Certificate Policy for the Chunghwa Telecom ecommerce Public Key Infrastructure

Version 1.9

Chunghwa Telecom Co., Ltd.

November 17, 2020

Contents

1. Introduction 1

1.1 Overview 2

1.1.1 Certificate Policy 2

1.1.2 Relationship between the CP and the CPS 3

1.1.3 Certificate Policy Object Identifiers cited by Certification Authority 3

1.2 Document Name and Identification 3

1.3 PKI Participants 6

1.3.1 Policy Management Authority 6

1.3.2 Certificate Authorities 6

1.3.3 Registration Authorities 12

1.3.4 Subscribers 13

1.3.5 Relying Parties 13

1.3.6 Other Participants 13

1.3.7 End Entities 13

1.4 Certificate Usage 14

1.4.1 Appropriate Certificate Uses 14

1.4.2 Prohibited Certificate Uses 20

1.5 Policy Administration 20

1.5.1 Organization Administering the Document 20

1.5.2 Contact Person 21

1.5.3 Person Determining CPS Suitability for the Policy 21

1.5.4 CPS Approval Procedures 22

1.6 Definitions and Acronyms 22

2. Publishing and Repository Responsibilities 23

2.1 Repositories 23

2.2 Publication of Certificate Information 23

2.3 Timing or Frequency of Publication 24

2.4 Access Controls on Repositories 24

3. Identification and Authentication 25

3.1 Naming 25
3.1.1 Types of Names 25
3.1.2 Need for Names to be Meaningful 25
3.1.3 Anonymity or Pseudonymity of Subscribers 25
3.1.4 Rules for Interpreting Various Name Forms 25
3.1.5 Uniqueness of Names 26
3.1.6 Recognition, Authentication, and Role of Trademarks 26
3.1.7 Dispute Resolution of Naming 26
3.2 Initial Identity Validation 26
3.2.1 Method to Prove Possession of Private Key 26
3.2.2 Authentication of Organization Identity 27
3.2.3 Authentication of Individual Identity 31
3.2.4 Non-verified Subscriber Information 34
3.2.5 Validation of Authority 34
3.2.6 Criteria for Interoperation 35
3.2.7 Data Source Accuracy 35
3.3 Identification and Authentication for Re-key Requests 35
3.3.1 Identification and Authentication for Routine Re-key 35
3.3.2 Identification and Authentication for Re-key After Revocation 37
3.4 Identification and Authentication for Revocation Request 37
4. Certificate Life-cycle Operational Requirements 38
4.1 Certificate Application 38
4.1.1 Who Can Submit a Certificate Application 38
4.1.2 Enrollment Process and Responsibilities 38
4.2 Certificate Application Processing 38
4.2.1 Performing Identification and Authentication Functions 39
4.2.2 Approval or Rejection of Certificate Applications 40
4.2.3 Time to Process Certificate Applications 41
4.3 Certificate Issuance 41
4.3.1 CA Actions during Certificate Issuance 41
4.3.2 Notification to Subscriber by the CA of Issuance of Certificate 42
4.4 Certificate Acceptance 42

4.4.1 Conduct Constituting Certificate Acceptance 42
4.4.2 Publication of the Certificate by the CA 43
4.4.3 Notification of Certificate Issuance by the CA to Other Entities 43
4.5 Key Pair and Certificate Usage 43
4.5.1 Subscriber Private Key and Certificate Usage 43
4.5.2 Relying Party Public Key and Certificate Usage 43
4.6 Certificate Renewal 44
4.6.1 Circumstance for Certificate Renewal 44
4.6.2 Who May Request Renewal 44
4.6.3 Processing Certificate Renewal Requests 44
4.6.4 Notification of New Certificate Issuance to Subscriber 45
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate 45
4.6.6 Publication of the Renewal Certificate by the CA 45
4.6.7 Notification of Certificate Issuance by the CA to Other Entities 45
4.7 Certificate Re-key 45
4.7.1 Circumstance for Certificate Re-key 45
4.7.2 Who May Request Certification of a New Public Key 46
4.7.3 Processing Certificate Re-keying Requests 46
4.7.4 Notification of New Certificate Issuance to Subscriber 46
4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate 46
4.7.6 Publication of the Re-keyed Certificate by the CA 46
4.7.7 Notification of Certificate Issuance by the CA to Other Entities 46
4.8 Certificate Modification 46
4.8.1 Circumstance for Certificate Modification 46
4.8.2 Who May Request Certificate Modification 47
4.8.3 Processing Certificate Modification Requests 47
4.8.4 Notification of New Certificate Issuance to Subscriber 47
4.8.5 Conduct Constituting Acceptance of Modified Certificate 47
4.8.6 Publication of the Modified Certificate by the CA 47
4.8.7 Notification of Certificate Issuance by the CA to Other Entities 47
4.9 Certificate Revocation and Suspension 47
4.9.1 Circumstances for Revocation 48

4.9.2 Who Can Request Revocation 50
4.9.3 Procedure for Revocation Request 50
4.9.4 Revocation Request Grace Period 51
4.9.5 Time within Which CA Must Process the Revocation Request 51
4.9.6 Revocation Checking Requirement for Relying Parties 51
4.9.7 CRL Issuance Frequency 52
4.9.8 Maximum Latency for CRLs 53
4.9.9 On-line Revocation/Status Checking Availability 53
4.9.10 On-line Revocation Checking Requirements 53
4.9.11 Other Forms of Revocation Advertisements Available 53
4.9.12 Special Requirements Related to Key Compromise 54
4.9.13 Circumstances for Suspension 54
4.9.14 Who Can Request Suspension 54
4.9.15 Procedure for Suspension Request 54
4.9.16 Limits on Suspension Period 54
4.9.17 Procedure for Certificate Resumption 54
4.10 Certificate Status Services 54
4.10.1 Operational Characteristics 54
4.10.2 Service Availability 55
4.10.3 Operational Features 55
4.11 End of Subscription 55
4.12 Key Escrow and Recovery 55
4.12.1 Key Escrow and Recovery Policy and Practices 55
4.12.2 Session Key Encapsulation and Recovery Policy and Practices 55
5. Facility, Management, and Operational Controls 56
5.1 Physical Controls 56
5.1.1 Site Location and Construction 56
5.1.2 Physical Access 56
5.1.3 Power and Air Conditioning 57
5.1.4 Water Exposures 57
5.1.5 Fire Prevention and Protection 57
5.1.6 Media Storage 57

5.1.7 Waste Disposal 58
5.1.8 Off-site Backup 58
5.2 Procedural Controls 58
5.2.1 Trusted Roles 58
5.2.2 Number of Persons Required per Task 59
5.2.3 Identification and Authentication for Each Role 59
5.2.4 Roles Requiring Separation of Duties 59
5.3 Personnel Controls 60
5.3.1 Qualifications, Experience, and Clearance Requirements 60
5.3.2 Background Check Procedures 60
5.3.3 Training Requirements 61
5.3.4 Retraining Frequency and Requirements 61
5.3.5 Job Retation Frequency and Sequence 62
5.3.6 Sanctions for Unauthorized Actions 62
5.3.7 Independent Contractor Requirements 62
5.3.8 Documentation Supplied to Personnel 62
5.4 Audit Logging Procedures 62
5.4.1 Types of Events Recorded 63
5.4.2 Frequency of Processing Log 68
5.4.3 Retention Period for Audit Log 68
5.4.4 Protection of Audit Log 68
5.4.5 Audit Log Backup Procedures 69
5.4.6 Audit Collection System (Internal vs. External) 69
5.4.7 Notification to Event-causing Subject 69
5.4.8 Vulnerability Assessments 69
5.5 Records Archival 70
5.5.1 Types of Records Archived 70
5.5.2 Retention Period for Archive 71
5.5.3 Protection of Archive 71
5.5.4 Archive Backup Procedures 71
5.5.5 Requirements for Time-stamping of Records 71
5.5.6 Archive Collection System (Internal or External) 72

5.5.7 Procedures to Obtain and Verify Archive Information 72
5.6 Key Changeover 72
5.7 Compromise and Disaster Recovery 73
5.7.1 Incident and Compromise Handling Procedures 73
5.7.2 Computing Resources, Software, and/or Data are Corrupted 73
5.7.3 Entity Private Key Compromise Procedures 73
5.7.4 Business Continuity Capabilities after a Disaster 73
5.8 CA or RA Termination 74
6. Technical Security Controls 75
6.1 Key Pair Generation and Installation 75
6.1.1 Key Pair Generation 75
6.1.2Private Key Delivery to Subscriber 76
6.1.3 Public Key Delivery to Certificate Issuer 76
6.1.4 CA Public Key Delivery to Relying Parties 77
6.1.5 Key Sizes 77
6.1.6 Public Key Parameters Generation and Quality Checking 77
6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field) 78
6.2 Private Key Protection and Cryptographic Module Engineering Controls 78
6.2.1 Cryptographic Module Standards and Controls 78
6.2.2 Private Key (n out of m) Multi-person Control 79
6.2.3 Private Key Escrow 79
6.2.4 Private Key Backup 79
6.2.5 Private Key Archival 80
6.2.6 Private Key Transfer into or from a Cryptographic Module 80
6.2.7 Private Key Storage on Cryptographic Module 80
6.2.8 Method of Activating Private Key 80
6.2.9 Method of Deactivating Private Key 81
6.2.10 Method of Destroying Private Key 81
6.2.11 Cryptographic Module Rating 81
6.3 Other Aspects of Key Pair Management 81
6.3.1 Public Key Archival 81

6.3.2 Certificate Operational Periods and Key Pair Usage Periods 82
6.4 Activation Data 84
6.4.1 Activation Data Generation and Installation 84
6.4.2 Activation Data Protection 84
6.4.3 Other Aspects of Activation Data 84
6.5 Computer Security Controls 84
6.5.1 Specific Computer Security Technical Requirements 84
6.5.2 Computer Security Rating 85
6.6 Life Cycle Technical Controls 85
6.6.1 System Development Controls 85
6.6.2 Security Management Controls 86
6.6.3 Life Cycle Security Controls 87
6.7 Network Security Controls 87
6.8 Time-stamping 87
7. Certificate, CRL, and OCSP Profiles 88
7.1 Certificate Profile 88
7.1.1 Version Number(s) 88
7.1.2 Certificate Extensions 88
7.1.3 Algorithm Object Identifiers 88
7.1.4 Name Forms 88
7.1.5 Name Constraints 89
7.1.6 Certificate Policy Object Identifier 89
7.1.7 Usage of Policy Constraints Extension 89
7.1.8 Policy Qualifiers Syntax and Semantics 89
7.1.9 Processing Semantics for the Critical Certificate Policies Extension 89
7.2 CRL Profile 89
7.2.1 Version Number(s) 89
7.2.2 CRL and CRL Entry Extensions 90
7.3 OCSP Profile 90
7.3.1 Version Number(s) 90
7.3.2 OCSP Extensions 90
8. Compliance Audit and Other Assessments 91

8.1 Frequency or Circumstances of Assessment 91
8.2 Identity/Qualifications of Assessor 91
8.3 Assessor's Relationship to Assessed Entity 92
8.4 Topics Covered by Assessment 92
8.5 Actions Taken as a Result of a Deficiency 92
8.6 Communications of Results 93
9. Other Business and Legal Matters 94
9.1 Fees 94
9.1.1 Certificate Issuance or Renewal Fees 94
9.1.2 Certificate Access Fees 94
9.1.3 Revocation or Status Information Access Fees 94
9.1.4 Fees for Other Services 94
9.1.5 Refund Policy 94
9.2 Financial Responsibility 94
9.2.1 Insurance Coverage 94
9.2.2 Other Assets 94
9.2.3 Insurance or Warranty Coverage for End-Entities 94
9.3 Confidentiality of Business Information 95
9.3.1 Scope of Confidential Information 95
9.3.2 Information Not Within the Scope of Confidential Information 95
9.3.3 Responsibility to Protect Confidential Information 95
9.4 Privacy of Personal Information 95
9.4.1 Privacy Plan 95
9.4.2 Information Treated as Private 96
9.4.3 Information Not Deemed Private 96
9.4.4 Responsibility to Protect Private Information 96
9.4.5 Notice and Consent to Use Private Information 96
9.4.6 Disclosure Pursuant to Judicial or Administrative Process 97
9.4.7 Other Information Disclosure Circumstances 97
9.5 Intellectual Property Rights 97
9.6 Representations and Warranties 97
9.6.1 CA Representations and Warranties 97

9.6.2 RA Representations and Warranties 98
9.6.3 Subscriber Representations and Warranties 98
9.6.4 Relying Party Representations and Warranties 99
9.6.5 Representations and Warranties of Other Participants 100
9.7 Disclaimers of Warranties 100
9.8 Limitations of Liability 100
9.9 Indemnities 100
9.10 Term and Termination 101
9.10.1 Term 101
9.10.2 Termination 101
9.10.3 Effect of Termination and Survival 101
9.11 Individual Notices and Communications with Participants 101
9.12 Amendments 101
9.12.1 Procedure for Amendment 101
9.12.2 Notification Mechanism and Period 102
9.12.3 Circumstances under which OID Must Be Changed 102
9.13 Dispute Resolution Provisions 102
9.14 Governing Law 102
9.15 Compliance with Applicable Law 102
9.16 Miscellaneous Provisions 102
9.16.1 Entire Agreement 102
9.16.2 Assignment 103
9.16.3 Severability 103
9.16.4 Enforcement (Attorney's Fees and Waiver of Rights) 103
9.16.5 Force Majeure 103
9.17 Other Provisions 104
Appendix 1: Acronyms 105
Appendix 2: Definitions 107

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

Version	Date	Revision Summary
		certificate validity period to 825 days. (9) In Section 7.1.4 Name Form, added related 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. 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 and related international standards such as Internet Engineering Task Force (IETF) Request for Comments (RFC) 3647, ITU-T X.509, RFC 5280, CA/Browser Forum (http://www.cabforum.org) Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (Baseline Requirements) and CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates (EV SSL Certificate Guidelines) to provide guidance and requirements for what a CA in ePKI should include in its certification practice statement (CPS).

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 are 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

The document is the Certificate Policy for the Chunghwa Telecom e-commerce Public Key Infrastructure and was approved for publication on November 17, 2020. This CP is version 1.9. The latest version of this CP can be obtained at the website: https://eca.hinet.net or https://ePKI.com.tw. 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}

With regard to SSL certificates, if there is any inconsistency between

the CP/CPS and the Baseline Requirements, then the Baseline Requirements takes precedence. With regard to EV TLS/SSL certificates, if there is any inconsistency between the CP/CPS and the EV SSL Certificate Guidelines, then the EV SSL Certificate Guidelines takes precedence.

The certificates issued by subordinate CAs comply with the requirements defined in the Baseline Requirements and pass WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security (WebTrust for CA – SSL Baseline). The subordinate CA certificates and subscriber SSL certificates issued by the subordinate CA will be allowed to use CA/Browser Forum Organization Validation (OV) SSL CP OID ({joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate policies(1) baseline requirements(2) organization-validated(2) } (2.23.140.1.2.2)), Domain Validation (DV) SSL CP OID ({joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate policies(1) baseline requirements(2) domain-validated(1)} (2.23.140.1.2.1)) and Individual Validation (IV) SSL CP OID ({joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate policies(1) baseline requirements(2) individual-validated(3)} (2.23.140.1.2.3)) of the CA/Browser forum.

The SSL certificates issued by subordinate CAs conform to the EV SSL Certificate Guidelines and the individually negotiated certificate processing methods supported by application software providers (such as browsers or application system providers) may use the CP OID ({joint-iso-itu-t(2) international-organizations (23) ca-browser-forum(140) certificate-policies(1) ev-guidelines (1) } (2.23.140.1.1)) defined by the CA/Browser Forum for Extended Validation (EV) SSL certificates.

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

One policy management authority must be established for each PKI to ensure the continued and regular operation of the PKI. The Chunghwa Telecom Certificate Policy Management Authority (PMA) was established by CHT to be responsible for the administration of the ePKI. Within the PMA, one person shall be the convener concurrently served by a vice president or equivalent level manager in the Data Communications Business Group, Chunghwa Telecom Co., Ltd. One person shall be the executive secretary concurrently served by the Managing Director of Information Technology Department of Data Communications Business Group, Chunghwa Telecom Co., Ltd. Six to night persons shall be the PMA members served by the Managing Directors of the Enterprise Business Department, Marketing Department, Cloud System Department, Internet of Things Department, Information Technology Department and Internet Service Department at the Data Communication Business Group, Chunghwa Telecom Co., Ltd, as well as the personnel assigned by the President. Their duties are as follows:

(1) Authorize and supervise key generation of CAs in ePKI,

(2) Review ePKI CP,

(3) Review related technical specifications used in ePKI,

(4) Review ePKI CPS,

(5) Review interoperation applications submitted by cross-certified CAs,

(6) Review and approve the policy mapping for each incoming or cross-certified CA,

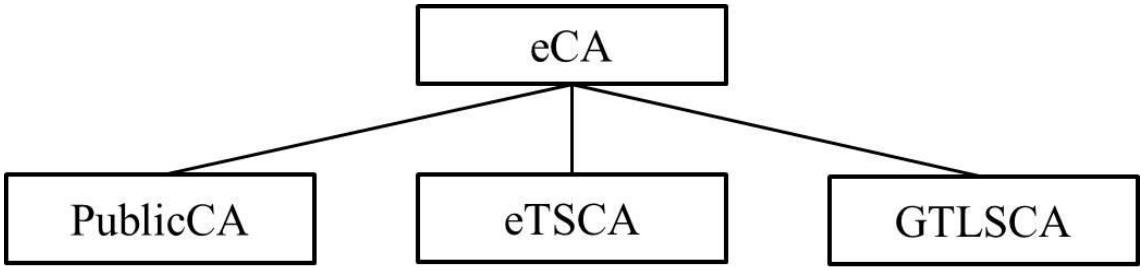
(7) Supervise cross-certified CA compliance with allowed CP to facilitate the continued operation of interconnection mechanisms, and

(8) Review ePKI TSA policy and ePKI TSA practice statement.

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 three Subordinate CAs, Public Certification Authority (PublicCA) and ePKI Timestamping Certification Authority (eTSCA) formed by CHT and Government TLS Certification Authority (GTLSCA) entrusted by National Development Council (NDC) with the task of operation. The architecture of ePKI is as follows:



1.3.2.1 ePKI Root Certification Authority

eCA is the root CA in the 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 authority revocation lists (CARLs) 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 important information, including download points, certificate serial numbers, SHA-1 certificate fingerprints, and SHA-256 certificate fingerprints, of eCA self-signed certificate that are consistent of this certificate policy and reported to each major application software providers' root certificate program for implantation, as well as disclosed in the external audit reports and management statements and registered in the Mozilla's and Microsoft's Common CA Database (CCADB) are specified as the following:

(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

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 established 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 three Subordinate CAs, PublicCA, eTSCA and GTLSCA. The subordinate CA certificates shall be disclosed in the external audit reports and management statements and registered in the Mozilla's and Microsoft's Common CA Database (CCADB). The first and the second-generation CA certificates of the PublicCA may be linked to the eCA's self-signed certificates that are still being used. The certificates of these mainly update the "Certificate Policies" extension field and certificate serial numbers, among other things. A few of CA certificates that can be used at the client-side but not disclosed in this CP shall be referred to the respository of the eCA website or the appendix of the external audit reports and management statements:

(1) CA certificate of the first-generation PublicCA

Public Certification Authority

Certificate Serial Number: 00 97 3c c9 4d 44 cf e9 a2 e1 4f 52 e9

a5 94 a1 5a

SHA-1 Certificate Fingerprints: d6 d5 c7 92 ad 6b 2e 3a b9 b4 23 01 4e 1b 40 e5 76 d8 ec bf

SHA-256 Certificate Fingerprints: 4B D1 6F 49 55 F3 F3 C9 C8 EA 48 EF 99 95 32 4D A5 12 17 24 F8 99 15 D5 F2 C9 1E B0 BA EF 23 37

Valid Period: May 16th, 2007 to May 16th, 2027

Key Type / Key Size: RSA 2048 with SHA-1

(2) CA certificate of the second-generation PublicCA

B1. 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

B2. 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

(3) 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

(4) 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

(5) CA certificate of the first-generation GTLSCA

Government TLS Certification Authority – G1

Certificate Serial Number: 00 99 6d 5f e9 ad e1 6c dc 8e cd bf ed b1 4a 32 95

SHA-1 Certificate Fingerprints: b2 d1 51 a7 68 d3 0c 3b 99 d8 6b 8b 25 81 56 08 c2 8a b2 cb

SHA-256 Certificate Fingerprints: 9d 1c da 1b 9e f3 95 af ce 7d e0 fe 74 de 6d 9f f5 e0 d2 a4 37 89 11 6c 00 c6 ba 5b f4 4b 98 23

Valid Period: July 19th, 2019 to August 19th, 2031

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

For organizations and individuals, subscribers refers to the name recorded as the certificate subject on the certificate and the entity in possession of the private key that corresponds with the certificate's public key. Subscribers must correctly use the certificate according to the certificate policies listed on the certificates. In addition, for the property categories such as application process, program code, server, (e.g. web server and SSL server) and hardware device, property is immovable so the certificate subscriber applying for the certificate shall be an individual or organization.

In the ePKI, subordinate CAs are not called subscribers in the CP when an above level CA issues a certificate to a subordinate CA, which is a lower level CA.

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 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

Assurance Level	Scope of Applications
	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.

The assurance level, authentication method, applicable scope, and reducible risks for SSL certificates, in addition to meet the aforesaid table, are described as follows:

Assurance Level and Cert Type	Authentication Method	Scope of Applications	Description of Reducible Risks
Level 1 DV SSL certificate	Follow the Baseline Requirements and assurance level 1 regulations to authenticate remote domain names and webpage services.	Provide communication channel encryption (communication channel encryption refers to 'faciliate encryption key exchange to achieve information transmission encryption between the subscriber's browser and website'). Suitable for use with protected network communications.	Provide an encryption protection to the non-monetary or non-property transactions where the probability of existence of malicious acts (e.g. online fraud, personal information breach, leakage of confidential information, etc.) is low.
Level 3 OV SSL certificate	Follow the Baseline Requirements and assurance level 3 regulations to authenticate the remote domain name and the webpage services	Provide communication channel encryption and must authenticate which organization owns the domain name. Suitable for use	Provide a robust authentication and high-level security to the following environments (included but not limited to): (1) the important monetary or property transactions; (2) internet

Assurance Level and Cert Type	Authentication Method	Scope of Applications	Description of Reducible Risks
	controlled by the applicant and authenticate which organization owns the domain name.	with protected network communications.	transactions where the probability of existence of malicious acts (e.g. online fraud, personal information breach, leakage of confidential information, etc.) is moderate.
Level 3 IV SSL certificate	Follow the Baseline Requirements and assurance level 3 regulations to authenticate the remote domain name and the webpage services controlled by the applicant and authenticate which natural person owns the domain name.	Provide communication channel encryption and must authenticate which natural person owns the domain name. Suitable for use with protected network communications.	Provide a robust authentication and high-level security to the following environments (included but not limited to): (1) the important monetary or property transactions; (2) internet transactions where the probability of existence of malicious acts (e.g. online fraud, personal information breach, leakage of confidential information, etc.) is moderate.
Level 3 EV SSL certificate	Follow the EV SSL Certificate Guidelines to authenticate which organization owns the remote domain name and webpage service, verify that organization truly exists in its legal jurisdiction, and participate in certificate transparency to prevent any mis-issuance of certificates.	Provide communication channel encryption and must authenticate which organization owns the domain name. Suitable for use with protected network communications. Browsers will show the green address bar and directly display the organization information of EV SSL certificate subject to facilitate subscribers to identify the	Provide a robust authentication and extremely high-level security to the following environments (included but not limited to): (1) transactions with high monetary or property value; (2) internet transactions where the probability of existence of malicious acts (e.g. online fraud, personal information breach, leakage of confidential information, etc.) is very high.

Assurance Level and Cert Type	Authentication Method	Scope of Applications	Description of Reducible Risks
		certificate holder.	

This CP provided 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; ■ 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

Authenticator Assurance Level	Descriptions
	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 a combination of two types of single-factor authentication. ■ If multi-factor authentication is taken, the available types of token include: ➢ Multi-factor encryption software; ➢ Multi-factor encryption equipment. ■ If the combination of two types of single-factor authentication is taken, 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 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

Authenticator Assurance Level	Descriptions
	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 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 for the following:

(1) Crime

(2) Control of military orders for nuclear, biological and chemical weapons

(3) Operation of nuclear equipment

(4) Aviation flight and control systems

(5) Scope of prohibitions announced under the law

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: +886 800-080-365

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://eca.hinet.net or https://epki.com.tw.

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, the Ministry of Economic Affairs (MOEA), 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 MOEA, 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 MOEA 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, Certificate Revocation List (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 also 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 CARL (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.

Certification Authority Authorization (CAA) Issuer Domain Names of ePKI include pki.hinet.net, eca.hinet.net and epki.com.tw.

2.3 Timing or Frequency of Publication

Follow the regulations in section 4.9.7 for CRL publication frequency. CP publication and any subsequent modifications shall be published in the eCA repository within seven calendar days upon the approval of the PMA. CAs shall publish their new or modified CPS to their repositories within seven calendar days 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 decide whether or not to accept the subject alternate name. If the CA requests that the subject alternate name be added to the certificate, it must be noted in the extension that it is a non-critical extension.

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 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.

Internal names or reserved IP addresses should not be used, for the Subject Name and Subject Alternative Name extension of server software certificates as stipulated in CA/Browser Forum guidelines.

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

The rules for interpreting name forms shall be established by CHT and included in the certificate profile.

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 also 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 certificate subject name may contain 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 three methods to prove possession are stipulated in the CP:

(1) The CA or RA generates the key pair for the subscriber:
The subscribers do not need to prove possession of the 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) 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.

(3) 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) Written document checking 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 not required.
Level 2	(1) Written document checking not required. (2) Subscriber submits organization information such as organization identity ID number (i.e. withholding

Assurance Level	Organization Identity Identification and Authentication
	tax ID number), organization name shall be checked against CA approval information. (3) In-person application not required.
Level 3	There are 3 types of organization identity authentication: (1) Private organization identity authentication Application information includes the organization name, location and representative name which is sufficient to identify the organization. The private organizations shall provide the photocopies of the related identification documents which are issued by the supervisory authorities and/or legally authorized entities (e.g. courts), with correctly registered window (such as Registry List of Company, Alteration of Company Registry List, Certificate of Corporate Registration, photocopies of Application Form for Registration of Withholding Entity Establishment (Alteration) (Notificaiton for Tax ID Number Assignation)); these identification documents shall be sealed with the company stamp and the personal stamp of its respresentative (both the stamps shall be consistent with the stamps on the registry record). 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 to the CA or RA. If the representative is unable to present the application in person, an agent shall be named in writing to present the application in person at the counter and the identity of the agent shall be authenticated in accordance with the assurance level 3 regulations under section 3.2.3. If the private organization has completed the registration procedure with the competent authorities or completed the counter identification and authentication procedure by the CA, RA or

Assurance Level	Organization Identity Identification and Authentication
	trusted authority or individual of the CA or RA (such as notary or account manager, project manager or sales manager of the Company to the private organization) and left behind registration or supporting information for identification and authentication (such as seal image or authentication stamp affixed to the application by notary of account manager, project manager or sales manager of the Company to the private organization) before certificate application, the CA or RA may allow submission of supporting information during certificate application in place of the above identification and authentication methods. The CA must evaluate the risk of trusting the supporting information to ensure the risk is no greater than adopting the above identification and authentication procedure. The CA or RA must have a capacity to authenticate the supporting information in order to accept the supporting information in place of the identification and authentication methods for certificate application. The above mentioned private organization refers to the corporate bodies, non-corporate bodies or the organizations belonging to the previous two. (2) Identity authentication for government agency, authority or unit The government agency, authority or unit follows the above private organization identity authentication method or official public document to apply for the certificate. The CA or RA must verify that the agency, authority or unit really exists and determine the authenticity of the public documents. (3) Identity authentication for organizations belonging to Chunghwa Telecom Organizations belonging to Chunghwa Telecom must apply for the certificate with official documents and the CA or RA must check if the agency or authority really exists and determine the

Assurance Level	Organization Identity Identification and Authentication
	authenticity of the public documents. In addition, an assurance level 3 certificate signature is issued through the ePKI for the above three categories of organization certificate application information. The representative does not need to submit the application in person. The CA or RA verifies the application information's digital signature. When an assurance level 3 organization certificate signature is issued through the ePKI for the server software certificate application information, the representative does not need to submit the application in person. The CA or RA verifies the certificate application information's digital signature.
Level 3 EV SSL	In compliance with the EV SSL Certificate Guidelines.
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 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

Assurance Level	Organization Identity Identification and Authentication
	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) Written documentation check 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 not required.
Level 2	(1) Written documentation checking 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 not required.
Level 3	(1) Check written documentation: The subscriber shall present at least one original approved photo ID (such as national ID card) during certificate application to the CA or RA to authenticate the subscriber's identity. If a subscriber (such as minor under 18

Assurance Level	Authentication of Individual Identity Procedure
	years old) is unable to submit the above photo ID, government issued written documentation (such as household registration) which is sufficient to prove the identity of the subscriber and one adult with legal capacity to guarantee the subscriber's identity in writing may be used in its place. The identity of the adult providing the written guarantee must pass through the above authentication. (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) and authenticate the identity of the agent in accordance with the above regulations. 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

Assurance Level	Authentication of Individual Identity Procedure
	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 3 EV SSL	In compliance with the EV SSL Certificate Guidelines.
Level 4	(1) Checking written 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 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. For example:

(1) Prove the existence of the organization through a third party identity verification service or database authentication or documentation from government authorities or authorized and accountable organizations.

(2) Verify that the individual holds the position of the certificate subject (organization or company) and is authorized to represent the certificate subject through telephone communications, mail, e-mail or other equivalent procedures.

(3) Verify that the individual represents the organization through face-to-face cross-checking of the identity at the counter or other trustworthy communication methods.

For certificates issued by the CA to organizations and individuals, if the e-mail address is recorded in the certificate subject alternative name field for secure e-mail use, how the RA verifies the certificate applicant is able to control the e-mail account listed in the certificate shall be stated in the CPS.

For DV SSL certificate applications, the method suggested in the Baseline Requirements shall be used to authenticate subscriber domain name control rights. For OV, IV and EV SSL certificate applications, except for validation of subscriber possession of domain name control rights by DV SSL certificate, the regulations in Sections 3.2.2 or 3.2.3 shall be followed to authenticate organization or individual identity. If there is an EV SSL certificate application, the contract signer and certificate approver authorization must be verified in accordance with the EV SSL Certificate

Guidelines. If the subordinate CA issues a SSL certificate, the validation method for domain control rights shall be stated in the CPS of the subordinate CA.

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, and CAs that issue SSL certificates are required to perform self-assessments at various times to ensure that their CP and CPS documents and their practices continue to comply with the Baseline Requirements.

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.

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

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 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.

A subscriber's identity shall be validated in accordance with the Baseline Requirements and Section 6.3.2.2 of this CP for DV (assurance level 1), OV (assurance level 3) and IV (assurance level 3) SSL certificates. Each subscriber shall re-establish its identity using the initial registration

processes of Section 3.2 if the identity has been validated for 398 days from the time of initial registration. Subscribers of EV (assurance level 3) SSL certificates shall establish their identities using the initial registration processes of Section 3.2 in accordance with the EV SSL Certificate Guidelines and Section 6.3.2.2 of this CP if the identity has been validated for 398 days 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), server software (such as Web Server or SSL Server) or program code do not have the capacity to act under the law so the organization or individual who administers the equipment or owns the program code 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.

Prior to issuing SSL certificates, for each dNSName marked in subjectAltName extension of the SSL certficates to be issued (i.e. each FQDN included in the certificate request filed by the applicant), the RAOs shall check them against the certification authority authorization (CAA)’s DNS resource records regulated by RFC 6844 as amended by Errata 5065 to the domain name system (DNS), and the certificates are only released when pass the check. CAA Issuer Domain Names of ePKI include pki.hinet.net, publicca.hinet.net, eca.hinet.net and epki.com.tw. CA shall clearly specify the set of Issuer Domain Names that the CA recognises in CAA "issue" or "issuewild" records as permitting it to issue SSL certificates in its CPS.

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.

As the Internet Corporation for Assigned Names and Numbers (ICANN) has opened the new generic top-level domain (gTLD), the root CAs requesting to join the CA trust list of browsers are required to verify that for their SSL certificates issued in the PKI, whether their subject alternative name, or the common name in the certificate subject name has recorded the internal server name. If the issued SSL certifcates have marked such domain names, ICANN gTLD notification must be subscribed.

CAs SHOULD NOT issue Certificates containing a new gTLD under consideration by ICANN. Prior to issuing a Certificate containing an Internal Name with a gTLD that ICANN has announced as under consideration to make operational, the CA MUST provide a warning to the applicant that the gTLD may soon become resolvable and that, at that time, the CA will revoke the Certificate once the gTLD starts its operation unless the applicant promptly registers the Domain Name. When a gTLD is delegated by inclusion in the IANA Root Zone Database, the Internal Name becomes a Domain Name, and at such time, a Certificate with such gTLD, which may have complied with these Requirements at the time it was issued, will be in a violation of these Requirements, unless the CA has verified the Subscriber’s rights in the Domain Name. The provisions below are intended to prevent such violation from happening.

Within 30 days after ICANN has approved a new gTLD for operation, as evidenced by publication of a contract with the gTLD operator on [www.ICANN.org] each CA MUST (1) compare the new gTLD against the CA’s records of valid certificates and (2) cease issuing Certificates

containing a Domain Name that includes the new gTLD until after the CA has first verified the Subscriber's control over or exclusive right to use the Domain Name in accordance with Section 3.2.2.4.

Within 120 days after the publication of a contract for a new gTLD is published on [www.icann.org], CAs MUST revoke each Certificate containing a Domain Name that includes the new gTLD unless the Subscriber is either the Domain Name Registrant or can demonstrate control over the Domain Name.

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

After CAs which issues assurance level 2, 3 and 4 certificates issues a certificate, the certificate applicant shall (1) review the content of the certificate to be issued or (2) review the content of the certificate after it is issued to indicate acceptance of the issued certificate before it is published on the repository. If the certificate applicant (1) refuses to accept the certificate information listed on the issued certificate after reviewing its contents, then the certificate is not issued or (2) refuses to accept the issued certificate after reviewing the content of the issued certificate, then the certificate is revoked by the CA. CAs operating at assurance levels 2, 3 and 4 shall specify the following in the CPS:

(1) Certificate applicant confirmation of the certificate acceptance or refusal method.

(2) Certificate field review by the certificate applicant before deciding whether to accept the certificate.

(3) Certificate processing method when the certificate applicant refuses to accept the certificate.

The above certificate applicant shall first review the certificate field including but not limited to the certificate subject name before deciding to accept the certificate. Before acceptance of the SSL server certificate, the

certificate applicant must review the certificate Subject Alternative Name field. If there is a secure e-mail application requirement and the e-mail address is listed on the certificate for organization or individual certificate applicants, the certificate Subject Alternative Namefield must also be reviewed.

Refusal of the certificate processing method by the certificate applicant involving fee collection and return issues shall be determined in accordance with Consumer Protection Act and fair-trade principles.

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 be able to control the private keys corresponding to the public key of their certificates and do not issue certificates to others. Subscribers shall protect their private keys from unauthorized use or disclosure and shall use their private keys for the correct key usage (i.e., the policy for key usage specified in the extension of the certificates). Subscribers shall correctly use their certificates adhering to the certificate policies listed in the certificates.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties should only use software that is compliant with the ITU-T X.509, IETF RFCs, Baseline Requirements or EV SSL Certificate Guidelines to verify the specific field and the validity of subscriber certificates. After the certificates' validity is confirmed through the CRLs (or CARLs) or OCSP services, the public key recorded in the certificate can be used to:

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

(2) Verify the identity of the document signature generator, and

(3) Establish secure communication channels with subscribers.

In addition, relying parties shall check the content of the certificatePolicies field of the issuing CA and subscriber certificates to confirm the assurance level 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 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 CARsL/CRLs. For revoked or suspended certificates prior to expiry, CAs shall list the information of revocation or suspension on the CARLs/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;

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

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

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 any circumstance indicating that use of a FQDN or IP address in the certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);

(5) The CA is made aware that a wildcard certificate has been used to authenticate a fraudulently misleading Subordinate FQDN;

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

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

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

(9) 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;

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

(11) The CA is made aware of a demonstrated or proven method that exposes the subscriber's private key to compromise, methods have been developed that can easily calculate it based on the public key (such as a Debian weak key, see https://wiki.debian.org/SSLkeys), or if there is clear evidence that the specific method used to generate the private key was flawed.

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 operating at assurance levels 1, 2, 3 and 4 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 operating at assurance levels 1, 2, 3 and 4 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, relying parties using certificates of assurance level 2 or higher must check the certificate status via CRLs (or CARLs) or OCSP services, as well as confirming that the authenticity, integrity, and validity of CRLs (or CARLs) or OCSP responses.

The certificate shall contain the CRL distribution points extension indicating CARL or CRL download URLs to aid relying parties in performing the revocation checking process. The matter of how often new certificate revocation data should be obtained is a determination to be made

by the relying party, considering the risk, responsibility, and consequences for using a certificate that the certificate status cannot be guaranteed. See Section 9.6.4 for related obligations.

4.9.7 CRL Issuance Frequency

eCA shall issue CARL and subordinate CA and subject CA shall issue CARL or CRL. Before the CARL and CRL are issued, the content shall be checked to verify the accuracy of the information. For example, use of software to scan the CARL or CRL to check the accuracy of information. The CARL or CRL shall be regularly announced. CARL or 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 information 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 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

Assurance Level	CARL Issuance Frequency	CRL Issuance Frequency
Level 4	At least once a day	At least once a day

4.9.8 Maximum Latency for CRLs

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

4.9.9 On-line Revocation/Status Checking Availability

CAs shall provide CRLs (or CARLs) for certificate status checking. CAs shall 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

In addition to providing CRLs (or CARLs), CAs may optionally support on-line certificate status checking to relying parties via OCSP services. Where OCSP services are supported, on-line certificate status information must be updated and available to relying parties. Relying parties using OCSP service need not obtain or process CRLs (or CARLs).

If a CA does support an OCSP service, the OCSP responder operated by the CA shall support the HTTP GET or POST method, as described in RFC 6960 and/or RFC 5019. CAs shall also specify the update frequency of the certificate status information provided via the OCSP service and the response rules of OCSP responder to the OCSP request received in their CPS.

4.9.11 Other Forms of Revocation Advertisements Available

In order to speed up and instantly complete the verification of the SSL certificates status of high-traffic websites, all CAs under ePKI support the operation of OCSP stapling. CAs shall ensure that the subscriber “staples” the OCSP response for the certificate in its TLS handshake.

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

As stated in Sections 4.9.1, 4.9.2 and 4.9.3.

4.9.13 Circumstances for Suspension

Certificate suspension is strictly forbidden for TLS/SSL certificates in accordance with Section 4.9.13 of the Baseline Requirements. CAs shall specify whether to provide the service of certificate suspension and resumption in their CPS.

4.9.14 Who Can Request Suspension

For SSL certificates, suspension is not allowed.

4.9.15 Procedure for Suspension Request

For SSL certificates, suspension is not allowed.

4.9.16 Limits on Suspension Period

For SSL certificates, suspension is not allowed.

4.9.17 Procedure for Certificate Resumption

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

Certificate suspension is strictly forbidden for SSL certificates in accordance with Section 4.9.13 of the Baseline Requirements.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

CAs shall provide a certificate status service either in the form of CRLs (or CARLs) or OCSP services or both. The public information of certificate

status shall contain the ones of revoked and suspended certificates and must not be removed until after the expiry date of the revoked certificates or the resumption of the suspended certificates.

4.10.2 Service Availability

CAs shall maintain 24x7 availability of certificate status service 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,

(5) CA/RA security principles and mechanisms, and

(6) Baseline Requirements (only for the CA that issues TLS/SSL certificates).

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		✓	✓	✓

Auditable Event/Assurance Level	Level 1	Level 2	Level 3	Level 4
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 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	✓	✓	✓	✓

Auditable Event/Assurance Level	Level 1	Level 2	Level 3	Level 4
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 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 CARL and Revocation List Profile Management				
A.13.1 All changes to CARL and 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			✓	✓

Auditable Event/Assurance Level	Level 1	Level 2	Level 3	Level 4
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 / 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		✓	✓	✓

Auditable Event/Assurance Level	Level 1	Level 2	Level 3	Level 4
A.15.4 Patches		✓	✓	✓
A.15.5 Security profiles			✓	✓
A.16 Physical Access / Site Security				
A.16.1 Personnel access to the CA facility			✓	✓
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. 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 CARLs / CRLs		✓	✓	✓
Audit logs	✓	✓	✓	✓
Other information or applications used to verify or substantiate archive contents		✓	✓	✓

Archived Information / Assurance Level	**Level 1**	**Level 2**	Level 3	**Level 4**
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	7 years
Level 2	7 years
Level 3	10 years
Level 4	20 years

If the retention period above cannot be reached with the storage media used, a system that regularly transfer 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 CARL/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 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
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	Must use 1024-bit RSA keys or other types of keys with equivalent security strength until December 31, 2013. Must use 2048-bit RSA keys or other types of keys with equivalent security strength until December 31, 2030. Should use 3072-bit RSA keys or other types of keys with equivalent security strength after December 31, 2030.
Level 1	
Level 2	
Level 3	
Level 4	Must at least use 4096-bit RSA keys or other types of keys with equivalent security strength.

6.1.6 Public Key Parameters Generation and Quality Checking

For RSA algorithms, public key parameters must be null. For other algorithms, the public key parameters are set in accordance with relevant international standards.

For RSA algorithms, parameter quality checking does not have to be performed but primality testing must be done. CAs shall state how related testing is performed in the CPS.

For other algorithms, follow relevant international standards including parameter quality testing.

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

CAs must set the key usage extension for subscriber certificates depending on their intended application of the key pairs. If a key contained in a certificate is used for digital signature (including authentication), the key usage extension of that certificate must set the digitalSignature bit. If a key contained in a certificate is used for key or data encryption, the key usage extension of that certificate must set the keyEncipherment or dataEncipherment bit. The key usage extension of CA certificates must set keyCertSign and cRLSign bits at least.

The Subordinate CA shall issue two key pairs to subscribers: one for data encryption; and the other for digital signatures and identity authentication. However, for support of legacy applications, e.g., S/MIME, certificates (including those at assurance levels 1, 2, 3, and test assurance level) may include a single key for the use with encryption and digital signature.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

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

6.2.1 Cryptographic Module Standards and Controls

The PMA shall ensure that the cryptographic module used in ePKI meets the requirements of FIPS 140-2 series or equivalent. CAs shall use the

cryptographic modules validated to the previous standards.

Cryptographic module requirements for each entity in ePKI, including eCA, Subordinate CA, RA, and subscriber, are shown in the following table. Each entity except the subscriber shall deem these requirements as the minimum level of cryptographic module protection. The levels listed in this table are defined referring to the FIPS 140-2 series.

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 operating at assurance level 3 and 4 shall comply with the multi-person control regulations in Chapter 5.

6.2.3 Private Key Escrow

Private signing keys may not be escrowed.

6.2.4 Private Key Backup

6.2.4.1 CA Private Signing Key Backup

For CAs operating at assurance level 3 and 4, backups of their private signing keys shall be done in accordance with multi-person control

procedures and stored at the backup site. Key backup procedures must be stated in the CPS.

6.2.4.2 Subscriber Private Signing Key Backup

Backups and copies may be made for subscriber private signing keys used for assurance level 1, 2 and 3 certificates but the subscriber must be in control.

Backups and copies may not be made for subscriber private signing keys for assurance level 4 certificates.

6.2.5 Private Key Archival

Private signing keys shall not be archived.

6.2.6 Private Key Transfer into or from a Cryptographic Module

When private keys are generated according to Section 6.1.1, CAs and RAs shall never allow the private keys to exist in plaintext outside the cryptographic module. The private keys are exported from the cryptographic module into backup tokens only for key backup/recovery or cryptographic module replacement according to the multi-person control method specified in Section 6.2.2. CAs and RAs shall encrypt or split the private keys and protects the private keys from disclosure when the keys are transferred out of the module or transported between cryptographic modules. After the private keys are imported, the related secret parameters generated during the transport process must be completely destroyed.

If the Issuing CA becomes aware that a subordinate CA private key has been communicated to an unauthorized person or an organization not affiliated with the Subordinate CA, then the 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

Follow the regulations 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

It is recommended that two key pairs shall be generated for certificates given to subscribers regardless of the assurance level; one for data encryption and the other for digital signature and identity authentication.

Subscribers' private keys used for signature and identity authentication shall not be escrowed, archived, and backed up. The CA to which the subscriber belongs may request the private keys used for encryption in the job requirement to be escrowed, archived or backed up.

6.3.1 Public Key Archival

Public key archival does not need to be performed again after certificate archival.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

6.3.2.1 Operational Periods for CA Public and Private Keys

All CAs under ePKI have maximum validity periods of:

Type of CA	Private Key Usage	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 CARLs, OCSP responder certificates, or OCSP Responses: 30 years	30 years
Subordinate CA / Cross-Certified CA	■ Issuing end-entity certificates: 10 years ■ Issuing CRLs, OCSP responder certificates, or OCSP Responses: 20 years	20 years

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

The validity of self-issued certificates cross-signed with old or new Root CA keys shall extend until self-signed certificate issued with the old Root CA key expires.

6.3.2.2 Operational Periods for Subscriber Public and Private Keys

The validity period of subscriber private keys is 10 years at most and the validity of subscriber certificates (including renewal certificates) shall not exceed the validity of issuing CA certificates.

For SSL certificates, the maximum validity period should meet the following requirements:

Issuance Date of Certificate	Validity Period
By June 30, 2016	In accordance with the regulations of the Subordinate CA or the cross-Certified CA, but the validity period of the certificate shall not exceed the validity period of the issuing CA for private key usage.
July 1, 2016 to Feb. 28, 2018	39 months
Mar. 1, 2018 to Aug. 31, 2020	825 Days
After Sep. 1, 2020	398 Days

6.3.2.3 SHA-1 Hash Function Algorithm Validity Period

According the international cryptography security assessment and the Baseline Requirements v.1.2.1 regulations, CAs will no longer use the SHA-1 Hash Function Algorithm to issue any new subscriber certificates or subordinate CA certificates starting from January 1, 2016. CAs can still use the SHA-1 Hash Function Algorithm to issue the certificate for verifying OCSP responses (i.e. CAs can use SHA-1 Hash Function Algorithm to issue OCSP responder certificates) until January 1, 2017. CAs can continue to use currently existing SHA-1 root CA certificates or cross certificates. SHA-2 SSL certificates shall not be issued with the private signing key corresponding to public key of the SHA-1 subordinate CA certificate. Starting from January 16, 2015, CAs should not use SHA-1 Hash Function Algorithm to issue SSL or code signing certificates with a certificate expiry date later than January 1, 2017.

Under the ePKI, each CA shall apply SHA-256 or Hash Function Algorithm with higher security level to issue OCSP responses.

Under the ePKI, the PublicCA eliminates all SHA-1 SSL certificates by the timeline specified in the Baseline Requirements. There are still a few of SHA-1 subscriber certificates issued by the PublicCA, such as security order placing certificate (valid for one year), not yet transferred to SHA-256 certificate. The PublicCA have conducted training for the application developers and the subscribers for transferring to SHA-256 certificates in application system. The subscribers have also been communicated to choose

some proper applications. The subscriber shall solely bear risks of using SHA-1 certificates. The subordinate CA shall stop issuing SHA-1 certificates no later than December 1, 2018.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The activation data of CAs' or subscribers' private keys and other related access control systems shall be adequately protected. For CAs operating at assurance levels 1, 2 and 3, the activation data is selected by appropriate individuals in trusted roles. For CAs operating at assurance level 4, the activation data shall be managed by appropriate individuals in trusted roles and shall be protected by the security mechanism of biometric data or cryptographic modules. If the activation data must be delivered, the delivery method must maintain the confidentiality and the integrity of the activation data.

6.4.2 Activation Data Protection

CAs must protect activation data used to unlock private keys from disclosure using a combination of password and access control mechanism. The activation data may be stored by biometric or memory methods. If a record needs to be kept, a cryptographic module with an equivalent security level must be used to ensure the security of the activation data. If the number of failed login attempts exceeds the maximum preset value in the CPS regulations, the protection system must be able to immediately lock the account and terminate the application program.

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 a 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 software used by CAs must be developed with good software engineering development methods such as the Capability Maturity Model Integration (CMMI). (2) Must prevent malicious software from being loaded onto the CA equipment. Only components authorized by security policy may be used for CA operations. (3) For RA hardware and software, check for malicious code on first use and scan periodically. (4) System development environment and test environment shall be separated from the on-line environment. (5) System development departments of CAs shall exercise

Assurance Level	System Development Controls
	the due care of a good management responsibility such as the signing of certificates of security compliance to ensure that there are no back doors or malicious programs; and the provision of program or hardware handover lists, test reports and administration manuals.

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) There must be no other applications, hardware devices, network connections, or component software installed by CAs that are not parts of the CA operation. (2) The CA system configurations and any modification and upgrade of functions must be documented and controlled. There must be a mechanism for detecting unauthorized modification to the software or configuration. (3) The CA software, when first installed, must be verified as being that supplied from the software supplier, with no modifications, and be the version intended for use.
Level 4	(1) The CA hardware and software must be dedicated to operating and supporting the CA functions. There must be no other applications, hardware devices, network connections or component software installed that are not parts of the CA operation. (2) The CA system configurations and any modification and upgrade of functions must be documented and controlled. There must be a mechanism for detecting unauthorized modifications to system software or configurations. (3) The CA software, when first installed, must be verified as being that supplied from the software supplier, with no modifications, and is the version intended for use. (4) CAs must verify the integrity of CA software at least

Assurance Level	Security Management Controls
	once a month. (5) CAs shall perform security management controls that comply with WebTrust for CA.

6.6.3 Life Cycle Security Controls

CAs shall disclose the key lifecycle security rating frequency in the 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 CARLs 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 CARLs) 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 system firewall systems and filtering routers.

6.8 Time-stamping

CA systems shall regularly synchronize with a reliable time service to ensure the accuracy of system clocks and that of the following items:

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

Clock adjustments are auditable events (see Section 5.4.1).

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

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

7.1.1 Version Number(s)

CAs shall issue ITU-T X.509 version 3 certificates.

7.1.2 Certificate Extensions

CAs must set certificate extensions in accordance with the ITU-T X.509, Baseline Requirements, and RFC 5280. Any CA is allowed to set other extensions, and the detail of these extensions including which ones shall be marked as critical shall be stated in its CPS. This helps the CA to achieve interoperability with its community in application services.

7.1.3 Algorithm Object Identifiers

Certificates issued under this CP shall use the following algorithm object identifiers (OID) during signing:

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)}

Certificates issued under this CP shall use the following OID to identify the algorithms used with to generate subject key:

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

7.1.4 Name Forms

CAs shall use ITU-T X.500 distinguished names in the subject and

issuer field. The attribute types of the distinguished names must be composed in accordance with the ITU-T X.509, Baseline Requirements, and RFC 5280.

As specified in RFC 5280, a Root CA must encode the DN in the subject field of its self-signed certificate identically to the DN in the issuer field in certificates (including Subordinate CA certificates, self-issued certificates, and cross-certificates) issued by that Root CA. Similarly, a Subordinate CA must encode the DN in the subject field of its certificate identically to the DN in the issuer field in subscriber certificates issued by that Subordinate CA.

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, it asserts 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

CAs must use the processing semantics for critical certificate policies extension in accordance with the ITU-T X.509, Baseline Requirements, and RFC 5280.

7.2 CRL Profile

7.2.1 Version Number(s)

eCA (or its Subordinate CAs) must issue ITU-T X.509 version 2 CARLs (or CRLs).

7.2.2 CRL and CRL Entry Extensions

The CRL extensions and CRL entry extensions in the CRLs (or CARLs) issued by CAs must comply with the ITU-T X.509, Baseline Requirements and RFC 5280.

7.3 OCSP Profile

The CA providing an OCSP service shall specify the OCSP version number and the used standards of OCSP extensions. The URL of the OCSP service shall be able to be obtained from the authority information access extension.

7.3.1 Version Number(s)

CAs should operate an OCSP service in compliance with RFC 5019 and RFC 6960.

7.3.2 OCSP Extensions

CAs shall provide OCSP extensions in accordance with the ITU-T X.509, Baseline Requirements, RFC 5019, and RFC 6960.

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. The CA that issues OV, DV or IV SSL certificates must complete another WebTrust for CA – SSL Baseline audit. In addition to completing the above two audits, the CA that issues EV SSL certificates must extra complete a WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL (WebTrust for CA – EV SSL) audit.

If a CA does not have a currently valid audit report indicating compliance with one of the aforementioned audits, then the CA shall successfully complete a point-in-time readiness assessment before issuing SSL certificates.

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.

According to the Baseline Requirements and WebTrust for CA – SSL Baseline, the CA that issues TLS/SSL certificates also must assign auditors to perform self-audits on at least a quarterly basis against a randomly selected sample of the greater of one certificate or at least three percent of the certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.

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, WebTrust for CA – EV SSL and WebTrust for CA – SSL Baseline 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. Audit practitioners who conduct WebTrust for CA – EV SSL audits shall take out a professional liability/errors and omissions insurance policy with a maximum claim amount of at least one million US dollars. 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 result are displayed with appropriate seals, including WebTrust for CA, WebTrust for CA – SSL Baseline or WebTrust for CA – EV SSL 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 three months, 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

CAs that issue EV SSL certificates shall disclose the insurance related to their respective performance and obligations and the corresponding coverage in their CPS, or explain the other assets covered in Section 9.2.2 under the EV SSL Certificate Guidelines. For example, the coverage includes the claims for damages arising out of (i) an error or omission in issuing or maintaining EV TLS/SSL certificates, or (ii) CA private key compromise.

There is no stipulation for CAs issuing other certificates.

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 any certificate application is deemed private information and only may be disclosed with the consent of the subscriber or in accordance with related laws and regulations. Information that cannot be obtained through the certificate and CARL or subscriber information obtained through certificate repository service and personal information to maintain the operation of CA trusted roles such as names together with palmprint or fingerprint characteristics, personal information on confidentiality agreements or contracts are deemed private information which requires protection. CAs and RAs shall implement security control measures to prevent personal information from unauthorized disclosure, leakage and 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 in 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 including installation only in servers which completely match the domain names recorded in the SSL certificates and no use of private keys corresponding to program code signed certificates to sign malicious software.

(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 CARL, 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 and any amendments are effective when published to eCA's webside and online repository. This CP remains effective until replaced with a newer version.

9.10.2 Termination

The CP and any amendments remain in effect until replaced by a newer version.

9.10.3 Effect of Termination and Survival

CHT will communicate the conditions and effect of this CP's termination via the eCA repository. The communication will specify which provisions survive termination. At a minimum, responsibilities related to protecting confidential information will survive termination.

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

CP OIDs will be changed if a change in the CP affects the purpose of certificate use and the level of assurance provided. Upon the CP OIDs has been changed, changes shall be made to the issuing CA's CPS accordingly.

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 entire agreement between the participants (as stated in Section 1.3) and supersedes all prior verbal or written representations between the parties on the same matters.

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.

The requirements regarding CAs in this CP comply with the Baseline Requirements and EV SSL Certificate Guidelines; however, if there is any inconsistency between the related domestic laws followed by this CP and the Baseline Requirements and EV SSL Certificate Guidelines, this CP may be adjusted to satisfy the requirements of the laws, and such adjustment shall be notified to CA/Browser Forum. If the domestic laws are not applicable anymore, or CA/Browser Forum revises the contents of the Baseline Requirements and EV SSL Certificate Guidelines to be compatible with the domestic laws, this CP will delete and amend the adjusted contents. The aforesaid actions shall be completed within 90 days.

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 but not limited to natural disasters, wars, terrorism or failures of the Internet. 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
CAA	Certification Authority Authorization	See Appendix 2
CCA	Cross Certification Agreement	See Appendix 2
CARL	Certification Authority Revocation List	See Appendix 2
CMMI	Capability Maturity Model Integration	See Appendix 2
CP	Certificate Policy	See Appendix 2
CPS	Certification Practice Statement	See Appendix 2
CRL	Certificate Revocation List	See Appendix 2
CT	Certificate Transparency	See Appendix 2
DN	Distinguished Name	
DNS	Domain Name System,	
DV	Domain Validation	See Appendix 2
eCA	ePKI Root Certification Authority	See Appendix 2
EE	End Entities	See Appendix 2
ePKI	Chunghwa Telecom ecommerce Public Key Infrastructure	See Appendix 2
EV	Extended Validation	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
IV	Individual Validation	See Appendix 2
NIST	(US Government) National Institute of Standards and Technology	See Appendix 2

Acronyms	Full Name	Definition
OCSP	Online Certificate Status Protocol	See Appendix 2
OID	Object Identifier	See Appendix 2
OV	Organization Validation	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
SSL	Secure Sockets Layer	See Appendix 2
TLS	Transport Layer Security	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
Capability Maturity Model Integration (CMMI)	CMMI is the successor of the Capability Maturity Model (CMM) and was developed by the Software Engineering Institute at Carnegie Mellon University. CMMI models provide guidance for developing or improving processes that meet the business goals of an organization. Its purpose is to help improve organizational performance.
Certificate	(1) Refers to verification information carrying a

	digital signature used to verify the identity and qualifications of the signer in electronic form [Article 2-6, Electronic Signatures Act] (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.
Certificate Approver	A natural person who is either the applicant, employed by the applicant, or an authorized agent who has express authority to represent the applicant to (i) act as a certificate requester and to authorize other employees or third parties to act as a certificate requester, and (ii) to approve EV SSL certificate requests submitted by other certificate requesters.
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, CARLs and CRLs.
Certification Authority Authorization (CAA)	The certification authority authorization (CAA) DNS resource record allows a DNS domain name holder to specify one or more certification authorities (CAs) authorized to issue certificates for that domain. CAA resource records allow a public certification authority to implement additional controls to reduce the risk of unintended certificate mis-issue. [RFC 6844]
Certification Authority	A signed and timestamped list. The list contains the serial numbers of revoked CA The list contains the

Revocation List (CARL)	serial numbers of revoked CA public key certificates (including subordinate CA certificates and cross-certificates).
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.
Certificate Transparency (CT)	Certificate transparency is an open platform for the public monitoring and auditing of all certificates on the Internet (SSL certificate is the priority objective at the current stage). The information given to domain owners, CA and domain subscribers on issued and existing is provided to judge if the certificate has been misissued or maliciously issued. In other words, the purpose is to provide a public monitoring and information disclosure environment which can be used to monitor TLS/SSL certificate systems and review certain TLS/SSL certificates to lessen certificate-related risks. Certificate transparency is mainly comprised of certificate journals, certificate monitors and certificate auditors.
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.
Contract Signer	Applicant, personnel employed by the applicant or an authorized representative for which applicant has made a declaration of intent to act as his/her representative or a natural person who has the right to represent the applicant in signing the purchase agreement.
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.
Domain Name System (DNS)	A distributed database used to automatically convert the IP address to domain name.
Domain Validation (DV)	SSL certificate approval and issuance, authentication of subscriber domain name control but no authentication of subscriber organization or individual identity. Therefore, linking to a website installed by a DV SSL certificate can provide a TLS encryption channel but it is not known who the owner of that website is.
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.
Extended Validation (EV)	Validation process defined in the EV SSL Certificate Guidelines.
EV Certificate	Certificate subject information including the information validated in accordance with EV SSL Certificate Guidelines.
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	An unambiguous domain name that specifies the

Domain Name (FQDN)	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.
Individual Validation (IV)	Outside of subscriber domain name control rights and follows certificate assurance level identification and authentication of subscriber personal identity. Therefore, connecting to an IV SSL certificate installed website can provide a TLS encryption channel. It is known which individual is the owner of that website and ensure the integrity of data transmission.
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 affects 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.
Naming Authority	A competent authority responsible for assigning a unique identifying name and ensuring that each unique identifying name is meaningful and unique within its field.
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	(1) One type of unique alphanumeric / numeric

(OID)	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.
Organization Validation (OV)	In the SSL certificate approval process, except for identification and authentication of subscriber domain name control rights, following the certificate assurance level to identify and authenticate the identity of subscriber organizations and individuals. So connection to an organization validation SSL certificate installed websites is able to provide TLS encryption channels, know who the owner of the website is and ensure the integrity of the transmitted information.
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.
Reserved IP Addresses	IPv4 and IPv6 addresses are reserved in the IANA setting. See http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml and http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml
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.
Secure Sockets	Protocol issued by Netscape through promotion of their web browser which can encrypt network

Layer (SSL)	communication in the transport layer and ensure the integrity of transmitted information and perform identity authentication on the server and client. The advantage of the secure socket layer protocol is it is independent and separate from the application layer protocol. High level application layer protocol (such as: HTTP, FTP and Telnet) may be established on top of SSL. The SSL protocol completes encryption algorithm, communication secret key agreement and server authentication work before the application layer protocol communication. This protocol is a successor to the Transport Layer Security (TLS) protocol.
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 CARLs 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.
Transport Layer Security (TLS)	SSL protocol established in RFC 2246 by the IETF. Called Transport Layer Security (TLS). Latest version is RFC 5246 which is the TLS 1.2 protocol.
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.