Public Certification Authority Certification Practice Statement of Chunghwa Telecom

(PublicCA CPS)

Version 1.6

Chunghwa Telecom Co., Ltd.

February 4, 2016

Contents

Public Certification Authority Certification Practice Statement of Chunghwa Telecom Abstract

Chunghwa Telecom Co., Ltd. has established the Certification Practice Statement (CPS) of the Public Certification Authority of Chunghwa Telecom (PublicCA) in accordance with Article 11 of the Digital Signatures Act and the Regulations on Required Information for Certification Practice Statements promulgated by the Ministry of Economic Affairs. Establishment and revision of the CPS shall be published in the company website after approval by the competent authorities for issuance of certification service.

I. Competent Authority Approval No.: Chin-Shang-Tzu No. 10502201620 .

II. Types of Issued Certificates:

Natural person, organization, equipment and application software certificates.

III. Certificate Assurance Levels:

The PublicCA operates in accordance with relevant regulations of the Certification Policy (CP) of the Chunghwa Telecom ecommerce Public Key Infrastructure (ePKI) and issues level 1, 2 and 3 certificates as defined in the issuing CP in accordance with the identity authentication procedures of the certificate applicants for issue to different classes of natural persons, organizations, equipment or application software (see section 1.3.5.1).

IV. Applicable Scope:

Certificates issued by the PublicCA are used for identity certification and data encryption required by e-commerce and e-government Internet and financial transactions.

Subscribers and related relying parties of the PublicCA must exercise due care in the use of certification issued by the PublicCA and must not depart from the CPS, relevant laws and regulations and the certificate usage restrictions and prohibitions stipulated in contracts between the PublicCA, subscribers and relevant relying parties.

V. Important Matters Regarding Legal Responsibilities

1. Damage Indemnification Responsibility of the PublicCA

In the event that damages are suffered by subscribers or relying parties in relevant certification operations of the PublicCA and the registration authority due to intentional or unintentional failure to follow the CPS and relevant operation regulations, the PublicCA or the RA shall respectively be responsible for indemnity. The subscriber may make an indemnity claim in accordance with relevant provisions of the contract with the PublicCA or the RA; and the relying party is entitled to make an indemnity claim in accordance with relevant laws and regulations.

2. Exemption of Responsibility of the PublicCA

In the event that damages occur due to subscriber or related relying party failure to follow the CPS, relevant laws and

regulations or the contract set down between the PublicCA, the subscriber and the relevant relying party or any damages occur that are not attributable to the PublicCA, that subscriber or the relying party shall bear sole liability.

3. Exemption of Responsibility of the Registration Authority

In the event that a relying party suffers damages due to reasons attributable to the subscriber or any damages occur due to reasons not attributable to the RA, that subscriber or relying party shall bear sole liability.

In the event that damages occur due to subscriber or related relying party failure to follow the CPS, relevant laws and regulations or the contract entered into between the PublicCA, the subscriber and the relevant relying party or any damages occur that are not attributable to the RA, that subscriber or the relying party shall bear sole liability.

4. Exemption Provisions

In the event that damages are caused by a force majeure or reasons not attributable to the PublicCA and RA, the PublicCA and the RA shall not bear any legal responsibility. If the damages occurred due to exceeding the clear usage limitations set down by the PublicCA and RA, the PublicCA and the RA shall not bear any legal responsibility.

In the event that some certification services have to be suspended temporarily because of system maintenance, conversion or expansion of the PublicCA, the PublicCA may give advance notification in the repository to temporarily

suspend certificate service. Subscribers or relying parties may not request compensation for damages from the PublicCA based on the above-mentioned actions.

5. Financial Responsibility

The PublicCA has financial guaranty from Chunghwa Telecom Co., Ltd. The PublicCA shall perform financial audits in accordance with relevant laws and regulations.

6. Subscriber Obligations

Subscribers shall properly safeguard and use their private keys. Suspension, revocation, renewal or re-issuance of subscriber certificates shall conform to the regulations in Chapter 4 of the CPS but the subscriber shall assume the obligations of all use of the certificate before any changes are made.

VI. Other Important Matters

1. The registration work of RAs belonging to the PublicCA is authorized by the PublicCA.

2. The subscriber must comply with the relevant regulations of the CPS and ensure that all of the submitted application information is correct.

3. The relying party must confirm the accuracy, validity and usage restrictions of the certificate being relied on in order to reasonably rely on the certificates issued by the PublicCA.

The Company shall retain an impartial third party to conduct audits of PublicCA operations.

4. The standards used for audits are Trust Service Principles and Criteria for Certification Authorities and WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security

1. Introduction

1.1 Overview

1.1.1 Certification Practice Statement

The name of this document is Public Certification Authority Certification Practice Statement (CPS) of Chunghwa Telecom. The CPS is stipulated to follow the Certification Policy (CP) for the Chunghwa Telecom ecommerce Public Key Infrastructure and complies with related international standards such as the Internet Engineering Task Force (IETF) RFC 3647, ITU-T X.509, IETF PKIX Working Group RFC 5280, CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, CA/Browser Forum Network and Certificate System Security Requirements.

The PublicCA is the Level 1 Subordinate CA of the Chunghwa Telecom ecommerce Public Key Infrastructure (ePKI), and is responsible for issuance and administration of natural person, organization, equipment and application software certificates in the ePKI. The Chunghwa Telecom ePKI Root Certification Authority (eCA) is the highest level CA and trust anchor of the ePKI and Chunghwa Telecom Co., Ltd. is responsible for is operation and setup. Relying parties can directly trust the certificates of the eCA itself.

1.1.2 CPS Applicability

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

1.2 Document Name and Identification

This version is 1.6 and the issue date of this version is February 4, 2016. The latest version of this CPS can be obtained from:

http://publicCA.hinet.net

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

Assurance Level	OID Name	OID Value
Level 1	id-cht-ePKI-certpolicy-class1Assurance	{id-cht-ePKI-certpolicy 1}
Level 2	id-cht-ePKI-certpolicy-class2Assurance	{id-cht-ePKI-certpolicy 2}
Level 3	id-cht-ePKI-certpolicy-class3Assurance	{id-cht-ePKI-certpolicy 3}

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

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

Assurance Level	OID Name	OID Value
Level 1	id-pen-cht-ePKI-certpolicy-class1 Assurance	{id-pen-cht-ePKI-certpolicy 1}
Level 2	id-pen-cht-ePKI-certpolicy-class2 Assurance	{id-pen-cht-ePKI-certpolicy 2}

Assurance Level	OID Name	OID Value
Level 3	id-pen-cht-ePKI-certpolicy-class3 Assurance	{id-pen-cht-ePKI-certpolicy 3}

The SSL server software certificates issued by the PublicCA conform to the requirements defined in the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates and pass the external audit of AICPA/CPA WebTrust for Certification Authorities Trust Services Principles and Criteria for Certification Authorities – SSL Baseline Requirements Audit Criteria– Version 1.1 in November 2014 and shall be allowed to use for organization validation (OV) SSL CP OID （{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) organization-validated(2)} (2.23.140.1.2.2)）) and domain validation (DV) SSL CP OID （{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) domain-validated(1)} (2.23.140.1.2.1)） and individual validation (IV) SSL CP OID （{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) individual-validated(3)} (2.23.140.1.2.3)）of the CA/Browser Forum:

This CPS conforms to the current version of the CA/Browser Forum Baseline Requirements for the Issuance and Management of

Publicly-Trusted Certificates published at http://www.cabforum.org. If there are any inconsistencies between this CPS and the latest version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, the provisions of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates shall take precedence.

1.3 PKI Participants

The key members of the PublicCA include:

(1) PublicCA

(2) RAs

(3) Subscribers

(4) Relying Parties

1.3.1 PublicCA

The PublicCA, established and operated by Chunghwa Telecom Co., Ltd., operates and issues natural person, organization, equipment and application software certificates in accordance with CP regulations.

1.3.2 RAs

The RA is responsible for collection and authentication of subscriber identity and certificate-related information. The RA is comprised of one or more RA counters authorized under the organization approved by the PublicCA. Each RA counter has an RA officer (RAO) who is responsible for performing certification

application, revocation, rekey, renewal work for different groups and classes.

PublicCA RA is divided into two major categories: general RA and dedicated RA. Dedicated RA are set up and operated independently by customers that have signed contracts with the Company.

1.3.3 Subscribers

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

Certification entity	Subscriber
Natural person	Himself
Organization	Trustee of authorized organization
Equipment	Owner of equipment
Application software	Owner of application software

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

1.3.4 Relying Parties

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

certificate may be used for the following work after checking the validity of the certificate:

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

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

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

1.3.5 Other Participants

The PublicCA selects other authorities, which provide related trust services, such as attribute authority, time stamp authority (TSA), data archiving service and card management center as the collaborative partners, the related information shall be disclosed on the website and the collaboration mechanism and mutual rights and obligations shall be set down in the CPS to ensure the efficiency and reliability of PublicCA quality.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

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

Transport layer security (TLS) and secure socket layer (SSL) protocols, time stamping servers and dedicated servers can be used for

the transmission of equipment and application software certificates.

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

Assurance Level	Applicable Type of Certificates	Verification	Applicable Scope
Level 1	Natural person, organization, equipment or application software	Use e-mail methods to verify that the applicant can operate the e-mail account.	Use e-mail notification to verify that the applicant can operate 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 and transmit the message or the symmetric key to guarantee its confidentiality but it is not suitable for on-line transactions that require certification. For example,

			information encryption and signatures required for e-mails.
Level 2	Natural person, organization ,equipment or application software	Applicant does not need to apply in person at counter but must provide legal and proper documentation proving personal or organization identity. After the certificate registration checker cross checks the information provided by the applicant or the system automatically compares with a reliable database to make sure the applicant information is correct.	Suitable for use with information which may be tampered with but the network environment has no malicious tampering (data interception is possible but likelihood is not high). Not suitable for the signing of important documents (life essential and high value transaction documents). For example, information encryption and identity authentication for small value e-commerce transactions.
Level 3	Natural person, organization ,equipment or application software	Applicant needs to apply in person at counter. The certificate registration checker checks the accuracy of application information or uses assurance level 3 certificate signature approved by government public key infrastructure or ePKI to submit the application. The system automatically compares the applicant's information to verify its	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. Suitable for information encryption and identity

		accuracy.	authentication required for e-commerce transactions, e-government or financial transactions. Including (but not limited to) the following applications: e-bank electronic transactions, account transfer authorization, account notifications, applicant instruction services, Internet orders, Internet tax filing, on-line document approval, Internet identity authentication and TLS encryption channels and secure e-mails.

Regarding SSL certificates, the assurance level, authentication method, scope of usage, risk and consequences shall not only comply with the corresponding scope of usage in the table above but also the description below:

Assurance Level and Certificate Type	Authentication Method	Scope of Usage	Risk and Consequences
Level 2 DV SSL certificate	Follow CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates and assurance level 2 regulations to	Provides communication channel encryption (communication channel encryption refers to ‘faciliate encryption key	Suitable for use with protected network communications where risk and consequences of data breach is low. Includes non-cash

	authenticate remote domain names and webpage services.	exchange to achieve information transmission encryption between the subscriber's browser and website'). Suitable for use with protected network communications.	transaction or transactions where there is not much of a possibility of fraud or malicious access.
Level 3 OV SSL certificate	Follow CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates and assurance level 3 regulations to authenticate that the applicant can control which group is in possession of the remote domain name, webpage services and which organization owns the domain name.	Provides communication channel encryption and must authenticate which organization owns the domain name. Suitable for use with protected network communications.	Suitable for use with protected network communications where risk and consequences of data breach is moderate. Includes major cash or property transactions, fraud risk or involving the possibility of malicious access of personal information.
Level 3 IV SSL certificate	Follow CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates and assurance level 3 regulations to authenticate that the applicant can control which group	Provides communication channel encryption and must authenticate which natural person owns the domain name. Suitable for use with protected network communications.	Suitable for use with protected network communications where risk and consequences or data breach is moderate. Includes major cash and property transactions,

	is in possession of the remote domain name, webpage services and which natural person owns the domain name.		fraud risk or involving the possibility of malicious access of personal information.

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

1.4.2 Restricted Certificate Uses

Subscribers shall carefully select trustworthy computer environments and application systems before private key use to prevent loss of rights due to theft or misuse of private keys by malicious hardware or software.

Relying parties shall check if the certificate type, assurance level and key usage conforms to use requirements before the certificate is issued by the PublicCA.

Relying parties shall appropriately use the individual keys in accordance with the key usage recorded on the certificate stipulated in section 6.1.7 and correctly process the critical extension certificate attribute information listed in the certificate extension field.

1.4.3 Prohibited Certificate Uses

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

(1) Crime

(2) Control of military orders and war situations as well as nuclear,

biological and chemical weapons

(3) Operation of nuclear equipment

(4) Aviation flight and control systems

(5) Scope of prohibitions announced under the law

1.5 Policy Administration

1.5.1 Organization Administering the Document

Chunghwa Telecom Co., Ltd.

1.5.2 Contact Person

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

Phone: 0800080365

Address: Public Certification Authority of Chunghwa Telecom, Data Communication Building, No. 21, Hsin-Yi Road, Sec.1, Taipei City 10048, Taiwan, R.O.C.

E-mail: caservice@cht.com.tw

If there is any other contact information or changes to the contact information, please check the following website: http://publicCA.hinet.net

1.5.3 Person Determining CPS Suitability for the Policy

The PublicCA shall first check whether the CPS conforms to relevant CP regulations and then submit the CPS to the Policy

Management Committee for review and approval. After approval, the PublicCA shall officially use the CP established for this ePKI.

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

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

1.5.4 CPS Approval Procedure

The CPS is published by the PublicCA following approval by the MOEA, the competent authority of the Electronic Signatures Act.

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

1.6 Definitions and Acronyms

See Appendix 1 for a table of abbreviations and definitions and Appendix 2 for the glossary.

2. Publishing and Repository Responsibilities

2.1 Repository Responsibility

The repository, under the management of the PublicCA, publishes and stores the PublicCA issued certificates, certificate revocation lists (CRL) and the CPS and provides inquiry services to subscribers and relying parties. The repository provides 24-hour round-the-clock service. The Internet address of the PublicCA repository is: http://publicCA.hinet.net. The repository will resume normal operation within two working days if unable to operate normally for some reason.

The responsibility of the repository includes:

(1) Regularly publish issued certificates, and revoked certificates and CRL in accordance with section 2.2.
(2) Publish the latest CPS information.
(3) Access control of the repository shall comply with the provisions in Section 2.4.
(4) Publish external audit results.
(5) Guarantee the accessibility status and availability of the repository information.

2.2 Publication of PublicCA Information

(1) This CPS.
(2) CRLs.

(3) Certificates of the PublicCA (until the expiry of all certificates issued with private key corresponding to that certificate's public key).
(4) Issued certificates.
(5) Privacy protection policy.
(6) The latest PublicCA-related news.

2.3 Publishing Method and Frequency

(1) The CPS shall be published after approval by the competent authorities. CPS revisions shall be published in the repository in accordance with Chapter 2.
(2) CRLs are issued by the PublicCA at least twice a day and published in the repository.
(3) The PublicCA's own certificates are published in the repository after acceptance by an upper level eCA.

2.4 Access Controls

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

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

maintain accessibility and availability.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

The PublicCA uses the X.500 Distinguished Name (DN) for the certificate subject name of issued certificates.

3.1.2 Need for Names to be Meaningful

The certificate subject names of certificates issued by the PublicCA shall comply with our country's related subject naming rules. The names should be sufficient to represent the subject name.

The CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates shall be followed for the certificate subject name and subject alternate name in the SSL server software certificate. Internal names or reserved IP addresses shall not be used.

Fully qualified domain names (FQDN) shall be recorded as the common names and certificate subject name fields on the SSL server software certificate.

The DN for organization validation (OV) SSL server software certificate shall include the organization name field to verify the 3.2.2 organization identity information.

The DN for individual validation (IV) SSL server software

certificate shall include the surname and given name field to verify the 3.2.3 individual identity information.

Multiple fully qualified domain names controlled by the subscriber may be recorded on the certificate subject name field of a multi-domain SSL server certificate.

Wildcard characters (*) used in the wildcard SSL server certificate are placed at the farthest left position of the fully qualified domain names in the certificate subject name's common name field and subject alternative name field for use with all websites inside that sub-domain.

Multiple wildcard domains or and multiple fully qualified domain names may be recorded in the certificate subject alternative name field for content delivery network (CDN) SSL server software certificates.

3.1.3 Anonymity or Psuedonymity of Subscribers

The PublicCA does not currently issue anonymous or pseudonymous certificates to end subscribers.

3.1.4 Rules for Interpreting Name Forms

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

3.1.5 Uniqueness of Names

The PublicCA's X.500 Distinguished Name for first generation CA certificates is:

C=TW,

O=Chunghwa Telecom Co., Ltd.,

OU=Public Certification Authority

In favor of facilitate international interoperability, the PublicCA's X.500 distinguished name for second generation CA certificates uses the following format:

C=TW,

O=Chunghwa Telecom Co., Ltd.,

OU=Public Certification Authority - Gn

Where, n=2,3…

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

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

3.1.6 Recognition, Authentication and Role of Trademarks

The certificate subject name provided by subscribers must comply with relevant regulations in our country's Trademark Act and Fair Trade Act. The PublicCA shall not bear the responsibility for reviewing whether or not the certificate subject name provided by the subscriber complies with the above regulations. Related disputes and arbitration

shall not be the obligation of the PublicCA 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 the PublicCA and the subscriber should file a request with the relevant competent authorities or court.

If the identification name used by the subscriber is proven by relevant competent authorities 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 the PublicCA may revoke that subscriber's certificate.

3.2 Initial Registration

3.2.1 Method to Prove Possession of Private Key

The PublicCA shall verify that the private key is possessed by the individual. There are two ways to record the public key pair in the certificate.

(1) The RA generates key pairs on behalf of the subscriber, and the subscriber's public key pair is delivered by the RA to the PublicCA via secure channels during certification issuance. Therefore, it is not necessary to prove possession of the private key when the subscriber applies for a certificate.

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

3.2.2 Procedure for Authentication of Organization Identity

The identification required for organization identification and authentication, and the authentication and verification procedures which need to be performed at the counter are determined based on the assurance level and relevant regulations as shown in the Table below:

Assurance Level	Procedure for Authentication of Organization Identity
Level 1	(1) No written document checking. (2) Applicant only needs to have e-mail address to apply for certificate. (3) In-person application at counter is not required.
Level 2	(1) Written identification checking is not required. (2) Applicant submits organization information such as organization identity ID number (i.e. withholding tax ID number) and organization name. The PublicCA has the right to cross check the information against government supplied databases or registered information in a trusted third party's database to verify the applicant's identity.

Assurance Level	Procedure for Authentication of Organization Identity
	(3) In-person application at counter is not required.
Level 3	There are 3 types of organization identity authentication: (1) Private organization identity authentication The private organization must submit copies of the correct certification documents (such as company change registration form, legal person registration certificate) which have been approved by the competent authority or a legally authorized body (such as a court) to the RAO. The copies of the certification documents shall be affixed with the seal of the organization and responsible person (must match the seal used at the time of company registration). The RAO shall check the authenticity of the application information submitted by the organization and representative identity and verify 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, an agent may be appointed to submit the application at the counter of his/her behalf. The assurance level 3 regulations for authentication of the identity of representatives in Section 3.2.3 shall be followed. If the private organization has completed the

Assurance Level	Procedure for Authentication of Organization Identity
	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 the Company 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 the Company to the private organization) before certificate application, the CA or RA may allow submission of supporting information during certificate application in place of the above identification and authentication methods. The above mentioned civil 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 authentication The government agency or authority follows the above private organization identity authentication method or official public document to apply for the certificate. The CA or RA must verify that the agency or authority really

Assurance Level	Procedure for Authentication of Organization Identity
	exists and determine the authenticity of the official documents. (3) Chunghwa Telecom's organization unit's Identity authentication Organizations belonging to Chunghwa Telecom must apply for the certificate with official documents and the RA must check if the agency or authority really exists and determine the authenticity of the public documents. 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. When there is digital signature by a private key corresponding to an assurance level 3 organization certificate issued through the ePKI for the server software 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 equipment or application software application information is valid.

3.2.3 Procedure for Authentication of Individual Identity

There are different regulations regarding identification documents, checking procedure and whether in-person application at the counter is necessary for individual identity authentication at different assurance levels as shown in the Table below:

Assurance Level	Procedure for Authentication of Organization Identity
Level 1	(1) Written documentation checking is not required. (2) Applicant only needs to have e-mail address to apply for certificate. Identification and authentication procedure does not need to be performed. (3) In-person application at counter is not required.
Level 2	(1) Written documentation checking is not required. (2) Subscriber submits personal information including personal identification code (such as ID card number) and name. The PublicCA has the right to cross check the information against government supplied databases or registered information in a trusted third party's database to verify the applicant's identity. (3) In-person application at counter is not required
Level 3	(1) Check written documentation: The applicant shall provide information which includes name, ID number and birthdate and at least present at least one original approved photo ID (such

Assurance Level	Procedure for Authentication of Organization Identity
	as national ID card) during certificate application to the RAO to authenticate the applicant's identity. If an applicant (such as minor under 18 years old) is unable to submit the above photo ID, government issued written documentation (such as household registration) sufficient to prove the identity of the applicant and one adult with legal capacity to guarantee the applicant's identity in writing may be used in its place. The identity of the adult providing the written guarantee must pass through the above authentication. (2) Personal information submitted by the applicant such as personal identification code (ID card number), name and address (household registration address) shall be checked against the information registered with the competent authority (such as household registration information) or other information registered with a trusted third party recognized by the competent authority. (3) Counter application: The applicant must verify his / her identity in person 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

Assurance Level	Procedure for Authentication of Organization Identity
	authenticity of the letter of appointment (such as the subscriber's seal on the letter of appointment) and authenticate the identity of the agent in accordance with the above regulations. If an 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) Use of natural person certificate IC to apply 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 that the digital signature is valid. (5) Individual identity authentication for equipment or application software certificate applications In addition to the above four types of identity authentication procedures, the private key digital signature corresponding to an assurance level 3

Assurance Level	Procedure for Authentication of Organization Identity
	individual certificate issued through the ePKI made also be used for application. The applicant does not need to verify his/her identity in person at the counter but the RA system or RAO shall verify that the digital signature is valid. This type of certificate is especially suitable for small office, home office (SOHO) applications.

3.2.4 Non-Verified Subscriber Information

Whether the common name on assurance level 1 individual certificates is the legal name of the certificate applicant need not to be verified.

3.2.5 Validation of Authority

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

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

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

or other equivalent procedures.

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

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

(1) Use the organization registration initial review window to verify that the e-mail address filled out by the certificate applicant is personally owned by the certificate applicant.

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

(3) Use the organization's personnel database or LDAP service to obtain the correct e-mail account of the certificate subject.

For DV SSL application software certificate applications, the method suggested on the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates shall be used to select a single or a number of ways (see table below) to authenticate subscriber domain name control rights. For OV and IV SSL application certificate applications, except for validation of subscriber possession of domain name control rights by DV SSL application software certificate, the regulations in section 3.2.2 or 3.2.3 shall be

followed to authenticate organization or individual identity.

Item	Domain name control validation method
1	Directly check with the domain name registrar if the applicant is the domain name registrant.
2	Have the domain name registrar provide information such as address, telephone or e-mail address to directly contact and verify domain name registrant.
3	Use information listed by WHOIS service (such as “registrant”,“technical" and“administrative”fields) to contact and verify domain name registrant by e-mail or telephone. Or use domain name registrar to click on the activation link in the e-mail sent by the PublicCA and fill in the authentication code in the e-mail for complete verification.
4	Directly contact and verify using the prefix admin, administrator, webmaster, hostmaster or postmaster in the domain name as the e-mail account (for example, if the certificate application domain name is abc.com, send e-mails to admin@abc.com, administrator@abc.com, webmaster@abc.com, hostmaster@abc.com or postmaster@abc.com). Or the above recipient clicks on the activation link in the e-mail sent by the PublicCA and fills in the authentication code in the e-mail to complete verification.
5	For stipulated control changes in specific webpage content, certificate applicants show their actual control of qualified

domains, For example, the RA provides one basic webpage and asks the certificate technology contact person to place the fully qualified domain name to be registered for the SSL certificate application so it can be seen by the certificate RAO.

6 Provide letter of authorization to appoint an agent to apply for the SSL certificate. The identity authentication of the appointer and appointee shall be done in accordance with the regulations in sections 3.2.2 and 3.2.3.

7 Use of other verification methods. The Public CA or certificate RAO maintains written evidence to verify that the certificate applicant is the domain registrant or possesses the control rights to the domain name and has at least the same assurance level as the above methods.

3.3 Re-key Request Identification and Authentication

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 3.1.

3.3.1 Certificate Renewal Re-key

When the subscriber requests certificate renewal, the private key

pair is used to add the signature to the certificate application file. The certificate application file is submitted to the RA. The RA shall use that subscriber's public key to verify the digital signature on that certificate application to identify the subscriber identity. Expired, suspended and revoked certificates may not be renewed. The certificate may be renewed up until the subscriber public key usage time limit in section 6.3.2.2 at the latest to maintain key pair security.

3.3.2 Certificate Revocation Re-key

If the subscriber private key needs to be re-keyed due to certificate revocation, the subscriber shall reapply for the certificate with the PublicCA. The RA shall perform subscriber identification and authentication for the certificate reapplication in accordance with the regulations in section 3.2.

3.4 Identification and Authentication for Certificate Revocation Request

The PublicCA 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 regulations in section 3.2.

4. Certificate Lifecycle Operational Standards

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Organizations and individuals may submit certificate applications.

If it is a property class such as computer and communications equipment (router, firewall, database security audit software) or application software (web server, e-mail server or Lync service), the certificate applicant is the owner of the equipment or application software since property has no legal capacity to act.

4.1.2 Enrollment Process and Responsibilities

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

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

submitted for the application.

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

(3) After obtaining the certificate issued by the PublicCA, 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 the PublicCA 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 procedure is as follows:

(1) The certificate applicant fills out the information on the certification application and agrees to the subscriber terms and conditions.
(2) The certificate applicant sends the certificate application information and related certification information to the RA.
(3) If the certificate applicant self-generates the keys, a PKCS#10 Certificate signing request is created and signed with the private key. The certificate application file is submitted to the RA during the certificate application.

4.2.1 Performing Identification and Authentication Functions

The PublicCA 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 the regulations in section 3.2 of the CPS. The certificate applicant shall submit correct and complete factual information. The information required for the certificate application shall contain required and optional information. Only the information listed on the certificate profile is recorded on the certificate. The information submitted by the certificate applicant and contact records kept by the PublicCA and RA during the application process shall be properly kept in a secure, auditable manner in accordance with CP and CPS regulations.

Starting from January 1, 2016, the PublicCA checks the domain name system (DNS) and looks up the FQDN recorded on the SSL certification application case FQDN to determine if there is a certification authority authorization (CAA) DNS resource record. If the CAA DNS resource record exists and the PublicCA is not recorded as the authorized SSL certificate issuance CA, the PublicCA shall deem this certificate application as approval of authorization of the PublicCA for the SSL certificates issued by this domain and ask the subscriber to go to this domain name system to renew authorization of the CA to issue certificate DNS resource record for entry with the PublicCA.

4.2.2 Approval and Rejection of Certificate Applications

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

If the identity authentication work is not successfully completed, the PublicCA may reject the certificate application. Except for applicant identity identification and authentication reasons, the PublicCA and RAs may refuse to use the certificate for other reasons. The PublicCA and RAs may also reject certificate application from applicants who have previously been rejected or have previously violated the subscriber terms and conditions.

4.2.3 Time to Process Certificate Applications

The PublicCA and RAs shall complete the certificate application processing 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 the PublicCA to issue certificates depends on the certificate group and type. These times may be disclosed in the subscriber terms and conditions, contract or RA website.

Provided that OV SSL certificate and IV SSL certificate application cases are accepted and comply with related regulations, the RAO shall normally complete the review procedure within two working days. After the subscriber completes certificate acceptance, the PublicCA shall complete the certificate issuance work within one working day.

4.3 Certificate Issuance Procedure

4.3.1 CA Actions during Certificate Issuance

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

Certificate issuance steps are follows:

(1) The RA submits the certificate application information from the review process to the PublicCA.
(2) When the PublicCA receives the certificate application information submitted by the RA, the authorization status of the relevant RA is first checked, the authorized assurance level and scope is verified and then the certificate is issued based of the certificate application information submitted by the RA.
(3) If the RA authorized assurance level and scope does not

comply with the certificate application, the PublicCA sends back the related erroneous message to the RA and refuse to perform related subsequent work. If there are any questions, the RA may directly contact the PublicCA to understand where the problem is.

(4) In order to ensure the security, integrity and non-repudiability of the information transmitted by the PublicCA and RA, the certificate application information is encrypted with a digital signature and transmitted through the network by transport layer security (TLS) means.

(5) The PublicCA reserves the right to refuse certificate issuance to any entity. The Public CA shall not bear any liability for damages to certificate applicants.

4.3.2 Notification to Subscribers

After the PublicCA completes certificate issuance, the subscriber is notified to pick up the certificate or the RA is used to notify the subscriber to pick up the certificate.

If the PublicCA 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 Procedure

There are two types of certificate acceptance procedures for certificates issued by the PublicCA:

(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. For example, if a SSL server software certificate applicant finds the fully qualified domain on other required TLS encrypted channels have not been applied for registration when pre-reviewing the certificate subject name field on the issued SSL certificate, issuance of that SSL certificate may be refused. A new certificate application may be submitted in accordance with section 4.2.

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

The certificate field is reviewed by above certificate applicant before deciding whether or not to accept the certificate; the review shall at least include the certificate subject name. Before accepting the SSL server certificate, the certificate applicant must review the certificate subject name field. If the organization or individual e-mail address is submitted for secure e-mail use, the organization or

individual certificate applicant shall review e-mail address recorded in the certificate subject name field and submit consistent information for the application before certificate acceptance.

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

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

4.4.1 Circumstances Constituting Certificate Acceptance

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

4.4.2 Publication of the Certificate by the PublicCA

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

4.4.3 Notification by the PublicCA to Other Entities

Not stipulated

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers refer to the entities who request and obtain certificates approved by the PublicCA. Their relationship with the certificate subject is shown in the table in section 1.3.3 of the CPS. Usage of different assurance level certificates is stipulated in section 1.4.1 of the CPS. Subscriber key pair generation shall comply with the regulations in section 6.1.1 of the CPS. Subscribers must independently possess and control the right and capability to the private key corresponding to the certificate. Subscribers themselves do not issue certificates to others. Subscribers shall protect the private key from unauthorized use or disclosure. Private keys may only be used for correct key usages (key usages are recorded in the certificate's extension field) such as digital signatures and key encryption. Subscribers must correctly use certificates according to the CP listed on the certificate.

4.5.2 Relying Party 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, Internet Engineering Task Force (IETF) RFC, CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates related standards and specifications.

Relying parties shall verify the validity if 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 integrity of the electronic documents with digital signatures.

(2) Verify the identity of the document signature author.

(3) Establish secure communication channels with the subscriber.

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

For example, relying parties may only trust SSL/TLS handshakes that conform to the following conditions:

(1) Digital signature or SSL/TLS session is generated through the corresponding valid certificate and the certificate accuracy can be verified through the certificate chain.

(2) Related CRL or OCSP response messages are checked for certificate and unrevoked certificates used by relying parties.

(3) Certificates are used according their CPS regulations and certificate usage.

4.6 Certificate Renewal

4.6.1 Circumstances for Certificate Renewal

Unrevoked certificates which are about to expire may be renewed

under the following circumstances:

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

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

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

4.6.2 Who May Request Renewal

The original certificate subscriber subject or authorized representative whose certificates that are about to expired.

4.6.3 Certificate Renewal Procedure

The private key is used to add a signature to the Certificate Signing Request when the subscriber makes a certificate renewal request and the certificate application file is submitted to the RA. The RA uses the subscriber's public key to verify the digital signature on the certificate application file to authenticate the subscriber's identity.

4.6.4 Subscriber Instructions for Certificate Renewal

Expired, suspended, revoked certificates may not be renewed. The certificate may be renewed at the latest until the subscriber public key usage time limit in section 6.3.2.2 to maintain key pair security.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

After certificate applicant confirms that there are no errors in the information of the issued certificate, the certificate renewal is deemed as

being accepted.

4.6.6 Publication of the Renewal Certificate by the CA

The PublicCA repository service regularly publishes the issued renewal certificates or delivers the certificate to the certificate applicant after renewal to achieve certificate publication. The RA may negotiate with the PublicCA about certificate delivery by the RA to the certificate applicant.

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

Certificate RA may receive notification of renewal certificate issuance.

4.7 Certificate Re-Key

4.7.1 Circumstances for Certificate Re-Key

4.7.1.1 Circumstances for PublicCA Subordinate CA Certificate Re-Key

The PublicCA private key shall be routinely re-keyed in accordance with the regulations in section 6.3.2 so the new private key is used instead of the old private key to issue certificates. Notification shall be made at appropriate time to all entities that trust the PublicCA certificate authorities. The PublicCA shall issue subscriber certificates and CRLs with the new private key and the new certificates shall be published in the repository for subscriber download. The old private key shall still be

used to issue CRLs and on-line certificate status responses to maintain and protect all subscriber certificates issued with the old private key until their expiry.

The PublicCA shall re-key the key pairs used to issue certificates before the usage period of the certificate issued with the private key expires at the latest. After the key pair is re-keyed, the PublicCA shall apply for new certificates from the above level CA (ePKI Root Certification Authority (eCA)) in accordance with the regulations in section 4.2 of the eCA CPS. The eCA shall issue the new certificate and notify the PublicCA.

If the PublicCA's own certificate has been revoked and use of its private key has been suspended, the key pair must be re-keyed.

4.7.1.2 Circumstances for Subscriber Certificate Re-Key

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

For subscribers which hold assurance level 2, 3 and 4 certificates, if the certificate has not been revoked, the PublicCA or RA may start to process the re-key and new certificate application one month before the expiry of the subscriber private key usage period. The new certificate application procedures are implemented in accordance with the regulations in section 4.1 and 4.2.

After the subscriber certificate is revoked, its private key shall be suspended. After the key pair is re-keyed, a new certificate may be applied for with the CA or RA in accordance with the regulations in section 4.2.

4.7.2 Who May Request Certificate Re-Key

(1) The PublicCA may submit a subordinate CA application with the eCA.

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

4.7.3 Certificate Re-Key Procedure

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

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

4.7.4 Subscriber Certificate Re-Key Instructions

Subscriber private keys must be routinely re-keyed in accordance with the regulations in section 6.3.2.

After the subscriber certificate is revoked, its private key shall be suspended. After the key pair is re-keyed, a new certificate may be applied for with the CA or RA in accordance with the regulations in section 4.2.

For subscribers which hold assurance level 2, 3 and 4 certificates, if the certificate has not been revoked, the PublicCA or RA may start to process the re-key and new certificate application one month before the expiry of the subscriber private key usage period. The new certificate

application procedures are implemented in accordance with the regulations in section 4.1 and 4.2.

4.7.5 Circumstances Constituting Acceptance of Certificate Re-Key

For circumstances constituting acceptance of the CA certificate re-key by the PublicCA, see section 4.7.5 in the eCA CPS.

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

4.7.6 Publication of the Re-Key by the PublicCA

The PublicCA repository service regularly publishes the new certificates issued through certificate re-key or delivers the new certificate to the certificate applicant to achieve certificate re-key publication. The RA may negotiate with the PublicCA about certificate delivery by the RA to the certificate applicant.

4.7.7 Notification by the PublicCA to Other Entities

RA may receive notification of subscriber certificate re-key.

After the subscriber CA certificate is issued by the PublicCA, the PublicCA shall publish the subscriber CA certificate on the PublicCA website repository to facilitate notification of other entities.

4.8 Certificate Modification

4.8.1 Circumstances for Certificate Modification

Certificate modifications are some differences between the authentication information in one new certificate and an old certificate (for example a new e-mail address or other relatively unimportant attribute information) from the same certificate subject which conforms to relevant regulations in the CP and CPS. The new certificate may have a new certificate subject public key or use the original subject public key but the certificate expiry date and the original certificate expiry date are the same. After the certificate is modified, the old certificate shall be revoked.

If there are any changes to 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. The procedures in section 4.1 and 4.2 shall be followed to process the certificate application.

4.8.2 Who May Request Certificate Modification

Subscribers, RAs or legally authorized third parties (such as agents authorized by the organization and legal heirs of the natural person).

4.8.3 Certificate Modification Procedure

(1) The certificate modification applicant shall submit the certificate modification request in accordance with the guidelines

established by the RA. After the RA receives the certificate modification request the review procedure is followed and all the changes in the new certificate application request and the original certificate revocation request are kept for recordkeeping including the applicant name, contact information reason for the new certificate application, reason for the original certificate revocation and the time and date of the original certificate revocation to serve a basis for subsequent accountability. See sections 4.2 and 4.9 for the guidelines established by the RA. For example, if the certificate modification applicant is asked to add a signature to the certificate application file corresponding to its private key and submit the certificate application file to the RA, the RA shall verify the digital signature on that certificate application file with the subscriber's public key to authenticate the subscriber's identity.

(2) After the RA completes the review work, the new certificate application and the original certificate revocation request is sent to the PublicCA.

(3) When the PublicCA receives the new certificate application and the original certificate revocation request information, the PublicCA first checks the authorization status of the relevant RA to verify that its authorized assurance level and scope. Afterward, the certificate is used based on the new certificate application sent by the RA. Then, the certificate corresponding to the original certificate revocation request sent by the RA is revoked.

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

(5) In order to ensure the security, integrity and non-repudiability of the information transmitted by the PublicCA and RA, the certificate application information is affixed with a digital signature, encrypted and transmitted through the network by transport layer security (TLS) means.

(6) The RA shall set the time interval between the certificate modification new certificate application and original certificate revocation. For example, after the modified certificate issuance is completed and the subscriber uses the new certificate without error, the original certificate shall be revoked within two weeks after the new certificate is validated.

4.8.4 Instructions for Certificate Modifications Made by Subscribers

If the subscriber finds their information is incorrect as the certificate modification is accepted or inconsistent information is submitted during the application process, the subscriber shall promptly notify the RA. Otherwise, it shall be deemed that the subscriber consents to abide by the rights and obligations in the CPS and related contracts.

4.8.5 Circumstances Constituting Acceptance of Certificate Modification

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

4.8.6 Publication of Certification Modification by the PublicCA

The PublicCA repository service regularly publishes the new certificates issued through certificate modification or delivers the new certificate to the certificate applicant to achieve certificate modification publication. The RA may negotiate with the PublicCA about certificate delivery by the RA to the certificate applicant.

4.8.7 Notification by the PublicCA to Other Entities

Not stipulated

4.9 Certificate Suspension and Termination

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

4.9.1 Circumstances for Certificate Revocation

The certificate subscriber shall submit a certificate revocation

request application under (but not limited to) any of the following circumstances:

(1) Private key lost, stolen, modified, disclosed without authorization or has been subject to other damage or misuse.
(2) The information listed on the certificate is sufficient to have a significant effect on subscriber trust.
(3) Certificate is no longer needed for use.

In addition, the PublicCA must notify the subscriber in advance of certificate revocation under the following circumstances.

(4) Some items listed on the certificate known to be untrue.

(5) Known misuse, counterfeiting or compromise of the certificate subscriber's signature private key.

(6) Known PublicCA private key or information system misuse, counterfeiting or compromise which affects the reliability of the certificate.

(7) Known failure to issue the certificate in accordance with CPS regulations and procedures.

(8) Subscriber violation or inability to follow the regulations or obligations in the CPS or any other contracts and relevant laws.

(9) Notification by judicial or prosecution authority or in accordance with related legal regulations.

When the PublicCA terminates its service, if there is no CA to take over the PublicCA service, the competent authorities shall be notified to arrange for other CA to take over the service. If still no other CA can take over the service, the PublicCA shall publish the revoked certificates in the repository and notify all certificate-related persons 30 days prior to service termination.

4.9.2 Who Can Request Certificate Revocation

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

4.9.3 Certificate Revocation Procedure

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

(2) After the RA completes the review work, the certificate revocation application information is sent to the PublicCA.

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

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

(5) In order to ensure the security, integrity and non-repudiability of

the information transmitted by the PublicCA and RA, the certificate application information is affixed with a digital signature, encrypted and transmitted through the network by transport layer security (TLS) means.

4.9.4 Certificate 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 the PublicCA within one hour. When the subscriber's private key is lost or suspect or known to be compromised or the information recorded on 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. The PublicCA may extend the certificate revocation grace period when deemed necessary.

4.9.5 Time Period for the CA to Process Certificate Revocation Requests

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

4.9.6 Certificate Revocation Checking Requirements for Relying Parties

Before using a certificate issued by the PublicCA, the relying

parties shall first check the CRL or on-line certificate inquiry status published by the PublicCA to verify the validity of that certificate.

The PublicCA publishes suspended and revoked certification information on the repository for checking purposes. There are no restrictions for the checking of CRL by relying parties. The website is as follows:

http://publicca.hinet.net

4.9.7 CRL Issuance Frequency

The CRL issuance frequency of the PublicCA is at least twice per day. Issued CRL are valid for no more than 36 hours. Before the CRL expires, the PublicCA 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 PublicCA repository to receive the updated certificate revocation information.

4.9.8 Maximum Latency for CRL Publishing

The PublicCA shall publish the CRL at the latest before the nextUpdate listed on the CRL.

4.9.9 OCSP Service

When the OCSP service is used by relying parties, the relying parties shall examine the digital signature on the related inquiry result information to verify the integrity of the information source.

The PublicCA supports OCSP stapling operation to complete the real time on-line SSL certificate status checking work in order to speed up high traffic website SSL certificate validation.

4.9.10 On-Line Certificate Status Inquiry Rules

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

According to CA/Browser Forum guidelines, the SHA-1 Hash Function Algorithm can still be used to issue and verify OCSP response message certificates until December 31, 2016. The signature private keys corresponding to PublicCA's SHA-1 CA certificates use SHA-1 Hash Algorithm to issue and verify OCSP response message certificates. The issuance and verification of OCSP response message certificate will be switched to the use of SHA 256 Hash Algorithm by December 31, 2016 at the latest. The signature private key corresponding to PublicCA second generation SHA 256 CA certificates shall use the SHA 256 Hash Algorithm to issue and verify the OCSP response message certificate.

4.9.11 Other Forms of Revocation Advertising

No other forms of revocation advertising are currently provided.

4.9.12 Other Special Requirements during Key Compromise

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

4.9.13 Circumstances for Certificate Suspension

Subscribers may apply for certificate suspension under the following two circumstances:

(1) Suspected theft of certificate key pair.

(2) Independently determine that is necessary to apply for certificate suspension.

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

(1) The subscriber is ordered to suspend operations.

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

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

4.9.14 Who Can Request Certificate Suspension

The following two groups may apply for certificate suspension:

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

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

4.9.15 Procedure for Certificate Suspension

Subscribers submit the request. After the RA examines the application for accuracy and errors, a digital signature is affixed and the information is transmitted to the PublicCA. The PublicCA then immediately suspends the certificate. If the above suspension request does not pass review, the PublicCA shall refuse the certificate suspension request.

4.9.16 Processing and Suspension Period for Suspended Certificates

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

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

If the subscriber cancels the certificate suspension during the certificate suspension period, certificate use is resumed and the certificate recovers its validity.

4.9.17 Procedure for Certificate Resumption

The subscriber submits the request. After the RA examines the application for accuracy and errors, a digital signature is affixed and the information is transmitted to the PublicCA. The PublicCA then immediately resumes use of the certificate. If the above resumption request does not pass review, the PublicCA shall refuse the certificate resumption request.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The PublicCA submits the CRL and provides OCSP service at the

CRL distribution point recorded on the subscriber certificate.

4.10.2 Service Availability

The PublicCA shall provide 24x7 uninterrupted certificate status services.

4.10.3 Available Functions

Not stipulated.

4.11 Service Termination

Service termination refers to the termination of PublicCA services to certificate subscribers including termination of PublicCA services provided to subscribers upon certification expiry or service termination upon subscriber certification revocation.

The CA shall allow the subscriber not to renew or cancel the purchase of certificate services in the event of invalidation of the subscriber agreement terms and conditions.

4.12 Private Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

Private keys used for signatures may not be escrowed.

4.12.2 Session Key Encapsulation and Recovery Policy and Practice

The PublicCA does not currently support session key encapsulation

and recovery.

5. Physical, Procedural and Personnel Security Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

The PublicCA 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 PublicCA equipment.

5.1.2 Physical Access

The PublicCA has established suitable measures to control connections to PublicCA service hardware, software and hardware cryptographic module.

The PublicCA 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 PublicCA system.

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

The following checks and records need to be made when PublicCA 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 Electrical Power and Air Conditioning

In addition to municipal power, the power system at the PublicCA 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 PublicCA facility has a constant temperature and humidity system to provide an optimal operation environment for the facility.

5.1.4 Flood Prevention and Protection

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

5.1.8 Off-site Backup

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

5.2 Procedural Controls

In order to ensure that system procedures have a suitable assurance level, the PublicCA uses procedural controls to specify the trusted roles of PublicCA 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 PublicCA 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 five PKI personnel roles assigned by the PublicCA are administrator, officer, auditor, operator and controller to prevent 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 five roles are as follows:

The administrator is responsible for:

- Installation, configuration and maintenance of the PublicCA system.

- Creation and maintenance of system user accounts.
- Generation and backup of PublicCA keys.

The officer is responsible for:

- Activation / suspension of certificate issuance services.
- Activation / suspension of certificate revocation services.

The auditor is responsible for:

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

The operator is responsible for:

- Daily operation and maintenance of system equipment.
- System backup and recovery.
- Storage media updating.
- System hardware and software updates.
- Network and website maintenance: Set up system for security, virus protection system and network security event detection and reporting.

The controller is responsible for:

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

5.2.2 Role Assignment

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

- ■Only one person may assume the role of administrator, officer and auditor but the person may also assume the role of operator.
- ■The controller may not concurrently assume any of the other four roles.
- ■A person serving a trusted role is not allowed to perform self-audits.

5.2.3 Number of Persons Required Per Task

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

- ■ Administrator

At least 3 qualified individuals are needed.

- ■ Officer

At least 2 qualified individuals are needed.

- ■ Auditor

At least 2 qualified individuals are needed.

- ■ Operator

At least 2 qualified individuals are needed.

■ Controller

At least 2 qualified individuals are needed.

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

Assignments	Administrator	Officer	Auditor	Operator	Controller
Installation, configuration, and maintenance of the PublicCA system	2				1
Establishment and maintenance of system user accounts	2				1
Generation and backup of PublicCA keys	2		1		1
Activation / suspension of certificate issuance services		2			1
Activation / suspension of certificate revocation services		2			1
Checking, maintenance and archiving of audit logs			1		1
Daily operation and maintenance of system equipment				1	1
System backup and recovery				1	1
Storage media updating				1	1
Hardware and software updates outside the PublicCA certificate management system				1	1
Network and website maintenance				1	1

5.2.4 Identification and Authentication for each Role

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

Operating system account management by the PublicCA host uses login account numbers, password and groups to identify and authenticate administrator, officer, auditor and operator roles.

5.3 Personnel Controls

5.3.1 Background, Qualifications, Experience and Security Clearance Requirements

1. Security evaluation for personnel selection

   Personnel selection includes the following items:

   (1) Personality evaluation

   (2) Applicant experience evaluation

   (3) Academic and professional skills and qualifications evaluation

   (4) Personal identity check.

   (5) Trustworthiness.

2. Management of Personnel Evaluation

   All PublicCA personnel performing certificate work shall have their qualifications reviewed at the initial time of employment to

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

3. Appointment, Dismissal and Transfer

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

4. Duty of Confidentiality Agreement

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

5.3.2 Background Check Procedures

The PublicCA 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

Trusted Role	Training Requirements
Administrator	1. PublicCA security principles and mechanism. 2. Installation, configuration, and maintenance of the PublicCA operation procedures. 3. Establishment and maintenance of system user accounts operation procedures. 4. Audit parameter configuration setting procedures. 5. PublicCA key generation and backup operation procedures. 6. Disaster recovery and continuous operation procedure.
Officer	1. PublicCA security principles and mechanism. 2. PublicCA system software and hardware use and operation procedures 3. Certification issuance operation procedure. 4. Certification revocation operation procedure. 5. Disaster recovery and continuous operation procedure.
Auditor	1. PublicCA security principles and mechanism. 2. PublicCA system software and hardware use and operation procedures 3. PublicCA key generation and backup operation procedures. 4. Audit log check, upkeep and archiving procedures. 5. Disaster recovery and continuous operation procedure.
Operator	1. Daily operation and maintenance procedures for system equipment. 2. System backup and recovery procedure 3. Upgrading of storage media procedure. 4. Disaster recovery and continuous operation procedure. 5. Network and website maintenance procedure.
Controller	1. Physical access authorization setting procedure. 2. Disaster recovery and continuous operation procedure.

5.3.4 Retraining Requirements and Frequency

All related personnel at the PublicCA shall be familiar with any changes to PublicCA 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 trust roles. May not receive work reassignments.

2. Operators with the requisite training and clearance may be reassigned to the position of administrator, officer or auditor after two years.

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

5.3.6 Sanctions for Unauthorized Actions

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

5.3.7 Contract Employee Requirements

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

5.3.8 Documents Supplied to Personnel

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

5.4 Security Audit Procedure

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

5.4.1 Types of Audited Events

(1) Key generation

- PublicCA key generation times (not mandated for single use or single session keys)

(2) Private key loading and storage

- Loading the private key into a system component
- All access to private keys kept by the PublicCA 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 Audit File Processing Frequency

The PublicCA 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.

The PublicCA shall check the audit logs once every two months.

5.4.3 Retention Period for Audit Logs

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 Files

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) The PublicCA shall routinely archive event logs.

(2) The PublicCA shall store the event logs in a secure protected site.

5.4.6 Security Audit System

Audit logs shall be kept on all PublicCA 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

Starting from January 2015, PublicCA certificate RAs shall conduct a vulnerability scan at least once each year and take remedy measures.

Starting from July 2014, the PublicCA shall follow the methods and frequency stipulated in the AICPA/CPA WebTrust $^{SM/TM}$ for

Certification Authorities Trust Services Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.0 and CA/Browser Forum NETWORK AND CERTIFICATE SYSTEM SECURITY REQUIREMENTS Version 1.0 to perform vulnerability assessments at least once per quarter. Penetration testing shall be conducted at least once per year. The PublicCA also must conduct penetration testing after it is determined that there is a significant upgrade or modification to the application program or infrastructure. The PublicCA shall record the skills and tools and follow ethics, competitive relations and independence guidelines for those personnel or groups capable of implementing reliable vulnerability scanning, penetration testing, information security diagnosis or security surveillance.

5.5 Records Archival

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

(1) Important tracking records regarding the PublicCA'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 Recorded Events

The PublicCA retains the following information in its archives:

(1) PublicCA 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) PublicCA re-key records
(11) Issued or announced CRLs
(12) Audit logs
(13) Used to verify and validate the content of files and other information or application programs
(14) Audit personnel requirement documents

5.5.2 Retention Period for Archive

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

5.5.3 Protection of Archive

(1) Amendments, modifications and deletion of archived information not allowed by any user.
(2) Transfer of archived information to another storage media

which has passed through the PublicCA authorization procedure.

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

5.5.4 Archive Backup Procedures

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

5.5.5 Requirements for Record Timestamping

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

5.5.6 Archive Information Collection System

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 on written

documents must be verified.

5.6 Key Changeover

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

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

5.7 Key Compromise and Disaster Recovery Procedures

5.7.1 Emergency and System Compromise Handling Procedures

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

5.7.2 Computing Resources, Software and Data Corruption Recovery Procedure

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

If the Public CA’s computer equipment is damaged or unable to

operate, but the PublicCA signature key has not been destroyed, priority shall be given to restoring operation of the PublicCA repository and quickly reestablishing certificate issuance and management capabilities.

5.7.3 PublicCA Signature Key Compromise Recovery Procedure

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

(1) Publish in the repository, notify subscribers and relying parties
(2) Revoke the PublicCA signature key certificate and issued subscriber certificates.
(3) Generate new key pairs in accordance with the procedures in section 5.6. New certificates are published in the repository for subscriber and relying party downloading.

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

5.7.4 PublicCA Security Facilities Disaster Recovery Procedure

The PublicCA 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 PublicCA repository operations and quickly reestablishing certificate issuance and management capabilities.

5.7.5 PublicCA Signature Key Certificate Revocation Recovery Procedure

Revoked PublicCA signature key certificates shall be published in

the repository and relying parties shall be notified. New key pairs shall be generated in accordance with section 5.6. New certificates shall be published in the repository for subscriber and relying parties downloading.

The PublicCA shall conduct at least one PublicCA signature key certificate revocation drill each year.

5.8 PublicCA Service Termination

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

(1) The PublicCA shall notify the competent authority (MOEA) and subscribers of the service termination 30 days in advance.
(2) The PublicCA 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 PublicCA service, a

report shall be submitted to the competent authority to arrange for other CA to take over this service.

- If the competent authority arranges for other CA to take over the service but no other CA takes over the service, the PublicCA shall revoke the still valid certificates, publish the revoked certificates in the repository and notify all certificate-related persons 30 days prior to service termination. The PublicCA shall refund the certificate issuance and renewal fees based on the certificate validity.

- The competent authorities, if necessary, may publish the certificates which are still valid at the time of revocation.

6. Technical Security Controls

This chapter describes the technical security controls implemented by the PublicCA.

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The PublicCA and subscribers generate pseudo random numbers, public keys and key pairs within the hardware secure module in accordance with the regulations in section 6.2.1.

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

PublicCA key generation is witnessed by related personnel.

6.1.1.1 Subscriber Key Pair Generation

Key pairs are generated by the PublicCA or subscribers themselves.

6.1.2 Private Keys Delivery to Subscriber

If the RA generates a key for a subscriber, the RAO delivers the token (such as IC card) containing the subscriber key to the subscriber after the certificate is issued by the RA.

6.1.3 Delivery of Subscriber Public Keys to the CA

If the RA generates a key for a subscriber, the RA shall deliver the subscriber public key to the CA via secure channels.

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

Secure channels referred in this Chapter are the use of transport layer security (TLS) or other equivalent or higher level data encryption transmission methods.

6.1.4 CA Public Keys Delivery to Relying Parties

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

6.1.5 Key Sizes

The PublicCA uses 2048 bit RSA keys and SHA-1 / SHA 256 hash function algorithms to issue certificates.

Subscribers must use at least 1024 bit RSA keys or other key types of equivalent security strength on and before December 31, 2013.

Subscribers must use at least 2048 bit RSA keys or other key types

of equivalent security strength on and before December 31, 2030.

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

6.1.6 Public Key Parameters Generation and Quality Checking

The public key parameter of the RSA algorithm is null.

The PublicCA 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 cryptographic modules but this does not guarantee that this prime number is a strong prime.

6.1.7 Key Usage Purposes

The Public CA's signature private key is used to issue certificates and CRLs. The Public CA's own public key certificate is issued by the eCA. The key usage bits used for the certificate's usage extension field setting are keyCertSign and cRLSign.

When the tokens used by subscribers are IC cards and card reader function USB tokens, the subscriber certificate contains two key pairs for signature and encryption.

When the tokens used by subscribers are non-IC cards or non-USB tokens, the subscriber certificate contains one key pair for signature and encryption.

The key usages for server application software certificate are signature and decryption. When necessary, the certificate shall

concurrently contain two key usages for signature and encryption.

6.2 Private Key Protection and Cryptographic ModuleEngineering Controls

6.2.1 Cryptographic Module Standards and Controls

The PublicCA uses hardware cryptographic modules that pass FIPS 140-2 Level 3 certification requirements.

Storage media for subscriber key pairs comply with ISO 7816 IC card or other carriers.

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

For security controls of PublicCA private key backup splitting, m-out-of-n key splitting method is used for PublicCA backup and recovery.

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

6.2.3 Private Key Escrow

The Public CA's signature private key is not escrowed. The PublicCA shall not be responsible for the safekeeping of subscriber private keys.

6.2.4 Private Key Backup

Backups of PublicCA private keys are made according to the key

splitting multi-person control methods in section 6.2.2 and IC cards verified with FIPS 140-2 Level 2 or above standards may serve as the private key splitting storage media.

6.2.5 Private Key Archival

PublicCA signature private keys are not archived but archiving of public key is done by certificate information methods in accordance with section 5.5.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

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

(1) Key generation or cryptographic module replacement.

(2) For key splitting backup recovery, the secret splitting (*m*-out-of-*n* control) method is used in the circumstance to recover the PublicCA private key. Once the private key secret splitting IC card is recovered, the complete private key is written into the hardware cryptographic module.

(3) When the cryptographic module is replaced, encryption is used for the private key importation method to ensure that key plain code is not exposed outside the cryptographic module during the importation process and the related confidential parameters generated during the importation process are completely destroyed after the private key importation is completed.

6.2.7 Private Key Storage on Cryptographic Modules

Follow the regulations in sections 6.1.1 and 6.2.1.

6.2.8 Method of Activating Private Key

PublicCA private key activation is controlled by multi-person control of the different usage IC cards kept by administrator and officer.

No other regulations have been established for subscriber private key activation methods.

6.2.9 Method of Deactivating Private Key

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

The PublicCA does not provide subscriber private key deactivation service.

6.2.10 Method of Destroying Private Key

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

In addition to destroying the old PublicCA private key in the hardware cryptographic module, physical destruction of the backup secretly held IC card for the secret key is done during the PublicCA key renewal.

If services are permanently not provided for one key stored in the module but it is still accessible, all private keys (already used or

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

If services are permanent not provided for one key stored in the cryptographic module, all private keys used by that secure module are erased from its security module.

No other regulations have been established for subscriber private key destruction methods.

6.3 Other Aspects of Key Pair Management

Subscribers must self-administer key pairs. The PublicCA is not responsible for safeguarding subscriber private keys.

6.3.1 Public Key Archival

The PublicCA 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 Period

6.3.2.1 PublicCA Public and Private Key Usage Periods

The RSA key size for PublicCA public and private keys is 2048 bits. The maximum usage period for private and public keys is 20 years. The maximum usage period for certificates issued with private keys in 10 years but issued CRLs, OCSP service server certificates and OCSP

service reply message usage are not subject to these restrictions.

6.3.2.2 Subscriber Public and Private Key Usage Periods

The key size for PublicCA public and private keys is RSA 2048 bit. The use period for private keys is 10 years. The maximum validity period for public keys is 10 years.

According to section 6.3.2 of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, the maximum validity period of SSL certificates may not exceed 39 months.

The old RSA 1024 bit certificates, except where the risk is borne individually by the Chinatrust Group, may be used until the expiration of their validity period. The remaining various RSA1024 bit certificates including SSL certificates were all revoked prior to December 31, 2013.

6.3.2.3 SHA-1 Hash Function Algorithm Validity Period

According the international cryptography security assessment and the CA/Browser Forum's Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates regulations, CAs will no longer use the SHA-1 Hash Function Algorithm to issue any new subscriber certificates or subordinate CA certificates starting from January 1, 2016. CA can still use the SHA-1 Hash Function Algorithm to issue OCSP response message certificates (use SHA-1 Hash Function Algorithm to issue OSCP server certificate) until January 1, 2017. CA can continue to use currently existing SHA-1 root CA certificates or cross certificates. SHA-2 SSL certificates shall not be issued with the corresponding signature private keys of the SHA-1 subordinate CA certificate. Starting from January 16, 2015, CA should not use SHA-1

Hash Function Algorithm to issue SSL or code signing certificates with a certificate expiry date later than January 1, 2017 because the application software providers are in the process of disapproving and / or removing the SHA-1 Hash Function Algorithm from software. The risk of continued use of SHA-1 certificates negotiated between the CA and subscribers shall be borne separately.

The PublicCA shall adopt related measures such as advance generation of PublicCA second generation key pairs to apply for RSA 2048 w/SHA 256 certificates from the eCA. Regarding SSL certificates held by subscribers beyond the January 1, 2017 expiry date, after notifying the subscriber of the SHA-1 certificate phase out policy and the support level of the SHA 256 hash function algorithm of various application software, replacement issue of RSA 2048 w/SHA 256 SSL certificates is provided to ensure that the subscriber selects appropriate application software and phases out the RSA 2048 w/SHA-1 SSL certificates. The accompanying measures for other types of certificates shall be posted on the PublicCA website.

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 m-out-of-n control IC cards. The activation data obtained from the IC card must be input as the IC card personal identification number (PIN).

6.4.2 Activation Data Protection

Activation data is protected by the m-out-of-n control IC card.

Administrators are responsible for remembering the IC card PIN. The PIN may not be stored in any media. During IC card handover, a new PIN is set by the new administrator.

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

6.4.3 Other Aspects of Activation Data

The PublicCA private key activation data is not archived.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

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

(1) Trusted role or identity authentication login.
(2) Provide discretionary access control.
(3) Provide security audit capability.
(4) Access control restrictions for certificate services and PKI trusted roles.

6.5.2 Computer Security Rating

PublicCA servers use Common Criteria EAL 4 certified computer operating systems.

6.6 Lifecycle Technical Controls

6.6.1 System Development Controls

Quality control for PublicCA system development complies with CMMI standards.

RA hardware and software must be checked for malicious code during initial use and regularly scanned.

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

The system developer shall exercise the due care of a good administrator and sign a security warranty guaranteeing there are no back doors or malicious programs and provide a product or program handover list, testing report and system management manuals to the PublicCA as well as conduct program version controls.

6.6.2 Security Management Controls

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

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

The PublicCA records and controls system configurations and any modification or function upgrades as well as detect unauthorized modifications to system software and configurations.

The PublicCA shall reference the methodologies and standards in ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, ISO/IEC 31000 and

AICPA/CPA Trust Service Principles and Criteria for Certification Authorities and CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates and CA/Browser Forum 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 PublicCA servers and repository have firewalls and are connected to external networks. The repository is placed on the outside service area (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 PublicCA have digital signature protection and are manually delivered from the PublicCA server to the repository.

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

Private Key control activities not belonging to the PublicCA are allowed to activate mechanisms such as the SSL VPN to perform problem detection and troubleshooting in emergency situations. The use of SSL VPN is automatically recorded in the audit service and internal audit

personnel are responsible for the review of the SSL VPN audit records in accordance with the regulations in section 6.6.2.

6.8 Time Stamping

The PublicCA 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) Certificate issuance times.

(2) Certificate revocation times.

(3) CRL issuance times.

(4) System event occurrence times.

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

7. Certificate, CRL and OCSP Service Profiles

7.1 Certificate Profile

The certificates issued by the PublicCA conform to the current version of the ITU-T X.509, CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, IETF PKIX Working Group RFC 5280 and other regulations.

7.1.1 Version Number(s)

The PublicCA issues X.509 V3 version certificates.

7.1.2 Certificate Extensions

The certificate extensions of the certificates issued by the PublicCA conform to the current versions of the ITU-T X.509, CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, PKIX Working Group RFC 5280 or other regulations.

7.1.3 Algorithm Object Identifiers

The algorithm OIDs used for signatures on PublicCA issued certificates are:

sha-1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}

(OID：1.2.840.113549.1.1.5)：

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

(OID：1.2.840.113549.1.1.11)

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

(OID：1.2.840.113549.1.1.12)

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

(OID：1.2.840.113549.1.1.13)

The algorithm OID used during PublicCA issued certificate generation of subject keys are:

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

(OID:1.2.840.113549.1.1.1)

7.1.4 Name Forms

The subject and issuer fields of the certificate must use the X.500 distinguished name and the name attribute type shall comply with the current version of the ITU-T X.509, CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates and IETF PKIX Working Group RFC 5280 or other regulations.

7.1.5 Name Constraints

Name constraints are not used.

7.1.6 Certificate Policy Object Identifier

The ePKI certificate policy object identifier is used for the

certificate policy object identifier on PublicCA issued certificates.

The CA/Browser Forum subject-identity-validated OID (2.23.140.1.2.2) is used as the certificate policy object identifiers for PublicCA issued organization authentication SSL certificates.

The CA/Browser Forum domain-validated OID(2.23.140.1.2.1) is used as the certificate policy object identifiers for PublicCA issued domain authentication SSL certificates.

The CA/Browser Forum individual-validated OID(2.23.140.1.2.3) is used as the certificate policy object identifiers for PublicCA issued individual validated SSL certificates.

7.1.7 Usage of Policy Constraints Extension

PublicCA issued certificates do not contain policy constraints extension.

7.1.8 Policy Qualifiers Syntax and Semantics

PublicCA issued certificates do not contain policy qualifiers.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

The certificate policy extensions contained in PublicCA issued certificates are not recorded as critical extensions.

7.2 CRL Profile

7.2.1 Version Number(s)

The PublicCA issues ITU-T X.509 v2 version CRLs.

7.2.2 CRL Extensions

PublicCA issued CRL conforms with the current version of the ITU-T X.509, CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, IETF PKIX Working Group RFC 5280 or other related regulations.

7.3 OCSP Service Profile

The PublicCA provides OCSP services complies with IETF PKIX Working Group RFC 2560 and RFC 5019 standards and the PublicCA OCSP service website is contained in the Authority Info Access (AIA) extension.

7.3.1 Version Number(s)

The OCSP query packets from the PublicCA OCSP service include the following information:

- Version number
- Target certificate identifier

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

PublicCA OCSP service response packets contain the following basic fields:

Field	Description
Version number	v.1 (0x0)
OCSP server ID (Responder ID)	OCSP server subject DN)
Produced Time	Response packet sign time

Target certificate identifier	Includes: Hash algorithm, certificate issuer name, certificate issuer key and certificate number of target certificate
Certificate Status	Certificate status code (0: valid /1: revoked /2: unknown)
ThisUpdate/NextUpdate	Recommended validity region for this response packet includes: ThisUpdate and NextUpdate
Signature Algorithm	Response packet signature algorithm, can be sha256WithRSAEncryption or sha1WithRSAEncryption
Signature	OCSP server signature
Certificates	OCSP server certificate

7.3.2 OCSP Service Extensions

The OCSP response packet for PublicCA OCSP service includes the following extensions:

- OCSP server authority key identifier

If the OCSP query packet contains a nonce field, the OCSP response packet also must contain the same nonce field.

8. Compliance Audit Methods

8.1 Frequency of Audits

The PublicCA received one annual external audit and one non-routine internal audit with an audit period of no more than 12 months to ensure that PublicCA operations are in compliance with the security regulations and procedures in the CP and CPS. The standards used for the audit are Trust Service Principles and Criteria for Certification Authorities and WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security. The latter is mainly for SSL certificate issuance.

8.2 Identity / Qualifications of Audit Personnel

The Company shall retain an auditor to perform the PublicCA compliance audit work who is familiar with PublicCA operations and has been authorized by AICPA/CPA as a licensed WebTrust practitioner to perform Trust Services Principles and Criteria for Certification Authorities and WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security to provide fair and impartial audit services. Audit personnel shall be a qualified and authorized Certified Information Systems Auditor (CISA) or have equivalent qualifications and shall at least possess the experience of conducting a WebTrust for CA signature audit twice at 4 man-days or

the experience of conducting a CA information security management audit twice at 8 man-days. The PublicCA shall conduct identity identification of audit personnel during audits.

8.3 Audit Personnel Relationship to the Audited Party

The Company shall retain an impartial third party to conduct audits of PublicCA operations.

8.4 Scope of Audit

The scope of audit is stipulated as follows:

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

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

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

If it is a RA responsible for the review of assurance level 1 and 2 certificate applications and revocation requests, the RA shall undergo one external audit every two years noting any CP / CPS non-compliance or exceptions and the actions taken to correct the deficiencies.

If it is a RA responsible for review of assurance level 3 certificate applications and revocation requests, the RA shall undergo one external

audit every year noting any CP / CPS non-compliance or exceptions and the actions taken to correct the deficiencies.

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

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

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

(2) If the compliance audit has not been completed or there are special developments, the Company 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, the Company must conduct the related review or examination.

The Company 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 the Company and the

personnel conducting the audit and examination.

Audit personnel shall conduct at least one continuous internal audit of the SSL certificate RA and on at least a quarterly basis against a randomly selected sample of the greater of one certificate or at least three percent of the certificates issued by it during the period commencing immediately after the previous self-audit sample was taken for the PublicCA in accordance with the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates and WebTrust$^{SM/TM}$ for Certification Authorities - SSL Baseline with Network Security .

8.5 Action Taken as a Result of Deficiency

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

(1) Record non-conformities.

(2) Notify the PublicCA about the non-conformities.

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

8.6 Scope and Method of Audit Result Disclosure

Except for systems that could possibly be attacked and the scope specified in section 9.3, PublicCA shall announce the information which should be publicly stated by the auditor. The audit results are displayed on the PublicCA website's front page using WebTrust ® for Certification Authorities and WebTrust® for Certification Authorities – SSL Baseline Requirements seals. The compliance audit and management declaration may be viewed by clicking on the seals. The most recent compliance audit and management's assertions shall be made publicly available in the respository within three months after the end of the audit period. If the posting of the latest audit results needs to be postponed for some reason, the CA shall provide a letter of explanation signed by the qualified auditor.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance and Renewal Fees

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

9.1.2 Certificate Access Fees

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

9.1.3 Certificate Revocation or Status Information Access Fees

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

9.1.4 Refund Procedure

With regard to the certificate issuance and renewal fees collected by the PublicCA, if a subscriber is unable to use a certificate due to oversight by the PublicCA, the PublicCA shall issue a new certificate

after conducting an investigation. If the subscriber does not accept the newly issued certificate, the PublicCA 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

The PublicCA is operated by Chunghwa Telecom Co., Ltd. Its financial responsibilities are the responsibilities of Chunghwa Telecom Co., Ltd. If the competent authority has insurance regulations for the certification authority in the future, the PublicCA will cooperate accordingly. .

9.2.2 Other Assets

PublicCA finances are a part of the overall finances of the Chunghwa Telecom Co., Ltd. Chunghwa Telecom Co., Ltd. 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. The PublicCA can provide self-insured asset prices based on the Company's financial reports. The Company's finances are sound. The ratio of current assets to current liabilities meets the lower than 1.0 requirement in the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates.

9.2.3 End Entities Insurance or Warranty Obligations

End entities (subscriber and relying parties) insurance or warranty obligations are not stipulated.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

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

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

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

9.3.2 Information Not Within the Scope of

Confidential Information

(1) Identification information and information listed on the certificate, unless stipulated otherwise, is not deemed to be confidential information.

(2) Issued certificates, revoked certificates, suspension information and the CRLs published in the PublicCA are not deemed to be confidential information.

9.3.3 Responsibility to Protect Confidential Information

The PublicCA shall handle subscriber application information in accordance with the Electronic Signatures Act, Trust Service Principles and Criteria for Certification Authorities standards, CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security and Personal Information Protection Act.

9.4 Privacy of Personal Information

9.4.1 Privacy Protection Plan

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

9.4.2 Types of Private Information

Any personal information listed on any certificate application is

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

9.4.3 Information Not Deemed Private

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

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

9.4.4 Responsibility to Protect Private Information

The personal information required for the operation of the PublicCA, in either paper or digital form, must be security stored and protected in accordance with the personal information protection and privacy rights declaration posted on the website and comply with related regulations in the Electronic Signatures Act, Trust Service Principles and Criteria for Certification Authorities standards, CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, Trust Services Principles

and Criteria for Certification Authorities – SSL Baseline with Network Security and Personal Information Protection Act related regulations. The PublicCA shall negotiate protection of private information with RAs.

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 CPS. The subscriber may check the subscriber's own application information specified in section 9.3.1 paragraph (3). However, the PublicCA shall reserve the right to collect reasonable fees from subscribers applying for access to this information.

9.4.6 Disclosure Pursuant to Judicial Process

If there is investigative or evidence collection requirements by judicial, administrative or law enforcement authorities, the information privacy regulations in section 9.4.2 must be checked in accordance with legal procedures. However, the PublicCA shall reserve the right to collect reasonable fees from authorities applying for access to this information.

9.4.7 Other Information Disclosure Circumstances

Subscriber personal information obtained during PublicCA operations is handled in accordance with related laws and regulations 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 the PublicCA:

(1) PublicCA and RA key pair and key splitting.

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

(3) Certificates and CRLs issued by the PublicCA.

(4) This CPS.

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

9.6 Representations and Warranties

9.6.1 PublicCA Representations and Warranties

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

(1) Comply with CP and CPS in operations.

(2) Perform certificate application identification and authentication.

(3) Provide certificate issuance and publication services.

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

(5) Issue and publish CRLs.

(6) Issue and provide OCSP response messages.

(7) Securely generate PublicCA and RA private keys.

(8) Secure management of private keys.

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

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

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

9.6.2 Registration Authority Representations and Warranties

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

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

RA obligations include:

(1) Provide certificate application services.

(2) Perform certificate application identification and authentication.

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

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

the PublicCA.

(5) Implement identification and authentication procedures for RAO.

(6) Manage RA private keys.

9.6.3 Subscriber Representations and Warranties

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

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

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

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

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

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

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

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

9.6.4 Relying Parties Representations and Warranties

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

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

(2) Relying parties shall first check if the certificate assurance level protect their rights during use of certificates issued by the PublicCA.

(3) Relying parties shall check the certificate and key usage listed on the certificate during use of certificates issued by the PublicCA.

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

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

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

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

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

9.6.5 Other Participant Representations and Warranties

Not stipulated

9.7 Disclaimer

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

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

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

9.8 Limitations of Liability

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

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

9.9 Compensation

9.9.1 PublicCA Compensation Liability

If the subscriber or relying parties claim compensation for damages suffered by a subscriber or relying parties due to the intentional or unintentional failure of the PublicCA to follow the CPS, relevant laws

and regulations and the provisions of contracts signed between the PublicCA, 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 the PublicCA and RA. Relying parties shall request compensation in accordance with relevant laws and regulations. The total compensation limit of the PublicCA for each subscriber or relying party is shown in the Table below. If the subscriber or relying party has signed a contract with the Company, the certificate scope of use and transaction compensation limit shall be determined separately.

Certificate Assurance Level	Compensation Limit (NTD)
Level 1	3,000
Level 2	100,000
Level 3	3,000,000

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

9.9.2 RA Compensation Liability

If subscribers or relying parties suffer damages due to the RA intentional or unintentional failure to follow the CPS, related laws and regulations or subscriber and related party contract provisions 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 related parties shall be made in accordance with relevant laws and regulations.

9.10 Term and Termination

9.10.1 Term

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

9.10.2 Termination

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

9.10.3 Effect of Termination and Survival

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

9.11 Individual Notices and Communication with Participants

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

9.12 Amendments

9.12.1 Procedure for Amendment

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

9.12.2 Notification Mechanism and Period

9.12.2.1 Notification Mechanism

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

9.12.2.2 Modification Items

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

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

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

9.12.2.3 Comment Reply Period

The reply period for comments on change items is:

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

Where the impact of section 9.12.2.2 (2) is less significant, the

reply period is within 7 calendar days of the posting date.

9.12.2.4 Comment Handling Mechanism

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

9.12.2.5 Final Notification Period

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

9.12.3 Circumstances under which the OID Must Be Changed

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

9.13 Dispute Resolution

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

9.14 Governing Law

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

9.15 Applicable Law

Related ROC laws and regulations must be followed with regard to the interpretation of any agreement signed based on the CP and CPS.

9.16 General Provisions

9.16.1 Entire Agreement

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

9.16.2 Assignment

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

9.16.3 Severability

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

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

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

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

9.16.5 Force Majeure

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

9.17 Other Provisions

Not stipulated

Appendix 1: Acronyms and Definitions

Acronyms	Full Name	Definition
AIA	Authority Info Access	See Appendix 2.
AICPA	American Institute of Certified Public Accountants	See Appendix 2.
CA	Certification Authority	See Appendix 2.
CAA	Certification Authority Authorization	See Appendix 2.
CARL	Certification Authority Revocation List	See Appendix 2.
CMM	Capability Maturity Model	See Appendix 2.
CP	Certificate Policy	See Appendix 2.
CPA	Chartered Professional Accountants Canada	See Appendix 2.
CP OID	CP Object Identifier	
CPS	Certification Practice Statement	See Appendix 2.
CARL	Certificate Authority Revocation List	See Appendix 2.
CDN	Content Delivery Network	See Appendix 2.
CRL	Certificate Revocation List	See Appendix 2.
DN	Distinguished Name	
DNS	Domain Name System	See Appendix 2.
DV	Domain Validation	See Appendix 2.

Acronyms	Full Name	Definition
eCA	ePKI Root Certification Authority	See Appendix 2.
EE	End Entities	See Appendix 2.
ePKI	Chunghwa Telecom ecommerce Public Key Infrastructure	See Appendix 2.
FIPS	(US Government) Federal Information Processing Standard	See Appendix 2.
FQDN	Fully Qualified Domain Name	See Appendix 2.
IANA	Internet Assigned Numbers Authority, IANA	See Appendix 2.
IETF	Internet Engineering Task Force	See Appendix 2.
IV	Individual Validation	See Appendix 2.
NIST	(US Government) National Institute of Standards and Technology	See Appendix 2.
OCSP	Online Certificate Status Protocol	
OID	Object Identifier	See Appendix 2.
OV	Organization Validation	See Appendix 2.
PIN	Personal Identification Number	
PKCS	Public-Key Cryptography Standard	See Appendix 2.
PKI	Public Key Infrastructure	See Appendix 2.

Acronyms	Full Name	Definition
RA	Registration Authority	See Appendix 2.
RFC	Request for Comments	See Appendix 2.
SSL	Security Socket Layer	See Appendix 2.
TLS	Transport Layer Security	See Appendix 2.
UPS	Uninterrupted Power System	See Appendix 2.

Appendix 2: Glossary

Access	Use the information processing capabilities of system resources
Access Control	Authorization procedure for access to information system resources given to subscribers, programs, procedures and other systems.
Activation Data	The private data required besides keys to access the cryptographic module (such as data used to activate the private key for signatures or encryption).
American Institute of Certified Public Accountants (AICPA)	Institution which jointly drafted The Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy system standards with the Chartered Professional Accountants Canada and the management organization for WebTrust for CA and SSL Baseline Requirement & Network Security mark.
Applicant	Subscribers who request certificates from a CA and have not yet completed the certificate procedure.
Archive	A physically separate storage site for long-term information (storage site for important information) which can be used to support audit, usage and integrity services.
Assurance	A reliable basis to determine that an entity conforms to certain security requirements (see Article 2-1, Chapter 1 for the rules which should be stated in CPS)
Assurance Level	A level possessing a relative assurance level (see Article 2-1, Chapter 1 for the rules which should be stated in CPS)
Audit	Assessment of whether system controls are adequate and ensure conformance with existing policy and operation procedures, and independent checking and review of recommended required improvements to existing controls, policies and

	procedures.
Audit Data	Activity logs of a system organized in the order of time of occurrence that can be used to reconstruct or investigate the time sequence or changes that occurred during a certain event.
Authenticate	(1) Authentication is the process by which a claimed identity is verified. (A Guide to Understanding Identification and Authentication in Trusted Systems, National Computer Security Center) (2)Determination of identity authenticity when an identity of a certain entity is shown.
Authentication	(1)The process of establishing confidence in the identity of users or information systems. (2)Security measures used for information transmission, messages and ways to authorize individuals to receive certain types of information. (3) "authentication" is proof of identification. Mutual authentication refers to authentication mutually conducted between two parties during communication activities.
Authority Info Access (AIA)	Records extensions related to certificate authority information access. The content may include: OCSP service sites and certificate issuance authority certificate verification path downloading site.
Backup	Information or program copying that can be used for recovery purposes when needed.
Binding	The process for binding (connecting) two related information elements.
Biometric	The physical or behavioral attributes of a person.
CA Certificate	Certificates issued by CAs.
Capability Maturity	Software Process Assessment (SPA) and Software

Model (CMM)	Capability Evaluation (SCE) from the Software Engineering Institute (SEI) at Carnegie Mellon University (CMU) serves as the basic framework to assist software developers find places for improvement in software development processes.
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 of the Electronic Signatures Act) (2) Digital presentation of information. The contents include: A. Issuing certificate authority B. Subscriber name or identity C. Subscriber public key D. Certificate validity period E. Certification authority digital signature The term 'certificate' referred to in the certificate policy specifically refers to ITU-T X.509 v.3 format certificates which states the certificate policy object identifier in the 'certificate policy' field.
Certification Authority (CA)	(1) The agency or natural person that issues certificate (Article 2.5 of the Electronic Signatures Act) (2) The competent body trusted by the subscriber. Its functions are the issuance and administration of ITU-T X.509 format public key certificates, CARLs and CRLs.
Certification Authority Authorization (CAA)	According to RFC 6844 (http:tools.ietf.org/html/rfc6844) : The Certification Authority Authorization DNS Resource Record permits the domain name owner in the DNS to designate one or more CAs to receive authorization to help that domain with

	certificate issuance. Posting of the CAA resource record allows publicly trusted CA to implement extra controls to reduce reforeseen certificate misissuance risk.
Certification Authority Revocation List (CARL)	A signed and time stamped list. The list contains the serial numbers of revoked CA The list contains the serial numbers of revoked CA public key certificates (including subordinate CA certificates and cross-certificates).
Certificate Policy (CP)	(1)Refers to a named set of rules that indicates the applicability to a certain community or class of application with common security requirements (Article 2.3 Chapter 1, in the Regulations on the Required Information for Certification Practice Statements) (2)Certificate policy refers to the dedicated profile administration policy established for the electronic transactions performed through certificate administration. Certificate policy covers a variety of issues including the formation, generation, delivery, auditing, administration and restoration after compromise. Certificate policy indirectly controls the use and operation of certificate security systems to protect the transactions performed by the communication systems. The security services required for certain application are provided through control of the certificate extension field methods, certificate

	policy and related technology.
Certification Practice Statement (CPS)	(1)External notification by the certificate authority used to describe the practice statement of the certificate authority governing certificate issuance and processing of other certification work. (Article 2.7 Electronic Signatures Act) (2)Announcement of a statement that certain procedures of the certificate authority for certificate work (including issuance, suspension, revocation, renewal and access) comply with certain requirements (listed in the certificate policy or other service contracts).
Certificate Revocation List (CRL)	(1)The certificate revocation list digitally signed by the certification authority provided for relying party use. (Article 2.8, Chapter 1 in the 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.
Chartered Professional Accountants Canada (CPA)	Institution which jointly drafted The Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy system standards with the American Institute of Certified Public Accountants (AICPA) and the management organization for WebTrust for CA and SSL Baseline Requirement & Network Security mark. Canadian Institute of Chartered Accountants is abbreviated as CICA.
Component Private Key	Private keys associated with certificate issuance equipment functions as opposed to private keys associated with operators or administrators.
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.
Content Delivery Network (CDN)	Use Internet interconnection with computer network systems to provide a highly efficient, expandable, low cost network for transmit content to users.
Cross-Certificate	A certificate used to establish a trust relationship between two root CA. This certificate is a type of CA certificate and not a subscriber certificate.
Cryptographic 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.
Crypto period	The validity period set for each key.
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 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	Entity which offers registration of domain names to natural persons or individuals including: (1) The

Registrar	Internet Corporation for Assigned Names and Numbers (ICANN), (2) a national domain name authority/registry), (3) Network Information Center and its participants, contractors, representatives, successors or assignees.
Domain Name System (DNS)	A distributed database used to automatically convert the IP address to domain name.
Domain Valiadition (DV)	Before SSL certificate approval and issuance, authentication of subscriber domain name control rights but no authentication of subscriber organization or individual identity, therefore, connection to a domain validation SSL certificate installed websites is able to provide SSL encryption channels but is unable to know who the owner of the website is.
Dual-Use Certificate	Certificates that may be used for digital signatures or data encryption.
Duration	A certificate field made up of two subfields “start time of the validity period” (notBefore) and “end time of the validity period” (notBefore).
E-commerce	Provision of goods for sale and other services through the use of network technology (specifically the Internet).
Encryption Certificate	A certificate including a public key used for encryption of electronic messages, files, documents or other information. This key can also be used to establish or exchange a variety of short-term secret keys for encryption.
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)	In order to promote Electronic Policy and create a sound e-commerce infrastructure, the Chunghwa Telecom Co., Ltd. shall follow the ITU-T X.509 standards to establish the public key infrastructure for use with various applications in e-commerce and e-government.
Chunghwa Telecom ecommerce Public Key Infrastructure Policy Management Committee (ePKI Policy Management Committee)	An organization which was established for the purpose of: Discuss and review the ePKI CP and electronic certificate system framework, accept subordinate CA and subject CA interoperation applications and other matters such as review and study of CPS and electronic certificate management matters.
ePKI Root CA (eCA)	The Chunghwa Telecom Public Key Infrastructure Root Certification Authority (Root CA) is the top level certificate authority in this hierarchical public key infrastructure. Their public keys are the trust anchor.
Federal Information Processing Standard (FIPS)	Except for military organizations in the US Federal Government System, information processing standard for all government organizations and government subcontractors. The security requirement standard for the cryptographic module is FIPS no. 140 standard (FIPS 140). FIPS 140-2 divides the cryptographic module into 11 types of security requirements. Each security requirement type is then divided into

	4 security levels.
Firewall	An access restriction gateway between networks which complies with near-end (local area) security policy.
Fully Qualified Domain Name (FQDN)	An unambiguous domain name that specifies the exact location of a computer within the domain's hierarchy. The fully qualified domain name consists of two parts: the host name (service name) and domain name. For example, ourserver.ourdomain.com.tw. ourserver is the host name and ourdomain.com.tw is the domain name. In this name, ourdomain is the second-level domain, .com is the generic top-level domain, (gTLD) and .tw is the country code top-level domain (ccTLD). A fully qualified domain name always starts with a host name.
Identification	A statement of who the user is (globally known). (A Guide to Understanding Identification and Authentication in Trusted Systems). "identification" is a statement of who the user is (globally known)
Individual Validation (IV)	Except for identification and authentication of natural person subscriber's domain control rights, identification and authentication of subscriber personal identity according to the certificate's assurance level during the SSL certificate approval process. Therefore, linking to the install IV SSL certificate website can provide a TLS encryption channel. It is known which individual is the owner of that website to ensure the integrity of data transmission.
Integrity	Protecting information so that it is not subject to unauthorized modification or damage. Preserve information in an untampered state during

	transmission and storage following generation at its source until receipt by the final recipient.
Internet Assigned Numbers Authority (IANA)	Internet address assignment authority responsible for administering IP addresses, domains, names and many other parameters used with the Internet.
Internet Engineering Task Force (IETF)	Responsible for the development and promotion of Internet standards. Official website is at: https://www.ietf.org/ . Its vision is the generation of high quality technical documents affects how man designs, uses and manages the Internet and allows the Internet to operate smoothly.
Issuing CA	For a particular certificate, the CA that issues the certificate is the issuing CA.
Key Escrow	Storage of related information using the subscriber's private key and according to the terms of the mandatory subscriber escrow agreement (or similar contract). The terms of this escrow agreement requires that one or more than one agencies have possession of the subscriber key provided it is beneficial to the subscriber, employer or another party in accordance with the provisions of the agreement.
Key Exchange	Mutual exchange of keys to establish a secure communication processing procedure.
Key Generation Material	Random numbers, pseudo random numbers and other password parameters used to generate keys.
Key Pair	Two mathematically linked keys possessing the following attributes: (1)One of the keys is used for encryption. This encrypted data may only be decrypted by the other key. (2)It is impossible to determine one key from another (from a mathematical calculation standpoint).
Naming Authority	A competent authority responsible for assigning a

	unique identifying name and ensuring that each unique identifying name is meaningful and unique within its field.
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 in the 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 Stapling	After one-time access of “time limit” OCSP response message (i.e. two hours, shorter than the next day posting of CRL and immediate) by the SSL website server of the OCSP service, the SSL website directly sends back the OCSP response to the subscriber (generally a browser) the next time

	so the subscriber does not need to inquire about the SSL certificate status from the CA OCSP service each time a connection is made to the high-traffic TLS website. This type of system directly provides a SSL certificate validity message with digital signature at a specific time interval from the CA OCSP server to the subscriber to address the privacy concerns of the OCSP server possibly leaning about which subscribers have tried to browse the SSL website.
Out-of-Band	Delivery method other than ordinary information delivery channels. If the delivery method is by electric cable, a special secure channel may be the use of physical registered mail.
Organization Validation, (OV)	In the SSL certificate approval process, except for identification and authentication of subscriber domain name control rights, following the certificate assurance level to identify and authenticate the identity of subscriber organizations and individuals. Therefore. connection to a website installaed by an Organization Validation SSL certificate is able to provide SSL encryption channels, in order to know who is the owner of the website and ensure the integrity of the transmitted information.
Private Key	(1)The key in the signature key pair used to generate digital signatures. (2) The key in the encryption key pair used to decrypt secret information. This key must be kept secret under these two circumstances.
Public Key	(1)The key in the signature key pair used to verify the validity of the digital signature. (2)The key in the encryption key pair used for encrypting secret information. These keys must be made public (usually in a digital certificate form) under these two circumstances.

Public-Key Cryptography 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.
Registration Authority (RA)	(1) Responsible for checking the identity and other attributes of the certificate applicant but does not issue or administer certificates. The nature and scope of obligations borne by the registration authority are set down in the applicable certificate policy or agreement. (2) An entity responsible for the identity identification and authentication of the certificate subject which does not issue certificates.
Re-key (a certificate)	Changing the key values used in the cryptographic system application program. It is commonly achieved by issuing a new certificate for the new public key.
Relying Party	(1)Recipient of a certificate who acts in reliance of that certificate or a digital signature to verify the public key listed in the certificate, or the counterpart to identify (or its attributes) of the subject named in a trusted certificate and public key listed in the certificate. (Article 2.6, Chapter 1 in the Regulations on Required Information for Certification Practice Statements) (2)The individual or agency which receives information including a certificate and digital signature (the public key listed on the certificate may be used to verify the digital signature) and may rely on this information.
Renew (a certificate)	The procedure for issuing a new certificate to renew the validity of information bound together

	with the public key.
Repository	(1)A trustworthy system used to store and retrieve certificates and other information relevant to certification. (Article 2.7, Chapter 1 in the Regulations on Required Information for Certificate Practice Statements) (2)The database containing the certificate policy and certificate-related information.
Reserved IP Addresses	IPv4 and IPv6 addresses reserved in the IANA setting. See: http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml and http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml
Revoke a Certificate	Termination of a certificate prior to its expiry date.
Request for Comments, (RFC)	A series of memos issued by the Internet Engineer Task Force that include Internet, UNIX and Internet community standards, protocols and procedures for number assignment.
Secure Socket 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.

Secret Key	Shared secret in the symmetric cryptosystem, identity authentication of the subscriber is performed by sharing other secrets through passwords, PIN or remote host (or service). The single key is jointly held by two parties. The sender uses it to encrypt the transmitted information and the receiver uses it to decrypt the information. This jointly held key is generated with previously agreed upon algorithms.
Signature Certificate	Public key certificates which contains a digital signature public key used for verification purposes (not used for data encryption or other cryptographic uses).
Subject CA	For a CA certificate, the certificate authority referred to in the certificate subject of the certificate is the subject CA for that certificate.
Subordinate CA	In the public key infrastructure hierarchy, certificates that are issued by another certificate authority and the activities of the certificate authority are restricted to this other certificate authority.
Subscriber	(1)Refers to a subject named or identified in the certificate that holds the private key that corresponds with the public key listed in the certificate. (Article 2.5, Chapter 1 Regulations on Required Information for Certification Practice Statements) (2) An entity having the following attributes including (but not limited to) individuals, organizations, server software or network devices: (a) Subject listed on an issued certificate. (b) A private key that corresponds to the public

	key listed on the certificate. (c) Other partiers that do not issue certificates.
Technical Non-Repudiation	Technical evidence provided by the public key system to support non-repudiation security service.
Threat	Any status or event which may cause damage (including destruction, disclosure, malicious tampering or denial of service) to information systems. Can be divided into internal threats and outside threats. Internal threats are use of authorization to employ information destruction, disclosure, tampering or denial of service methods to damage the information system. Outside threats are an outside unauthorized entity which has the potential to damage the information system (including information destruction, tampering, disclosure and interruption of service).
Time Stamp	Trusted authority proves that a certain digital object exists at a certain time through digital signature.
Transport Layer Security (TLS)	SSL protocol established in RFC 2246 by the IETF. Called Transport Layer Security (TLS). Latest version is RFC 5246 which is the TLS 1.2 protocol.
Trust List	List of trusted certificates used by relying parties to authenticate certificates.
Trusted Certificate	Certificate trusted by relying party obtained through a secure and reliable transmission method. The public key contained in this type of certificate comes from a trusted path. Also called a trust anchor.
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)
Zeroize	Method to delete electronically stored information. Storage of changed information to prevent information recovery.