CHT SMIME Certification Authority
Certification Practice Statement

(CHT SMIME CA CPS)

Version 1.0

Chunghwa Telecom Co., Ltd.

December 30, 2020

Contents

1. Introduction 1
1.1 Overview 1
1.1.1 Certification Practice Statement 1
1.1.2 CPS Applicability 2
1.2 Document Name and Identification 2
1.3 PKI Participants 3
1.3.1 Certification Authorities 3
1.3.2 Registration Authorities 3
1.3.3 Subscribers 3
1.3.4 Relying Parties 4
1.3.5 Other Participants 4
1.4 Certificate Usage 5
1.4.1 Appropriate Certificate Uses 5
1.4.2 Prohibited Certificate Uses 6
1.5 Policy Administration 6
1.5.1 Organization Administering the Document 6
1.5.2 Contact Person 7
1.5.3 Person Determining CPS Suitability for the Policy 7
1.5.4 CPS Approval Procedures 8
1.6 Definitions and Acronyms 8
1.6.1 Acronyms 8
1.6.2 Definitions 10
2. Publication and Repository Responsibilities 25
2.1 Repositories 25
2.2 Publication of Certification Information 25
2.3 Time or Frequency of Publication 25
2.4 Access Controls on Repositories 26
3. Identification and Authentication 27
3.1 Naming 27
3.1.1 Types of Names 27
3.1.2 Need for Names to be Meaningful 27
3.1.3 Anonymity or Psuedonymity of Subscribers 27
3.1.4 Rules for Interpreting Various Name Forms 27
3.1.5 Uniqueness of Names 28
3.1.6 Recognition, Authentication, and Role of Trademarks 28
3.1.7 Resolution Procedure for Naming Disputes 29
3.2 Initial Identity Validation 29
3.2.1 Method to Prove Possession of Private Key 29

3.2.2 Authentication of Organization Identity 30
3.2.3 Authentication of Individual Identity 33
3.2.4 Non-verified Subscriber Information 35
3.2.5 Validation of Authority 35
3.2.6 Criteria for Interoperation 36
3.2.7 Data Source Accuracy 37
3.3 Identification and Authentication for Re-key Requests 37
3.3.1 Identification and Authentication for Routine Re-key 37
3.3.2 Identification and Authentication for Re-key after Revocation 38
3.4 Identification and Authentication for Revocation Request 38
4. Certificate Life-cycle Operational Requirements 39
4.1 Certificate Application 39
4.1.1 Who Can Submit a Certificate Application 39
4.1.2 Enrollment Process and Responsibilities 39
4.2 Certificate Application Processing 40
4.2.1 Performing Identification and Authentication Functions 40
4.2.2 Approval or Rejection of Certificate Applications 41
4.2.3 Time to Process Certificate Applications 41
4.3 Certificate Issuance 42
4.3.1 CA Actions during Certificate Issuance 42
4.3.2 Notification to Subscriber by the CA of Issuance of Certificate 43
4.4 Certificate Acceptance 43
4.4.1 Conduct Constituting Certificate Acceptance 44
4.4.2 Publication of the Certificate by the CA 45
4.4.3 Notification of Certificate Issuance by the CA to Other Entities 45
4.5 Key Pair and Certificate Usage 45
4.5.1 Subscriber Private Key and Certificate Usage 45
4.5.2 Relying Party Public Key and Certificate Usage 45
4.6 Certificate Renewal 46
4.6.1 Circumstances for Certificate Renewal 46
4.6.2 Who May Request Renewal 47
4.6.3 Processing Certificate Renewal Requests 47
4.6.4 Notification of New Certificate Issuance to Subscriber 47
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate 47
4.6.6 Publication of the Renewal Certificate by the CA 47
4.6.7 Notification of Certificate Issuance by the CA to Other Entities 47
4.7 Certificate Re-Key 47
4.7.1 Circumstance for Certificate Re-key 47
4.7.2 Who May Request Certification of a New Public Key 48
4.7.3 Processing Certificate Re-keying Requests 48
4.7.4 Notification of New Certificate Issuance to Subscriber 48
4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate 48
4.7.6 Publication of the Re-keyed Certificate by the CA 48

4.7.7 Notification of Certificate Issuance by the CA to Other Entities 48
4.8 Certificate Modification 48
4.8.1 Circumstance for Certificate Modification 48
4.8.2 Who May Request Certificate Modification 49
4.8.3 Processing Certificate Modification Requests 49
4.8.4 Notification of New Certificate Issuance to Subscriber 49
4.8.5 Conduct Constituting Acceptance of Modified Certificate 49
4.8.6 Publication of the Modified Certificate by the CA 49
4.8.7 Notification of Certificate Issuance by the CA to Other Entities 49
4.9 Certificate Revocation and Suspension 49
4.9.1 Circumstances for Revocation 49
4.9.2 Who Can Request Revocation 51
4.9.3 Procedure for Revocation Request 52
4.9.4 Revocation Request Grace Period 53
4.9.5 Time within Which CA Must Process the Revocation Request 54
4.9.6 Revocation Checking Requirement for Relying Parties 54
4.9.7 CRL Issuance Frequency 55
4.9.8 Maximum Latency for CRLs 55
4.9.9 On-line Revocation/Status Checking Availability 55
4.9.10 On-line Revocation Checking Requirements 55
4.9.11 Other Forms of Revocation Advertisements Available 57
4.9.12 Special Requirements Related to Key Compromise 57
4.9.13 Circumstances for Suspension 57
4.9.14 Who Can Request Suspension 57
4.9.15 Procedure for Suspension Request 57
4.9.16 Limits on Suspension Period 57
4.9.17 Procedure for Certificate Resumption 57
4.10 Certificate Status Services 57
4.10.1 Operational Characteristics 57
4.10.2 Service Availability 58
4.10.3 Optional Features 58
4.11 End of Subscription 58
4.12 Key Escrow and Recovery 58
4.12.1 Key Escrow and Recovery Policy and Practices 58
4.12.2 Session Key Encapsulation and Recovery Policy and Practices 58
5. Facility, Management, and Operation Controls 59
5.1 Physical Controls 59
5.1.1 Site Location and Construction 59
5.1.2 Physical Access 59
5.1.3 Power and Air Conditioning 60
5.1.4 Water Exposures 60
5.1.5 Fire Prevention and Protection 61
5.1.6 Media Storage 61
5.1.7 Waste Disposal 61

5.1.8 Off-site Backup 61
5.2 Procedural Controls 61
5.2.1 Trusted Roles 62
5.2.2 Number of Persons Required per Task 63
5.2.3 Identification and Authentication for Each Role 65
5.2.4 Roles Requiring Separation of Duties 66
5.3 Personnel Controls 66
5.3.1 Qualifications, Experience, and Clearance Requirements 66
5.3.2 Background Check Procedures 67
5.3.3 Training Requirements 68
5.3.4 Retraining Frequency and Requirements 69
5.3.5 Job Rotation Frequency and Sequence 69
5.3.6 Sanctions for Unauthorized Actions 70
5.3.7 Independent Contractor Requirements 70
5.3.8 Documentation Supplied to Personnel 70
5.4 Audit Logging Procedures 70
5.4.1 Types of Events Recorded 70
5.4.2 Frequency of Processing Log 71
5.4.3 Retention Period for Audit Log 71
5.4.4 Protection of Audit Log 72
5.4.5 Audit Log Backup Procedures 72
5.4.6 Audit Collection System (Internal vs. External) 72
5.4.7 Notification to Event-causing Subject 72
5.4.8 Vulnerability Assessments 72
5.5 Records Archival 73
5.5.1 Types of Records Archived 73
5.5.2 Retention Period for Archive 74
5.5.3 Protection of Archive 74
5.5.4 Archive Backup Procedures 74
5.5.5 Requirements for Time-stamping of Records 75
5.5.6 Archive Collection System (Internal or External) 75
5.5.7 Procedures to Obtain and Verify Archive Information 75
5.6 Key Changeover 75
5.7 Compromise and Disaster Recovery 76
5.7.1 Incident and Compromise Handling Procedures 76
5.7.2 Computing Resources, Software, and/or Data Are Corrupted 76
5.7.3 Entity Private Key Compromise Procedures 76
5.7.4 Business Continuity Capabilities after a Disaster 77
5.8 CA or RA Termination 77
6. Technical Security Controls 79
6.1 Key Pair Generation and Installation 79
6.1.1 Key Pair Generation 79
6.1.2 Private Keys Delivery to Subscriber 79

6.1.3 Public Key Delivery to Certificate Issuer 79
6.1.4 CA Public Key Delivery to Relying Parties 80
6.1.5 Key Sizes 80
6.1.6 Public Key Parameters Generation and Quality Checking 81
6.1.7 keyUsage Purposes (as per X.509 v3 Key Usage Field) 81
6.2 Private Key Protection and Cryptographic Module Engineering Controls 82
6.2.1 Cryptographic Module Standards and Controls 82
6.2.2 Private Key (n-out-of-m) Multi-person Control 82
6.2.3 Private Key Escrow 83
6.2.4 Private Key Backup 83
6.2.5 Private Key Archival 83
6.2.6 Private Key Transfer into or from a Cryptographic Module 83
6.2.7 Private Key Storage on Cryptographic Module 84
6.2.8 Method of Activating Private Key 84
6.2.9 Method of Deactivating Private Key 85
6.2.10 Method of Destroying Private Key 85
6.2.11. Cryptographic Module Rating 86
6.3 Other Aspects of Key Pair Management 86
6.3.1 Public Key Archival 86
6.3.2 Certificate Operational Periods and Key Pair Usage Periods 86
6.4 Activation Data 87
6.4.1 Activation Data Generation and Installation 87
6.4.2 Activation Data Protection 87
6.4.3 Other Aspects of Activation Data 87
6.5 Computer Security Controls 88
6.5.1 Specific Computer Security Technical Requirements 88
6.5.2 Computer Security Rating 88
6.6 Life Cycle Technical Controls 88
6.6.1 System Development Controls 88
6.6.2 Security Management Controls 89
6.6.3 Life Cycle Security Controls 89
6.7 Network Security Controls 89
6.8 Time-stamping 90
7. Certificate, CRL, and OCSP Profiles 91
7.1 Certificate Profile 91
7.1.1 Version Number(s) 91
7.1.2 Certificate Extensions 91
7.1.3 Algorithm Object Identifiers 94
7.1.4 Name Forms 95
7.1.5 Name Constraints 97
7.1.6 Certificate Policy Object Identifier 97
7.1.7 Usage of Policy Constraints Extension 98

7.1.8 Policy Qualifiers Syntax and Semantics 98
7.1.9 Processing Semantics for the Critical Certificate Policies Extension 98
7.2 CRL Profile 98
7.2.1 Version Number(s) 98
7.2.2 CRL and CRL Entry Extensions 98
7.3 OCSP Profile 98
7.3.1 Version Number(s) 98
7.3.2 OCSP Extensions 100
7.3.3 Regulations for Operation of OCSP 100
8. Compliance Audit and Other Assessments 101
8.1 Frequency or Circumstances of Assessment 101
8.2 Identity/Qualifications of Assessor 101
8.3 Assessor's Relationship to Assessed Entity 101
8.4 Topics Covered by Assessment 102
8.5 Actions Taken as a Result of Deficiency 103
8.6 Communications of Results 104
9. Other Business and Legal Matters 105
9.1 Fees 105
9.1.1 Certificate Issuance or Renewal Fees 105
9.1.2 Certificate Access Fees 105
9.1.3 Revocation or Status Information Access Fees 105
9.1.4 Fees for Other Services 105
9.1.5 Refund Policy 105
9.2 Financial Responsibility 106
9.2.1 Insurance Coverage 106
9.2.2 Other Assets 106
9.2.3 Insurance or Warranty Coverage for End-Entities 106
9.3 Confidentiality of Business Information 107
9.3.1 Scope of Confidential Information 107
9.3.2 Information Not Within the Scope of Confidential Information 107
9.3.3 Responsibility to Protect Confidential Information 107
9.4 Privacy of Personal Information 108
9.4.1 Privacy Plan 108
9.4.2 Information Treated as Private 108
9.4.3 Information Not Deemed Private 108
9.4.4 Responsibility to Protect Private Information 109
9.4.5 Notice and Consent to Use Private Information 109
9.4.6 Disclosure Pursuant to Judicial or Administrative Process 109
9.4.7 Other Information Disclosure Circumstances 109
9.5 Intellectual Property Rights 110

9.6 Representations and Warranties 110
9.6.1 CA Representations and Warranties 110
9.6.2 RA Representations and Warranties 111
9.6.3 Subscriber Representations and Warranties 111
9.6.4 Relying Party Representations and Warranties 112
9.6.5 Representations and Warranties of Other Participants 113
9.7 Disclaimers of Warranties 113
9.8 Limitations of Liability 113
9.9 Indemnities 114
9.9.1 Indemnification by CHT SMIME CA 114
9.9.2 Indemnification by RA 114
9.10 Term and Termination 114
9.10.1 Term 114
9.10.2 Termination 115
9.10.3 Effect of Termination and Survival 115
9.11 Individual Notices and Communications with Participants 115
9.12 Amendments 115
9.12.1 Procedure for Amendment 115
9.12.2 Notification Mechanism and Period 115
9.12.3 Circumstances under which OID Must Be Changed 116
9.13 Dispute Resolution Provisions 116
9.14 Governing Law 116
9.15 Compliance with Applicable Law 116
9.16 Miscellaneous Provisions 116
9.16.1 Entire Agreement 116
9.16.2 Assignment 116
9.16.3 Severability 117
9.16.4 Enforcement (Attorney's Fees and Waiver of Rights) 117
9.16.5 Force Majeure 117
9.17 Other Provisions 117

CPS Version Control

Version	Date	Revision Summary
0.95	Oct. 21, 2020	First Released.
1.0	Dec. 30, 2020	Version approved by the competent authority, MOEA (covering version 0.95 approved by the PMA)

1. Introduction

1.1 Overview

According to the ePKI CP, ePKI Root Certification Authority (eCA) is a top-level CA and a trust anchor of ePKI. eCA must maintain a high level of credibility that relying parties can directly trust its certificates. CHT SMIME Certification Authority (CHT SMIME CA) is a level-one Subordinate CA of eCA that obtains certificates from eCA and is responsible for the issuance and management of S/MIME certificates for natural person and organizations.

1.1.1 Certification Practice Statement

CHT SMIME CA Certification Practice Statement (CPS) describes the practices used to comply with the ePKI Certificate Policy (CP), official versions of the

(1) Electronic Signatures Act and

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

of R.O.C. and official versions of related international standards or regulations, including

(1) The Internet Engineering Task Force (IETF) request for comments (RFC) 3647, RFC 5280, RFC 6960, RFC 5019, and RFC 8550;

(2) ITU-T X.509;

(3) Microsoft Trusted Root Program Requirements;

(4) Apple Root Store Program;

(5) Mozilla Root Store Policy;

(6) Chromium Project Root Store Certificate Policy;

(7) Google S/MIME certificate profiles; and

(8) Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (Baseline Requirements), and Network and Certificate System Security Requirements published by CA/Browser Forum (http://www.cabforum.org),

to provide guidance and requirements for what CHT SMIME CA should include in its CPS.

1.1.2 CPS Applicability

The practice statement stipulated in this CPS applies to CHT SMIME CA, RAs, subscribers, relying parties, repository and other participants.

1.2 Document Name and Identification

This document is CHT SMIME CA Certification Practice Statement and was approved for publication on December 30, 2020. This CPS is version 1.0. The current version of this CPS can be obtained at the website: https://smimeca.hinet.net.

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

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
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}

1.3 PKI Participants

The related members of CHT SMIME CA include:

(1) CHT SMIME CA

(2) RAs

(3) Subscribers

(4) Relying Parties

1.3.1 Certification Authorities

CHT SMIME CA, established and operated by Chunghwa Telecom Co., Ltd. (CHT), operates in accordance with the ePKI CP and issues S/MIME certificates for natural person and organizations.

1.3.2 Registration Authorities

The RA is responsible for collection and authentication of subscriber identity and certificate-related information. The RA is comprised of one or more RA counters authorized under the organization approved by CHT SMIME CA. Each RA counter has an RA officer (RAO) who is responsible for performing certification application, revocation, and rekey work for different certificate groups and classes, and the verificataion of authorization domain names for S/MIME certificates.

1.3.3 Subscribers

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

Certificate entity	Subscriber
Natural person	Himself

Organization	Trustee of authorized organization
Application software	Owner of application software

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

1.3.4 Relying Parties

The relying party refers to a third party that acts in reliance of the relationship between the certificate subject name and the public key. Relying parties shall verify the validity of the certificate used based on the related CA certificate and certificate status information. After verifying the validity of the certificate, the certificate may be used for the following purposes:

(1) Verify the identity of the e-mail signature author.
(2) Verify the integrity of the e-mail protected with digital signatures.
(3) Encrypt e-mail content.

1.3.5 Other Participants

If CHT SMIME CA selects other related authorities which provide trust services as collaborative partners, the related information shall be disclosed on the website and the mutual operation mechanisms and the rights and obligations of each other shall be specified in this CPS to ensure the efficiency and reliability of the service quality provided by CHT SMIME CA.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

CHT SMIME CA issues assurance level 1, 2 and 3 certificates as defined in the CP (including certificates for signature and encryption use).

The appropriate certificate uses for each certificate assurance level is as follows:

Assurance Level	Applicable Scope
Level 1	Use e-mail notification to verify that the applicant can control the e-mail account. Suitable for use in network environments in which the risk of malicious activity is considered to be low or a higher assurance level cannot be provided. When used for digital signatures, it can identify that the subscriber originates from a certain e-mail account or guarantee the integrity of the signed document. When used for encryption, the relying party can use the subscriber's certificate public key to encrypt the symmetric key to guarantee the confidentiality of e-mail content. Not suitable for online transactions that require identification and non-repudiation/content commitment.
Level 2	Suitable for use with information which may be tampered with but the network environment has no malicious tampering (data interception is possible but likelihood is not high). Not suitable for the signing and encryption of important e-mails (life essential and high value transaction documents).
Level 3	Suitable for use in network 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 may include on-line cash or property transactions on keys. Used to secure online transactions that require identification and non-repudiation/content commitment.

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

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 shall check if the certificate type, assurance level and keyUsage conforms to their requirements before the certificate is issued by CHT SMIME CA.

Relying parties shall appropriately use the individual keys in compliance with the keyUsage field included in the certificate stipulated in Section 6.1.7 and correctly process the certificate attribute information listed in the certificate extension marked as critical.

1.4.2 Prohibited Certificate Uses

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

(1) Crime;
(2) Military command and nuclear, biological and chemical weapons control;
(3) Operation of nuclear equipment; and
(4) Aviation flight and control systems.

1.5 Policy Administration

1.5.1 Organization Administering the Document

Chunghwa Telecom Co., Ltd.

1.5.2 Contact Person

1.5.2.1 CPS Related Issues

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

E-mail: caservice@cht.com.tw

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

Other information can be found at https://smimeca.hinet.net.

1.5.2.2 Certificate Problem Report

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

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

1.5.3 Person Determining CPS Suitability for the Policy

CHT SMIME CA shall first check whether this CPS conforms to the ePKI CP regulations and then submit the CPS to the Chunghwa Telecom Certificate Policy Management Authority (PMA) for review and approval. After approval, CHT SMIME CA is able to officially reference the ePKI CP. (See eCA repository https://eca.hinet.net/repository_a.htm)

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

by the competent authority, the Ministry of Economic Affairs (MOEA).

CHT SMIME CA conducts regular self-audits to demonstrate that it has operated with the assurance level under the ePKI CP. In order to ensure smooth operation of certificates by the CAs under ePKI by operating systems, browsers, and software platforms, ePKI has applied to the root certificate programs for operating systems, browsers and software platforms. The self-signed certificates issued by eCA are widely deployed in the CA trust lists of software platforms. According to the regulations of the root certificate program, external audits of CHT SMIME CA and eCA are conducted annually and the latest CPS as well as the external audit results are submitted to the root certificate programs. CHT SMIME CA also continues to maintain the audit seal published in the CHT SMIME CA website.

1.5.4 CPS Approval Procedures

This CPS is published by CHT SMIME CA following approval by the MOEA, the competent authority of the Electronic Signatures Act. This CPS must be revised in response to any revision of the ePKI CP, and the revised CPS must be submitted to the PMA and MOEA for approval.

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

1.6 Definitions and Acronyms

1.6.1 Acronyms

Acronyms	Full Name	Definition
AIA	Authority Information Access	See Section 1.6.2.
CA	Certification Authority	See Section 1.6.2.

Acronyms	Full Name	Definition
CMMI	Capability Maturity Model Integration	See Section 1.6.2.
CP	Certificate Policy	See Section 1.6.2.
CP OID	CP Object Identifier	
CPS	Certification Practice Statement	See Section 1.6.2.
CRL	Certificate Revocation List	See Section 1.6.2.
DN	Distinguished Name	
DNS	Domain Name System	See Section 1.6.2.
eCA	ePKI Root Certification Authority	See Section 1.6.2.
EE	End Entities	See Section 1.6.2.
ePKI	Chunghwa Telecom ecommerce Public Key Infrastructure	See Section 1.6.2.
FIPS	(US Government) Federal Information Processing Standard	See Section 1.6.2.
FQDN	Fully Qualified Domain Name	See Section 1.6.2.
IANA	Internet Assigned Numbers Authority, IANA	See Section 1.6.2.
IETF	Internet Engineering Task Force	See Section 1.6.2.
NIST	(US Government) National Institute of Standards and Technology	See Section 1.6.2.
OCSP	Online Certificate Status Protocol	See Section 1.6.2.
OID	Object Identifier	See Section 1.6.2.
PIN	Personal Identification Number	
PKCS	Public-Key Cryptography	See Section 1.6.2.

Acronyms	Full Name	Definition
	Standard	
PKI	Public Key Infrastructure	See Section 1.6.2.
QGIS	Qualified Government Information Source	See Section 1.6.2.
QTIS	Qualified Government Tax Information Source	See Section 1.6.2.
RA	Registration Authority	See Section 1.6.2.
RFC	Request for Comments	See Section 1.6.2.
SSL	Secure Sockets Layer	See Section 1.6.2.
TLS	Transport Layer Security	See Section 1.6.2.
UPS	Uninterrupted Power System	See Section 1.6.2.

1.6.2 Definitions

Access	Use the information processing capabilities of system resources
Access Control	Authorization procedure for access to information system resources given to subscribers, programs, procedures and other systems.
Activation Data	Private data, other than keys, that are required to access cryptographic modules and that need to be protected (i.e., unlock private keys for signing or decryption events).
Applicant	Subscribers who request certificates from a CA and have not yet completed the certificate procedure.
Application Software Suppliers	Vendors of browser software or other relying party applications that display or use certificates and root certificates.
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.
Authenticate	(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.
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.
Authorization Domain Name	The Domain Name used to obtain authorization for certificate issuance for a given FQDN. The CA may use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. If the FQDN contains a wildcard character, then the CA MUST remove all wildcard labels from the left most portion of requested FQDN. The CA may prune zero or more labels from left to right until encountering a Base Domain Name and may use any one of the intermediate values for the purpose of domain validation.
Backup	Information or program copying that can be used for recovery purposes when needed.
Base Domain Name	The portion of an applied-for FQDN that is the first domain name node left of a registry controlled or public suffix plus the registry-controlled or public suffix (e.g. "example.co.uk" or "example.com"). For FQDNs where the right-most domain name node is a gTLD having ICANN Specification 13 in its registry agreement, the gTLD itself may be used as the Base Domain Name.
Baseline Requirements	“The Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates” issued by CA/Browser Forum, and all the amendments.
Binding	The process for binding (connecting) two related information elements.
CA Certificate	Certificates issued by CAs.
Capability	CMMI is the successor of the Capability Maturity

Maturity Model Integration (CMMI)	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 this CPS specifically refers to ITU-T X.509 v.3 format certificates which states the certificate policy object identifier in the 'certificate policy' field.
Certification Authority (CA)	(1) The agency or natural person that issues certificate [Article 2-5, Electronic Signatures Act] (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.
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 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 Problem Reports	The complaints regarding suspected cracking of keys, certificate misused, or other types of fraud, cracks, abuse, or inappropriate behaviors related to certificates.
Certificate Re-key	Changing the key pair used in a cryptographic system application. It is commonly achieved by issuing a new certificate that contains the new public key.
Certificate Revocation	To prematurely terminate the operational period of a certificate prior to its expiry date.
Certificate Revocation List (CRL)	(1) The certificate revocation list digitally signed by the certification authority provided for relying party use. [Article 2-8, Chapter 1, Regulations on Required Information for Certification Practice Statements] (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.

Chunghwa Telecom Certificate Policy Management Authority (PMA)	An organization which was established for electronic certificate management matters, such as (i) discussion and review of the CP and the electronic certificate framework of the PKI owned by CHT and (ii) review of interoperation requests submitted by subordinate CAs and cross-certified CAs and that of CPS.
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.
Cryptographic Module	A set of hardware, software, firmware or combination of the above used to run cryptologic or programs (including crypto algorithms) and included within the cryptographic boundaries of the module.
Data Integrity	Information that has been subjected to unauthorized access or accidental modification, damage or loss.
Digital Signature	An electronic signature generated by use of mathematic algorithm or other means to create a certain length of digital data encrypted by the signatory's private key and capable of being verified by the public key. [Article 2-3, Electronic Signatures Act]
Domain Contact	The Domain Name Registrant, technical contact, or administrative contract (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record.
Domain Name	A node label assigned by the domain name system. Converts the IP address into a text name that is easily remembered by humans.
Domain Name Registrant	Sometimes referred to as the domain name owner, but it is more appropriate to say a certain individual or entity who have registered with the Domain Name Registrar to have the right to use a

	domain name and the Domain Name Registrant or WHOIS has listed the 'registrant' as a natural person or legal person.
Domain Name Registrar	A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns).
Domain Name System (DNS)	A distributed database used to automatically convert the IP address to domain name.
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.
End-Entity Certificate	Certificates issued to end-entities.
Chunghwa Telecom ecommerce Public Key Infrastructure (ePKI)	A hierarchical PKI established by CHT in compliance with ITU-T X.509 to promote electronic services. It can be used within various applications in e-commerce and e-government.
ePKI Root CA (eCA)	The Root CA and top-level CA in ePKI, and its public key is the trust anchor of ePKI.
Federal	Except for military organizations in the US Federal

Information Processing Standard (FIPS)	Government System, information processing standard for all government organizations and government subcontractors. The security requirement standard for the cryptographic module is FIPS no. 140 standard (FIPS 140). FIPS 140-2 divides the cryptographic module into 11 types of security requirements. Each security requirement type is then divided into 4 security levels.
Firewall	An access restriction gateway between networks which complies with near-end (local area) security policy.
Fully Qualified Domain Name (FQDN)	An unambiguous domain name that specifies the exact location of a computer within the domain's hierarchy. The fully qualified domain name consists of two parts: the host name (service name) and domain name. For example, ourserver.ourdomain.com.tw, ourserver is the host name and ourdomain.com.tw is the domain name. In this name, ourdomain is the third-level domain, com is the second-level domain name and tw is the country code top-level domain (ccTLD). A fully qualified domain name always starts with a host name. For example, www.ourdomain.com，www is the host name. Ourdomain is the the second-level domain name. com is Generic Top-Level Domain, gTLD.
Identification	A statement of who the user is. [A Guide to Understanding Identification and Authentication in Trusted Systems] A way that can be used to describe or claim the identity of an individual or entity, e.g., user account, name or e-mail.
Internet Assigned Numbers Authority (IANA)	An organization that oversees the allocation of global IP address, domain names and many other parameters used for Internet.
Internet Engineering Task Force (IETF)	Responsible for the development and promotion of Internet standards. Official website is at: https://www.ietf.org/. Its vision is the generation of

	high quality technical documents affects how man designs, uses and manages the Internet and allows the Internet to operate smoothly.
Issuing CA	For a particular certificate, the CA that issues the certificate is the issuing CA.
Jurisdiction of Incorporation	In the context of a Private Organization, the country and (where applicable) the state or province or locality where the organization's legal existence was established by a filing with (or an act of) an appropriate government agency or entity (e.g., where it was incorporated). In the context of a Government Entity, the country and (where applicable) the state or province where the Entity's legal existence was created by law.
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 related keys having the following properties: (1) One (public) key can be used to encrypt a message that can only be decrypted by using the other (private) key, and (2) It is computationally infeasible to determine one key from another.
National Institute of Standards and Technology (NIST)	Official website is at http://www.nist.gov/. Its mission is to promote U.S. innovation and industry competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. The hardware cryptographic module standards and certification, key security assessment and U.S. federal government civil servant and contractor identity card standards defined by NIST are widely referenced and

	employed.
Non-Repudiation	Provide proof of delivery to the information sender and proof of sender identity to the receiver so neither party may repudiate the processing of this information after the fact. Technically speaking, non-repudiation refers to the guarantee that this signature must be signed by the corresponding private key if a certain public key can be used to verify a certain digital signature for a trusted party. Legally speaking, non-repudiation refers to the establishment of a possession and control system for private signature keys.
Object Identifier (OID)	(1) One type of unique alphanumeric / numeric identified registered under the International Standard Organization registration standard which could be used to identify the uniquely corresponding certificate policy; where the certificate policy is modified, the OID is not changed accordingly. [Article 2-4, Chapter 1, Regulations on Required Information for Certification Practice Statements] (2) When a special form of code, object or object type is registered with the International Standard Organization (ISO), the unique code may be used as an identified. For example, this code can be used in the public key infrastructure to indicate what certificate policy and cryptographic algorithms are used.
Online Certificate Status Protocol (OCSP)	The Online Certificate Status Protocol is a type of online certificate checking protocol which lets the application software of relying parties to determine the status (such as revoked or valid) of a certain certificate.
OCSP Responder	The online server that is authorized, maintained, and operated by the CA, and connects to the repository to process the certificate status request.
OCSP Stapling	This is a form of TLS/SSL Certificate Status Request extension, which may replace the OCSP to check X.509 certificate status. In practice, a website may obtain a “time limited

	(e.g. two hours)" OCSP response from the OCSP Responder and cache it. Next, this cached OCSP response will be sent to the subscriber (typically a browser) whenever initiating the TLS Handshake. The subscriber only needs to verify the validity of that OCSP response without sending the request of OCSP to the CA. In that way, the subscriber will not need to request the TLS/SSL certificate status from the CA when connecting to a high traffic TLS website, and thus to decrease the burden of the CA. This mechanism also prevents the privacy concern that the OCSP Responder knows which subscribers attempting to browsing that TLS website by having the TLS website referring the TLS/SSL certificate validity message issued regularly by the OCSP Responder to the CA.
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 Standard (PKCS)	In order to promote the use of public key technology, the RSA laboratory under the RSA Information Security Company has developed a series of public key cryptography standards that are widely used by the industry.
Public Key Infrastructure (PKI)	A set of law, policy, standards, personnel, equipment, facilities, technology, processes, audits and services developed on a broad scale and management of asymmetric cryptography and public key certificates.

Qualified Auditor	Accountant firms, entities, or individuals that satisfy the auditor qualification requirements specified in Section 8.2 of the Baseline Requirements, as well as independent from the audited parties.
Qualified Government Information Source (QGIS)	A regularly-updated and current, publicly available, database designed for the purpose of accurately providing the information for which it is consulted, and which is generally recognized as a dependable source of such information provided that it is maintained by a Government Entity, such as Ministry of Economic Affairs Bussiness & Factory Registration Database, the reporting of data is required by law, and false or misleading reporting is punishable with criminal or civil penalties. Nothing in the EV SSL Certificate Guidelines shall prohibit the use of third-party vendors to obtain the information from the Government Entity provided that the third party obtains the information directly from the Government Entity.
Qualified Government Tax Information Source (QTIS)	A Qualified Governmental Information Source that specifically contains tax information relating to Private Organizations, Business Entities, or Individuals. Such as Fiscal Information Agency, Ministry of Finance in Taiwan and IFS in USA.
Random Value	A value specified by a CA to the Applicant that exhibits at least 112 bits of entropy.
Registration Authority (RA)	(1) Responsible for checking the identity and other attributes of the certificate applicant but does not issue or administer certificates. The nature and scope of obligations borne by the registration authority are set down in the applicable certificate policy or agreement. (2) An entity responsible for the identity identification and authentication of the certificate subject which does not issue certificates.
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.
Repository	(1) A system for storing and retrieving certificates or other information relevant to certificates. [Article 2-7, Chapter 1, Regulations on Required Information for Certificate Practice Statements] (2) A database that contains information and data relating to certificates as specified in the CP/CPS.
Request for Comments (RFC)	A series of memos issued by the Internet Engineer Task Force that include Internet, UNIX and Internet community standards, protocols and procedures for number assignment.
Secure Sockets Layer	Protocol issued by Netscape through introduction of their web browser which can encrypt network communication in the transport layer and ensure the integrity of transmitted information and perform identity authentication on the server and client. 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.

Subordinate CA	In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA.
Subscriber	An entity that (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	A digitally signed assertion by a trusted authority that a specific digital object existed at a certain time.
Transport Layer Security (TLS)	TLS 1.0 was first defined in RFC 2246 by the IETF based on the SSL 3.0 and updated in RFC 5246 and RFC 6176 as TLS 1.2. The current version is TLS 1.3 defined in RFC 8446 by the IETF in 2018.
Trust List	List of trusted certificates used by relying parties to authenticate certificates.
Trusted Certificate	Certificate trusted by relying party obtained through a secure and reliable transmission method. The public key contained in this type of certificate comes from a trusted path. Also called a trust anchor.

Trustworthy System	Computer hardware, software and programs which possess the following attributes: (1) Functions that protect again intrusion and misuse. (2) Provides reasonably accessible, reliable and accurate operations. (3) Appropriate implementation of preset function. (4) Security procedures uniformly accepted by the general public.
Uninterrupted Power System (UPS)	Provide uninterrupted backup power to loading equipment in the event of abnormal power conditions (such as power outage, interference or power surge) to allow uninterrupted operation of servers, switches and other critical equipment and precision instruments to prevent loss of calculation data, communication network interruption and loss of instrument control.
Validation	The process of identification of certificate applicants. Validation is a subset of identification and refers to identification in the context of establishment of the identity of certificate applicants. [RFC 3647]
WebTrust	The current version of CPA Canada's WebTrust Program(s) for Certification Authorities.
WHOIS	Information retrieved directly from the Domain Name Registrar or registry operator via the protocol defined in RFC 3912, the Registry Data Access Protocol defined in RFC 7482, or an HTTPS website.
Zeroize	Method to delete electronically stored information. Storage of changed information to prevent information recovery.

2. Publication and Repository Responsibilities

2.1 Repositories

The CHT SMIME CA repository is responsible for the publication and storage of certificates and certificate revocation lists (CRLs) issued by CHT SMIME CA and this CPS and provides inquiry services to subscribers and relying parties. The repository provides 24-hour round-the-clock service. The website of the CHT SMIME CA repository is located at http://smimeca.hinet.net. The repository will resume normal operation within two working days if unable to operate normally for some reason.

2.2 Publication of Certification Information

CHT SMIME CA shall take responsibility for making the following information publicly accessible in its repository:

(1) This CPS and the ePKI CP,
(2) Certificate revocation information,
(3) CHT SMIME CA certificates (until the expiry of all certificates issued with private key corresponding to that certificate's public key),
(4) Issued certificates,
(5) Privacy protection policy,
(6) Related latest news regarding CHT SMIME CA, and
(7) The latest external audit report (as specified in Section 8.6).

2.3 Time or Frequency of Publication

(1) This CPS is reviewed and updated annually, and a dated changelog is state in the "Document History" section even if no other changes are make to this document. New or modified version of this CPS is published in the repository within 7 calendar

days upon receiving the approval letter from the competent authority,

(2) The ePKI CP complied with by CHT SMIME CA is published in the repository within 7 calendar days upon the approval of the PMA,

(3) CHT SMIME CA issues CRLs at least twice a day and publishes CRLs in the repository, and

(4) CHT SMIME CA certificates are published in the repository within 7 calendar days after accepting issuance by the upper level CA.

2.4 Access Controls on Repositories

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

The information published by CHT SMIME CA under Section 2.2 is primarily provid for inquiring by subscribers and relying parties. CHT SMIME CA implements access control where it provides read-only access to prevent anyone from unauthorized writing operation, which would put repository security in risk.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

CHT SMIME CA certificates are issued with subject Distinguished Names (DNs) which meet the requirements of X.500 naming and RFC 822 naming.

3.1.2 Need for Names to be Meaningful

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

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

3.1.3 Anonymity or Psuedonymity of Subscribers

CHT SMIME CA does not issue end entity anonymous certificates. As a principle, CHT SMIME CA may not issue pseudonymous certificates either.

3.1.4 Rules for Interpreting Various Name Forms

The rules for interpreting name forms follow ITU-T X.520 name attribute definition.

3.1.5 Uniqueness of Names

The X.500 DN for CHT SMIME CA's CA certificates is:

C=TW,

O=Chunghwa Telecom Co., Ltd.,

CN=CHT SMIME CA - Gn, where n = 1, 2, …

CHT SMIME CA applies various naming attributes defined in X.520 standard for assembly to ensure the uniqueness of each subject name in a certificate and the compliance of the X.500 naming space. The uniqueness of subject name in subscriber certificates is enforced by (but not limit to) assembling the following naming attributes defined in the X.520 standard:

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

3.1.6 Recognition, Authentication, and Role of Trademarks

The certificate subject name, including trademark or any name, business or company name or representation protected by law, provided by subscribers must comply with relevant regulations in our country's Trademark Act and Fair-Trade Act. CHT SMIME CA shall not bear the responsibility for reviewing whether the certificate subject name provided by the subscriber complies with the above regulations. Related disputes and arbitration shall not be the obligation of CHT SMIME CA and the subscriber shall handle matters in accordance with regular administrative and judicial remedies.

3.1.7 Resolution Procedure for Naming Disputes

When subscribers have identical identification names, the subscriber who submitted the application first shall be given priority for use. Relevant disputes or arbitration shall not be the obligation of CHT SMIME CA and the subscriber should file a request with the relevant competent authorities (institutions) or court.

If the identification name used by the subscriber is proven by relevant competent authorities (institutions) or the authority with the right of interpretation that the identification name is owned by other applicant, that subscriber shall assume relevant legal responsibility and CHT SMIME CA may revoke that subscriber's certificate (please refer to Section 4.9.1).

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

CHT SMIME CA shall verify that the individual possesses the private key, which can be divided into the following cases:

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

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

3.2.2 Authentication of Organization Identity

The applicant must demonstrate control of its email address, see Section 3.2.5. The certification document required for organization identification and authentication, and the authentication and verification procedures whether need to be performed at the counter are determined based on various assurance levels as shown in the following Table 3-1.

Table 3-1

Assurance Level	Procedures for Authentication of Organization Identity
Level 1	There is no requirement to link the applicant to a specific real-life identity. Any attributes provided in conjunction with the authentication process are self-asserted. (1) No identity verification required. (2) In-person identity proofing at counter is not required.
Level 2	Evidence supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity. (1) No identity verification required. (2) In-person identity proofing at counter is not required. (3) The applicant is required to provide organization information such as organization ID number (i.e. withholding tax ID number) and organization name. CHT SMIME CA may additionally cross-check the information provided by the applicant for consistency with available government or third-party data sources.
Level 3	The identification procedure must be carried out in person at the counter or on-site, and the identification procedure must be carried out by personnel authorized and trained by CHT SMIME CA. (1) Private organization identity authentication The private organization must submit copies of the correct certification documents (see Table 3-2) issued by the competent authority or a legally authorized body (such as a court) to the RAO. The RAO shall check the authenticity of the application information submitted by the organization and representative identity and verify

Assurance Level	Procedures for Authentication of Organization Identity
	that the representative has the right to apply for the certificate in the organization's name. The representative shall submit the application at the CA or RA counter in person. If the representative is unable to submit the application at the counter in person, at least one of the following regulations shall be followed: (a) an agent may be appointed to submit the application at the counter of his/her behalf, and the RA must validate the agent's identity with the authentication procedures stated in Section 3.2.3 as to assurance level 3 certificates; (b) A letter attesting that Subject Information is correct written by a notary, accountant, lawyer, government official, or other reliable third party customarily relied upon for such information; or (c) A site visit by CHT SMIME CA personnel or a third party who is acting as an agent for the CA. If the private organization has completed the registration procedure with the competent authority or completed the counter identification and authentication procedure by the CA, RA or CA-trusted authority or individual of the CA or RA (such as notary or account manager, project manager or sales manager of CHT to the private organization) in compliance with the above counter identification and authentication procedure 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 CHT 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 aforementioned private organization refers to the private corporate bodies, unincorporated bodies or the organizations belonging to the two previous. (2) Government agency's or authority's identity

Assurance Level	Procedures for Authentication of Organization Identity
	authentication The government agency or authority may use official public document to apply for the certificates. The CA or RA must verify that the agency or authority really exists and determine the authenticity of the official documents. (3) CHT's organization unit's identity authentication Organizations belonging to CHT must apply for the certificate with written application or e-form, and the RA must verify legal existence and unit name of the applied unit. Validation of the organization's legal existence, organization name, registration number, business or operational existence can be conducted by cross-checking with the information obtained from a qualified government information source (QGIS) such as the MOEA industry and business registration database, a qualified government tax information source (QTIS) such as the Fiscal Information Agency of MOF, or a reliable means of communications. The RAO can therefore confirm the identity of the applicant. In addition, when there is digital signature by a private key corresponding to an assurance level 3 certificate issued through the GPKI for the above three categories of organization certificate application information, the representative does not need to submit the application at the counter in person. The RA system or RAO shall verify whether the digital signature on the application information is valid.

Table 3-2

Type of Oganization	Relevant certified documents or method
Company or its affiliated companies	Photocopy of company registration form or company change registration form.
Business	Photocopy of the latest business registration application replied by the registration authority.

Taiwan branch of foreign company	Photocopy of Taiwan branch of foreign company registration form or company change registration form approved by competent authority.
Consortium/ corporation/ Administrative legal person/Other organizations or groups	(1) Photocopy of registration certificates of the Organization; and (2) Photocopy of withholding unit establishment (change) registration application (uniform invoice number assignment notice); or photocopy of the seal certificate of the district court registry.
Government agency (authority) or education institute	Electronic exchange of official documents is used within which a color scan file of the sealed certificate application as an attachment.

3.2.3 Authentication of Individual Identity

The applicant must demonstrate control of its email address, see Section 3.2.5. The identification document required for individual identification and authentication, and the authentication and verification procedures whether need to be performed at the counter are determined based on various assurance levels as shown in the Table below.

Assurance Level	**Procedures for Authentication of Individual Identity**
Level 1	There is no requirement to link the applicant to a specific real-life identity. Any attributes provided in conjunction with the authentication process are self-asserted. (1) No identity verification required. (2) In-person identity proofing at counter is not required.
Level 2	Evidence supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity. (1) No identity verification required. (2) The applicant is required to provide a legible copy of a valid government issued national identity document or photo ID (such as National ID, passport or health

Assurance Level	Procedures for Authentication of Individual Identity
	insurance card), and CHT SMIME CA will verify the information through reliable communications. (3) In-person identity proofing at counter is not required
Level 3	(1) Identity proofing examination: The applicant shall provide information that includes name, national ID number and birthdate and at least present a national government-issued photo ID (such as national ID card, passport or health insurance card) to the RAO to examine whether they are authentic and unexpired. If an applicant (such as minor under 18 years old) is unable to submit the above photo ID, government-issued credentials (such as household registration) sufficient to prove the identity of the applicant and one adult with legal capacity to guarantee the applicant's identity in writing may be used in its place. The identity of the adult providing the guarantee must pass through the above authentication. (2) The applicant is required to provide personal information including personal identification code (such as National ID or passport number), name and address (household registration address). PublicCA has the right to cross-check it 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 applicant must in-person proofing his / her identity at the CA or RA counter. If the applicant is unable to present the application in person at the counter, the applicant may submit a letter of appointment to appoint an agent to submit the application 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.

Assurance Level	Procedures for Authentication of Individual Identity
	If an applicant has previously passed through the CA, RA or CA trusted authority or individual (such as household registration office or notary) 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 applicant does not need to apply in person but the CA or RA needs to verify the supporting information. (4) Apply with Citizen Digital Certificate IC Card When a private key digital signature corresponding to an assurance level 3 certificate issued by the MOICA is used, the applicant does not need to verify his / her identity in person with the RAO but the RA system or RAO shall verify whether the digital signature is valid. (5) Apply with the assurance level 3 certificate issued by ePKI The applicant does not need to in-person proofing his / her identity at the CA or RA counter if the request is applied with an assurance level 3 certificate issued by ePKI (e.g., Electronic identification IC card). The RA system or RAO shall verify that the digital signature is valid.

3.2.4 Non-verified Subscriber Information

The common name of an assurance level 1 certificate is not verified as the legal name of the subscriber. Therefore, a unique email address is included in the Common Name field as the certificate subject DN.

3.2.5 Validation of Authority

When a certificate lifecycle activity such as a certificate application or revocation request is submitted by an individual (an authorized representative) related to the certificate subject, CHT SMIME CA or its

RA shall perform a validation of authority to verify that the individual can represent the certificate subject, such as:

(1) Confirming the organization legal existence through third-party identity verification service or database, or documents issued by government or authorized organizations;

(2) Using telephone, postal letter, e-mail, SMS or fax obtained from the reliable methods specified in Section 3.2.2.1 of the Baseline Requirements or any equivalent way to confirm that the individual affiliated with the certificate subject (organization or company) and is authorized to represent the certificate subject; or

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

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

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

(2) Confirm that the applicant indeed owns or controls the authorization domain name of the e-mail address to be contained in the certificates in accordance with the domain validation method stated in Section 3.2.2.4 of the Baseline Requirements.

3.2.6 Criteria for Interoperation

CHT SMIME CA is not a Root CA. Not appliable.

3.2.7 Data Source Accuracy

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

(1) The age of the information provided,

(2) The frequency of updates to the information source,

(3) The data provider and purpose of the data collection,

(4) The public accessibility of the data availability, and

(5) The relative difficulty in falsifying or altering the data.

3.3 Identification and Authentication for Re-key Requests

If the subscriber's private key needs to be renewed upon expiry of the certificate usage period, certificate rekey work may be performed and the subscriber may re-apply for certification. Identification and authentication shall be performed in accordance with the regulations in Section 3.2.

3.3.1 Identification and Authentication for Routine Re-key

Two months before the subscriber's certificate is about to expire, the system will send an email to remind the subscriber to re-apply for the certificate. The RA shall identify and authenticate the subscriber in accordance with the provisions in Section 3.2. During certificate application, the RA shall use that subscriber's public key to verify the digital signature on the CSR to identify the subscriber's identity.

3.3.2 Identification and Authentication for Re-key after Revocation

If the subscriber private key needs to be re-keyed due to certificate revocation, the subscriber shall re-apply for the certificate with CHT SMIME CA. The RA shall identify and authenticate the subscriber in accordance with the provisions in Section 3.2.

3.4 Identification and Authentication for Revocation Request

CHT SMIME CA or RA must perform authentication of the certificate revocation application to verify that the applicant has the right to submit the certificate revocation. The authentication procedure for certificate revocation applications is the same as the provisions in Section 3.2.

4. Certificate Life-cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Organizations and individuals may submit certificate applications.

4.1.2 Enrollment Process and Responsibilities

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

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

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

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

using the certificate.

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

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

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

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

4.2 Certificate Application Processing

The certificate application procedures are as follows:

(1) The certificate applicant fills out the information on the certification request and agrees to the subscriber agreements.

(2) The certificate applicant sends the certificate request information and related certification information to the RA.

(3) If the certificate applicant self-generates the keys, a PKCS#10 CSR is created and signed with the private key. The certificate request file is submitted to the RA during the certificate application.

4.2.1 Performing Identification and Authentication Functions

CHT SMIME CA and RAs shall ensure that the system and procedure are sufficient to verify that the subscriber identity complies with CP and

CPS regulations. The initial registration procedure is implemented in accordance with Section 3.2 of this CPS. The certificate applicant shall submit correct and complete factual information. The information required for the certificate application shall contain required and optional information. Only the information listed on the certificate profile is recorded on the certificate. The information submitted by the certificate applicant and contact records kept by CHT SMIME CA and RA during the application process shall be properly kept in a secure, auditable manner in accordance with the ePKI CP and this CPS.

4.2.2 Approval or Rejection of Certificate Applications

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

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

4.2.3 Time to Process Certificate Applications

CHT SMIME CA and RAs shall complete the certificate application within a reasonable period of time. Provided that the information submitted by the applicant is complete and complies with CP, CPS and checking requirements, the RAO shall quickly complete the certificate application review. The time needed by RA to process certificate applications and CHT SMIME CA to issue the certificates depends on the certificate group and

type. These times may be disclosed in the subscriber agreements, contract or RA website.

If S/MIME certificate applications are accepted and complied with related regulations, the RAO shall normally complete the review procedure within two working days. After the subscriber completes certificate acceptance, CHT SMIME CA shall complete the certificate issuance work within one working day.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

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

Certificate issuance steps are follows:

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

(2) When CHT SMIME CA receives the certificate application submitted by the RA, the authorization status of the RA is first checked, the authorized assurance level and scope is verified and then the certificate is issued according to the information of the certificate application submitted by the RA.

(3) If the authorized assurance level and scope of the RA does not comply with the certificate application, CHT SMIME CA will send back the related erroneous message to the RA and refuse to perform related subsequent work. If there are any questions, the RA may directly contact CHT SMIME CA to understand where the problem is.

(4) In order to ensure the security, integrity and non-repudiability of the data transmitted between CHT SMIME CA and RA, the data of the certificate application is encrypted with a digital signature and transmitted through the network by TLS protocol.

(5) CHT SMIME CA reserves the right to refuse certificate issuance to any entity. CHT SMIME CA shall not bear any liability for damages to the applicant who is refused to issue the certificate.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

After CHT SMIME CA completes certificate issuance, the subscriber is notified to draw the certificate or the RA is used to notify the subscriber to draw the certificate.

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

4.4 Certificate Acceptance

There are two types of certificate acceptance procedures for certificates issued by CHT SMIME CA:

(1) The certificate applicant pre-reviews the content of the certificate to be issued. The certificate applicant reviews the information recorded on the certificate for accuracy and provides consistent information for the application. If the certificate applicant refuses to accept the information recorded on the certificate after reviewing the certificate content, the certificate is not issued. A new certificate application may be submitted in accordance with

Section 4.2.

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

The certificate field is reviewed by above certificate applicant before deciding whether or not to accept the certificate; the review shall at least include the subject name field and the e-mail address contained in the Subject Alternative Name Extension for consistent before certificate acceptance.

Acceptance of the certificate is deemed as the certificate applicant's consent to comply with the rights and obligations in this CPS or related contracts.

If there is fee collection or refund problems involved with certificate refusal, the certificate applicant shall handle the matter in accordance with the contract established in compliance with the Consumer Protection Act and Fair-Trade Act.

4.4.1 Conduct Constituting Certificate Acceptance

The certificate applicant pre-reviews the certificate content or reviews for the certificate content for errors. The certificate is published by CHT SMIME CA in the repository or delivered to the certificate applicant.

4.4.2 Publication of the Certificate by the CA

The CHT SMIME CA repository service regularly publishes the issued certificates or delivers the certificate to the certificate applicant to achieve certificate publication. The RA may negotiate with CHT SMIME CA about certificate delivery by the RA to the certificate applicant.

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

Subscribers refer to the entities that request and obtain certificates approved by CHT SMIME CA. Their relationship with the certificate subject is shown in the table in Section 1.3.3 of this CPS. Scope of applications regarding different assurance level certificates is stipulated in Section 1.4.1 of this CPS. Key pairs of subscribers shall be generated in compliance with Section 6.1.1 of this CPS. Subscribers must be able to control the private keys and do not issue certificates to others. Subscribers shall protect their private keys from unauthorized use or disclosure and shall use their private keys only for the correct key usage (i.e., the policy for key usage specified in the extension of the certificates), such as digitalsignatures or keyEncryption. 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 refer to third parties who trust the connecting relationship between the certificate subject name and public key. Relying parties shall use software that is compliant with ITU-T X.509, IETF RFCs and S/MIME certificate profile requirements of Google.

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

(1) Verify the identity of the e-mail signature author.
(2) Verify the integrity of the e-mail protected with digital signatures.
(3) Encrypt e-mail content.

The above certificate status information may be obtained from CRL or OCSP services. The cRLDistributionPoints location can be obtained from the certificate details. In addition, the relying parties shall check the content of the certificate policies extension of the issuing CA and subscriber certificates to confirm the assurance level of the certificates.

A Relying Party should rely on a digital signature only if:

(1) Digital signature is generated through the corresponding valid certificate and the certificate accuracy can be verified through the certificate chain;
(2) The certificate is not revoked and the relying party checked the revocation status of the certificate prior to the certificate's use by referring to the relevant CRLs or OCSP responses; and
(3) The certificate is being used for its intended purpose and in accordance with this CPS.

4.6 Certificate Renewal

CHT SMIME CA does not allow certificate renewal, subscribers shall generate new key pairs and apply for a new certificate, where initial identity validation shall be conducted as well.

4.6.1 Circumstances for Certificate Renewal

Not appliable.

4.6.2 Who May Request Renewal

Not appliable.

4.6.3 Processing Certificate Renewal Requests

Not appliable.

4.6.4 Notification of New Certificate Issuance to Subscriber

Not appliable.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Not appliable.

4.6.6 Publication of the Renewal Certificate by the CA

Not appliable.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Not appliable.

4.7 Certificate Re-Key

4.7.1 Circumstance for Certificate Re-key

The subscriber's private key shall be routinely re-keyed in accordance with the subscriber's private key usage period regulations in Section 6.3.2.

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

After the subscriber's certificate is revoked, use of its private key shall be suspended. After the key pair is re-keyed, a new certificate may be requested from CHT SMIME CA in accordance with Section 4.2.

4.7.2 Who May Request Certification of a New Public Key

A subscriber or legally authorized third party (e.g., a representative authorized by the organization).

4.7.3 Processing Certificate Re-keying Requests

For subscriber certificate re-keying, subscribers shall submit a new certificate application to CHT SMIME CA. The related procedures must be implemented in accordance with 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

As stated in Section 4.4.3.

4.8 Certificate Modification

4.8.1 Circumstance for Certificate Modification

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

procedures in Sections 4.1 and 4.2. CHT SMIME CA does not allow certificate modification, subscribers shall generate new key pairs and apply for a new certificate, where initial identity validation shall be conducted as well.

4.8.2 Who May Request Certificate Modification

Not appliable.

4.8.3 Processing Certificate Modification Requests

Not appliable.

4.8.4 Notification of New Certificate Issuance to Subscriber

Not appliable.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not appliable.

4.8.6 Publication of the Modified Certificate by the CA

Not appliable.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.9 Certificate Revocation and Suspension

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

4.9.1 Circumstances for Revocation

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

(1) The subscriber requests in writing to CHT SMIME CA that they wish to revoke the certificate;
(2) The subscriber notifies CHT SMIME CA that the original certificate request was not authorized and does not retroactively grant authorization;
(3) CHT SMIME CA obtains evidence that the subscriber's private key corresponding to the public key in the certificate suffered a key compromise;
(4) CHT SMIME CA obtains evidence that the validation of ownership or control for the e-mail address in the certificate should not be relied upon.

CHT SMIME CA 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) CHT SMIME CA obtains evidence that the certificate was misused;
(3) CHT SMIME 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) CHT SMIME CA is made aware of any circumstance indicating that use of the authorization domain name in the S/MIME 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) CHT SMIME CA is made aware that a certificate has been used to authenticate a fraudulently misleading Subordinate FQDN;

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

(7) CHT SMIME CA is made aware that the certificate was not issued in accordance with these requirements or the ePKI CP or this CPS;

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

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

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

(11) CHT SMIME CA is made aware of a demonstrated or proven method that exposes the subscriber's private key to compromise or if there is clear evidence that the specific method used to generate the private key was flawed;

(12) Under the circumstance that the payment deadline has expired and the subscriber has been notified, the subscriber has still not paid the fee; or

(13) CHT SMIME CA receives a notice or learns in other ways that the e-mail address contained in the certificate is no longer used.

CHT SMIME CA may at its own discretion revoke subscriber certificaters under the aforementioned circumstances.

4.9.2 Who Can Request Revocation

Subscribers, CHT SMIME CA, RAs or legally authorized third party (such as judicial or prosecution authorities, agents authorized by the

organization, and legal heirs of natural person) can request revocation.

In addition, a subscriber, relying party, application software suppliers or other third party may submit certificate problem report to advise CHT SMIME CA a reasonable reason to revoke the certificate.

4.9.3 Procedure for Revocation Request

(1) The certificate revocation applicant shall submit the certificate revocation request in accordance with the guidelines established by the RA. After the RA receives the certificate revocation request, the relevant review procedures are implemented and records of all certificate revocation requests are kept including applicant name, contact information, reason for revocation, time and date of revocation to serve a basis for subsequent accountability;

(2) After the RA completes the review work, the certificate revocation application information is sent to CHT SMIME CA;

(3) When CHT SMIME CA receives the certificate revocation application information sent by the RA, CHT SMIME CA first checks the authorization status of the relevant RA to verify that its authorized assurance level and scope. Afterward, the certificate is revoked based on the certificate revocation request sent by the RA;

(4) If the application does not pass the above checking, CHT SMIME CA shall send the related erroneous message to the RA and refuse to handle subsequent related work. If the RA has any questions, the RA may directly contact CHT SMIME CA to understand the source of the problem;

(5) In order to ensure the security, integrity and non-repudiability of the data transmitted between CHT SMIME CA and its RA, the data of the certificate application is encrypted with a digital

signature and transmitted through the network by TLS protocol;

(6) CHT SMIME CA uses the same CA private key issuing the certificate to publish the revoked certificate serial number and the reason for revocation to the CRL by the digital signature;

(7) Provide a timelier OCSP service (e.g. the status of being revoked, the status of being applied, or the status is valid); and

(8) CHT SMIME CA receives certificate problem reports and provides 24x7 availability of certificate problem response mechanism, as specified in Section 4.9.3.1.

4.9.3.1 Mechanism for Responding the Certificate Problems

Under “the Announcement of CPS” at the repository, CHT SMIME CA provides the guidelines for certificate problem reports. Subscribers relying parties, application software suppliers, and other third parties may submit certificate problem reports through the information specified in Section 1.5.2.2 under the circumstances of the private keys are cracked, the certificates are mis-issued, or the certificates are forged, cracked, abused, or used inappropriately.

4.9.4 Revocation Request Grace Period

The certificate revocation request grace period refers to the time to submit a certificate revocation request when the subscriber has confirmed the certificate revocation circumstances. The RA shall report suspect RA private key compromise circumstances to CHT SMIME CA within one hour. When the subscriber’s private key is lost or suspect or known to be compromised or the information appearing in the certificate has expired or is inaccurate, the subscriber shall promptly submit a certificate revocation application to the RA. The certificate revocation request grace period is two working days. CHT SMIME CA may extend the certificate revocation grace period when deemed necessary.

4.9.5 Time within Which CA Must Process the Revocation Request

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

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

(1) The nature of the alleged problem (scope, context, severity, magnitude, risk of harm);
(2) The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties);
(3) The number of certificate problem reports received about a particular certificate or subscriber;
(4) The entity making the complaint; and
(5) Relevant legislation.

4.9.6 Revocation Checking Requirement for Relying Parties

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

CHT SMIME CA publishes the information of suspended and revoked certificates to the repository for checking purposes. There are no restrictions for the checking of CRL by relying parties. The website is located at http://smimeca.hinet.net.

4.9.7 CRL Issuance Frequency

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

4.9.8 Maximum Latency for CRLs

After a CRL is produced by CHT SMIME CA, it will be released immediately. The system has no pre-signed behavior.

4.9.9 On-line Revocation/Status Checking Availability

CHT SMIME CA provides the inquiry to certificate revocation/status by CRL, webpage certificate inquiries and download, and OCSP responses.

CHT SMIME CA uses OCSP Responder to provide the OCSP responses complying with RFC 6960 and RFC 5019 standards. CHT SMIME CA uses the private signing key to issue the OCSP Responder certificates with the security strength at least RSA 2048 w/SHA-256 with which the relying parties can verify the digital signatures of the OCSP responses and confirm the integrity of the information sources.

4.9.10 On-line Revocation Checking Requirements

Relying parties shall check the validity of certificates by using the

CRLs or OCSP service in accordance with Section 4.9.6 or 4.9.9, respectively.

Thr OCSP responder uses 2048-bit RSA keys and SHA-256 hash function algorithm to issue OCSP responses.

CHT SMIME CA provides the OCSP service, and the OCSP responder operated by CHT SMIME CA supports the HTTP-based POST and GET methods, as described in RFC 6960 and RFC 5019.

The OCSP of CHT SMIME CA is updated at least once per hour, and the validity period of the OCSP responses is greater than or equal to 8 hours and less than 16 hours. Relying parties should check the information of nextUpdate field before checking the certificate through the OCSP response provided by CHT SMIME CA, and determine whether to trust the information by themselves.

A certificate serial number within an OCSP request may be one of three options, which are "assigned", "reserved" and "unused". The “assigned” certificate serial number means the serial number of the certificate issued by CHT SMIME CA; the “reserved” certificate serial number is the serial number of precertificates required for issuing TLS/SSL certificates; and the certificate serial number that does not meet the aforementioned conditions is the "unused" certificate serial number. CHT SMIME CA does not provide the issuance of TLS/SSL certificates, so no pre-signed certificates have been issued. In other words, the OCSP responder only allows a request for the status of a certificate serial number that is “assigned” or "unused".

If the OCSP responder receives a request for the status of a certificate serial number that is “assigned”, the responder shall respond with the status at that time of the certificate assigned with that serial number. If the OCSP responders receive a request for the status of a certificate serial number that is “unused”, the responder shall not respond with a "good" status. CHT

SMIME CA shall monitor the responder for such requests as part of its security response procedures.

4.9.11 Other Forms of Revocation Advertisements Available

CHT SMIME CA supports OCSP stapling based on RFC 4366.

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

CHT SMIME CA does not allow certificate suspension.

4.9.14 Who Can Request Suspension

Not appliable.

4.9.15 Procedure for Suspension Request

Not appliable.

4.9.16 Limits on Suspension Period

Not appliable.

4.9.17 Procedure for Certificate Resumption

Not appliable.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

CHT SMIME CA provides CRL service and the HTTP URL of the CRL service is presented in the CRL distribution points extension of its subscriber certificates. CHT SMIME CA also provides OCSP service.

Revocation entries on the CRLs or OCSP responses must not be removed until after the expiry date of the revoked certificates.

4.10.2 Service Availability

CHT SMIME CA maintains 24x7 availability of certificate status service.

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

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

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

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

CHT SMIME CA and subscriber's private signing keys shall not be escrowed.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

CHT SMIME CA does not currently support session key encapsulation and recovery.

5. Facility, Management, and Operation Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

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

5.1.2 Physical Access

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

The CHT SMIME CA facility has a total of four levels of security control. On the first and second levels, there are year-round entrance and building security controls in place. On the third level, access is controlled to this floor using a card access control system. On the fourth level, a fingerprint recognition control system is used to control access for facility personnel. The fingerprint scanner uses 3D sampling technology which is capable of detecting whether the fingerprint is from a live object by fingerprint depth and color.

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

software or hardware security module.

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

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

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

(1) Check if system equipment is operating normally.

(2) Check if the computer racks are locked.

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

5.1.3 Power and Air Conditioning

In addition to municipal power, the power system at the CHT SMIME CA facility is equipped with a generator (with enough fuel for six days of continuous operation) and an uninterrupted power system (UPS). The system is capable of automatically switching between municipal power and generator power. At least six hours of power can be supplied for repository backup work.

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

5.1.4 Water Exposures

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

5.1.5 Fire Prevention and Protection

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

5.1.6 Media Storage

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

5.1.7 Waste Disposal

When the documents of CHT SMIME CA detailed in Section 9.3.1 are no longer in use, it shall be shredded by the paper shredder. Any magnetic tape, hard disk, floppy disk, MO and other forms of memory shall be formatted to erase the information stored on them before scrapping. Optical disks shall be physically destroyed.

5.1.8 Off-site Backup

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

5.2 Procedural Controls

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

5.2.1 Trusted Roles

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

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

The administrator is responsible for:

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

The CA officer is responsible for:

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

The internal auditor is responsible for:

- Checking, maintenance and archiving of audit logs
- Conducting or supervising internal audits to ensure CHT SMIME CA is operating in accordance with this CPS

The system operator is responsible for:

- Daily operation and maintenance of system equipment
- System backup and recovery

- Storage media updating
- System hardware and software updates
- Website maintenance
- Set up protection mechanisms for system security and threats of virus or malware

The physical security controller is responsible for:

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

The cyber security coordinator is responsible for:

- Maintenance of the network and network facilities
- Patches management for the vulnerabilities of the network facilities
- The cyber security of CHT SMIME CA
- The detection and report of the cyber security events

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

- Researching, applying, or providing the anti-virus, anti-hacking, and anti-malicious software technologies or measures to ensure the security of the system and the network
- Reporting the collected threats or vulnerabilities of computer virus to the administrator or the cyber security coordinator for patches management

5.2.2 Number of Persons Required per Task

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

- Administrator

  At least 3 qualified individuals are needed.

- CA Officer

  At least 2 qualified individuals are needed.

- Internal Auditor

  At least 2 qualified individuals are needed.

- System Operator

  At least 2 qualified individuals are needed.

- Physical security controller

  At least 2 qualified individuals are needed.

- Cyber security coordinator

  At least 1 qualified individual.

- Anti-virus and anti-hacking coordinator

  At least 1 qualified individual.

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

Assignments	Administrator	CA Officer	Internal Auditor	System Operator	Physical security controller	Cyber security coordinator	Anti-virus and anti-hacking coordinator
Installation, configuration, and maintenance of the CHT SMIME CA system	2				1		
Establishment and maintenance of system user accounts	2				1		
Generation and backup of CHT SMIME CA keys	2		1		1		
Activation / deactivation of certificate issuance services		2			1		
Activation / deactivation of certificate revocation services		2			1		
Activate/deactivate the issuance services of CRL		2			1		
Checking, maintenance and archiving of audit logs			1		1		
Daily operation and maintenance of system				1	1		

Assignments	Administrator	CA Officer	Internal Auditor	System Operator	Physical security controller	Cyber security coordinator	Anti-virus and anti-hacking coordinator
equipment							
System backup and recovery				1	1		
Storage media updating				1	1		
Hardware and software updates outside the CHT SMIME CA certificate management system				1	1		
Website maintenance				1	1		
Daily operation and maintenance of the network and network facilities				1	1	1	
Patching the vulnerabilities of the network facilities	1				1	1	
Reporting the threats and vulnerabilities of computer virus							1
keep the antivirus system's signatures update and patches for the vulnerabilities				1	1		

5.2.3 Identification and Authentication for Each Role

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

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

Operating system account management by the CHT SMIME CA host uses login account numbers, passwords and groups to identify and

authenticate administrator, CA officer, internal auditor and system operator. CHT SMIME CA uses the user's account, password, and system account administration functions, or other security mechanisms to identify the role of the cyber security coordinator.

5.2.4 Roles Requiring Separation of Duties

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

- Administrator, CA officer, internal auditor, and cyber security coordinator cannot assume any other roles among these four trust roles at the same time, but administrator, CA officer, and internal auditor can be system operator at the same time; and
- Physical security controller shall not concurrently assume any role of administrator, CA officer, internal auditor, and system operator.

A person serving a trusted role is not allowed to perform self-audit.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

(1) Security evaluation for personnel selection

Personnel selection includes the following items:

(a) Personality evaluation;
(b) Applicant experience evaluation;
(c) Academic and professional skills and qualifications evaluation;
(d) Personal identity check; and
(e) Evaluation of personnel conduct.

(2) Management of Personnel Evaluation

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

(3) Appointment, Dismissal and Transfer

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

(4) Duty of Confidentiality Agreement

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

5.3.2 Background Check Procedures

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

5.3.3 Training Requirements

Trusted Role	Training Requirements
Administrator	(1) CHT SMIME CA security principles and mechanism. (2) Installation, configuration, and maintenance of the CHT SMIME CA operation procedures. (3) Establishment and maintenance of system user accounts operation procedures. (4) Audit parameter configuration setting procedures. (5) CHT SMIME CA key generation and backup operation procedures. (6) Disaster recovery and continuous operation procedure.
CA Officer	(1) CHT SMIME CA security principles and mechanism. (2) CHT SMIME CA system software and hardware use and operation procedures. (3) Activation/deactivation of certification issuance operation procedure. (4) Activation/ deactivation of certification revocation operation procedure. (5) Activation/ deactivation of certificate CRL issuance service operation. (6) Disaster recovery and continuous operation procedure.
Internal Auditor	(1) CHT SMIME CA security principles and mechanism. (2) CHT SMIME CA system software and hardware use and operation procedures. (3) CHT SMIME CA key generation and backup operation procedures. (4) Audit log check, upkeep and archiving procedures. (5) Disaster recovery and continuous operation procedure.
System Operator	(1) Daily operation and maintenance procedures for system equipment. (2) System backup and recovery procedure. (3) Upgrading of storage media procedure. (4) Disaster recovery and continuous operation procedure. (5) Network and website maintenance procedure.
Physical security controller	(1) Physical access authorization setting procedure. (2) Disaster recovery and continuous operation procedure.
Cyber security coordinator	(1) Maintenance of the network and network facilities. (2) Security mechanism for the network.

Trusted Role	Training Requirements
Anti-virus and anti-hacking coordinator	(1) Prevention and control to the threats and vulnerabilities of computer virus. (2) Security mechanism for the operating system and the network.

5.3.4 Retraining Frequency and Requirements

All related personnel at CHT SMIME CA shall be familiar with any changes to CHT SMIME CA and related work procedures, laws and regulations. When there is any significant change, an appropriate amount of training time shall be scheduled within one month to conduct retraining and the training status shall be recorded to ensure that work procedures and regulatory changes are understood.

5.3.5 Job Rotation Frequency and Sequence

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

(2) System operators with the requisite training and clearance may be reassigned to the position of administrator, CA officer or internal auditor after two years.

(3) Administrator, CA officer and internal auditor who have not concurrently served in the position of system operator may be reassigned to the position of administrator, CA officer or internal auditor after serving one full year as system operator.

(4) Only personnel with a full two years of experience as a cyber security coordinator as well as the requisite training and clearance may be reassigned to the position of administrator, CA officer, or internal auditor.

(5) Only personnel with a full two years of experience as an anti-virus

and anti-hacking coordinator as well as the requisite training and clearance may be reassigned to the position of administrator, CA officer, or internal auditor.

5.3.6 Sanctions for Unauthorized Actions

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

5.3.7 Independent Contractor Requirements

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

5.3.8 Documentation Supplied to Personnel

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

5.4 Audit Logging Procedures

Auditable security audit logs are kept in accordance with the archive retention regulations stated in Section 5.5.2.

5.4.1 Types of Events Recorded

(1) Key generation

- Key generation of CHT SMIME CA (not mandated for the generation of keys that are used once or only once).

(2) Private key loading and storage

- Loading the private key into a system component.
- All access to private keys kept by CHT SMIME CA for key

recovery work.

(3) Certificate registration

- Certificate registration request procedure.

(4) Certificate revocation

- Certificate revocation request procedure.

(5) Account administration

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

(6) Certificate profile management

- Certificate profile changes.

(7) CRL profile management

- CRL profile changes.

(8) Physical access / site security

- Known or suspect violation of physical security regulations.

(9) Anomalies

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

5.4.2 Frequency of Processing Log

CHT SMIME CA shall routinely review audit logs and explain major events. Review work includes examining all log entries and conducting a final complete check for any warnings or anomalies. Audit checking results shall be documented.

CHT SMIME CA shall check the audit logs once every two months.

5.4.3 Retention Period for Audit Log

Audit logs shall be retained on-site for two months and the log

retention management system shall be operated in accordance with the regulations in Sections 5.4.4, 5.4.5 and 5.4.6.

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

5.4.4 Protection of Audit Log

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

5.4.5 Audit Log Backup Procedures

Electronic audit logs are backed up at least once a month.

(1) CHT SMIME CA shall routinely archive event logs.

(2) CHT SMIME CA shall store the event logs in a secure protected site.

5.4.6 Audit Collection System (Internal vs. External)

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

5.4.7 Notification to Event-causing Subject

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

5.4.8 Vulnerability Assessments

The RAs conduct a vulnerability scan at least once each year and take remedy measures.

CHT SMIME CA conducts the vulnerability assessments at least once

per quarter and the penetration testing at least once per year. CHT SMIME CA will implement the enhancement and correction measures after the penetration testing and the vulnerability assessment. CHT SMIME CA also must conduct penetration testing after it is determined that there is a significant upgrade or modification to the application program or infrastructure. CHT SMIME CA shall record the skills, tools, followed ethics, competitive relations and independence guidelines for those personnel or groups capable of implementing reliable vulnerability scanning, penetration testing, or information security diagnosis or security surveillance.

5.5 Records Archival

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

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

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

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

5.5.1 Types of Records Archived

CHT SMIME CA retains the following information in its archives:

(1) CHT SMIME CA accreditation information from competent authorities.

(2) CPS.
(3) Major contracts.
(4) System and equipment configuration settings.
(5) System and configuration setting modifications and updates.
(6) Certificate application information.
(7) Revocation request information.
(8) Subscriber identity identification information stipulated in Section 3.2.
(9) Issued and published certificates.
(10) CHT SMIME CA re-key records.
(11) Issued or announced CRLs.
(12) Audit logs.
(13) Other data or application programs used to verify and corroborate the archived content.
(14) Documents required by the auditor.

5.5.2 Retention Period for Archive

CHT SMIME CA retains archived data for at least 10 years. The application programs used to process archived data are retained for 10 years.

5.5.3 Protection of Archive

(1) Amendments, modifications and deletion of archived information not allowed by any user.
(2) Transfer of archived information to another storage media which has passed through the CHT SMIME CA authorization procedure.
(3) Archived information stored in a secure, protected location.

5.5.4 Archive Backup Procedures

CHT SMIME CA electronic records shall be regularly backed up and

saved in storage media in accordance with backup procedures. Paper records shall be regularly sorted and filed by CHT SMIME CA.

5.5.5 Requirements for Time-stamping of Records

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

5.5.6 Archive Collection System (Internal or External)

There is currently no archive information collection system.

5.5.7 Procedures to Obtain and Verify Archive Information

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

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

5.6 Key Changeover

CHT SMIME CA shall periodically change its private keys in accordance with Section 6.3.2 and shall change its key pair before the usage period of its private key issuing subscriber certificates has expired. After key changeover, an application for a new certificate shall be submitted to eCA. The new certificate shall be published in the repository for subscribers and relying parties downloading.

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

If CHT SMIME CA's certificate has been revoked, CHT SMIME CA shall stop using its private keys and shall change its private keys.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

CHT SMIME CA establishes incident and compromise reporting and handling procedures and conducts drills annually.

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

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

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

5.7.3 Entity Private Key Compromise Procedures

In the event of signature key compromise, the PMA, eCA and application software suppliers shall be notified, and CHT SMIME CA implements the following recovery procedures:

(1) Publish in the repository and notify subscribers and relying parties about the event of key compromise.

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

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

CHT SMIME CA shall conduct the drills at least once a year.

5.7.4 Business Continuity Capabilities after a Disaster

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

5.8 CA or RA Termination

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

(1) CHT SMIME CA shall notify the competent authority (MOEA) and subscribers 30 days prior to of the scheduled termination of service.

(2) CHT SMIME CA shall take the following measures when terminating their service:

- For certificates which are valid at the time of termination, arrangements shall be made for other CA to take over the service. Matters regarding service termination and service acceptance by other CAs shall be published in the repository and subscribers with valid certificates stall be notified. This

shall not apply if notification cannot be made.

- All records and files during the operation period shall be handed over to the other CA that is taking over this service.
- If there is no CA willing to take over the CHT SMIME CA service, a report shall be submitted to the competent authority to arrange for other CA to take over this service.
- If the competent authority arranges for other CA to take over the service but no other CA takes over the service, CHT SMIME CA shall revoke the still valid certificates, publish the revoked certificates in the repository and notify all certificate-related persons 30 days prior to the scheduled termination of service. CHT SMIME CA will refund the certificate issuance and renewal fees based on the propotion of the certificate validity.
- The competent authorities, if necessary, may publish the certificates which are still valid at the time of revocation.

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

6. Technical Security Controls

This chapter describes the technical security controls implemented by CHT SMIME CA.

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

CHT SMIME CA and subscribers generate pseudo random numbers and public key pairs within the hardware security module in accordance with Section 6.2.1.

According to the regulations in Section 6.2.1, CHT SMIME CA generates key pairs within the hardware security module by using the algorithm and the procedures that meets NIST FIPS 140-2 standard. The private keys are imported and exported in accordance with Sections 6.2.2 and 6.2.6.

CHT SMIME CA key generation is witnessed and videotaped by those related personnel who have signed key initiation witness document (the public key of the generated key pair is listed on it). The related personnel shall include the members of the PMA and the internal auditor.

6.1.1.1 Subscriber Key Pair Generation

Subscriber key pairs are generated by the RA (for chip token) or by themselves (could be software or HSM).

6.1.2 Private Keys Delivery to Subscriber

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

6.1.3 Public Key Delivery to Certificate Issuer

If the RA generates a key pair for a subscriber, the RA shall deliver

the subscriber public key to CHT SMIME CA via secure channels.

If a subscriber self-generates a key pair, the subscriber shall deliver the public key to the RA via a CSR file with PKCS# 10 format. The RA shall delivery the public key to CHT SMIME CA via secure channels after it is verified that the subscriber is in possession of the corresponding private key in accordance with the regulations in Section 3.2.1.

Secure channels referred in this Chapter are the use of TLS or other equivalent or higher level data encryption transmission protocols.

6.1.4 CA Public Key Delivery to Relying Parties

CHT SMIME CA's own public key are issued by eCA and published in the CHT SMIME CA repository for direct downloading and installation by subscribers and relying parties. Relying parties shall obtain the eCA's public key or self-signed certificate via secure channels according to the eCA CPS before using the CHT SMIME CA public key certificate. Relying parties shall then validate the signature on the CHT SMIME CA public key certificate to ensure the trustworthiness of the public key in the public key certificate.

6.1.5 Key Sizes

CHT SMIME CA uses 4096-bit or the above RSA keys and SHA-256 hash function algorithm to issue certificates.

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

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

If CHT SMIME CA uses Elliptic Curve Cryptography (ECC) algorithm to issue certificates, the key size will comply with NIST P-256 or P-384.

For ECDSA keys, CHT SMIME CA shall use one of the following curve-hash pairs: P-256 with SHA-256, P-384 with SHA-384.

6.1.6 Public Key Parameters Generation and Quality Checking

The public key parameter of the RSA algorithm is null.

CHT SMIME CA signature key pair uses the NIST FIPS 186-4 standard to generate the prime numbers needed for the RSA algorithm and ensure that the prime number is a strong prime.

The subscriber key may generate the prime numbers needed for the RSA algorithm inside the IC card or other software/hardware security modules but this does not guarantee that this prime number is a strong prime.

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

If the certificates are issued with Elliptic Curve Cryptosystem (ECC) algorithm, CHT SMIME CA shall follow the requirements of Sections 5.6.2.3.2 and 5.6.2.3.3 in NIST SP 800-56A Revision 2 to confirm the validity of all keys using either the ECC Full Public Key Validation Routine or the ECC Partial Public Key Validation Routine.

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

CHT SMIME CA’s private signing key is used to issue certificates and CRLs. CHT SMIME CA’s own public key certificate is issued by eCA, and the keyUsage bits of keyCertSign and cRLSign are set. If the private

signing Key of CHT SMIME CA is used for signing OCSP responses, then the digitalSignature bit MUST also be set where others must not be set. The keyUsage extension must contain emailProtection, where the values serverAuth, codeSigning, timestamping, and anyExtendedKeyUsage must not be set.

For S/MIME certificates, the keyUsage bits of digitalSignature and/or nonRepudiation are set, where dataEncipherment and/or keyEncipherment may be set, and others must not be set. The keyUsage extension must contain emailProtection, where the values serverAuth, codeSigning, timestamping, and anyExtendedKeyUsage must not be set.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

CHT SMIME CA uses FIPS 140-2 Level 3 certified hardware security modules.

Storage media for subscriber key pairs may be:

Storage media	Certified standard
Chip	FIPS 140-2 Level 2, or Common Criteria EAL (EAL) 4+
HSM	FIPS 140-2 Level 3
Other tokens (e.g. Software)	None.

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

CHT SMIME CA key splitting multi-person control uses n-out-of-m LaGrange Polynomial Interpolation. It is a perfect secret sharing method which can used for private key splitting and recovery. Besides, n and m must be values greater than or equal to 2, and n must be less than or equal

to m. Use of this method can provide the highest security level for CHT SMIME CA private key multi-person control. Therefore, it can be used as the activation method for private keys as well (see Section 6.2.8).

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

6.2.3 Private Key Escrow

CHT SMIME CA's private signing key is not escrowed.

6.2.4 Private Key Backup

Backups of CHT SMIME CA private keys are made according to the key splitting multi-person control in Section 6.2.2 and IC cards verified with FIPS 140-2 Level 2 or above are used as the storage media for key splitting.

6.2.5 Private Key Archival

CHT SMIME CA does not archive private signing keys, but the corresponding public keys will be archived by certificate file format in accordance with Section 5.5.

6.2.6 Private Key Transfer into or from a Cryptographic Module

CHT SMIME CA transfers private keys into cryptographic modules under the following circumstances:

(1) Key generation;

(2) For the recovery of a backed up key, the secret splitting (*n-out-of-m* control) is used to recover the CHT SMIME CA private key with the splitted IC cards, and the complete private key is written into the hardware security module; and

(3) For the purpose of HSM transfer, the private keys are encrypted when transported between hardware security modules and never

exist in plaintext form. After the private keys are imported, the related secret parameters generated during the transport process must be completely destroyed.

6.2.7 Private Key Storage on Cryptographic Module

As stated in Sections 6.1.1 and 6.2.1.

6.2.8 Method of Activating Private Key

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

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

(1) If it is an IC card, the private keys shall be activated by the subscribers' (whose identity is validated) configuration and the PINs only known to the subscribers.

(2) If it is a hardware security module, the private keys are activated by the IC cards controlled by multiple people. The controlling IC cards for different purposes are maintained by different people.

(3) If a mail gateway is used, the subscribers trust and escrow their private keys on the mail gateway server, and the activation method of the private keys is controlled by the mail gateway server.

(4) For other private key tokens, subscribers shall use strong passwords or other identification with the same level to activate the private keys, in order to prevent the unauthorized access or use of the private keys.

6.2.9 Method of Deactivating Private Key

The multi-person control in Section 6.2.2 are used to deactivate CHT SMIME CA private keys.

CHT SMIME CA does not provide subscriber private key deactivation service.

6.2.10 Method of Destroying Private Key

In order to prevent the theft of CHT SMIME CA private keys which could endanger the authenticity of the entire certificate, the private key must be destroyed at the end of the CHT SMIME CA key lifecycle. Therefore, when CHT SMIME CA completes the key renewal and eCA issues a new CHT SMIME CA certificate, after no additional certificates or CRL are issued (see Section 4.7), zeroization is done on the old CHT SMIME CA private key stored inside the hardware security module to ensure that the old CHT SMIME CA private key is destroyed.

In addition to destroying the old CHT SMIME CA private key in the hardware security module, physical destruction of the splitted IC cards with a backed up key inside shall be done as well during the CHT SMIME CA key renewal.

If services are permanently not provided by a cryptographic module but it is still accessible, all private keys (already used or possibly used) stored in that cryptographic module must be destroyed. After destroying the keys, the key management tools provided by this cryptographic module must be used to verify that the above keys no longer exist.

If services are permanent not provided by a cryptographic module, all used private keys stored in that cryptographic module must be erased from the cryptographic module.

The destruction method for subscriber private keys is not stipulated.

6.2.11. Cryptographic Module Rating

See Section 6.2.1.

6.3 Other Aspects of Key Pair Management

Subscribers must self-administer key pairs. CHT SMIME CA is not responsible for safeguarding subscriber private keys.

6.3.1 Public Key Archival

CHT SMIME CA performs subscriber certificate archival and securely controls the archival system in accordance with the regulations in Section 5.5. No additional archival of subscriber public keys is done.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

6.3.2.1 CHT SMIME CA Certificate Operational Periods and Key Pair Usage Periods

CHT SMIME CA certificate operational periods and key pair usage periods are:

Type of Cert.	Private Key Usage Period	Certificate Term
CA Certificate of CHT SMIME CA	■ Issuing subscriber certificates: 10 years ■ Issuing CRLs or OCSP responder certificates: 20 years	20 years
OCSP Responder Certificate	■ Issuing OCSP responses: 36 hours	36 hours

The new OCSP responder certificate is disclosed daily (provide the relying parties with the OCSP response signed by the new private key along with that certificate).

6.3.2.2 Subscriber Certificate Operational Periods and Key Pair Usage Periods

The key size of public and private keys for the subscriber in CHT SMIME CA is RSA 2048 bit or the above, or ECC-256 or the above when ECC algorithm is applied. The subscriber certificate operational periods and key pair usage periods are:

Type of Cert.	Private Key Usage Period	Certificate Term
S/MIME Certificate	■ See Section 6.1.7: less than 27 months	less than 27 months

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The random numbers for the activation data are generated and then written in the cryptographic module and then split into the n-out-of-m control IC cards. When accessing the activation data in the IC card, the personal identification number (PIN) of the IC card must be entered.

6.4.2 Activation Data Protection

Activation data is protected by the n-out-of-m control IC card. Personnel who hold the control cards are responsible for remembering the IC card PIN. The PIN shall not be stored in any media. During IC card handover, a new PIN is set by the new personnel who hold the control cards.

If there are over three failed login attempts, the controlled IC card is locked.

6.4.3 Other Aspects of Activation Data

The CHT SMIME CA private key activation data is not archived.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

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

(1) Trusted role or identity authentication login,

(2) Provide discretionary access control,

(3) Provide security audit capability, and

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

6.5.2 Computer Security Rating

CHT SMIME CA servers use EAL 3 certified computer operating systems.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

Quality control for CHT SMIME CA system development complies with CMMI standards.

The RA hardware and software shall be checked for malicious code during initial use and shall be regularly scanned by using tools, including anti-virus software or malware removal tools.

System development environments, testing environments and on-line operation environments shall be segregated.

The system research and development department shall exercise the due care of a good administrator, sign a security warranty guaranteeing

there are no back doors or malicious programs, and provide a product or program handover list, test report, system management manual, and source code scanning report to CHT SMIME CA as well as conduct program version control.

6.6.2 Security Management Controls

When loading software onto a CA system for the first time, CHT SMIME CA verifies that the software is the correct version and is supplied by the vendor free of any modifications.

CHT SMIME CA shall only use components with security authorization. Unrelated hardware devices, network connections or component software shall not be installed.

CHT SMIME CA documents and controls system configuration and any modification or upgrades of functions as well as detect unauthorized modifications to system software or configuration.

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

6.6.3 Life Cycle Security Controls

At least one assessment shall be conducted each year to determine if there is any risk of compromise for existing keys.

6.7 Network Security Controls

The CHT SMIME CA host and repository have firewalls and are connected to external networks. The repository is placed on the outside

service area (de-militarized zone, DMZ) in the firewall and connected to the Internet. Except during required maintenance or backup, the repository provides uninterrupted certificate and CRL inquiry services.

The certificates and CRLs issued by the CHT SMIME CA host have digital signature protection and are automatically delivered from the CHT SMIME CA host to the repository.

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

6.8 Time-stamping

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

(1) Time of subscriber certificate issuance,

(2) Time of subscriber certificate revocation,

(3) Time of CRL issuance, and

(4) Time of system event occurrence.

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

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

The certificates issued by CHT SMIME CA conform to the official versions of the ITU-T X.509, S/MIME certificate profile requirements of Google, RFC 8550 and RFC 5280.

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

7.1.1 Version Number(s)

CHT SMIME CA issues X.509 version 3 certificates.

7.1.2 Certificate Extensions

The extensions of the certificates issued by CHT SMIME CA are set in compliance with the official versions of the ITU-T X.509, S/MIME certificate profile requirements of Google, RFC 8550 and RFC 5280.

7.1.2.1 Subordinate CA Certificate of CHT SMIME CA

The extensions of Subordinate CA Certificate that eCA issued to CHT SMIME CA are described as follows:

a. certificatePolicies

This extension is required and marked as non-critical. It asserts the policy identifier. The policy qualifier field of this extension may be used to mark the published URL of the eCA CPS as needed.

b. cRLDistributionPoints

This extension is required and marked as non-critical. It contains the HTTP URL of eCA's CRL service.

c. authorityInfoAccess

This extension is required and marked as non-critical. It contains the HTTP URL of eCA's OCSP responder and the HTTP URL to download the self-signed certificate of eCA.

d. basicConstraints

This extension is required and marked as critical. The cA field is set to true. As a result of CHT SMIME CA does not sign the subordinate CA certificates downwards, the pathLenConstraint field is set to zero (0).

e. keyUsage

This extension is required and marked as critical. This extension is used to mark keyUsage bits as keyCertSign and cRLSign. CHT SMIME CA does not sign the OCSP response with the private signing key, but issues the OCSP responder certificate, and the OCSP responder issues OCSP responses, and thus the configuration does not use digitalSignature.

f. nameConstraints

The subordinate CA certificates issued to CHT SMIME CA by eCA do not have this certificate extension.

g. extKeyUsage

This extension is required and marked as non-critical. The "Secure Email" EKU is stated in Section 6.1.7.

7.1.2.2 Subscriber Certificate

a. certificatePolicies

This extension is required and marked as non-critical. It asserts the policy identifier. The policy qualifier field of this extension may be used to mark the published URL of this CPS as needed.

b. cRLDistributionPoints

This extension is required and marked as non-critical. It contains the HTTP URL of CHT SMIME CA's CRL service.

c. authorityInfoAccess

This extension is required and marked as non-critical. It contains the HTTP URL of CHT SMIME CA's OCSP responder and the HTTP URL to download the certificate of CHT SMIME CA.

d. basicConstraints

This extension is required and marked as critical. The cA field is set to true. As a result of PublicCA does not sign the subordinate CA certificates downwards, the pathLenConstraint field is set to zero (0).

e. keyUsage

This extension is required and marked as critical. The "Secure Email" EKU is stated in Section 6.1.7.

f. extKeyUsage

This extension is required and marked as non-critical. The "Secure Email" EKU is stated in Section 6.1.7.

g. authorityKeyIdentifier

This extension is required and marked as non-critical. The "Secure Email" EKU is stated in Section 6.1.7.

Unless the reasons to include certain data in the certificates are known, CHT SMIME CA does not allow certificates being issued in the following scenarios:

(1) Extensions that do not apply in the context of the public internet, such as the value in the Extended Key Usage extension for a service that is only valid in the context of a privately managed network, and

(2) Semantics that will mislead a Relying Party about the certificate information verified by CHT SMIME CA.

7.1.3 Algorithm Object Identifiers

The algorithm OIDs used for signatures on CHT SMIME CA issued certificates are:

sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}

(OID: 1.2.840.113549.1.1.11)

sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha384WithRSAEncryption(12)}

(OID: 1.2.840.113549.1.1.12)

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

(OID: 1.2.840.113549.1.1.13)

ecdsaWithSHA256	{iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2)}

(OID: 1.2.840.10045.4.3.2)

ecdsaWithSHA384	{iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA384(3)}

(OID: 1.2.840.10045.4.3.3)

ecdsaWithSHA512	{iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA512(4)}

(OID: 1.2.840.10045.4.3.4)

The algorithm OID used during CHT SMIME CA issued certificate generation of subject keys are:

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

(OID: 1.2.840.113549.1.1.1)

ecPublicKey	{iso(1) member-body(2) us(840) ansi-x962(10045) keyType(2) ecPublicKey(1)}

(OID: 1.2.840.10045.2.1)

For ECC algorithm, the OID of the elliptic curve parameter described below must also be noted:

secp256r1	{iso(1) member-body(2) us(840) ansi-x962(10045) curves(3) prime(1) prime256v1(7)}

(OID: 1.2.840.10045.3.1.7)

secp384r1	{iso(1) identified-organization(3) certicom(132) curve(0) ansip384r1(34)}

(OID: 1.3.132.0.34)

7.1.4 Name Forms

The subject and issuer fields of the certificate must use the X.500 distinguished name and the name attribute type shall comply with the official versions of the ITU-T X.509, S/MIME certificate profile requirements of Google, RFC 8550 and RFC 5280.

The Subject information in the CA certificates of CHT SMIME CA shall contain countryName (OID 2.5.4.6) field, the value of which is the double alphabet country code specified in ISO 3166-1 for the country where CHT SMIME CA locates. Besides, the organizationName (OID 2.5.4.10) field must be included, and the value of which is the identifier including the name able to identify CHT SMIME CA, trademark, or their meaningful name, for the purpose of identifying CHT SMIME CA more precisely; it is not allowed to contain the commonName only. For example: CA1. Please refer to Section 3.1.5 for the X.500 distinguished name of the CA certificate of CHT SMIME CA.

7.1.4.1 Issuer Information

According to RFC 5280 “Name Chaining”, the content of Issuer DN for the certificate issuer, shall be identical to the Subject DN of the issuing

CA. Therefore, for the subscriber certificate issued by CHT SMIME CA, the Issuer DN must be identical to the content of the Subject DN of CHT SMIME CA.

7.1.4.2 Subject Information–Subscriber Certificates

By issuing the subscriber certificates, CHT SMIME CA and RAs have complied with the procedures specified in the ePKI CP and/or this CPS, to ensure all the Subject information contained in these certificates are accurate. In addition, subject attributes MUST NOT contain only metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.

7.1.4.2.1 Subject Alternative Name Extension

The Subject Alternative Name Extensions for S/MIME certificates are as follows:

Certificate Extension	Required/Optional Extension
extension:subjectAltName	Required

The Subject Alternative Name Extension must be rfc822Name, and must not be dNSName, iPAddress, or uniformResourceIdentifier.

The Subject Alternative Name Extension will mark the e-mail address. The RAO shall validate the ownership or control of the e-mail address.

7.1.4.2.2 Subject Distinguished Name Fields

The Subject Distinguished Name Fields of S/MIME certificates issued by CHT SMIME CA are described as follows:

Certificate field	Levels 2 & 3 Organization S/MIME Certificates	Levels 2 & 3 Individual S/MIME Certificates	Level 1 S/MIME Certificates
subject:commonName (OID 2.5.4.3)	Δ	Δ	Δ
subject:organizationName (OID 2.5.4.10)	◯	Δ	Δ

Certificate field	Levels 2 & 3 Organization S/MIME Certificates	Levels 2 & 3 Individual S/MIME Certificates	Level 1 S/MIME Certificates
subject:givenName (OID 2.5.4.42) and subject:surname (OID 2.5.4.4)	×	Δ	Δ
subject:streetAddress (OID 2.5.4.9)	Δ	Δ	Δ
subject:localityName (OID 2.5.4.7)	Δ	Δ	Δ
subject:stateOrProvinceName (OID 2.5.4.8)	Δ	Δ	Δ
subject:postalCode(OID 2.5.4.17)	Δ	Δ	Δ
subject:countryName(OID 2.5.4.6)	○	○	Δ
subject:organizationUnitName (OID2.5.4.11)	Δ	Δ	Δ

Symbols' meaning:

Optional: Δ Required: ○ Prohibited: ×

7.1.4.3 Subject Information–CA Certificates

The CA certificates of CHT SMIME CA is validated and issued by eCA based on the procedures specified in the ePKI CP and/or eCA CPS. The Subject Distinguished Name Fields are as follows:

7.1.4.3.1 Subject Distinguished Name Field

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

7.1.5 Name Constraints

Name constraints are not used.

7.1.6 Certificate Policy Object Identifier

CHT SMIME CA issued certificates contain one or more policy OIDs, please refer to Section 1.2.

7.1.7 Usage of Policy Constraints Extension

Certificates issued by CHT SMIME CA do not contain policy constraints extension.

7.1.8 Policy Qualifiers Syntax and Semantics

Policy qualifiers may be used to mark the published URL of this CPS as needed.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

The certificate policy extensions contained in the certificates issued by CHT SMIME CA are not marked as critical.

7.2 CRL Profile

7.2.1 Version Number(s)

CHT SMIME CA issues ITU-T X.509 version 2 CRLs.

7.2.2 CRL and CRL Entry Extensions

The extensions of crlExtensions and crlEntryExtensions in the CRLs issued by CHT SMIME CA conform to the official versions of the ITU-T X.509, S/MIME certificate profile requirements of Google, RFC 8550 and RFC 5280.

7.3 OCSP Profile

CHT SMIME CA provides OCSP services in compliance with RFC 6960 and RFC 5019, and the URL of the CHT SMIME CA OCSP service is contained in the authorityInfoAccess extension of the certificate.

7.3.1 Version Number(s)

An OCSP request accepted by CHT SMIME CA shall contain the following information:

- Version number, and
- Target certificate identifier

The target certificate identifier contains the hash algorithm, the hash of the issuer's DN, the hash of the issuer's public key and the serial number of the target certificate.

The OCSP response issued by the OCSP responder shall contain the following basic fields:

Field	Description
Status	Response status, includes success, request format error, internal error, try again later, request no signature or request no certificate authorization, the following items must be included when status is successful
Version number	v.1 (0x0)
OCSP responding server ID (Responder ID)	The subject DN of OCSP responder
Produced Time	OCSP Response sign time
Target certificate identifier	The contents of this field include the hash algorithm, the hash of the issuer's DN, the hash of the issuer's public key and the serial number of the target certificate.
Certificate Status	Certificate status code (0: valid /1: revoked /2: unknown)
ThisUpdate/NextUpdate	Recommended validity region for this response packet includes: ThisUpdate and NextUpdate
Signature Algorithm	OCSP response signature algorithm, which can be either sha256WithRSAEncryption or ecdsaWithsha384
Signature	OCSP responder signature
Certificates	OCSP responder certificate

7.3.2 OCSP Extensions

The OCSP response signed by the OCSP responder includes the following extensions:

- Authority key identifier of the OCSP responder;
- If an OCSP request contains a nonce field, the OCSP response must also contain the same nonce field;

7.3.3 Regulations for Operation of OCSP

The operation of OCSP in CHT SMIME CA includes:

- Able to process and receive the OCSP request transmitted by HTTP Get/Post channel or method.

The certificate for OCSP responder used by the OCSP server is issued by CHT SMIME CA with short-term validity, and it shall be issued and updated regularly by CHT SMIME CA.

8. Compliance Audit and Other Assessments

8.1 Frequency or Circumstances of Assessment

CHT SMIME CA shall undergo routine external audits at least once per year (the audited period may not exceed 12 months) and non-routine internal audits to confirm that the security regulations and procedures of the ePKI CP and this CPS are being implemented and enforced. CHT SMIME CA undergoes an audit in accordance with the following schemes: "WebTrust for CAs v2.1 or newer" and "Principle 4 of WebTrust for CAs SSL Baseline with Network Security v2.3 or newer".

8.2 Identity/Qualifications of Assessor

CHT retains a qualified auditor, who is familiar with the operations of CHT SMIME CA and is authorized by WebTrust for CA program as a licensed WebTrust practitioner to perform WebTrust Principles and Criteria for Certification Authorities and WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security 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. CHT SMIME CA shall conduct identity identification of auditors during auditing.

8.3 Assessor's Relationship to Assessed Entity

CHT shall retain an impartial third party to conduct audits of CHT SMIME CA operations.

8.4 Topics Covered by Assessment

The assessment shall include the following topics:

(1) Whether CHT SMIME CA is operating in accordance with this CPS, including management and technical audit of the physical environment, personnel procedural controls, key control, certificate lifecycle control, and hardware cryptographic module control;

(2) Whether the RA of CHT SMIME CA complies with this CPS and related procedures; and

(3) Whether the requirements of this CPS are being implemented and enforced subject to the ePKI CP, and whether the requirements are suitable for the practical operations of CHT SMIME CA.

The RA responsible for the verification of levels 1 and 2 certificate requests or revocation may undergo the external audit every 2 years; record every non-compliance or exceptions with respect to the ePKI CP and this CPS; and take actions to correct the deficiencies.

The RA responsible for the verification of level 3 certificate requests or revocation shall undergo the external audit annually; record every non-compliance or exceptions with respect to the ePKI CP and this CPS; and take actions to correct the deficiencies.

Before an external RA establishes an interface with general RA, CHT SMIME CA assigns personnel to conduct a site survey to check the implementation status of related security measures.

If an organization or business under an externa RA is unable to undergo the above external audit due to regulations or other factors, the RA may state their exclusion from the scope of audit for that year in an audit

report or management's assertions but CHT reserves the rights to conduct a compliance audit on whether or not the above RA is in compliance with the ePKI CP and this CPS to reduce any risk derived from any non-conformity. CHT has the right the conduct the following (but not limited to) review and examination items to ensure the trustworthiness of CHT SMIME CA:

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

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

8.5 Actions Taken as a Result of Deficiency

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

(1) Note the discrepancy,
(2) Notify CHT SMIME CA about the discrepancy, and
(3) CHT SMIME CA shall submit an improvement plan regarding

the discrepancy items within 30 days and promptly implement it. The discrepancy items shall also be listed as follow-up audit tracking items. The RA is notified to make improvements to RA-related deficiencies.

8.6 Communications of Results

Except for any audit findings that could result in system attacks and the stipulations in Section 9.3, CHT SMIME CA shall make its audit report publicly available. Audit results are displayed with appropriate seals, including WebTrust for Certification Authorities and WebTrust for Certification Authorities – SSL Baseline Requirements seals, on CHT SMIME CA's homepage. The audit report and management's assertions may be viewed by clicking on the seals. CHT SMIME 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, CHT SMIME 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

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

9.1.2 Certificate Access Fees

If there is a charge, it should be stipulated in the relevant business contract terms and conditions.

9.1.3 Revocation or Status Information Access Fees

If there is a charge, it should be stipulated in the relevant business contract terms and conditions.

9.1.4 Fees for Other Services

No charge at the moment.

9.1.5 Refund Policy

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

9.2 Financial Responsibility

9.2.1 Insurance Coverage

CHT SMIME CA is owned and operated by CHT. Its financial responsibilities are the responsibilities of CHT.

9.2.2 Other Assets

CHT SMIME CA finances are a part of the overall finances of CHT. CHT is a publicly listed company. In accordance with Article 36 of the Securities and Exchange Act, annual financial reports duly audited and attested by a certified public accountant, approved by the board of directors and recognized by the supervisors are publically announced and registered with the competent authority within three months after the close of each fiscal year. Financial reports duly reviewed by a certified public accountant and reported to the board of directors are publicly announced and registered within 45 days after the end of the first, second and third quarters of each fiscal year. The operating status for the preceding month is publicly announced and registered within the first 10 days of each month. CHT SMIME CA can provide self-insured asset prices based on CHT's financial reports. CHT's finances are sound and its ratio of current assets to current liabilities is no lower than 1.0 which meets the requirement of the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates.

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation for end-entities (including subscribers and relying parties).

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The following information generated, received and kept by CHT SMIME CA or its RA is deemed confidential information:

(1) Private keys and passphrases used for operations,
(2) Key splitting safekeeping information,
(3) Subscriber application information,
(4) Audit and tracking logs generated and kept by CHT SMIME CA,
(5) Audit logs and reports made by audit personnel during the audit process, and
(6) Operation-related documents listed as confidential-level operations.

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

9.3.2 Information Not Within the Scope of Confidential Information

(1) Identification information and information listed in the certificate are not deemed confidential information unless stipulated otherwise, and
(2) Issued certificates, revoked certificates, suspended information and CRLs published in the CHT SMIME CA repository are not deemed confidential information.

9.3.3 Responsibility to Protect Confidential Information

CHT SMIME CA shall handle subscriber application information in accordance with the Electronic Signatures Act, WebTrust Principles and Criteria for Certification Authorities audit criteria, Principle 4 of WebTrust

Principles and Criteria for Certification Authorities – SSL Baseline with Network Security audit criteria and Personal Information Protection Act.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

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

9.4.2 Information Treated as Private

(1) The personal information listed on certificate applications should not be disclosed without the subscriber's consent or in accordance with related laws.
(2) Subscriber information that cannot be obtained through certificates, CRLs or certificate catalog service,
(3) Identifiable information of personnel in CHT SMIME CA such as names together with palmprint or fingerprint biometrics, and
(4) Personal information on confidentiality agreements or contracts.

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

9.4.3 Information Not Deemed Private

Identification information, information listed in certificates and certificates are not deemed private information unless stipulated otherwise.

Issued certificates, revoked certificates or suspension information and CRLs published in the CHT SMIME CA repository are not private information.

9.4.4 Responsibility to Protect Private Information

The personal information required for the operation of CHT SMIME CA, in either paper or digital form, must be security stored and protected in accordance with the personal information protection and privacy rights declaration posted on the website and must comply with the Electronic Signatures Act, audit criteria of WebTrust Principles and Criteria for Certification Authorities and Principle 4 of WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security, and Personal Information Protection Act. CHT SMIME CA shall negotiate the liability of protecting private information with its RA.

9.4.5 Notice and Consent to Use Private Information

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

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

If judicial, supervisory or law enforcement authorities need to check private information under Section 9.4.2 for investigation or evidence collection requirements, the matter shall be handled in accordance with law or regulation. However, CHT SMIME CA reserves the right to charge reasonable fees from authorities applying for access to this information.

9.4.7 Other Information Disclosure Circumstances

Subscriber personal information obtained during CHT SMIME CA operations is handled in accordance with related laws and may not be

disclosed externally to ensure the personal privacy of subscribers. This shall not apply if stipulated otherwise under the law.

9.5 Intellectual Property Rights

The following is the intellectual property of CHT SMIME CA:

(1) Key pairs and split keys of CHT SMIME CA and RA;
(2) Related documents or system development for certificate management of CHT SMIME CA;
(3) Certificates and CRLs issued by CHT SMIME CA; and
(4) This CPS.

This CPS may be freely downloaded from the CHT SMIME CA repository. CHT grants permission to copy (in full) and distribute this CPS on a free basis according to the Copyright Act of R.O.C., but it must be copied in full and copyright noted as being owned by CHT. CHT reserves the right to pursue legal action for any violation of the use or dissemination of this CPS.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

CHT SMIME CA shall follow the procedures in Chapter 4 of this CPS to perform related certificate management work. CHT SMIME CA represents and warranties the following obligations:

(1) Comply with the ePKI CP and this CPS;
(2) Perform certificate application identification and authentication;
(3) Provide certificate issuance and publication services;
(4) Revoke certificates;
(5) Issue and publish CRLs;
(6) Issue and provide OCSP response messages;
(7) Securely generate CHT SMIME CA and RA private keys;

(8) Secure management of private keys;

(9) Use private keys in accordance with Section 6.1.7 regulations;

(10) Support related certificate registration work performed by RAs; and

(11) Conduct identification and authentication of CA and RA personnel.

9.6.2 RA Representations and Warranties

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

RAs shall represent and warrant that:

(1) Certificate management is performed in compliance with the ePKI CP and this CPS,

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

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

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

(5) Identification and authentication procedures for RAO are Implemented, and

(6) RA private keys are securely managed.

9.6.3 Subscriber Representations and Warranties

For the clear interest of CHT SMIME CA and the certificate beneficiary, the applicant should guarantee that CHT SMIME CA would receive the applicant’s confirmation of the Subscriber Agreement prior to the issuance of a certificate.

Applicant shall represent and warrant to CHT SMIME CA that it will:

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

(2) Provide accurate and complete information to CHT SMIME CA and RA;

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

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

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

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

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

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

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

9.6.4 Relying Party Representations and Warranties

Each relying party represents and warrants to:

(1) Comply with the provisions of this CPS when using a certificate or inquiring the CHT SMIME CA repository;

(2) Check the certificate assurance level during use of certificates;

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

(4) Validate a certificate (issued by CHT SMIME CA) by using a CRL or OCSP published by CHT SMIME CA in accordance with

the proper certificate path validation procedure;

(5) Carefully select secure computer environments and reliable application systems. If the rights of subscribers and relying parties are infringed due to the use of an untrusted computer environment or application system, relying parties shall bear the responsibility solely;

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

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

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

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

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

9.8 Limitations of Liability

Except to the extent ePKI has issued and managed the certificate in accordance with this CPS, CHT SMIME CA shall not be liable to the subscribers or relying parties for any losses suffered as a result of use or reliance on such certificate. Otherwise, CHT SMIME CA will assume the

compensation liability no more than the amount stipulated in Section 9.9 of this CPS.

9.9 Indemnities

9.9.1 Indemnification by CHT SMIME CA

If subscribers or relying parties suffer damages due to the intentional or unintentional failure of CHT SMIME CA to follow the ePKI CP, this CPS, relevant laws and the provisions of contracts signed between CHT SMIME CA, subscribers and related relying parties when processing subscriber certificate-related work, the subscriber shall request compensation in accordance with the relevant provisions of the contract signed between CHT SMIME CA and RA. Relying parties shall request compensation in accordance with relevant laws and regulations.

9.9.2 Indemnification by RA

If subscribers or relying parties suffer damages due to the RA intentional or unintentional failure to follow this CPS, related laws or the provisions of contracts signed between the RA and subscribers/relying parties when processing subscriber certification registrations, the RA shall be held liable. Compensation claims by subscribers shall be made in accordance with related provisions in the contract set down with the RA. Compensation claims by relying parties shall be made in accordance with relevant laws and regulations.

9.10 Term and Termination

9.10.1 Term

This CPS is effective when approved by the Electronic Signatures Act competent authority and published to CHT SMIME CA’s repository.

9.10.2 Termination

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

9.10.3 Effect of Termination and Survival

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

9.11 Individual Notices and Communications with Participants

CHT SMIME CA, RAs, subscribers, relying parties shall adopt suitable methods for establishing mutual notification and communication channels including but not limited to official document, letter, telephone, fax, e-mail or secure e-mail.

9.12 Amendments

9.12.1 Procedure for Amendment

This CPS is reviewed annually, and an assessment is made to determine if the CPS needs to be amended to maintain its assurance level. This CPS shall be amended accordingly if the ePKI CP is amended or the OID is changed, and if so, changes to this CPS are indicated by appropriate numbering.

9.12.2 Notification Mechanism and Period

CHT SMIME CA will post appropriate notice on its websites of any major or significant changes to this CPS as well as any appropriate period by when the revised CPS becomes effective. If subscribers or relying parties have any comment on the change items, they can submit the comment within the comment period. Reassess to the changes and response

may or may not be made by CHT SMIME CA according to these comments.

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

9.12.3 Circumstances under which OID Must Be Changed

CP OIDs will be changed if a change in the ePKI 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 this CPS accordingly.

9.13 Dispute Resolution Provisions

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

9.14 Governing Law

For disputes involving CHT SMIME CA issued certificates, the applicable ROC laws shall govern.

9.15 Compliance with Applicable Law

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

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

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

9.16.2 Assignment

The participants, including CHT SMIME CA, RAs, subscribers, and

relying parties, may not assign or delegate their rights or obligations under this CPS to other parties in any form without a prior written notice to CHT SMIME CA.

9.16.3 Severability

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

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

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

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

9.16.5 Force Majeure

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

9.17 Other Provisions

No stipulation.