate usage and service quality.

For expired certificates, CAs may not accept certificate revocation or

suspension requests and/or list the information of revocation or suspension on the CRLs. For revoked or suspended certificates prior to expiry, CAs shall list the information of revocation or suspension on the CRLs at least once. After that, the information shall be removed.

4.9.1 Circumstances for Revocation

4.9.1.1 Reasons for Revoking a Subscriber Certificate

CAs 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 the CA that the original certificate request was not authorized and does not retroactively grant authorization; or

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

CAs 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) The CA obtains evidence that the certificate was misused;

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

(4) The CA is made aware of a material change in the information contained in the certificate;

(5) The CA is made aware that the certificate was not issued in accordance with these requirements or the CA's CP/CPS;

(6) The CA determines or is made aware that any of the information appearing in the certificate is inaccurate;

(7) The CA's right to issue certificates under these requirements expires

or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository;

(8) Revocation is required by the CA's CP and/or CPS; or

(9) There is a vulnerability in the key generation process that could lead to user keys being compromised.

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

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

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

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

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

(4) The Issuing CA obtains evidence that the certificate was misused;

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

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

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

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

(9) Revocation is required by the Issuing CA's CP and/or 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

Subscriber or entities, possessing a private key that corresponds to the public key in a certificate, may request revocation of the certificate to the issuing CA or the RA. Additionally, subscribers, relying parties, application software suppliers, and other third parties may submit certificate problem reports informing the issuing CA of reasonable cause to revoke the certificate.

4.9.3 Procedure for Revocation Request

After receiving the certificate revocation request, the CA or RA shall follow the regulations in section 4.9 and the CPS to identify and authenticate the identity of the applicant. If the identity identification and authentication is free of error and the reasons for the certificate revocation is reasonable (for example, CA key compromise may not be selected for no reason), the certificate revocation request may be approved.

If the certificate revocation request has been approved or a decision has been made to revoke the certificate, the CA or RA shall assign suitable personnel to perform the certificate revocation-related tasks in accordance with the regulations in section 5.2 and the CPS. The CA or RA shall notify the subscriber in a suitable manner after certificate revocation. CAs shall state the subscriber notification method after certificate revocation in the CPS.

If the certificate revocation is not approved, the CA or RA shall notify the subscriber in a suitable manner and clearly inform the subscriber of the reasons for denying the revocation request. CAs shall state the subscriber notification method for denial of certificate revocation in the CPS.

4.9.4 Revocation Request Grace Period

The revocation request grace period is the time available to the subscriber within which the subscriber must submit a revocation request after reasons for revocation have been identified. The CA and RA are required to report the suspected compromise of their CA or RA private key and request

revocation to the issuing CA within one hour of discovery. The issuing CA may extend revocation grace periods on a case-by-case basis.

4.9.5 Time within Which CA Must Process the Revocation Request

CAs shall begin investigating the facts and circumstances related to a certificate problem report and shall provide a preliminary report on its findings to both the subscriber and the entity who filed the problem report within 24 hours of receipt of the report.

CAs shall specify the criterions and procedures used to establish whether the certificate will be revoked in their CPS. The period from receipt of the certificate problem report or revocation request to published revocation must not exceed the time frame set forth in Section 4.9.1.

4.9.6 Revocation Checking Requirement for Relying Parties

Prior to relying on a certificate of assurance level 2 or higher, relying parties must check the certificate status through CRLs or OCSP services. Relying parties must consider the risks, responsibilities, and potential impacts they bear and determine for themselves when to obtain certificate revocation information.

CAs shall state the requirements for relying parties to check the certificate's revocation status in their CPS.

4.9.7 CRL Issuance Frequency

eCA shall issue CRL and subordinate CA and subject CA shall issue CRL. Before the CRL is issued, the content shall be checked to verify the accuracy of the information. For example, use software to scan the CRL to check the accuracy of information. The CRL shall be regularly announced. CRL are issued even if the certificate status has not changed to ensure the timeliness of the certificate status information.

The announcement of certificate status information shall store the certificate status information in the local cache after the next certificate status update is completed to assist offline or remote operation of application systems. CAs shall strengthen coordination between repositories to reduce the time it takes for the certificate status information to be generated and published in the repository. The primary repository should be stated in the

CPS regulations to allow subscribers to conveniently obtain the latest certificate status information from that repository.

When the certificate status information is announced, the expired certificate status information shall be removed independently from the repository. The regulations regarding the Certificate Authority Revocation Lists (CARL) and CRL issuance frequency are stated in the Table below:

Assurance Level	CARL Issuance Frequency	CRL Issuance Frequency
Test level	Not applicable	No stipulation
Level 1	Not applicable	No stipulation
Level 2	Not applicable	At least once every 3 days
Level 3	At least once a day	At least once a day
Level 4	At least once a day	At least once a day

4.9.8 Maximum Latency for CRLs

Each CRL should be published no later than the time specified in the nextUpdate field of the previously issued CRL for same scope.

4.9.9 On-line Revocation/Status Checking Availability

CAs shall at least provide a CRL and specify whether OCSP services are supported in their CPS. If a CA does support an OCSP service, its OCSP service must conform to RFC 6960 and/or RFC 5019.

4.9.10 On-line Revocation Checking Requirements

CAs shall state the method of online revocation checking for relying parties in their CPS. If a CA supports an OCSP service, the OCSP responder operated by the CA shall at least support the HTTP GET method, as described in RFC 6960 and/or RFC 5019.

4.9.11 Other Forms of Revocation Advertisements Available

CAs may use other methods to publicize the revoked certificates. Any

alternative method must meet the following requirements:

(1) The alternative method is described in CAs' approved CPS;
(2) The alternative method must provide authentication and integrity services commensurate with the assurance level of the certificate being verified; and
(3) The alternative method must meet the issuance and latency requirements for CRLs stated in Sections 4.9.7 and 4.9.8.

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 the issuing CA of the event. The issuing CA 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.

In case of a compromise of eCA's private key, eCA shall notify software suppliers, subscribers, and relying parties about the private key compromise event as soon as possible through the website or media. In case of a compromise of a subordinate CA's private key, eCA will publish a CRL to inform software suppliers, subscribers, and relying parties about the private key compromise event.

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 the issuing CA using the compromised private key; or
(2) Submitting the private key itself.

4.9.13 Circumstances for Suspension

CAs shall specify whether to provide the service of certificate suspension and resumption in their CPS.

4.9.14 Who Can Request Suspension

Subscribers whose certificates are suspended.

4.9.15 Procedure for Suspension Request

The CA shall specify the procedures for temporary certificate suspension in its CPS.

4.9.16 Limits on Suspension Period

The CA shall specify the restrictions during the temporary certificate suspension period in its CPS.

4.9.17 Procedure for Certificate Resumption

CAs shall specify whether to provide the service of certificate suspension and resumption in their CPS.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

CAs shall provide CRLs, and may additionally provide 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 relates to a suspended certificate, the entry shall not be removed until the certificate has been resumed or has expired.

4.10.2 Service Availability

CAs shall operate and maintain their CRL and optional OCSP capability with resources sufficient to provide a response time of 10 seconds or less under normal operating conditions.

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

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

4.10.3 Operational Features

No stipulation.

4.11 End of Subscription

End of subscription signifies that subscribers stop using CAs' services. CAs shall allow 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

Private signing keys may not be escrowed.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

CAs that support session key encapsulation and recovery shall specify their practices in their CPS.

5. Facility, Management, and Operational Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

There are no requirements for CAs operating under test level or assurance level 1. The site location and construction requirements for CAs operating under assurance level 2 or above must comply with provisions for housing of highly important and sensitive data and other physical security mechanisms, including access control, security, intrusion detection and video monitoring, to prevent unauthorized access.

5.1.2 Physical Access

There are no requirements for CAs operating under test level or assurance level 1. Physical access controls must be implemented for CA equipment after cryptographic module installation and activation for CAs operating under assurance level 2 or above to prevent unauthorized access. Even if the cryptographic module is not installed or activated, physical access controls shall be implemented for related CA equipment to reduce the risk of unauthorized activation or damage to the equipment.

The physical access control requirements for each assurance level are as follows:

For the CA operating with assurance levels 1 and 2:

(1) Protect unauthorized intrusion; and

(2) Portable storage media and documents containing sensitive information are kept in a secure location.

For the CA operating with assurance levels 3 and 4:

(1) 24-hour manual or electronic monitoring system;

(2) Maintain and review access log periodically; and

(3) At least two persons jointly when performing physical control over computer system and cryptographic module.

Since the eCA must issue certificates at all assurance levels, the

security system of its facility must be in compliance with the above requirements of assurance level 4. There are no requirements for physical access control of CAs operating at test level or assurance level 1 but they must be specified in the CPS.

The following checks must be done when personnel leave the CA facility to prevent unauthorized personnel from accessing the facility.

(1) The security containers are properly secured; and

(2) Physical security systems (e.g., door locks, vent covers) are functioning properly.

5.1.3 Power and Air Conditioning

There are no requirements for CAs operating under test level or assurance level 1. There must be sufficient electrical power and air conditioning backup equipment to support CA related systems which can operate or shut down normally when affected by external factors for CAs operating under assurance level 2 or above. Meanwhile, the UPS must provide at least 6 hours of power for backup of repository data, including issued certificates and CRL.

5.1.4 Water Exposures

CAs shall protect the facility of its CA equipment from water exposure.

5.1.5 Fire Prevention and Protection

There are no requirements for CAs operating under test level or assurance level 1. The CA facilities for CAs operating under assurance level 2 or above must have automatic fire detection and alarm functions and systems which include automatic fire extinguishing equipment. Manual switches should be placed on major entrances and exits to allow manual operation by on-site personnel during emergencies.

5.1.6 Media Storage

There are no requirements for CAs operating under test level or assurance level 1. Protective system-related storage media for CAs operating under assurance level 2 or above must be safe from accidental damage (water, fire and electromagnetic fields).

5.1.7 Waste Disposal

No stipulation.

5.1.8 Off-site Backup

CAs shall specify whether off-site backup is provided, the distance from CA hosts to the backup site, and the backup items in their CPS.

5.2 Procedural Controls

5.2.1 Trusted Roles

The CA must assign trusted roles to be responsible for performance of related task to serve as a foundation of trust. The fairness of the CA may be reduced if security goals cannot be reached due to an accident or human error. The CA may adopt the following two methods to enhance security:

(1) Guarantee that the personnel performing each role have received appropriate training and is completely trustworthy.

(2) Appropriately separate each task. Each task shall be assigned to more than one person to prevent one person from having the opportunity to perform malicious activities.

Trusted roles are defined as follows:

(1) **Administrator**: Responsible for the installation, setting and maintenance of CA related systems and also the establishment and maintenance of system subscriber accounts, setting of audit parameters and generation of component keys.

(2) **CA Officer**: Activate/deactivate the issuance/revocation services of certificate.

(3) **Internal Auditor**: Checks and maintains audit logs, execution of internal audits.

(4) **System Operator**: Performs system backup and troubleshooting.

(5) **Physical security controller**: Physical security controls.

(6) **Cyber security coordinator**: security protection of the network and network facilities.

(7) **Anti-virus and anti-hacking coordinator**: providing technologies or measures of anti-virus, anti-hacking, and/or anti-malware.

(8) **RA Officer (validation and vetting personnel, RAO)**: Responsible for processing certificate requests of issuance, revocation and re-key, including enrollment, identity identification and authentication.

5.2.2 Number of Persons Required per Task

CAs shall specify the number of persons required per task in their CPS.

5.2.3 Identification and Authentication for Each Role

Not required for the CA operating with test level and assurance level 1. For the CA operating with assurance level 2 or higher, personnel appointed to trusted roles must undergo identification and authentication before performing the tasks.

5.2.4 Roles Requiring Separation of Duties

In order to optimize the security of CA equipment and operations, CA roles requiring separation of duties are described as follows:

Assurance Level	Role Assignment Guidelines
Test level	No stipulation
Level 1	No stipulation
Level 2	Individual CA personnel shall be specifically designed the trusted roles defined in Section 5.2.1 and shall follow the regulations below: (1) An individual may assume only one of the administrator, CA officer, internal auditor, or cyber security coordinator roles. (2) Individuals designated as administrator, CA officer or internal auditor may also assume the system operator role. (3) Individuals designated as physical security controller may not assume any of the administrator, CA officer, internal auditor, or system operator role. (4) Individuals designated as RAO may not assume any of

Assurance Level	Role Assignment Guidelines
	the administrator, internal auditor, or system operator role. (5) Any individual designated as trusted role is allowed to perform self-audit.
Level 3	Same as Level 2
Level 4	Same as Level 2

5.3 Personnel Controls

CA shall be genuinely in control of personnel related to CA or RA operation and the task assignment for personnel shall comply with the following security control requirements:

(1) Documented work assignments.

(2) Conditions for performing tasks specified through regulations and contract provisions.

(3) Receive relevant training for tasks.

(4) Non-disclosure of sensitive information and certificate subscriber information by regulations and contract provisions.

(5) Work assignment must comply with conflict of interest avoidance principles.

5.3.1 Qualifications, Experience, and Clearance Requirements

CAs must conduct personnel identification work. Required qualifications for personnel selected for trusted roles are loyalty, trustworthiness, integrity and ROC citizenship. Regulations concerning personnel qualifications, selection, supervision and auditing shall be stated in the CPS.

5.3.2 Background Check Procedures

Background check procedures shall be stated in the CPS.

5.3.3 Training Requirements

CAs shall provide all personnel performing information verification duties with skills-training that covers:

(1) Basic Public Key Infrastructure knowledge,

(2) Authentication and vetting policies and procedures (including issuing CA's CP and/or CPS),

(3) Common threats to the information verification process (including phishing and other social engineering tactics),

(4) Disaster recovery and business continuity procedures, and

(5) CA/RA security principles and mechanisms.

CAs shall require RAO to pass an examination provided by the CAs on the information verification requirements outlined in the Baseline Requirements. CAs shall maintain records of such training and ensure that personnel entrusted with RAO maintain a skill level that enables them to perform such duties satisfactorily. CAs shall document that each RAO possesses the skills required by a task before allowing the RAO to perform that task.

5.3.4 Retraining Frequency and Requirements

All personnel acting in trusted roles must maintain skill levels consistent with CAs' training and performance programs. CAs shall make the personnel aware of any changes to the issuing CA's operations, such as software/hardware upgrades, work procedure changes or equipment replacement. If such operations change, the issuing CA shall provide documented retraining, in accordance with an executed training plan, to all trusted roles.

New personnel shall also take the training to meet the requirement of training programs. CAs shall review the training status of all personnel every year.

5.3.5 Job Retation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

The CA shall establish appropriate management rules to prevent unauthorized access to information by personnel and publish the relevant rules in the CPS. The CA shall take appropriate administrative and disciplinary action against personnel who have violated the CP or CPS regulations.

Appropriate administrative and disciplinary action shall be taken against eCA and repository host personnel who have violated the CP, the CPS or other procedures announced by the eCA.

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, whereas the document retention and event logging shall meet the requirements of Section 5.4.1.

5.3.8 Documentation Supplied to Personnel

The CA shall provide the CP, the CPS and documentation concerning other relevant regulations, policy and contracts to CA and RA personnel.

5.4 Audit Logging Procedures

CAs operating at test assurance level do not have to possess audit functions. CAs that issue other assurance level certificates shall possess appropriate audit log functions for related security events. Security audit logs shall be automatically generated by the system whenever possible. If not possible, records may be made in work logbooks, paper form or other physical form. All security logs, both electronic and non-electronic, shall be retained and made available during compliance audits. The security audit logs shall be maintained in accordance with the retention period for the archive stated in section 5.5.2.

5.4.1 Types of Events Recorded

Security audit functions of CA shall include security audits of the certificate administration system and the computer operating system upon which the certificate administration system depends. The following items

should be included in each audit entity (either automatically or manually recorded audit events):

(1) Type of event

(2) Entity that caused the event and operator identity

(3) Location or site of the event

(4) Time and date of event occurrence

(5) Result log of CA performing the certificate issuance or revocation procedure (regardless of successful or unsuccessful)

When an event occurs, the CA may decide independently whether to keep the audit log in electronic or physical form. The audit events recorded by CA operating at different assurance levels are stated in the Table below. Since these audit events need to be recorded and responded to, they are called auditable events:

Auditable Event/Assurance Level	**Level 1**	**Level 2**	**Level 3**	**Level 4**
Security Audit				
A.1.1 Any changes to the audit parameters e.g. audit frequency, type of event audit and new / old parameter contents		✓	✓	✓
A.1.2 Any attempt to delete or modify the audit logs.		✓	✓	✓
A.2 Identification and Authentication				
A.2.1 Successful and unsuccessful attempts to assume a role		✓	✓	✓
A.2.2 Change in the value of maximum authentication attempts		✓	✓	✓
A.2.3 Maximum number of unsuccessful authentication attempts when subscriber logs into the system		✓	✓	✓
A.2.4 An administrator unlocks an account that has been locked as a		✓	✓	✓

Auditable Event/Assurance Level	Level 1	Level 2	Level 3	Level 4
result of a number of unsuccessful authentication attempts				
A.2.5 An administrator changes the type of authenticator, e.g. from password to biometrics		✓	✓	✓
A.3 Key Generator				
A.3.1 When the CA generates a key (does not apply for single session or single use key generation)	✓	✓	✓	✓
A.4 Private Key Load and Storage				
A.4.1 Loading of component private key	✓	✓	✓	✓
A.4.2 All key recovery works and the access of the certificate subject private keys stored in the CA	✓	✓	✓	✓
A.5 Trusted Public Key Entry, Deletion and Storage				
A.5.1 All changes to the trusted public keys, including additions and deletions	✓	✓	✓	✓
A.6 Private Key Export				
A.6.1 The export of private keys (keys used for a single session or use are excluded)	✓	✓	✓	✓
A.7 Certificate Registration				
A.7.1 All certificate registration requests and processes	✓	✓	✓	✓
A.8 Certificate Revocation				
A.8.1 All certificate revocation requests and processes		✓	✓	✓
A.9 Certificate Status Change Approval				
A.9.1 The approval or rejection of		✓	✓	✓

Auditable Event/Assurance Level	Level 1	Level 2	Level 3	Level 4
a certificate status change request				
A.10 CA Configuration				
A.10.1 Any security-relevant changes to the configuration of the CA		✓	✓	✓
A.11 Account Administration				
A.11.1 Roles or users are added or deleted	✓	✓	✓	✓
A.11.2 The access control privileges of a user account or role is modified	✓	✓	✓	✓
A.12 Certificate Profile Management				
A.12.1 All changes to the certificate profile	✓	✓	✓	✓
A.13 CRL and Revocation List Profile Management				
A.13.1 All changes to CRL profiles		✓	✓	✓
A.14 Miscellaneous				
A.14.1 Installation of the operating system		✓	✓	✓
A.14.2 Installation of the CA system		✓	✓	✓
A.14.3 Installation of hardware cryptographic modules			✓	✓
A.14.4 Removal of hardware cryptographic modules			✓	✓
A.14.5 Destruction of cryptographic modules		✓	✓	✓
A.14.6 System startup		✓	✓	✓
A.14.7 Logon attempts to CA apps		✓	✓	✓
A.14.8 Receipt of hardware /			✓	✓

Auditable Event/Assurance Level	Level 1	Level 2	Level 3	Level 4
software				
A.14.9 Attempts to set passwords		✓	✓	✓
A.14.10 Attempts to modify passwords		✓	✓	✓
A.14.11 Backing up CA internal database		✓	✓	✓
A.14.12 Restoring CA internal database		✓	✓	✓
A.14.13 File manipulation (e.g. creation, renaming, moving)			✓	✓
A.14.14 Posting of any information to the repository			✓	✓
A.14.15 Access to the CA internal database			✓	✓
A.14.16 All certificate compromise notification requests		✓	✓	✓
A.14.17 Loading tokens with certificates			✓	✓
A.14.18 Transmission of token			✓	✓
A.14.19 Zeroize value of token		✓	✓	✓
A.14.20 Rekey of CA	✓	✓	✓	✓
A.15 Configuration Changes to the CA Server				
A.15.1 Hardware		✓	✓	✓
A.15.2 Software		✓	✓	✓
A.15.3 Operating system		✓	✓	✓
A.15.4 Patches		✓	✓	✓
A.15.5 Security profiles			✓	✓
A.16 Physical Access / Site Security				
A.16.1 Personnel access to the CA facility			✓	✓

Auditable Event/Assurance Level	Level 1	Level 2	Level 3	Level 4
A.16.2 Access to the CA server			✓	✓
A.16.3 Known or suspected violations of physical security		✓	✓	✓
A.17 Anomalies				
A.17.1 Software errors		✓	✓	✓
A.17.2 Software check integrity failures		✓	✓	✓
A.17.3 Receipt of improper messages			✓	✓
A.17.4 Misrouted messages			✓	✓
A.17.5 Network attacks (suspected or confirmed)		✓	✓	✓
A.17.6 Equipment failure	✓	✓	✓	✓
A.17.7 Electrical power outages			✓	✓
A.17.8 Uninterrupted power system (UPS) failure			✓	✓
A.17.9 Obvious and significant network service or access failure			✓	✓
A.17.10 Violations of Certificate Policy	✓	✓	✓	✓
A.17.11 Violations of Certification Practice Statement	✓	✓	✓	✓
A.17.12 Resetting operating system clock		✓	✓	✓

5.4.2 Frequency of Processing Log

Audit logs shall be reviewed as specified in the Table below and explanations added to the major events in the audit reports. Review work shall include verification of record tampering, examination of all log items and investigation of any alerts or irregularities in the logs. Actions taken as results of these reviews shall be documented.

Assurance Level	Frequency of Log Processing
Test level	No stipulation
Level 1	No stipulation
Level 2	No stipulation
Level 3	At least once every two months. Major security audit logs are reviewed by the CA after the previous audit review and further investigations shall be made of any possible malicious activities.
Level 4	At least once a month. Major security audit logs are reviewed by the CA after the previous audit review and further investigations shall be made of any possible malicious activities.

5.4.3 Retention Period for Audit Log

No stipulated for CAs operating with test level and assurance level 1.

The retention periods for security audit logs of CAs operating under assurance levels 2, 3 and 4 are at least two months. The log retention administration system regulations in Sections 5.4.4, 5.4.5, 5.4.6 and 5.5 shall also be followed.

After the end of the audit log retention period, the removal task shall be performed only by the internal auditor.

5.4.4 Protection of Audit Log

Protection for security audit files of CAs operating under the assurance level 1 or test level are not specified.

The electronic audit log system for CAs operating under assurance levels 2, 3 or 4 must include protection systems. Manually recorded audit information shall also be protected to prevent unauthorized reading, modification, or deletion.

5.4.5 Audit Log Backup Procedures

Assurance Level	Audit Log Backup Procedure
Test level	Not specified
Level 1	
Level 2	Backup of audit log files must be done at least once a month.
Level 3	
Level 4	Backup of audit log files must be done at least once a month. Off-site backup must be done at least once a month. Related off-site backup procedures shall be specified in the CPS.

5.4.6 Audit Collection System (Internal vs. External)

The security audit system can be inside or outside the certificate administration system. Audit procedures shall be activated upon certificate administration system startup and end only when the certificate administration system is shut down.

5.4.7 Notification to Event-causing Subject

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

5.4.8 Vulnerability Assessments

CAs operating under assurance levels 3 and 4 shall conduct routine security control vulnerability assessments. Penetration testing shall be conducted once per year. There is no vulnerability assessment requirement for CAs operating under test level or assurance levels 1 and 2.

For vulnerability assessment and penetration testing methods and frequency, CAs that issue SSL certificates shall conform to the requirements defined in WebTrust for CA – SSL Baseline and CA/Browser Forum Network and Certificate System Security Requirements.

5.5 Records Archival

5.5.1 Types of Records Archived

The following records shall be archived (not required for CAs operating

under the test assurance level) based upon the security requirements of various assurance levels.

Archived Information / Assurance Level	**Level 1**	**Level 2**	Level 3	**Level 4**
CA accreditation information (presumed use)	✓	✓	✓	✓
Certification Practice Statement	✓	✓	✓	✓
Major contracts	✓	✓	✓	✓
System and equipment configuration	✓	✓	✓	✓
Modifications and updates to systems or configurations	✓	✓	✓	✓
Certificate application data	✓	✓	✓	✓
Revocation request data		✓	✓	✓
Subscriber identity data specified in Section 3.2.3		✓	✓	✓
Document receipt and certificate acceptance		✓	✓	✓
Token activation log		✓	✓	✓
Issued or published certificates	✓	✓	✓	✓
CA rekey records	✓	✓	✓	✓
Issued and/or published CRLs		✓	✓	✓
Audit logs	✓	✓	✓	✓
Other information or applications used to verify or substantiate archive contents		✓	✓	✓
Document requests of audit personnel		✓	✓	✓

5.5.2 Retention Period for Archive

The minimum retention period for archive information is as follows:

Assurance Level	Minimum Retention Period
Test level	Not specified
Level 1	2 years
Level 2	2 years
Level 3	2 years
Level 4	20 years

If the retention period above cannot be reached with the storage media used, a system that regularly transfers archive information to new storage media must be established. The applications used to archive information must also be checked at regularly scheduled intervals (the length of the interval shall be determined by the CA competent authority).

5.5.3 Protection of Archive

There is no archive protection requirement for CAs operating under test level or assurance level 1.

For CAs operating under assurance levels 2, 3 and 4, the archive information must be stored at a location outside the CA and suitable protection provided. The protection level may not be lower than the protection level of the CA premises.

5.5.4 Archive Backup Procedures

Not specified.

5.5.5 Requirements for Time-stamping of Records

Not specified.

5.5.6 Archive Collection System (Internal or External)

Not specified.

5.5.7 Procedures to Obtain and Verify Archive Information

Procedures for the establishing, checking, formatting, packeting, transfer and storage of archive information by the CA shall be specified in the CPS.

5.6 Key Changeover

CA private keys shall be regularly renewed in accordance with the regulations in Section 6.3.2 so new private keys can be used to issue certificates in place of the old keys and all entities that rely on that CA certificate shall be notified at appropriate times.

eCA shall change its key pair used to issue certificates before the usage period of its private key has expired. eCA shall sign one new self-signed certificate and one self-issued issued mutually with the old and new private keys. The issuance procedure for these three new certificates is handled in accordance with the regulations in Section 4.3.

Subordinate CA shall renew the key pair used to issue certificates before the usage period of the certificate issued with that private key expires at the latest. After the key pair is renewed, the subordinate CA shall apply for a new certificate from the upper level CA in accordance with the regulations in Section 4.1. The superior CA must issue and publish the new CA certificate before the old CA certificate of the Subordinate CA has expired.

For root CA that is cross-certified with eCA, the time to change its key pairs depends on the CP that the Root CA complied with. After key changeover, whether the Root CA shall continue to request a cross-certificate to eCA is determined by the agreement or contract between the Root CA and CHT. If that CA wants to continue to apply for cross-certification with eCA, it shall be carried out in accordance with Section 4.2. In addition, a sufficient time is required to allow the PMA and eCA to process the request and to ensure that the eCA is able to issue and publish the new cross-certificate before the Root CA's old cross-certificate has expired.

The CA 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.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

CAs shall establish emergency and system compromise reporting and handling procedures as well as conduct annual drills.

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

In order to meet business continuity goals, CAs shall take various backup measures in accordance with CP and CPS regulations to minimize disaster losses due to computer resources, software or data corruption and quickly restore certificate issuance and administration capabilities.

CAs operating at assurance levels 3 and 4 shall conduct one computer resources, software or data corruption drill at least once a year.

5.7.3 Entity Private Key Compromise Procedures

CAs operating with assurance levels 2, 3 and 4 shall state the CA signature key compromise restoration procedure in the CPS or related documentation in order to quickly restore certificate issuance and administration capabilities.

CAs operating with assurance levels 3 and 4 shall conduct one CA signature key compromise drill at least once a year.

When the private key of a CA is compromised, the application software suppliers, subscribers, and relying parties should be notified immediately.

5.7.4 Business Continuity Capabilities after a Disaster

CAs operating with assurance level 2 or higher shall specify the steps of resuming CA facilities operation following a disaster in its CPS.

CAs operating with assurance levels 3 and 4 shall hold a drill of its disaster recovery plan at least annually.

5.8 CA or RA Termination

CAs shall terminate all or a portion of its digital certificate issuance and management operations subject to the Electronic Signatures Act.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The cryptographic module used by CA to issue certificates shall be an approved CHT cryptographic module of an equivalent security level for key generation.

The random numbers used during the key generation process shall use the algorithms in NIST FIPS 140-2 or NIST FIPS 140-3 standards and have a length and randomness that makes it computationally infeasible to calculate the same random sequence even if sufficient information and equipment are provided.

Protection shall be given to the private key stored in the cryptographic module to prevent its disclosure outside the cryptographic module. If the private key is generated in the cryptographic module, that key shall always be kept in that cryptographic module or encrypted and stored in the host. If the private key is generated outside the cryptographic module, that key shall be imported into the cryptographic module without leaving the key generation environment. The environment should assure that no personnel may use any method to obtain generated private keys without being detected. After the private key is stored in the cryptographic module, that key shall immediately be deleted from the key-generation environment.

CA shall take appropriate measures to ensure that the subscriber public key administered by the CA is a unique key in the ePKI.

Any random numbers generated by a key must be approved by CHT. The related regulations for subscriber random number, key pair and symmetric key generation and the hardware and software used are listed in the Table below:

Assurance Level	Key Generation Mechanism
Test level	Software or hardware
Level 1	Software or hardware
Level 2	Software or hardware
Level 3	Software or hardware

Assurance Level	Key Generation Mechanism
Level 4	Limited to hardware

6.1.2Private Key Delivery to Subscriber

If private keys are generated and stored inside the subscriber's cryptographic module, there is no need to deliver its private key.

If a token held by an entity (such as certificate subscriber or IC card issuance center) directly generates the key or the key is generated by another key generator and then delivered to that entity's token, the entity that generates and accepts the private key is deemed as the holder of that private key. However, if the above entity is not the subscriber who made the certificate application, the private key shall be delivered to the subscriber in a secure and auditable method.

When stored key hardware is delivered to the subscriber for all assurance levels, it should be ensured that the correct token and its activation data is delivered to the subscriber. The CA must maintain a record of the subscriber's acknowledgement of receipt of the token. When any system including secret sharing (such as code or PIN) is used, that system must ensure that only the applicant and eCA or subordinate CA are the only entities that hold that secret.

If the private key is generated by a CA, a RA or trusted third party, the cryptographic module must be securely delivered to the subscriber. The subscriber must acknowledge acceptance of the private key. The tracking records of cryptographic module storage location and status must be properly kept at least until the subscriber acknowledges acceptance of the cryptographic module.

Other persons except for subscribers may not have access or control of private keys under any circumstances. Any entity that generates a private signing key on behalf of the subscriber may not key a copy of that key.

6.1.3 Public Key Delivery to Certificate Issuer

The subscriber shall deliver its public key to the CA for identity authentication. Delivery methods include:

(1) Electronic message for certificate application sent by the RA;

(2) When keys are generated by a third party, CA or RA must obtain

the subscriber's public key through auditable secure channels;

(3) Other secure electronic mechanisms; or

(4) Secure non-electronic methods, e.g., delivering media stored the subscriber's public key via registered or express mail.

6.1.4 CA Public Key Delivery to Relying Parties

eCA must make its public key available at all times. Subordinate CAs must deliver an eCA self-signed certificate or public key to relying parties in a reliable manner, include:

(1) CAs stores eCA's self-signed certificate or public key into a token and delivers it to the relying party in a secure fashion;

(2) Out-of-band delivery of the eCA self-signed certificate or public key;

(3) Out-of-band delivery of the hash value or fingerprint of the eCA self-signed certificate or public key provided for user comparison (in-band hash value or fingerprint together with the certificate is not deemed as legitimate secure channel); or

(4) Other methods approved by the PMA.

The above out-of-band channels shall be specified in the eCA CPS. eCA shall publish the issued subordinate CA certificates in its repository.

6.1.5 Key Sizes

Assurance Level	Public Key
Test level Level 1 Level 2 Level 3	(1) Must use at least 1024-bit RSA keys or other types of keys with equivalent security strength on or before December 31, 2013. (2) Must use at least 2048-bit RSA keys or other types of keys with equivalent security strength from January 1, 2014 through December 31, 2030. (3) Must use 3072-bit RSA keys or other types of keys with equivalent security strength on or after January 1, 2031.
Level 4	Must use at least 4096-bit RSA keys or other types of keys with equivalent security strength.

6.1.6 Public Key Parameters Generation and Quality Checking

The generation and quality checking of public key parameters shall be

conducted in accordance with the adopted algorithms and relevant international standards.

CAs shall specify the principles for quality checking of public key parameters in their CPS.

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

Bit positions for keyCertSign and cRLSign must be set in the key usage extension of CA certificates. If the CA private key is used for signing OCSP responses, the digitalSignature bit must be set.

CAs must set the bits in the key usage extension of subscriber certificates according to the algorithm used for key pair generation and the intended key usage, but the keyCertSign and cRLSign bits must not be set.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

CAs shall implement physical and logical safeguards to prevent unauthorized certificate issuance. Protection of CA private keys outside the cryptographic module must consist of physical security, encryption, or a combination of both, implemented in a manner that prevents disclosure of CA private keys. CAs shall encrypt their private keys with an algorithm and key-length that, according to the state of the art, are capable of withstanding cryptanalytic attacks for the residual life of the encrypted key or key part.

6.2.1 Cryptographic Module Standards and Controls

The cryptographic module shall meet the requirements of FIPS 140-2, FIPS 140-3, or international standards with equivalent security strength. If the cryptographic module used cannot meet the aforementioned requirements due to limitations of the platform or equipment type, it may be adopted after the PMA has assessed and confirmed that it provides equivalent security protection capabilities.

Cryptographic module requirements for each entity in ePKI are shown in the following table. Except for subscribers, who shall comply with these requirements to the extent possible, each entity shall use these requirements as the minimum level of cryptographic module protection and may adopt a higher security level. The levels listed in this table are based on the security level definitions in FIPS 140-2 and FIPS 140-3.

Assurance Level / Entity	eCA	Subordinate CA	RA	Subscriber
Test level	Not applicable	Not stipulated	Not stipulated	Not stipulated
Level 1	Not applicable	Level 1 (hardware or software)	Level 1 (hardware or software)	Not stipulated
Level 2	Not applicable	Level 2 (hardware)	Level 1 (hardware or software)	Level 1 (hardware or software)
Level 3	Not applicable	Level 3 (hardware)	Level 2 (hardware)	Level 1 (hardware or software)
Level 4	Level 3 (hardware)	Level 3 (hardware)	Level 2 (hardware)	Level 2 (hardware)

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

The private signing keys of CAs issuing certificates of assurance level 3 or 4 shall be subject to the multi-person control procedures specified in Chapter 5.

6.2.3 Private Key Escrow

The private signing keys of CAs shall not be escrowed.

6.2.4 Private Key Backup

The private signing keys of CAs shall be backed up under multi-person control, and the backups shall be stored at a secure off-site location. CAs must specify the private key backup procedures in their CPS.

6.2.5 Private Key Archival

The private signing keys of CAs shall not be archived.

6.2.6 Private Key Transfer into or from a Cryptographic Module

Private keys may be exported from a cryptographic module to backup tokens, or imported from backup tokens into a cryptographic module, only for key backup, key recovery, or cryptographic module replacement. The

import or export process shall be controlled in accordance with the multi-person control procedures specified in Section 6.2.2. When private keys are exported from a cryptographic module or transferred between cryptographic modules, they shall be protected by encryption or key splitting under multi-person control to ensure that the private keys never exist in plaintext form. After the private keys are imported, all related secret parameters generated during the import process must be completely destroyed.

If the issuing CA becomes aware that a subordinate CA's private key has been communicated to an unauthorized person or an organization not affiliated with the subordinate CA, the issuing CA shall revoke all certificates that include the public key corresponding to the communicated private key.

6.2.7 Private Key Storage on Cryptographic Module

The requirements are specified in Sections 6.1.1 and 6.2.1.

6.2.8 Method of Activating Private Key

Identify authentication of the activator must be performed when the private key stored in the cryptographic module is activated. Acceptable authentication methods include (but are not limited to) pass-phrase, personal tokens, personal identification number (PIN) or biometrics. However, disclosure must be avoided when the activation data is input (should not be displayed).

Activated private keys should be safeguarded and unauthorized access should not be allowed.

6.2.9 Method of Deactivating Private Key

The cryptographic module must stop operation when not in use by means of the manual logout procedure or automatically stop operation after a period of non-operation (length of time stipulated in the CPS). If the hardware cryptographic module is no longer being used, it must be separated from the server and stored in a secure location.

6.2.10 Method of Destroying Private Key

When a private signing key and its backup is no longer needed or the certificate has expired and been revoked, the key must be destroyed. For

software cryptographic modules, CAs may destroy the private signing keys by overwriting the data. For hardware cryptographic modules, CAs may destroy the private signing keys by executing a "zeroize" command, but physical destruction of hardware is not required.

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

Public key archival is not required after the certificate has been archived 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

The maximum certificate terms and corresponding private key usage periods for CAs in ePKI are shown in the following table:

Type of CA	Private Key Usage Period	Certificate Term
Root CA	■ Issuing self-signed certificates: 15 years ■ Issuing self-issued certificates: no stipulation ■ Issuing cross-certificates: no stipulation ■ Issuing subordinate CA certificates: 15 years ■ Issuing CRLs, OCSP responder certificates, or OCSP responses: 30 years	30 years
Subordinate CA	■ Issuing subscriber certificates: 10 years ■ Issuing CRLs, OCSP responder certificates, or OCSP responses: 20 years	20 years

The validity period of subordinate CA certificates or cross-certificates issued by a Root CA shall not exceed the validity period of the Root CA's self-signed certificate.

The validity period of self-issued certificates issued for cross-signing between the Root CA's old and new keys shall not extend beyond the expiration of the self-signed certificate issued with the Root CA's old key.

6.3.2.2 Subscriber Certificate Operational Periods and Key Pair Usage Periods

The maximum certificate terms and corresponding private key usage periods for subscriber certificates in ePKI are shown in the following table:

Type of Certificate	Private Key Usage Period	Certificate Term
Time-stamp Certificate	15 months	135 months
Other Certificate	126 months	126 months

The validity period of subscriber certificates, including renewal certificates, shall not exceed the validity period of their issuing CA certificate.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Activation data for CA or subscriber private keys and other related access control mechanisms shall be adequately protected. For CAs operating at assurance levels 1, 2, and 3, the management method for the activation data may be selected by qualified individuals in trusted roles. For CAs operating at assurance level 4, the activation data shall be managed by qualified individuals in trusted roles and shall be protected using biometric data or the security mechanisms of cryptographic modules. If the activation data must be transmitted, the transmission method must maintain the confidentiality and integrity of the activation data.

6.4.2 Activation Data Protection

CAs must protect activation data used to activate private keys from disclosure by using a combination of passwords and access control mechanisms. The activation data may be protected through biometric mechanisms or retained by memorization. If a record of the activation data

needs to be kept, the record must be protected by a cryptographic module with a security level equivalent to that of the activation data to ensure its security. If the number of failed login attempts exceeds the maximum preset value specified in the CPS, the protection mechanism must be able to immediately lock the account or terminate the application.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The CA operating with assurance levels 3 and 4 and its ancillary parts must include the following computer security functions. These functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards:

(1) Authenticate the identity of users before permitting access to the system or applications,
(2) Manage privileges of users to limit users to their assigned roles,
(3) Provide security audit capability,
(4) Require use of cryptography for session communication and database security, and
(5) Support protection of process integrity and security control.

CA equipment must be 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. The CA shall enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The system development controls for CAs are as follows:

Assurance Level	System Development Controls
Test level	No stipulation.
Level 1	No stipulation.
Level 2 Level 3 Level 4	(1) The CA must ensure that the software used is developed in accordance with software engineering development methods. (2) The hardware and software must be dedicated and authorized. (3) The installation of malicious software on CA equipment must be prevented. (4) Software used by the RA must be checked for malicious code before its first use or any version update, and security scans must be performed periodically. (5) The system development and test environments shall be separated from the production environment. (6) Research and development units responsible for developing the CA system shall ensure that delivered products or programs do not contain unauthorized functions, backdoor programs, or malicious programs, and shall provide related delivery documents, test reports, and other security assessment documents.

6.6.2 Security Management Controls

The security management controls for CAs are as follows:

Assurance Level	Security Management Controls
Test level Level 1 Level 2 Level 3	(1) Software or hardware unrelated to the operation shall not be installed. (2) The CA system configurations and their modification history must be documented and controlled. (3) There must be a mechanism for detecting unauthorized modifications to the CA software or configurations. (4) When installing software, CAs must confirm that the software is the correct version and has not been tampered with.

	(5) CAs shall perform security management controls in compliance with the WebTrust for CAs audit scheme.
Level 4	(1) Software or hardware unrelated to the operation shall not be installed. (2) The CA system configurations and their modification history must be documented and controlled. (3) There must be a mechanism for detecting unauthorized modifications to the CA software or configurations. (4) When installing software, CAs must confirm that the software is the correct version and has not been tampered with. (5) The integrity of CA software must be verified before each execution. (6) CAs shall perform security management controls in compliance with the WebTrust for CAs audit scheme.

6.6.3 Life Cycle Security Controls

CAs may determine the life cycle security control measures according to their needs and specify them in their CPS.

6.7 Network Security Controls

CA hosts are not connected to external networks while their repositories are connected to the Internet to provide uninterrupted services (except during required maintenance or backup). The certificates and CRLs issued by the CA hosts are manually delivered from the CA hosts physically segregated from the external Internet to the repository and all information (certificates and CRLs) have digital signature protection. The CA repository is protected against denial of service and intrusion attacks by system patch updates, system vulnerability scanning, intrusion detection/prevention system firewall systems and filtering routers.

The CA shall continuously monitor system health and security events, conduct network and host vulnerability scans at least quarterly, and perform penetration testing at least annually. Remediation timeframes depend on the severity of the vulnerability: critical vulnerabilities shall be evaluated within 96 hours, while high and medium vulnerabilities shall be resolved within 45 to 90 days. Exceptions shall be documented, risk-assessed, and archived.

6.8 Time-stamping

CA systems shall be synchronized periodically with a reliable time source, or their system clocks shall be adjusted through automated or manual procedures when necessary, to maintain the accuracy of system clocks and ensure the accuracy of the following time information:

(1) Time of certificate issuance,
(2) Time of certificate revocation,
(3) Time of CRL issuance, and
(4) Time of system event occurrence.

Clock adjustments of CA systems are auditable events (see Section 5.4.1).

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

Certificates issued by CAs shall comply with ITU-T X.509 and RFC 5280.

CAs must ensure that the serial number of each certificate they issue is a non-sequential number greater than zero (0) and less than 2^{159}, containing at least 64 bits of output from a Cryptographically Secure Pseudorandom Number Generator (CSPRNG).

7.1.1 Version Number(s)

CAs shall issue ITU-T X.509 v3 certificates.

7.1.2 Certificate Extensions

CAs must set certificate extensions in accordance with ITU-T X.509 and RFC 5280. The certificate extensions adopted by CAs shall be specified in their CPS, with an indication of whether each extension is marked as critical.

7.1.3 Algorithm Object Identifiers

The algorithm OIDs that may be used in certificates issued by CAs are as follows:

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)}
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)}

When generating ECDSA key pairs using the aforementioned elliptic curve cryptographic algorithms, the OID for the elliptic curve parameters shall be configured according to the key size as follows:

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

CAs shall use ITU-T X.500 distinguished names in the subject and issuer fields of certificates. The attribute types of the distinguished names must be composed in accordance with ITU-T X.509 and RFC 5280.

The encoded content of the issuer distinguished name field of each certificate in the certification path shall be byte-for-byte identical with the encoded form of the subject distinguished name field of the issuing CA certificate. In addition, for each CA certificate in the certification path, the encoded content of the subject distinguished name field shall be byte-for-byte identical among all certificates whose subject distinguished names can be compared as equal, including expired and revoked certificates.

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

When CAs issue a certificate containing one of the CP OIDs set forth in Section 1.2, the inclusion of such a CP OID indicates that the certificate

was issued and is managed in accordance with the requirements applicable to that CP OID.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Processing semantics for the critical certificate policies extension must be in accordance with ITU-T X.509 and RFC 5280.

7.2 CRL Profile

CRLs issued by CAs shall comply with RFC 5280.

7.2.1 Version Number(s)

CAs shall issue ITU-T X.509 v2 CRLs.

7.2.2 CRL and CRL Entry Extensions

The CRL extensions and CRL entry extensions shall comply with ITU-T X.509 and RFC 5280.

7.3 OCSP Profile

If CAs provide OCSP services, the OCSP protocol version and the standards adopted for OCSP extensions shall be specified in their CPS. The HTTP URL of the CA's OCSP responder shall be included in the authority information access (AIA) extension of certificates.

7.3.1 Version Number(s)

The OCSP protocol version shall comply with RFC 6960 and/or RFC 5019.

7.3.2 OCSP Extensions

OCSP extensions shall comply with RFC 6960 and/or RFC 5019.

8. Compliance Audit and Other Assessments

The CA that issues assurance level 2 or higher certificates shall conduct a compliance audit in accordance with WebTrust for CA to ensure that the requirements of this CP and their CPS are being implemented and enforced.

8.1 Frequency or Circumstances of Assessment

CAs shall undergo routine external audits. Audits of CAs operating with assurance levels 3 or 4 shall be conducted at least once per year and the audited period may not exceed 12 months. Audits of CA operating with assurance level 2 shall be conducted at least once every two years. There are no regulations for CAs operating with test level and assurance level 1.

CAs shall conduct routine and non-routine audits on its subordinate CAs and RAs to ensure that the subordinate entities are operating in compliance with their CPS.

8.2 Identity/Qualifications of Assessor

Audit personnel shall be independent from the audited CA and may be performed by a qualified auditor that possesses the following qualifications:

(1) Impartial third parties, or

(2) An entity which is independent from the audited CA in organization division.

Audit personnel shall submit an impartial and independent assessment. CHT retains the qualified auditor who is familiar with CA operations and is authorized by WebTrust for CA program as a licensed WebTrust practitioner to perform WebTrust for CA audit standards 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 for CA seal audit twice at 4 man-days or the experience of conducting a CA information security management audit twice at 8 man-days and be familiar with CA certificate issuance and administration regulations. CAs shall conduct identity identification of auditors during auditing.

8.3 Assessor’s Relationship to Assessed Entity

The audit personnel shall be independent from the audited CA, as

specified in Section 8.2.

8.4 Topics Covered by Assessment

The assessment shall include the following topics:

(1) Whether a CA is operating in accordance with the CPS,

(2) Whether the requirements of the CA's CPS are being implemented and enforced subject to this CP,

(3) Audit personnel may conduct audits of organizations related to CA operations such as RA.

(4) If a CCA is signed between the CA and other root CA, that Root CA shall be considered in the assessment to ensure that the Root CA's compliance with the CCA.

8.5 Actions Taken as a Result of a Deficiency

If audit personnel find a discrepancy between the requirements of this CP or the stipulations in the CCA and the design, operation, or maintenance of a CA, the following actions shall be performed:

(1) Note the discrepancy, and

(2) Notify the responsible authority promptly about the discrepancy, and if the discrepancy is a critical fault, the PMA shall be notified as well.

The CA where the discrepancy occurred shall make improvements based on the audit report and the stipulations in this CP or the CCA.

8.6 Communications of Results

Except for any audit findings that could result in system attacks and the stipulations in Section 9.3, an audited CA shall make its audit report publicly available. Audit results are displayed with appropriate seals, including WebTrust for CA seals, on the CA's homepage. The audit report and management's assertions may be viewed by clicking on the seals. The CA 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 92 days, the CA shall provide an explanatory letter signed by the qualified auditor.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

No stipulation.

9.1.2 Certificate Access Fees

No stipulation.

9.1.3 Revocation or Status Information Access Fees

No stipulation.

9.1.4 Fees for Other Services

No stipulation.

9.1.5 Refund Policy

No stipulation.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

No stipulation.

9.2.2 Other Assets

See Section 9.2.1.

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 information generated, received and kept by CAs is deemed confidential information. Personnel currently and previously employed by the CA and various audit personnel shall bear the duty of confidentiality towards confidential information. Confidential information includes:

(1) Any personal or organization information provided during the certificate application may not be disclosed without subscriber permission and in accordance with laws and regulations.

(2) The private keys and passwords used for CA operation are deemed confidential information and may not be disclosed.

(3) Audit logs may not be fully disclosed unless under the circumstances specified in section 8.6.

CAs shall state the types of confidential information in CPS.

9.3.2 Information Not Within the Scope of Confidential Information

(1) Certificates, CRLs, revoked and suspended certificates are not deemed confidential information. Certificate revocation and suspension information is non-confidential information and may not be externally disclosed.

(2) Identification information or information recorded on certifications is not deemed confidential information or private information unless specified otherwise.

CAs shall state the types of non-confidential information in the CPS.

9.3.3 Responsibility to Protect Confidential Information

CAs shall implement security controls to prevent the disclosure or destruction of confidential information.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

CAs shall post its personal information statement and privacy declaration on its website. CAs implements privacy impact assessment, personal information risk assessments and related measures for its privacy protection plan.

9.4.2 Information Treated as Private

The personal information listed on certificate applications should not be disclosed without the subscriber's consent or in accordance with related laws. Subscriber information that cannot be obtained through certificates, CRLs or

certificate catalog service, identifiable information of personnel in CAs such as names together with palmprint or fingerprint biometrics, and personal information on confidentiality agreements or contracts are deemed private information which requires protection. CAs 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

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

Issued certificates published in the repository, revoked certificates or suspension information and CRL is not deemed confidential or private information.

9.4.4 Responsibility to Protect Private Information

The personal information required for CA operation shall be securely stored and protected in accordance with the Electronic Signatures Act, WebTrust for CA audit criteria and relevant regulations of the Personal Information Protection Act. CAs must negotiate private information protection obligations with RAs.

9.4.5 Notice and Consent to Use Private Information

To abide by the Personal Information Protection Act and related regulations, any personal information shall not be used in other areas without the consent of the subscriber or unless stipulated otherwise in the personal information protection and privacy rights declaration and the CP. Regulations related to paragraph 3 confidential information in section 9.3.1 shall be established in the CA CPS.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Unless permitted by the CP or in order to comply with legal or governmental regulatory requirements or judicial rulings, CAs shall not disclose private information to any third party. Regulations regarding provision of private information to judicial personnel stipulated in section 9.4.2 shall be established in the CA CPS.

9.4.7 Other Information Disclosure Circumstances

Follow relevant laws and regulations. Regulations regarding provision of confidential information to subscribers stipulated in section 9.3.1 shall be established in the CA CPS.

9.5 Intellectual Property Rights

CHT owns the intellectual property rights of this CP. CHT grants permission to copy (in full) and distribute this CP on a free basis according to the Copyright Act of our country, which need to be indicated that the copyright is owned by CHT. CHT reserves the right to pursue legal action for any violation of the use or dissemination of this CP.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

CAs must undertake and guarantee the following obligations:

(1) If the CA uses any assurance level OID set down in the CP during CA certificate issuance, it means that the CA guarantees the information contained in the issued certificate follows CP regulations. Unless in compliance with CP regulations, the CA may not use the CP OID for any assurance level set down in the CP for issued certificates.

(2) Implement certificate application identification and authentication procedures.

(3) Issue and post certificates.

(4) Revoke certificates.

(5) Issue and post CRLs.

(6) Issue and provide on-line certificate status inquiry protocol service response message.

(7) Implement CA personnel identification and authentication procedures.

(8) Safely generate CA private keys.

(9) Protection of CA private keys.

(10) If a RA undertakes certificate registration work, the obligations of

the RA shall be stated in the CPS or RA contract or agreement.

9.6.2 RA Representations and Warranties

RA must undertake and guarantee the following obligations:

(1) Provide certificate application services.

(2) Identify and authenticate certificate applications,

(3) Notify subscribers regarding CA and RA duties and obligations.

(4) Notify subscribers about the CP and CPS-related regulations that need to be followed when obtaining or using CA-issued certificates.

(5) Implement certificate registration checking personnel identification and authentication procedure.

(6) Administer RA private key.

(7) Legal liability arising from performance of registration work.

9.6.3 Subscriber Representations and Warranties

Subscribers shall undertake and guaramtee the following obligations:

(1) Securely generate private keys and prevent private keys from being compromised.

(2) Provide correct and complete information to the CA and RA.

(3) Follow the regulations and procedures in Chapters 3 and 4.

(4) Check correctness of the certificate information before certificate use.

(5) Properly safeguard and use private keys (not stipulated for certificate issued at test assurance level).

(6) Immediately notify the CA in the event of private key compromise (not stipulated for certificate issued at test assurance level).

(7) Appropriate suspension of certificates and CA notification includes (a) possible misunderstanding regarding changes to information submitted to the CA or information recorded on the certificates (b) any actual or suspect misure or compromise of private keys corresponding to the public key recorded on the certificate.

(8) Correctly use certificates. Only use for legal and authorized use purposes in the CPS and subscriber acceptance clauses.

(9) Proper suspension of certificates and corresponding private keys after certificate expiry.

9.6.4 Relying Party Representations and Warranties

Relying parties using certificates issued by the CA shall undertake and guarantee the following obligations:

(1) Familiar with certificate application scope and assurance level.

(2) Use certificates in accordance with certificate usage.

(3) Correctly examine digital signatures.

(4) Correctly examine the CRL or OCSP response message to verify the validity of certificates. (not stipulated for certificates issued at test assurance level)

(5) Check key usage recorded on certificates.

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

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

(8) Acceptance of a certificate issued by the CA indicates understanding and agreement of the CA's legal liability clauses in accordance with the scope of certificate use outlined in the CA's CPS.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

CAs shall state the disclaimers and limitations in their CPS to exclude errors that are not the responsibility of CAs. However, CAs may not exclude errors arising from self-negligence.

9.8 Limitations of Liability

CAs shall specify the limitations of liability in their CPS.

9.9 Indemnities

As stated in Article 14 of the Electronic Signatures Act, "A certification service provider shall be liable for any damage caused by its operation or other certification-related process to the parties, or to a bona fide person who relies on the certificate, unless the certification service provider proves that it has not acted negligently. Where a certification service provider clearly specifies the limitation for the use of the certificate, it shall not be liable for any damage arising from a contrary use."

CAs shall specify the compensation responsibility to subscribers and relying parties in their CPS. For example,

(1) CAs shall include any indemnification requirements for a subscriber's fraudulent misrepresentations on the certificate application under which the issuing CA issued the subscriber an inaccurate certificate in their Subscriber Agreements, and

(2) CAs shall include any indemnification requirements for relying parties' use of a certificate without properly checking revocation information or use of a certificate for purposes beyond what the CA permits in a Relying Party Agreement.

9.10 Term and Termination

9.10.1 Term

This CP is effective when published to eCA's repository.

9.10.2 Termination

The new version of this CP is announced after being approved by the PMA, and the current version is terminated.

9.10.3 Effect of Termination and Survival

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

9.11 Individual Notices and Communications with Participants

CHT accepts digitally signed or paper notices related to this CP that are

addressed to the locations specified in Section 1.5.2 of this CP. Notices are deemed effective after the sender receives a valid and digitally signed acknowledgment of receipt from CHT. If an acknowledgement of receipt is not received within five days, the sender must resend the notice in paper form using either an express delivery or a registered mail.

CAs shall specify the way of individual notices and communications with the participants prior to implementation of any planned change to the infrastructure in their CPS.

9.12 Amendments

9.12.1 Procedure for Amendment

The PMA shall review this CP at least annually. CAs shall review their CPS at least once a year to maintain the assurance level.

9.12.2 Notification Mechanism and Period

CAs shall post appropriate notice on its websites of any major or significant changes that could have a significant impact to subscribers. CAs shall specify the notification mechanism and period for change items in their CPS.

9.12.3 Circumstances under which OID Must Be Changed

The CP OID need not be changed if a change to the CP does not affect the certificate usage purposes and assurance level asserted by the CP. When the CP OID is changed, corresponding changes shall be made to the CPS.

9.13 Dispute Resolution Provisions

The parties to the dispute arising out of the use of certificates issued under this CP shall strive in their negotiations to reach a consensus. If negotiation fails, CHT may establish dispute settlement procedures to secure an interpretation. CAs shall specify the procedures utilized to resolve disputes in their CPS.

9.14 Governing Law

For disputes involving PKI issued certificates, related ROC laws and regulations shall govern.

9.15 Compliance with Applicable Law

All CAs operating under this CP are required to comply with applicable laws and regulations of R.O.C.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

The commitments set forth in this CP constitute the final and entire agreement between the participants (as stated in Section 1.3).

CAs shall obligate RAs by contracts or agreements to comply with this CP and applicable industry standards and guidelines. CAs shall obligate subscribers or relying parties using its products and services to enter into an agreement that delineates the terms associated with the product or service.

9.16.2 Assignment

The participants as stated in Section 1.3 may not assign or delegate their rights or obligations under this CP to other parties in any form without a prior written notice to CHT.

9.16.3 Severability

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

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

In the event that eCA suffers damages attributable to an intentional or unintentional violation of this CP by a subscriber or relying party, eCA may seek compensation for damages and indemnification and attorney’s fees from the responsible party related to the dispute or litigation. eCA’s failure to assert rights with regard to the violation of this CP to the party does not waive eCA’s right to pursue the violation of this CP later or in the future.

9.16.5 Force Majeure

CAs are not liable for any delay or failure to perform an obligation under this CP to the extent that the delay or failure is caused by a force majeure or other circumstances not attributable to CAs, including natural

disasters, wars, or terrorism which may cause the interruption of telecommunications network. CAs may specify other exemption provisions in their CPS but may not exclude mistakes arising from self-negligence.

9.17 Other Provisions

No stipulation.

Appendix 1: Acronyms

Acronyms	Full Name	Definition
AAL	Authenticator Assurance Level	
AATL	Adobe Approved Trust List	
AIA	Authority Infomation Access	See Appendix 2
CA	Certification Authority	See Appendix 2
CCA	Cross Certification Agreement	See Appendix 2
CP	Certificate Policy	See Appendix 2
CPS	Certification Practice Statement	See Appendix 2
CRL	Certificate Revocation List	See Appendix 2
DN	Distinguished Name	
DNS	Domain Name System	
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
IANA	Internet Assigned Numbers Authority	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 Standards	See Appendix 2
RA	Registration Authority	See Appendix 2
RFC	Request for Comments	See Appendix 2
UPS	Uninterrupted Power System	See Appendix 2

Appendix 2: Definitions

Access	Use of information processing capabilities of system resources.
Access Control	Authorization processing procedure for access to information system resources given to subscribers, programs, procedures and other systems.
Activation Data	The private data required besides keys to access the cryptographic module (such as data used to activate the private key for signatures or encryption).
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) Process for authenticating that a certain claimed identity is legal and belongs to the claimant. [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] (2) Safety measures used to secure data transmission or ways to authorize the privilege of individuals upon receiving certain types of information. (3) Authentication is the process by which a claimed identity is verified. [A Guide to Understanding Identification and Authentication in Trusted Systems] 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.
Backup	Information or program copying that can be used for recovery purposes when needed.
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
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] (2) Digital presentation of information. The contents include: A. Issuing certificate authority B. Subscriber name or identity

	C. Subscriber public key D. Certificate validity period E. Certification authority digital signature The term 'certificate' referred to in the certificate policy 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] (2) The competent body trusted by the subscriber. Its functions are the issuance and administration of ITU-T X.509 format public key certificates and CRLs.
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] (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 field 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]

	(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 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] (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.
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 type of certificate used to establish a trust relationship between two root CAs. This certificate is a type of CA certificates and not a subscriber certificate.
Cross Certification Agreement (CCA)	The items and individual liability and obligation authority agreement that must be followed by the eCA and subject CA when the subjectCA joins the ePKI.
Cryptographic Module	A set of hardware, software, firmware or combination of the above used to run cryptologic or programs (including cryptoalgorithms) 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.
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.
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]
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: (1) Those responsible for the safeguarding and use of certificate public keys. (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.
Chunghwa Telecom ecommerce Public Key Infrastructure (ePKI)	In order to promote Electronic Policy and create a sound e-commerce infrastructure, the Chunghwa Telecom Co., Ltd. shall follow the ITU-T X.509 standards to establish the public key infrastructure for use with various applications in e-commerce and e-government.
Chunghwa Telecom Certificate Policy Management Authority (PMA)	An organization which was established for the purpose of: Discuss and review the ePKI CP and electronic certificate system framework, accept subordinate CA and subject CA interoperation applications and other matters such as review and study of CPS and electronic certificate management matters.
ePKI Root CA (eCA)	The Chunghwa Telecom Public Key Infrastructure Root Certification Authority (Root CA) is the top level certificate authority in this hierarchical public

	key infrastructure. Their public keys are the trust anchor.
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 second-level domain, .com is the generic top-level domain, (gTLD) and .tw is the country code top-level domain (ccTLD). A fully qualified domain name always starts with a host name.
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.
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 affect how man designs, uses and manages the Internet and allows the Internet to operate smoothly.
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 Pair	Two mathematically linked keys possessing the following attributes: (1) One of the keys is used for encryption. This encrypted data may only be decrypted by the other key. (2) It is impossible to determine one key from another (from a mathematical calculation standpoint).
Internet Assigned Numbers Authority (IANA)	An organization that oversees the allocation of global IP address, domain names and many other parameters used for Internet.
Issuing CA	For an individual certificate, the CA that issues a certain certificate is the issuing CA.
National Institute of Standards and Technology (NIST)	Official website is at: http://www.nist.gov/ Similar to our Bureau of Standards, Metrology and Inspection. Its mission is to promote American innovation and industry competitiveness, encourage metrology, standards and technology to increase economic security and improve quality of life. NIST hardware cryptographic module standards and certification, key security assessment and federal government civil servant and contractor identity card standard are widely referenced and used.
Non-Repudiation	Technical evidence provided by the public key cryptosystem to support non-repudiation security service. Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. Technical non-repudiation refers to the guarantee that if a public key is used to validate a digital signature, that signature must be signed by the corresponding

	private key for a relying party.
Object Identifier (OID)	(1) One type of unique alphanumeric / numeric identifier 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] (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)	Online Certificate Status Protocol is a type of online certificate checking protocol which allows the relying party's application software to determine the certificate status (for example, revoked, valid).
Out-of-Band	A communication method (between parties) that differs from the current on-line methods and can be regarded as a special secure channel, e.g., one party uses physical registered mail to communicate with another party.
Private Key	(1) The key in the signature key pair used to generate digital signatures. (2) The key in the encryption key pair used to decrypt secret information. 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. These keys must be made public (usually in a digital certificate form) under these two

	circumstances.
Public Key Cryptography Standards (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 combination of law, policy, standards, personnel, equipment, facilities, technology, processes, audits and services developed on a broad scale and administration of asymmetric cryptography and public key certificates.
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. (2) An entity responsible for the identity identification and authentication of the certificate subject which does not issue certificates.
Re-key (a certificate)	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] (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.

Renew (a certificate)	The procedure for issuing a new certificate to renew the validity of information bound together with the public key.
Repository	(1) A trustworthy system used to store and retrieve certificates and other information relevant to certification. [Article 2-7, Chapter 1, Regulations on Required Information for Certification Practice Statements] (2) The database containing the certificate policy and certificate-related information.
Revoke a Certificate	Termination of certificate operations prior to its expiry date.
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.
Root Certification Authority (Root CA)	The highest level certificate authority in a public key infrastructure. In addition to issuing subordinate CA and self-signed certificates, the application software provider is responsible for dissemination of self-signed certificates. Chinese is the language of highest level certificate authority.
Self-Issued Certificate	Self-issued certificate is the certificate issued when the root CA replacing keys or when the certificate policy needing. It is issued by the root CAs of two generations to each other by using the private keys, to establish the certificate-trusted path between the old and new keys or the interconnection of the certificate policies.
Self-Signed Certificate	Self-signed certificate means the certificate whose name of the issuer is identical to the name of the certificate subject. In other words, it is a certificate issued by using the private key of a pair of keys to focusing the paring public key and other information. A self-signed certificate under a PKI may be used as the trust anchor of a certificate path. The subject of certificate issuance is the eCA itself. This certificate contains the public key of the eCA and

	the name of the issuer is identical to the name of the certificate subject. It may be used by the relying parties to verify the digital signature of self-issued certificates, subordinate CA certificates, cross-certificates and CRLs issued by the eCA.
Subject CA	For a CA certificate, the certificate authority referred to in the certificate subject of the certificate is the subject CA for that certificate.
Subordinate CA	In the public key infrastructure hierarchy, certificates that are issued by another certificate authority and the activities of the certificate authority are restricted to this other certificate authority.
Subscriber	An entity that (1) is the subject named or identified in a certificate issued to that entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual, an organization, an application or network device.
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	Trusted authority proves that a certain digital object exists at a certain time through digital signature.
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.
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]
WebTrust	The current version of CPA Canada's WebTrust Program(s) for Certification Authorities.
Zeroize	Method to delete electronically stored information. Storage of changed information to prevent information recovery.