Certificate Policy for the Chunghwa Telecom ecommerce Public Key Infrastructure

Version 1.1

Chunghwa Telecom Co., Ltd.

December 22, 2014

Contents

1. Introduction

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

The public key infrastructure (PKI) hierarchy established for this infrastructure is based on ITU-T X.509 standards included the PKI trust anchor - ePKI Root Certification Authority (eCA) and subordinate CAs formed by the Company. Certificates issued by ePKI may be used for various applications in e-commerce and e-government to provide secure, reliable and fast network services.

The Certificate Policy (CP) is a policy document drafted in accordance with the Electronic Signatures Act and related international standards such as Internet Engineering Task Force (IETF) RFC 3647, ITU-T X.509, IETF PKIX Working Group RFC 5280 and CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates to serve as a basis for the Certification Practice Statement (CPS) established by CAs in the ePKI.

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

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

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

(2) The CA-related system work procedures including certificate

issuance and administration and private key delivery.

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

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

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

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

1.1 Overview

1.1.1 Certificate Policy

Certificate policy (CP) is one form of network certification information technology guidelines. CP refers to one set of rules listed for a certain subject or circumstance for which certificates are used. The subject or circumstance may be a certain community or joint security

requirement application. The CP OID for five assurance levels has been registered in the ePKI for use by the CA to indicate the assurance level when a certificate is issued for a certain purpose. The CA can directly use the registered CP OID and relying parties may use the CP OID to check whether the applicability of the issued certificates are correct.

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

1.1.2 Relationship between CP and CPS

CA must state what criteria is used for each CP assurance level in the CPS.

1.1.3 Certificate Policy Object Identifiers cited by Certification Authority

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

1.2 Document Name and Identification

The name of this policy is the Certificate Policy for the Chunghwa Telecom ecommerce Public Key Infrastructure. This is version 1.1. The announcement date was December 22, 2014. The latest version of this CP can be obtained at the website: http://ePKI.com.tw. The CP of certificates issued by the CA (not including self-signed certificates) must be recorded in the certificatePolicies extension field of the certificate. The CP OIDs are registered in the id-cht arc as follows:

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

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

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

Assurance Level	OID Name	OID Value

Assurance Level	OID Name	OID Value
Test Level	id-cht-ePKI-certpolicy-testAssurance	{id-cht-ePKI-certpolicy 0}
Level 1	id-cht-ePKI-certpolicy-class1Assurance	{id-cht-ePKI-certpolicy 1}
Level 2	id-cht-ePKI-certpolicy-class2Assurance	{id-cht-ePKI-certpolicy 2}
Level 3	id-cht-ePKI-certpolicy-class3Assurance	{id-cht-ePKI-certpolicy 3}
Level 4	id-cht-ePKI-certpolicy- class4Assurance	{id-cht-ePKI-certpolicy 4}

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

id-pen-cht ::= {1 3 6 1 4 1 23459}

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

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

Assurance Level	OID Name	OID Value
Test Level	id-pen-cht-ePKI-certpolicy-testAssurance	{id-pen-cht-ePKI-certpolicy 0}
Level 1	id-pen-cht-ePKI-certpolicy-class1Assurance	{id-pen-cht-ePKI-certpolicy 1}
Level 2	id-pen-cht-ePKI-certpolicy-class2Assurance	{id-pen-cht-ePKI-certpolicy 2}
Level 3	id-pen-cht-ePKI-certpolicy-class3Assurance	{id-pen-cht-ePKI-certpolicy 3}
Level 4	id-pen-cht-ePKI-certpolicy-class4Assurance	{id-pen-cht-ePKI-certpolicy 4}

For SSL certificate issuance, this CP complies with the current official version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates issued from the CA/Browser Forum website at http://www.cabforum.org. If there are discrepancies between the CP and CA CPS with regard to SSL certificate

issuance and current official version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates issued from the CA/Browser Forum, precedence shall be given to the provisions of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates.

The certificates issued by subordinate CAs (currently Chunghwa Telecom Public Certification Authority) comply with the requirements defined in the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates and pass AICPA/CPA WebTrust for Certification Authorities Trust Services Principles and Criteria for Certification Authorities - SSL Baseline Requirements Audit Criteria Version 1.1 or its latest version. The subordinate CA certificates and subscriber SSL certificates issued by will be allowed to use CA/Browser Forum organization validation (OV) and domain validation (DV) SSL CP OID of the CA/Browser forum:

OID Name	OID Value
joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) subject-identity-validated(2)	{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) **1 2 2**}
{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) domain-validated(1)}	{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) **1 2 1**}

1.3 PKI Participants

1.3.1 Policy Management Committee

One policy management committee must be established for each PKI to ensure the continued and regular operation of the PKI. For this ePKI, the Company has specifically established the ePKI Policy Management Committee (hereinafter referred to as the Policy Management Committee) to be responsible for the administration of the ePKI and Policy Management Committee organization work and other tasks described below. Within the Committee, one person shall be the convener concurrently served by a vice president or equivalent level manager in the Data Communications Branch, Chunghwa Telecom. One

person shall be the executive secretary concurrently served by Data Communications Branch Communication Security Division director. Ten persons shall be committee members served by the directors of the Business Planning Department, Corporate Client Department, Marketing Department, Government Network Department, Cloud System Department, Internet of Things Department, Convergences System Department and Information Department at the Data Communication Branch, Chunghwa Telecom. Their duties are as follows:

(1) Supervise ePKI CA key generation.
(2) Review ePKI CP.
(3) Review ePKI related technical specifications.
(4) Review ePKI CPS.
(5) Review subject CA interoperability applications.
(6) Review and approve ePKI entrants or the corresponding relationship of the CP of the CA who has the cross-certified relationship with ePKI.
(7) Supervise subject CA compliance with allowed CP to facilitate the continued operation of interconnection mechanisms.

1.3.2 Certificate Authority

1.3.2.1 ePKI Root Certification Authority

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

(1) Responsible for issuance and administration of eCA certificates including self-signed certificates, self-issued certificates and certificates issued by the subordinate CA.
(2) Establishes cross-certification procedure between eCA and CA outside the ePKI including issuance and administration of CA cross certificates outside the ePKI.
(3) Publishes issued certificates and certification authority revocation lists (CARLs) in the repository and ensures normal operation of the repository.

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

1.3.2.2 Subordinate CA

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

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

1.3.3 Registration Authorities

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

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

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

1.3.4 Subscribers

For organizations and individuals, subscribers refers to the name recorded as the certificate subject on the certificate and the entity in possession of the private key that corresponds with the certificate's public key. Subscribers must correctly use the certificate according to the

certificate policies listed on the certificates. In addition, for the category of property such as application process, program code, server software (e.g. web server and SSL server) and hardware device, property is immovable so the certificate subscriber applying for the certificate shall be an individual or organization.

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

1.3.5 Relying Parties

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

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

1.3.6 Other Participants

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

1.3.7 End Entities

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

(1) Private key holders responsible for the safeguarding and use of certificates.
(2) A third party (not a private key holder or a CA) which trusts certificates issued by the CA in the ePKI.

1.4 Certificate Usage

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

1.4.1 Appropriate Certificate Uses

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

Assurance Level	Scope of Usage
Test Level	Only provided by test use. No legal liability borne for the transmitted data.
Level 1	Applicant ability to operate the e-mail account verified by e-mail. Suitable for use in network environments with a low risk of malicious tampering or inability to provide a higher assurance level. When used for a digital signature, can be used to determine if a subscriber comes from a certain e-mail account and ensure the integrity of the signed document. When used for encryption, relying parties can use the subscriber certificate's public key to encrypt and transmit messages or symmetric key to ensure privacy but is not suitable for online transactions when identity authentication and non-repudiation is required.
Level 2	Suitable for use in Internet environment where information may be tampered with but malicious tampering is not present (information interception is possible but the probability is not high). Not suitable for the signing of importance documents (life-related or high value transaction documents). Suitable for data encryption and identity verification of small value

	e-commerce transactions.
Level 3	Suitable for use in Internet environments in which there are malicious users, which intercept or tamper with information, and risks, which are greater than the environment of Class 2. Transmitted information includes on-line cash transactions.
Level 4	Suitable for use in Internet environments where potential threats to data are high or the cost to restore tampered data is high. Transmitted information includes high value on-line transactions and highly confidential documents.

1.4.2 Restricted Certificate Use

EEs shall choose a certificate with a suitable assurance level based on the security requirements which are needed for their application system.

When using a private key, the subscriber shall choose a secure computer environment and trusted application systems to prevent theft of the private key which could harm one's interests.

Relying parties shall follow the key usage regulations in section 6.1.7, use the keys in a suitable manner and use the certificate validation mathods defined in international standards (such as ITU-T X.509 or IETF RFC5280) to verify the validity of the certificate.

1.4.3 Prohibited Certificate Uses

Certificates issued by CAs under the ePKI are prohibited from being used for the following:

(1) Crime

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

(3) Operation of nuclear equipment

(4) Aviation flight and control systems

(5) Scope of prohibitions announced under the law

1.5 Policy Administration

1.5.1 Organization Administering the Document

Chunghwa Telecom Co., Ltd.

1.5.2 Contact Person

If you have suggestions regards the CP, contact the Company:

Phone: 0800080365

Address: ePKI Root Certification Authority, Data Communication Building, No. 21, Hsin-Yi Road, Sec.1, Taipei City, Taiwan, R.O.C.

E-mail: caservice@cht.com.tw。

Check this site at http://epki.com.tw for related contact information.

1.5.3 Person Determining CPS Suitability for the Policy

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

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

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

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

1.5.4 CPS Approval Procedure

The CA CPS must follow relevant laws and comply with this CP and obtain approval from the Company and the MOEA, the competent authority of the Electronic Signatures Act. If the CPS must be revised together with the posted CP revisions, the CPS is submitted to the Policy Management Committee and MOEA.

1.6 Definitions and Acronyms

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

2. Publishing and Repository Responsibilities

2.1 Repositories

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

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

CA repository services shall be responsible for the following obligations:

(1) Regularly publish issued certificates.
(2) Regularly publish revoked and suspended certificate information.
(3) Public the latest CP and CPS information.
(4) Repository access controls must follow the regulations in section 2.3.

2.2 Publication of Certificate Information

CA shall routinely publish in the repository:

(1) CP and CPS.

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

(3) Online Certificate Status Protocol (OCSP) service

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

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

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

(7) Privacy protection policy.

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

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

2.3 Publishing Frequency

Follow the regulations in section 4.9 for CRL publication frequency. CP publication and any subsequent modifications shall be published in the eCA repository within 7 calendar days following Policy Management Committee approval.

2.4 Access Controls

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

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

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

3. Identification and Authentication Procedures

3.1 Naming

3.1.1 Type of Names

The subject name of the PKI certificate conforms to the distinguished name (DN) of X.500.

For certificate applications, the CA has the right to decide whether or not to accept the subject alternate name. If the CA requests that the subject alternate name be added to the certificate, it must be noted in the extension that it is a non-critical extension.

3.1.2 Need for Names to be Meaningful

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

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

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

3.1.3 Anonymity and Pseudonymity of Subscribers

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

3.1.4 Rules for Interpreting Name Forms

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

3.1.5 Uniqueness of Names

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

3.1.6 Recognition, Authentication and Role of Trademarks

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

3.1.7 Name Claim Dispute Resolution Procedure

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

The Company is the arbitration authority for PKI name claim disputes.

3.2 Initial Registration

3.2.1 Method to Prove Possession of Private Key

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

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

(1) The CA or RA generates the key pair for the subscriber:
The subscribers does not need to prove possession of the private key but must undergo identity identification in accordance with the regulations in sections 3.2.2 and 3.2.3 to obtain the private key and activation data. The regulations in section 6.1.2 are followed to deliver the private key to the subscriber.

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

(3) Key pair self-generated by subscriber:

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

3.2.2 Authentication of Organization Identity Procedure

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

Assurance Level	Organization Identity Identification and Authentication
Test level	Not stipulated
Level 1	(1) Written document checking not required. (2) Applicant only needs to have e-mail address to apply for certificate. Identification and authentication procedure does not need to be performed. (3) In-person application at counter not required.
Level 2	(1) Written document checking not required. (2) Subscriber submits organization information such as organization identity ID number (ie withholding tax

Assurance Level	Organization Identity Identification and Authentication
	ID number), organization name shall be checked against CA approval information. (3) In-person application not required.
Level 3	There are 3 types of organization identity authentication: (1) Private organization identity authentication Application information includes the organization name, location and representative name which is sufficient to identify the organization. In addition to verifying the authenticity of the application information and representative identity, the CA or RA shall verify that the representation has the right to apply for certificate using the name of the organization. The representative shall present the application in person at the counter to the CA or RA. If the representative is unable to present the application in person, an agent shall be named in writing to present the application in person at the counter and the identity of the agent shall be authenticated in accordance with the assurance level 3 regulations under section 3.2.3. If the private organization has completed the registration procedure with the competent authorities or completed the counter identification and authentication procedure by the CA, RA or 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

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

Assurance Level	Organization Identity Identification and Authentication
	really exists and determine the authenticity of the public documents. (3) Identity authentication for organizations belonging to Chunghwa Telecom Organizations belonging to Chunghwa Telecom must apply for the certificate with official documents and the CA or RA must check if the agency or authority really exists and determine the authenticity of the public documents. In addition, an assurance level 3 certificate signature is issued through the ePKI for the above three categories of organization certificate application information. The representative does not need to submit the application in person. The CA or RA verifies the application information's digital signature. When an assurance level 3 organization certificate signature is issued through the ePKI for the server software certificate application information, the representative does not need to submit the application in person. The CA or RA verifies the certificate application information's digital signature.
Level 4	Organization identity authentication can be divided into the following two types:

Assurance Level	Organization Identity Identification and Authentication
	(1) Private organization identity authentication Application information includes the organization name, location and representative name which is sufficient to identify the organization. In addition to verifying the authenticity of the application information and representative identity, the CA or RA shall verify that the representation has the right to apply for certificate using the name of the organization. The representative shall present the application in person at the counter with the CA or RA. The above mentioned private organization refers to the private corporate bodies, non-corporate bodies or the organizations belonging to the previous two. (2) Identity authentication for organizations belonging to Chunghwa Telecom Organizations belonging to Chunghwa Telecom who must apply for the certificate shall appoint an individual by official document who can be authenticated by the CA or RA. The representative of the agency or authority shall apply for the certificate with the CA or RA in person. The CA or RA shall verify that the agency or authority really exists and the authenticity of the public document. The identity of the individual representing the agency or authority shall be authenticated in accordance with the

Assurance Level	Organization Identity Identification and Authentication
	assurance level 4 regulations under section 3.2.3.

3.2.3 Authentication of Individual Identity Procedure

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

Assurance Level	**Authentication of Individual Identity Procedure**
Test level	Not stipulated
Level 1	(1) Written documentation check not required. (2) Applicant only needs to have an e-mail address to apply for certificate. Identification and authentication procedure does not need to be performed. (3) In-person application not required.
Level 2	(1) Written documentation checking not required. (2) Subscriber submits personal information including personal identication code (such as ID card number) and name which is checked against CA recognized information. (3) In-person application not required.

Assurance Level	Authentication of Individual Identity Procedure
Level 3	(1) Check written documentation: The subscriber shall present at least one original approved photo ID (such as national ID card) during certificate application to the CA or RA to authenticate the subscriber's identity. If a subscriber (such as minor under 18 years old) is unable to submit the above photo ID, government issued written documentation (such as household registration) which is sufficient to prove the identity of the subscriber and one adult with legal capacity to guarantee the subscriber's identity in writing may be used in its place. The identity of the adult providing the written guarantee must pass through the above authentication. (2) Personal information submitted by the subscriber such as personal identification code (ID card number), name and address (household registration address) shall be checked against the information registered with the competent authority (such as household registration information) or other information registered with a trusted third party recognized by the competent authority. (3) Counter application: The subscriber must verify his / her identity in person at the CA or RA. If the subscriber is unable to

Assurance Level	Authentication of Individual Identity Procedure
	present the application in person, the subscriber may submit a letter of appointment to appoint an agent to submit the application in person on their behalf but the CA or RA must verify the authenticity of the letter of appointment (such as the subscriber's seal on the letter of appointment) and authenticate the identity of the agent in accordance with the above regulations. If an individual has previously passed through the CA, RA or CA trusted authority or individual (such as household registration office, notary or personnel authorized by the Company) counter identification and authentication procedure which conforms to the above regulations and supporting identification and authentication information (such as seal certification) has been submitted, the individual does not need to apply in person. The CA or RA needs to verify the supporting information. (4) Use MOICA certificates to apply for certificate When a digital signature with an assurance level 3 certificate issued by the MOICA is applied for certificate, the subscriber does not need to verify his / her identity in person at the CA or RA but the CA or RA shall verify that the digital signature is valid. (5) When a digital signature with an assurance level 3 personal certificate issued through the ePKI for

Assurance Level	Authentication of Individual Identity Procedure
	hardware devices or server software certificates, the representative does not need to apply in person at the counter but the CA or RA shall verify the digital signature for the certificate application information.
Level 4	(1) Checking written documentation: The subscriber shall at least present one original approved photo ID (such as national ID card) during certificate application for authentication of the subscriber identity by the CA and RA. (2) Subscriber submits personal information including personal identication code (such as ID card number), name and address (such as household registration address) which is checked against the information registered with competent authorities (such as household registration agency). (3) The subscriber must verify his identity with the CA or RA when applying in person.

3.2.4 Non-Verified Subscriber Information

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

3.2.5 Validition of Authority

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

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

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

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

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

For DV SSL 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 authenticate subscriber domain name control rights. For OV SSL application certificate applications, except for validation of subscriber possession of domain name control rights by DV SSL application software certificate, the regulations in sections 3.2.2 or 3.2.3 shall be followed to authenticate organization or individual identity. If the subordinate CA issues a SSL certificate, the validation method for domain control rights shall be stated in the CPS of the subordinate CA.

3.2.6 Criteria of Interoperation

Not stipulated.

3.3 Identification and Authentication for Re-Key Requests

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

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

The subordinate CA subscriber must comply with the authentication requests listed in the Table below when renewing a key.

Assurance Level	**Authentication Requirements for Subscriber Certificate Re-Key**
Test level	Not stipulated

Assurance Level	Authentication Requirements for Subscriber Certificate Re-Key
Level 1	For subscriber identity, the existing signature key can be used for authentication and authentication may be conducted in accordance with the initial registration authentication procedures in section 3.2.
Level 2	For subscriber identity, the existing subscriber key can be used for authentication and authentication may be conducted in accordance with the initial registration authentication procedures in section 3.2 but if 15 years has passed since initial registration, initial registration must be performed again in accordance with the regulations in section 3.2.
Level 3	For subscriber identity, the existing subscriber key can be used for authentication and authentication may be conducted in accordance with the initial registration authentication procedures in section 3.2 but if 9 years has passed since initial registration, initial registration must be performed again in accordance with the regulations in section 3.2.
Level 4	For subscriber identity, the existing subscriber key can be used for authentication and authentication may be conducted in accordance with the initial registration authentication procedures in section 3.2 but if 3 years has passed initial registration, initial registration must be performed again in accordance with the regulations in section 3.2.

3.3.1 Renew Identification and Authentication

CA certificates may not be renewed. Only subscriber certificates may be renewed. Existing signature keys may be used for authentication.

3.3.2 Rekey Identification and Authentication after Revocation

New certificate issuance after certificate revocation shall be performed in accordance with the regulations in section 3.2. The subscriber must repeat the initial registration procedure.

3.4 Certificate Revocation Request Identification and Authentication

The CA or RA must authenticate the certificate revocation request. The CA shall follow the applicant identity authentication method listed in section 4.9 of the CPS to determine if the applicant has the rights to submit the certificate revocation request.

Regardless of whether the private key has been compromised, private key signatures and the certificates being revoked may be used to authenticate the identity of the person making the certificate revocation request.

4. Certificate Lifecycle Operational Standards

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

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

Subordinate CA certificate applicants include organizations or individuals.

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

4.1.2 Registration Procedure and Responsibility

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

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

(2) Use the certificate in a correct manner.

(3) Properly safeguard and use the private keys (not required for

certificates issued at the test assurance level).

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

4.2 Certificate Application Procedure

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

The eCA may accept certificate applications from CA established by the Company to become a level 1 subordinate CA in the PKI. The application procedure shall be determined separately by the Policy Management Committee.

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

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

For eCA issued certificates to CA outside the PKI, the Policy Management Committee and the CA shall negotiate to determine whether or not to recognize the cross certificates issued by the CA to other CA.

4.2.1 Performing Identification and Authentication Functions

The CA shall ensure that the system and procedures for authenticating subscriber identity conform to CP and CPS regulations. The initial registration procedures shall be implemented in accordance

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

4.2.2 Approval or Rejection of Certificate Applications

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

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

4.2.3 Time to Process Certificate Applications

Provided that the applicant submits the information in full which conforms to CP and CPS requirements, the CA and RA shall complete the certification application processing within a reasonable period of time. The time to process certificate applications may be stated in the CPS, subscriber terms and conditions or the certificate applicant contract.

4.3 Certificate Issuance Procedure

4.3.1 CA Actions during Certificate Issuance

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

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

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

4.3.2 Notification to Certificate Applicant by the CA of Certificate Issuance

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

If the CA or RA does not approve the certificate issuance, the certificate application shall be notified in a suitable manner and the

reason for refusing to issue the certificate shall be clearly stated. In addition to applicant identity identification and authentication reasons, the CA may refuse to issue the certificate for other reasons. CAs operating at assurance levels 1, 2, 3 and 4 shall state the notification methods for certificate issuance refusal in the CPS.

4.4 Certificate Acceptance Procedure

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

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

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

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

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

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

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

4.4.1 Circumstances Constituting Certificate Acceptance

The certificate applicant shall review the certificate content for errors prior to issuance. The CA then publishes the certificate on the repository or delivers the certificate to the applicant.

4.4.2 Publication of the Certificate by the CA

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

4.4.3 Notification by the CA to Other Entities

Not stipulated.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

A subscriber is an entity which has applied for and obtained a certificate. For organizations and individuals, a subscriber is the name listed as the certificate subject and the entity that possesses the private key corresponding to the certificate public key. For property (such as applications, hardware and equipment), it does not have the capacity to act so the certificate subscriber is the individual or organization applying

for certificate. Subscriber key pair generation shall conform to the regulations in section 6.1.1 of the CP. The subscriber must also have the right and capability to independently possess and control the private key corresponding to the certificate. Subscribers do not issue certificates to others. Subscribers shall protect against unauthorized use and disclosure of the private key and only use the private key for correct key usage (key usage is listed in the certificate extension field). The subscriber must correctly use the certificate as stated in the CP recorded on the certificate.

4.5.2 Relying Parties and Certificate Usage

The relying party refers to the third party with a connecting relationship with the certificate subject name and public key. The relying parties shall use software that conform to 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 or guidelines.

The relying party must follow the corresponding CA certificates and certificate status information to verify the validity of the certificate used. After verifying the validity of the certificate, the certificate can be used to perform the following work:

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

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

(3) Establish secure communication channels between subscribers.

The above certificate status information may be obtained through the CRL or OCSP service, CRL distribution point location can be found in

the certificate details. In addition, the relying parties shall check the CA and subject certificate CP to confirm the certificate assurance level.

4.6 Certificate Renewal

Renewal of CA certificates is not allowed. Only subscriber certificates can be renewed.

4.6.1 Circumstances for Certificate Renewal

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

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

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

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

4.6.2 Request Renewal Applicant

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

4.6.3 Certificate Renewal Procedure

When the subscriber applies for certification renewal, the private key is used to sign the certificate application file and the certificate application file is submitted to the RA. The RA uses the subscriber's public key to verify the digital signature on the certificate application file to authenticate the subscriber identity.

4.6.4 Subscriber Instructions for Certificate Renewal

Expired, suspended or revoked certificates may not be renewed. Certificates may be extended at the latest to the subscriber public key usage period limit specified in section 6.3.2.2 to ensure key pair security.

4.6.5 Circumstances Constituting Acceptance of a Renewal Certificate

The certificate application shall first review the content of issued renewed certificate for errors. The certificate shall be published by the CA in the repository or delivered to the certificate applicant.

4.6.6 Publication of the Renewed Certificate by the CA

The CA repository service shall regularly publish the renewed certificates issued to subscribers. RA may negotiate with CA regarding RA delivery of certificates to the subscriber.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Not stipulated

4.7 Certificate Re-Key

4.7.1 Circumstances for Certificate Re-Key

CA private keys shall be regularly renewed in accordance with the regulations in section 6.3.2. The new private key is used in place of the old private key to issue certificates and notify all entities which rely on this CA at an appropriate time. CRL or on-line certificate status responses for the old private key must still be made in order to maintain and protect all subscriber certificates issued with the old key until they are expired.

If the CA certificate is revoked, its private key must be suspended

and the key pair must be renewed.

The eCA shall renew the key pair used to issue certificates before the usage period for the private key used to issue certificates expires at the latest and issue one new self-signed certificate and one self-issued certificate mutually issued with the new and old private key. The issuance procedure for these three new certificates shall be conducted in accordance with the regulations in section 4.2.

The subordinate CA shall renew the key pair used to issue certificates before the usage period for the private key used to issue certificates expires at the latest. After renewing the key pair, the subordinate CA shall apply for a new certificate from the upper level CA in accordance with the regulations in section 4.2. The uppler level CA must issue and publish the lower level CA's new certificate before the lower level CA's certificate expires.

For eCA cross certification with CA outside the PKI, the re-key time shall be decided independently by the CA in accordance with the CP. If the CA needs to continue to apply for cross certificate with eCA after the rekey, it shall be determined by agreement or contract between the CA and the Contract. If the CA needs to continue to apply for a cross certificate with the eCA for the rekey, the application shall be made in accordance with section 4.2 and enough time shall be reserved for the Policy Management Committee and eCA to process the cross certificate application to ensure that the new cross certificate is issued and published by the eCA before the CA cross certificate is expired.

4.7.2 Who May Request Certificate Re-Key

CAs may accept certificate re-key requests as long as the original

subscriber or the authorized representative which is able to represent the subscriber complies with appropriate key and certificate lifecycle management responsibilities to safeguard the private key corresponding to that certificate. The certificate request file for certificate re-key shall include the new public key.

4.7.3 Certificate Re-Key Procedure

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

4.7.4 Subscriber Instructions for Certificate Re-Key

Routine re-key of subscriber private keys must be done in accordance with the regulations in section 6.3.2.

After a subscriber certificate is revoked, use of the private key is stopped. After the key pair is renewed, a new certificate application may be submitted to the CA or RA in accordance with the regulations in section 4.2.

For subscribers that hold assurance level 2, 3 or 4 certificates which have not been revoked, the CA or RA may start to accept re-key and new certificate applications one month before the validity period of the subscriber’s private key expires. New certificate application procedures are implemented in accordance with the regulations in section 4.2.

4.7.5 Circumstances Constituting Acceptance of Certificate Re-Key

Certificate issuance notification to the certificate applicant by the

CA, delivery of issued certificates to applicants or actual use of the certificate by the subscriber are all circumstances which constitute acceptance of certificate re-key.

Subscribers accepting CA issued certificates shall bear the following obligations:

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

(2) Use certificates in a proper manner.

(3) Properly safeguard and use private keys (no requirement for test assurance level certificates).

(4) Immediately notify CAs in the event of private key compromise (no requirement for test assurance level certificates).

4.7.6 Publication of the Certificate Re-Key by the CA

CA repository services shall regularly publish the certificates issued by certificate re-key. RA may negotiate with CA regarding RA delivery of certificates to the subscriber.

4.7.7 Notification by the CA to Other Entities

Not stipulated

4.8 Certification Modification

4.8.1 Circumstances for Certificate Modification

Certification modificate is when the authentication information on the one certificate provided same certificate subject is slightly different than the old certificate (such as e-mail address or other relatively unimportant attribute information) which conforms to relevant CP and CPS regulations. New certificates may have a new certificate subject public key or use the original subject public key but the certificate expiry date is the same as the expiry date on the original certificate. The old

certificate shall be revoked after certificate modification.

4.8.2 Who May Request Certificate Modification

Certificate subscriber subject or authorized representative.

4.8.3 Certificate Modification Procedure

As stated in section 4.2.

4.8.4 Subscriber Instructions for Certificate Modification

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

If the certificate with the certificate modification is refused, the CA or RA shall notify the certificate applicant in an appropriate manner and clearly state the reasons why the certificate issuance was refused. In addition to applicant identity identification and authentication, the CA may refuse to issue the certificate for other reasons. CAs operating at assurance levels 1, 2, 3 and 4 shall state the notification method for refusing certificate modifications in the CPS.

4.8.5 Circumstances Constituting Acceptance of Modified Certificate

The certificate applicant shall first review the content of the issued or unissued certificate for errors. The certificate shall be published by the CA in the repository or delivered to the certificate applicant.

4.8.6 Publication of the Modified Certificate by the CA

The CA repository shall routinely publish issued certificates that have undergone modification. The RA may negotiate with the CA regarding RA delivery of certificates to the subscriber.

4.8.7 Notification by the CA to Other Entities

Not stipulated

4.9 Certificate Suspension and Revocation

All CAs except for those CAs operating at a test assurance level shall provide certificate revocation services. The CA may decide whether or not to provide certificate suspension services depending on certificate usage and service quality.

CAs providing certificate revocation and suspension services shall specify the certificate revocation and suspension service times in the CPS.

CAs providing certificate revocation and suspension services shall specify the service provision methods, certificate revocation request procedures and processing locations and websites in the CPS.

After certificate revocation or suspension, the CA shall list the revoked or suspended certificates in the CARL and CRL and post them in the repository at the next scheduled publication time of the CARL or CRL at the latest. The published certificate status information shall include the revoked and suspended certificates until the certificates expire or use is resumed.

For expired certificates, the CA may not accept certificate revocation or suspension requests and may not list the certificate revocation or suspension information on the CARL and CRL. For revoked or suspended certificates prior to expiry, the CA shall list the revoked or suspended information on the CARL or CRL at least once.

4.9.1 Circumstances for Revocation

Certificates must be revoked under the following three circumstances:

(1) In the event of proven or suspected compromise of the subscriber private key (private key IC card in possession), the subscriber shall immediately notify the CA (not required for test assurance level certificates) so the unexpired public key certificates corresponding to that private key may be revoked.

(2) In the event of proven compromise of the CA private key, the unexpired cross certificate issued to the CA must be revoked.

(3) If certificate subject information or attribute modification (such as subject name modification, subject registration number or code change, subject identity disappearance due to disbandment or death) which is sufficient to affect the accuracy of recorded information, then the unexpired certificate(s) with that certificate subject must be revoked.

In addition to the above circumstances which require certificate revocation, the subscriber may submit a certificate revocation request within the certificate validity period for other reasons.

If a CA or RA proves that a subscriber has violated the subscriber obligations in the CP or CPS, the CA may revoke that subscriber's certificate.

If a CA proves or suspects that their private key has been compromised, the CA may revoke all certificates issued by that private key.

If an upper level CA proves that a lower level CA has violated the CP or CPS, the upper level CA may revoke the certificates of that lower level CA.

If a CA proves that its cross-certified CA has violated the CP or its CPS, the CA may revoke the cross certificates of that CA.

If the Policy Management Committee decides that an eCA self-signed certificate or self-issued certificate must be revoked (such as suspect eCA private key compromise), the Policy Management Committee may revoke the eCA self-signed certificate and self-issued certificate.

4.9.2 Who Can Request Revocation

If certificate revocation or other circumstances occur as stipulated in section 4.9.1, subscribers or entities possessing a private key may submit a certificate revocation request to the CA or RAwithin the certificate validity period.

A CA may revoke subscriber, subordinate CA or subject CA certificate in accordance with the regulations in section 4.9.1.

4.9.3 Procedure for Certificate Revocation

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

If the certificate revocation request has been approved or a decision has been made to revoke the certificate, the CA or RA shall assign suitable personnel to perform the certificate revocation-related tasks in accordance with the regulations in section 5.2 and the CPS. The CA or RA shall notify the subscriber in a suitable manner after certificate revocation. CAs operating at assurance levels 1, 2, 3 and 4 shall state the subscriber notification method after certificate revocation in the CPS.

If the certificate revocation is not approved, the CA or RA shall notify the subscriber in a suitable manner and clearly inform the subscriber of the reasons for denying the revocation request. CAs operating at assurance levels 1, 2, 3 and 4 shall state the subscriber notification method for denial of certificate revocation in the CPS.

4.9.4 Certificate Revocation Request Grace Period

If it is necessary for a subscriber or CA to revoke a certificate, the subscriber or CA shall promptly submit the request to the CA who issued the certificate.

The for certificate revocation request grace period is the time that must be given to submit certificate revocation request after the subscriber has confirmed the certificate revocation event. The CA and RA must report the suspect CA or RA private key compromise event within one hour to the CA issuing the certificate. If there is a private key that is lost or suspected or confirmed to be compromised or the information recorded on the certificate is expired and inaccurate, the subscriber shall promptly submit a certificate revocation request. If necessary, the CA may extend the certificate revocation request grace period on a case by case basis.

4.9.5 Time Period for CA to Process Certificate Revocation Request

Except for assurance level 4, CAs shall complete the certificate revocation work within one working day after receiving the certificate revocation request.

4.9.6 Certificate Revocation Checking Requirements for Relying Parties

Relying parties using assurance level 2, 3 and 4 shall check the current CARL and CRL or use the OCSP service to check the current certificate status prior to certificate use. The authenticity and integrity of the CARL and CRL must also be verified. Relying parties must take into consideration the risk, responsibility and possible effects to determine independently the interval length for obtaining new certificate revocation information. See the regulations in section 9.6.4 for related obligations.

4.9.7 CARL and CRL Issuance Frequency

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

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

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

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

Assurance Level	**CARL Issuance Frequency**	**CRL Issuance Frequency**
Test level	Not applicable	Not stipulated
Level 1	Not applicable	Not stipulated
Level 2	Not applicable	At least once every 3 days
Level 3	At least once a day	At least once a day
Level 4	At least once a day	At least once a day

4.9.8 Maximum Latency for CARLs and CRLs

Given that Internet service is provided normally, the CA shall announce the CARL and CRL before the nextUpdate recorded on the CARL or CRL at the latest.

4.9.9 On-Line Certificate Status Protocol Checking Service

In addition to providing CARL and CRL services, the CA may selectively provide OCSP service to relying parties. The on-line certificate status inquiry services provided by the CA must conform to IETF RFC 2560 or IETF RFC 6960 guidelines and the freshness of the

certificate status information provided must be at least equivalent to the freshness of the CARL and CRL. In other words, thisUpdate of the certificate status response must at least be equivalent to thisUpdate of the latest CARL or CRL. If on-line certificate status inquiry provided by the CA is used, the subscriber does not need to obtain or process the CARL or CRL announced by that CA. The CA shall list whether or not OCSP services are provided in the CPS.

4.9.10 On-Line Certificate Status Checking Rules

For relying parties that use assurance level 2, 3 and 4 certificates, if the CRL and CARL are not checked, the on-line certificate status checking methods must be used to perform on-line certificate status checking.

4.9.11 Other Forms of Revocation Advertising

Not stipulated

4.9.12 Other Special Requirementss during Key Compromise

Follow the related regulations in sections 4.9.1, 4.9.2 and 4.9.3 in the event of the key compromise.

4.9.13 Circumstances for Certificate Suspension

CAs that provide certificate suspension service shall state the circumstances for certificate suspension in the CPS.

4.9.14 Who Can Request Suspension

CAs that provide certificate suspension services shall state who is allowed to request certificate suspension in the CPS.

4.9.15 Procedure for Certificate Suspension

CAs that provide certificate suspension service shall state the procedure for certificate resumption in the CPS.

4.9.16 Processing Time and Suspension Period for Suspended Certificates

CAs that provide certificate suspension service shall state the processing time and suspension period for certificate suspension requests by subscribers in the CPS.

4.9.17 Procedure for Certificate Resumption

CAs that provide certificate suspension service shall state the certificate resumption procedure in the CPS.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

CAs shall provide CRL or OCSP service or both to provide certificate status service.

4.10.2 Service Availability

CAs shall provide 24*7 uninterrupted certificate status service.

4.10.3 Available Functions

Not stipulated

4.11 Service Termination

Service termination is the termination of CA services to certificate subscribers including termination of CA services to subscribers when certificate expires and termination of services when subscriber certificate is revoked.

CAs may allow subscribers to terminatetheir purchase of certificate services when services are terminated due to certificate revocation, expiry of unrenewed certificates or invalidation of subscriber 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 Practices

CAs which support session key encapsulation and recovery shall describes their practices in the CPS.

5. Non-Technical Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

There are no requirements for CAs operating under test level or assurance level 1. The site location and construction requirements for CAs operating under assurance level 2 or above must comply with facility standards for the housing of highly important and sensitive information and other physical security protection system including access control, security, intrusion detection and video monitoring to prevent unauthorized access to related CA equipment.

5.1.2 Physical Access

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

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

The physical access control requirements for CAs operating at assurance levels 1 and 2 are:

(1) Protect against unauthorized intrusion.

(2) Ensure that portable storage media containing sensitive information and documents are kept in a safe location.

The physical access control requirements for CAs operating at assurance levels 3 and 4 are:

(1) Set up a round-the-clock manual or electronic monitoring equipment to prevent unauthorized intrusion.

(2) Routine maintenance and examination of access log files.

At least two people must jointly conduct physical access control of computer systems and password modules.

Since the eCA must issue certificates at all assurance levels, the security system for the equipment environment must be in compliance with assurance level 4 physical access control regulations. There are no requirements for physical access control of CAs operating at test level or assurance level 1 but they must be specified in the CPS.

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

(1) Appropriate security is provided for security cabinets.

(2) Physical security systems (such as door locks and entry and exit access) are working properly.

5.1.3 Electrical Power and Air Conditioning

There are no requirements for CAs operating under test level or assurance level 1. There must be sufficient electrical power and air conditioning backup equipment to support CA related systems which can operate or shut down normally when affected by external factors for CAs

operating under assurance level 2 or above. UPS must also be provided which can provide at least 6 hours of backup power for repository backup data (including issued certificates and CRL).

5.1.4 Flood Prevention and Protection

The CA site must be in location that is safe from flood damage.

5.1.5 Fire Prevention and Protection

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

5.1.6 Media Storage

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

5.1.7 Waste Disposal

Not stipulated

5.1.8 Off-Site Backup

The CA shall state whether off-site backup is required or not, the distance of the backup site from the eCA facilities and the backup items in the CPS.

5.2 Procedural Controls

5.2.1 Trusted Roles

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

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

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

Trusted roles are defined as follows:

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

(2) Officer: Issues and revokes of certificates.

(3) Auditor: Checks and maintains audit logs.

(4) Operator: Performs system backup and troubleshooting.

5.2.1.1 Administrator

The administrator is principally responsible for:

(1) Installation, setting and maintenance of CA related systems.

(2) Establishment and maintenance of system subscriber accounts.

(3) Setting audit parameters.

(4) Generation and backup of CA keys.

5.2.1.2 Officer

The officer is principally responsible for:

(1) Registering new certificate subscribers and acceptance of certificate issuance requests.

(2) Checking authenticity of certificate subscriber identity and correctness of certificate information.

(3) Reviewing and performing certificate issuance.

(4) Accepting, reviewing and processing of certificate revocation requests.

5.2.1.3 Auditor

The auditor is principally responsible for:

(1) Checking, maintainance and archiving of audit logs.

(2) Conducting or supervising internal audits to ensure that the CA is in compliance with CPS regulations.

5.2.1.4 Operator

The operator is principally responsible for:

(1) Physical security controls for the system (such as facility access management, fire and flood prevention and air conditioning system).

(2) Daily operation and maintenance of the system equipment.

(3) System backup and restoration work.

(4) Storage media update.

(5) System software and hardware update.

(6) Network and website maintenance: Establish system security and anti-virus protection systems and network security event detection and reporting.

5.2.2 Role Assignments

The role assignment guidelines for the certification authority are as follows:

Assurance Level	Role Assignment Guidelines
Test level	Not stipulated
Level 1	Not stipulated
Level 2	Four trusted roles as specified in section 5.2.1. One person is allowed to perform more than one role but the roles of officer and administration may not be concurrently held by the same person.
Level 3	Four trusted roles as specified in section 5.2.1. One person is allowed to perform more than one role but the officer may not concurrently hold the roles of administrator and auditor.
Level 4	Four trusted roles as specified in section 5.2.1. Personnel and role assignments must comply with the following regulations: (1) Only one person may serve the role of administrator, officer or auditor but may concurrently hold the role of operator. (2) A person who serving a trusted role is not allowed to perform self-audits.

5.2.3 Number of Persons Required per Task

In order to optimize the security of CA equipment and operations, personnel role assignment must follow the regulations in section 5.2.2. The number of persons required per task shall be detailed in the CPS.

5.2.4 Identification and Authentication for Each Role

Not required for CAs operating under test level and assurance level 1. The personnel for CAs operating under assurance level 2 or above must undergo identification and authentication before performing the tasks for the role assigned.

5.3 Personnel Controls

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

(1) Documented work assignments.

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

(3) Receive relevant training for tasks.

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

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

5.3.1 Background, Qualifications, Experiences and Security

Requirements

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

5.3.2 Background Check Procedures

Background check procedures shall be stated in the CPS.

5.3.3 Instruction and Training Requirements

CA related personnel shall receive the following instruction and training:

(1) CA and RA security certification system.

(2) CA system use of PKI software.

(3) Responsibility to perform PKI work.

(4) Procedures for disaster restoration and sustainable operations.

5.3.4 Personnel Retraining Requirements and Frequency

CA personnel shall be familiar with CA-related work procedures and changes in laws and regulations. In the event of any major changes such as software / hardware upgrades, work procedure changes or equipment replacement, CA personnel shall receive instruction and training and the training records shall be kept.

New personnel shall also receive the respective instruction and training and also receive annual training based at the CA depending on their training status.

5.3.5 Job Retraining Frequency and Sequence

Not stipulated.

5.3.6 Sanctions for Unauthorized Actions

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

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

5.3.7 Contract Personnel Rules

Contract personnel who perform CA-related jobs shall comply with the CA's CPS regulations.

5.3.8 Documentation Supplied to Personnel

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

5.4 Security Audit Procedure

CAs operating at test assurance level do not have to possess audit functions. CAs that issue other assurance level certificates shall possess appropriate audit log functions for related security events. Security audit logs shall be automatically generated by the system whenever possible. If not possible, records may be made in work logbooks, paper form or other physical form. All security logs, both electronic and non-electronic, shall

be retained and made available during compliance audits. The security audit logs shall be maintained in accordance with the retention period for the archive stated in section 5.5.2.

5.4.1 Types of Events Recorded

Security audit functions of CA shall include security audits of the certificate administration system and the computer operating system upon which the certificate administration system depends. The following items should be included in each audit entity (either automatically or manually recorded audit events):

(1) Type of event

(2) Entity that caused the event and operator identity

(3) Location or site of the event

(4) Time and date of event occurrence

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

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

Auditable Event／ Assurance Level	**Level 1**	**Level 2**	**Level 3**	**Level 4**
A. Security Audit				

Auditable Event／ Assurance Level	Level 1	Level 2	Level 3	Level 4
A.1.1 Any changes to the audit parameters e.g. audit frequency, type of event audit and new / old parameter contents		✓	✓	✓
A.1.2 Any attempt to delete or modify the audit logs.		✓	✓	✓
A.2 Identification and Authentication				
A.2.1 Successful and unsuccessful attempts to assume a role		✓	✓	✓
A.2.2 Change in the value of maximum authentication attempts		✓	✓	✓
A.2.3 Maximum number of unsuccessful authentication attempts when subscriber logs into the system		✓	✓	✓
A.2.4 An administrator unlocks an account that has been locked as a result of a number of unsuccessful authentication attempts		✓	✓	✓
A.2.5 An administrator changes the type of authenticator, e.g. from password to biometrics		✓	✓	✓
A.3 Key Generator				
A.3.1 When the CA generates a key (does not apply for single session or single use key generation)	✓	✓	✓	✓
A.4 Private Key Load and Storage				

Auditable Event／ Assurance Level	Level 1	Level 2	Level 3	Level 4
A.4.1 Loadng of component private key	✓	✓	✓	✓
A.4.2 All key recovery works and the access of the certificate subject private keys stored in the CA	✓	✓	✓	✓
A.5 Trusted Public Key Entry, Deletion and Storage				
A.5.1 All changes to the trusted public keys, including additions and deletions	✓	✓	✓	✓
A.6 Private Key Export				
A.6.1 The export of private keys (keys used for a single session or use are excluded)	✓	✓	✓	✓
A.7 Certificate Registration				
A.7.1 All certificate registration requests and processes	✓	✓	✓	✓
A.8 Certificate Revocation				
A.8.1 All certificate revocation requests and processes		✓	✓	✓
A.9 Certificate Status Change Approval				
A.9.1 The approval or rejection of a certificate status change request		✓	✓	✓
A.10 CA Configuration				
A.10.1 Any security-relevant changes to the configuration of the CA		✓	✓	✓

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

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

Auditable Event／ Assurance Level	Level 1	Level 2	Level 3	Level 4
A.15.3 Operating system		✓	✓	✓
A.15.4 Patches		✓	✓	✓
A.15.5 Security profiles			✓	✓
A.16 Physical Access / Site Security				
A.16.1 Personnel access to the CA facility			✓	✓
A.16.2 Access to the CA server			✓	✓
A.16.3 Known or suspected violations of physical security		✓	✓	✓
A.17 Anomalies				
A.17.1 Software errors		✓	✓	✓
A.17.2 Software check integrity failures		✓	✓	✓
A.17.3 Receipt of improper messages			✓	✓
A.17.4 Misrouted messages			✓	✓
A.17.5 Network attacks (suspected or confirmed)		✓	✓	✓
A.17.6 Equipment failure	✓	✓	✓	✓
A.17.7 Electrical power outages			✓	✓
A.17.8 Uninterrupted power system (UPS) failure			✓	✓
A.17.9 Obvious and significant network service or access failure			✓	✓
A.17.10 Violations of Certificate	✓	✓	✓	✓

Auditable Event／ Assurance Level	Level 1	Level 2	Level 3	Level 4
Policy				
A.17.11 Violations of Certification Practice Statement	✓	✓	✓	✓
A.17.12 Resetting operating system clock		✓	✓	✓

5.4.2 Frequency of Log Processing

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

Assurance Level	Frequency of Log Processing
Test level	Not stipulated
Level 1	Not stipulated
Level 2	Not stipulated
Level 3	At least once every two months Major security audit logs are reviewed by the CA after the previous audit review and further investigations shall be made of any possible malicious activities.
Level 4	At least once a month Major security audit logs are reviewed by the CA after the previous audit review and further investigations shall be made of any possible malicious activities.

5.4.3 Retention Period for Audit Log

The retention periods for security audit logs of CAs operating under assurance level 1 or test level are not stipulated.

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

When the retention period for the audit log ends, the information requiring removal is removed by the auditor. Other personnel may not perform this task.

5.4.4 Protection of Audit Log Files

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

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

5.4.5 Audit Log Backup Procedures

Assurance Level	Audit Log Backup Procedure
Test level	Not specified
Level 1	
Level 2	Backup of audit log files must be done at least once a month.
Level 3	

Level 4	Backup of audit log files must be done at least once a month. Off-site backup must be done at least once a month. Related off-site backup procedures shall be specified in the CPS.

5.4.6 Security Audit System

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

5.4.7 Notification of Event-Causing Subject

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

5.4.8 Vulnerbility Assessments

CAs operating under assurance levels 3 and 4 shall conduct routine security control vulnerability assessments. There is no vulnerability assessment requirement for CAs operating under test level or assurance levels 1 and 2.

For vulnerability assessment and penetration testing methods and frequency, CAs that issue SSL certificates shall conform to the requirements defined in 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.

5.5 Records Archival Methods

5.5.1 Types of Recorded Events

The following records shall be archived (not required for CAs operating under the test assurance level) based upon the security requirements of various assurance levels.

Archived Information / Assurance Level	Level 1	Level 2	Level 3	Level 4
CA accreditation information (presumed use)	✓	✓	✓	✓
Certification Practice Statement	✓	✓	✓	✓
Major contracts	✓	✓	✓	✓
System and equipment configuration	✓	✓	✓	✓
Modifications and updates to systems or configurations	✓	✓	✓	✓
Certificate application data	✓	✓	✓	✓
Revocation request data		✓	✓	✓
Subscriber identity data specified in section 3.2.3		✓	✓	✓
Document receipt and certificate acceptance		✓	✓	✓
Token activation log		✓	✓	✓
Issued or published certificates	✓	✓	✓	✓
CA rekey records	✓	✓	✓	✓

Archived Information / Assurance Level	Level 1	Level 2	Level 3	Level 4
Issued and/or published CARLs / CRLs		✓	✓	✓
Audit logs	✓	✓	✓	✓
Other information or applications used to verify or substantiate archive contents		✓	✓	✓
Document requests of audit personnel		✓	✓	✓

5.5.2 Retention Period for Archive

The minimum retention period for archive information is as follows:

Assurance Level	Minimum Retention Period
Test level	Not specified
Level 1	Not specified
Level 2	5 years
Level 3	10 years
Level 4	20 years

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

5.5.3 Protection of Archive

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

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

5.5.4 Archive Backup Procedures

Not specified

5.5.5 Requirements for Record Timestamping

Not specified

5.5.6 Archive Information Collection System

Not specified

5.5.7 Procedures to Obtain and Verify Archive Information

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

5.6 Key Changeover

5.6.1 CA Key Changeover

CA private keys shall be regularly renewed in accordance with the regulations in section 6.3.2 so new private keys can be used to issue certificates in place of the old keys and all entities that rely on that CA certificate shall be notified at appropriate times. The old private key may still be used to issue CRL or on-lne certificate status responses to

maintain and protect all subscriber certificates issued with the old private key until they expire.

If the CA's own certificate is revoked, use of the private key is stopped and the key must be renewed.

eCA shall renew the key pair used to issue certificates before the usage period of the certificate issued with that private key expires at the latest and issue one new self-signed certificate and one self-issued issued mutually with the old and new private keys. The issuance procedure for these three new certificates is handled in accordance with the regulations in section 4.2.

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

For root CA cross-certified with the eCA outside the ePKI, thee key renewal time is independently determined by that CA in accordance with the CP. Whether or not that CA needs to continue to apply for cross-certification with the eCA after key renewal is determined by negotiations or contract between that CA and the Company. If that CA wants to continue to apply for cross-certification with the eCA after key renewal, it is handled in accordance with the regulations in section 4.2 and a sufficient amount of time is reserved to allow the Policy Management Committee and the eCA to process the cross-certifcation

application to ensure that the eCA is able to issue and announce the new cross certificate for that CA before that CA's certificate expires.

5.6.2 Subscriber Key Changeover

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

After a subscriber certificate is revoked, use of its private key is stopped. After key pair changeover, follow the regulations in section 4.1 to apply for a new certificate with the CA or RA.

For subscribers with assurance level 2, 3 and 4 certificates that have not been revoked, the CA or RA may start to accept rekey and new certificate applications one month before that subscriber public key expires. New certificate applications are handled in accordance with the regulations in section 4.1.

5.7 Key Compromise and Disaster Recovery Procedures

CA`s post-disaster recovery work shall prioritize repository restoration to allow normal provision of certificate status information.

5.7.1 Emergency and System Compromise Handling Procedure

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

5.7.2 Computer Resources, Software or Data Corruption Recovery Procedures

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

capabilities.

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

5.7.3 CA Signature Key Compromise Restoration Procedure

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

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

5.7.4 CA Security Facilities Post-Disaster Recovery

CAs operating at assurance levels 2, 3 and 4 shall state the steps to be followed to reestablish CA security facilities after natural and other disasters in the CPS or related documentation.

CAs operating at assurance levels 3 and 4 shall conduct one post-disaster recovery plan drill at least once a year.

5.7.5 CA Signature Key Certificate Revocation Restoration Procedure

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

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

5.8 CA or RA Termination of Services

CA termination of services shall be performed in accordance with relevant regulations in the Electronic Signatures Act.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

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

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

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

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

Any random numbers generated by a key must be approved by Chunghwa Telecom. The related regulations for subscriber random

number, key pair and symmetric key generation and the hardware and software used are listed in the Table below:

Assurance Level	Key Generation Mechanism
Test level	Software or hardware
Level 1	Software or hardware
Level 2	Software or hardware
Level 3	Software or hardware
Level 4	Limited to hardware

6.1.2Private Key Delivery to Subscriber

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

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

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

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

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

6.1.3 Public Key Delivery to Certificate Issuer

When a CA performs identity authentication on a subscriber, the subscriber must deliver the public key to the CA. Delivery methods include:

(1) Certificate application electronic message issued on their behalf by RA.

(2) When keys are generated by a third party, CA or RA must obtain the subscriber's public key through auditable secure channels.

(3) Completion through other secure electronic systems.

(4) Completion through secure non-electronic methods including (but not limited to) delivery of floppy disc (or other storage media) by registered or express mail.

6.1.4 CA Public Key Delivery to Relying Parties

eCA public key must be available at all times. Subordinate CAs must deliver an eCA self-issued certificate or public key to subscriber in a reliable manner. Reliable certificate delivery methods include the

following:

(1) The CA stores the eCA self-signed certificate or public key in a token and delivers it to the relying party in a secure fashion.

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

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

(4) Downloading of an eCA self-signed certificate or public key from a website with an equivalent or higher assurance level.

(5) Other methods approved by the Policy Management Committee.

The above out-of-band channels shall be stated in the CPS.

eCA issued subordinate CA certificates must be published in the CA repository.

6.1.5 Key Sizes

Assurance Level	**Public Key**
Test level	Must use 1024-bit RSA keys or other types of keys with equivalent security strength until 12/31/2013.
Level 1	
Level 2	Must use 2048-bit RSA keys or other types of keys with

Assurance Level	Public Key
Level 3	equivalent security strength until 12/31/2030. Should use 3072-bit RSA keys or other types of keys with equivalent security strength after 12/31/2030.
Level 4	Must at least use 4096-bit RSA keys or other types of keys with equivalent security strength.

6.1.6 Public Key Parameters Generation and Quality Checking

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

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

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

6.1.7 Key Usage Purposes

The public key certified in the certificates must state the key usage (signature and encryption) in the keyUsage extension in the ITU-T X.509 certificate. Certificates used for digital signatures (including authentication) shall set the digitalSignature bit. Certificates used for encryption shall set the keyEncipherment or dataEncipherment bit. CA certificates shall have two key usage bit sets: cRLSign and keyCertSign.

A single key for encryption and signature may be used test level and level 1, 2 and 3 certificates to support some old version Secure Multipurpose Internet Mail Extensions (S/MIME) application software. Unless stated otherwise in the CP, this type of dual-use certificate must

be generated and administered in accordance with signature certificate regulations. The Non-Repudiation Key Usage bit may not be set. It also may not be used for verification of signatures on important information. Subordinate CA at any assurance level shall issue two key pairs to subscribers: one for information encryption and one for digital signatures and identify authentication.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The Policy Management Committee shall determine the cryptographic module certification standard for the ePKI. The security requirement of the cryptographic module is in compliance with US FIPS 140-2 series or an equivalent security strength standard. The cryptographic modules used by CAs to issue certificates shall pass the following security certification standards.

Each entity in the ePKI, except for subscribers, must comply as best as possible with these requirements. The remaining entities shall use the requirements in the table below as the minimum requirements for cryptographic modules but may use an even higher security level. The levels listed in this table are defined in the FIPS 140-2 series.

Entity \ Assurance Level	**eCA**	**Subordinate CA**	**RA**	**Subscriber**
Test level	Not applicable	Not stipulated	Not stipulated	Not stipulated
Level 1	Not applicable	Level 1 (hardware or software)	Level 1 (hardware or software)	Not stipulated

Level 2	Not applicable	Level 2 (hardware or software)	Level 1 (hardware or software)	Level 1 (hardware or software)
Level 3	Not applicable	Level 2 (hardware)	Level 2 (hardware)	Level 1 (hardware or software)
Level 4	Level 3 (hardware)	Level 3 (hardware)	Level 2 (hardware)	Level 2 (hardware)

6.2.2 Private Key (n out of m) Multi-Person Control—RFC3647)

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

6.2.3 Private Key Escrow

Signature private keys may not be escrowed.

6.2.4 Private Key Backup

6.2.4.1 CA Signature Private Key Backup

For CAs operating at assurance level 3 and 4, backups of their signature private keys shall be done in accordance with multi-person control procedures and stored at the backup site. Key backup procedures must be stated in the CPS.

6.2.4.2 Subscriber Signature Private Key Backup

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

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

6.2.5 Private Key Archival

Archival is not allowed for signature private keys.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

Follow the key generation regulations in section 6.1.1. The eCA and RA shall not allow its private keys to be stored in plain text outside the hardware cryptographic module. The private key is only imported into the cryptographic module during eCA or RA key backup recovery or cryptographic module replacement and the multi-person control method shall be followed in section 6.2.2 when importing private keys into the cryptographic module. Encryption or key splitting may be used as the private key importation method to ensure that the private key plain text is not exposed outside the cryptographic module and guarantee that the encryption key is not disclosed. After the private key input is completed, the related secret parameters generated during the importation process shall be completely destroyed.

6.2.7 Private Key Storage on Cryptographic Module

Follow the regulations in sections 6.1.1 and 6.2.1.

6.2.8 Method of Activating Private Key

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

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

6.2.9 Method of Deactivating Private Key

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

6.2.10 Method of Destroying Private Key

When a signature private key and its backup is no longer needed or the certificate has expired and been revoked, the signature private key must be destroyed. For software encryption modules, the information is copied to the memory or storage medium which was originally occupied by the signature private key. For hardware encryption modules, the zeroization action must be performed but physical destruction does not have been done.

6.2.11 Cryptographic Module Rating

See section 6.2.1.

6.3 Other Aspects of Key Pair Management

It is recommended that two types of key pairs be issued for certificates given to subscribers regardless of the assurance level unless the old version of the application system complies with the regulations in section 6.1.7 even though it is technically feasible for a single key pair to be concurrently used for signature and encryption. One type is used for data encryption and the other type is used for digital signature and identity authentication.

Escrowal, archival or backup of signature and identity authentication private keys used by subscribers absolutely may not be done. The CA belonging to the subscriber may request encryption of the private key for escrowal, archival or backup tasks.

6.3.1 Public Key Archival

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

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

6.3.2.1 Operational Periods for CA Public and Private Keys

The usage period of CA public and private keys varies depending on the key strength level as follows:

(1) RSA 4096 bit or other types of public key pairs with equivalent security strength: The validity period of the public and private keys is 30 years at most. However, the usage period of private key issued certificates may not exceed 15 years.

(2) RSA 3072 bit or other types of public key pairs with equivalent security strength: The validity period of the public and private keys is 30 years at most. However, the usage period of private key issued certificates may not exceed 15 years.

(3) RSA 2048 bit or other types of public key pairs with equivalent security strength: The validity period of the public and private keys is 20 years at most. However, the usage period of private key issued certificates may not exceed 10 years.

The above 3 types of conditions but CA signature private keys used to issue CARL or CRL, OCSP service server certificates or OCSP service response messages are not subject to the above usage period restrictions

for private key-issued certificates and may be used until the subordinate CA certificate (if the CA is a root CA) or CA issued subscriber certificate expires.

eCA self-signed certificate lifecycle periods do not exceed 30 years.

The sum of the certificate lifecycles of certificates issued by the eCA to the subordinate CA plus the signature private key lifecycle used by the eCA to sign certificates may not exceed the eCA self-signed certificate lifespan.

The two self-issued certificates issued by the eCA in response to its signature key renewal, their certificate lifecycle period may not exceed the validity period of the old self-signed certificate.

6.3.2.2 Operational Periods for Subscriber Public and Private Keys

The usage periods for subscriber keys are determined based on key length. If the key has security strength equivalent to RSA 1024 bits, the usage period for private keys is at most five years. In principle, the usage period may extend to December 31, 2013 at the latest. If the key has security strength equivalent to RSA 2048 bits, the usage period for private keys is at most 10 years. The total validity period for certificates (including extensions) is at most the same as the key usage period. Use of RSA 1024 bit SSL certificates is prohibited after December 31, 2013 and must be revoked.

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 v.1.2.1 regulations, certificate authorities will no longer use the SHA-1 Hash Function Algorithm to issue any new subscriber certificates or subordinate CA

certificates starting from January 1, 2016. CAs can still use the SHA-1 Hash Function Algorithm to issue OCSP response message certificates (use SHA-1 Hash Function Algorithm to issue OSCP server certificates) until January 1, 2017. CAs can continue to use currently existing SHA-1 root CA certificates or cross certificates. SHA-2 SSL certificates shall not be issued with the corresponding signature private keys of the SHA-1 subordinate CA certificate. Starting from January 16, 2015, CAs should not use SHA-1 Hash Function Algorithm to issue SSL or code signing certificates with a certificate expiry date later than January 1, 2017 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.

CAs shall adopt related measures to ensure that the subscribers choose appropriate application software and phase out SHA-1 certificates.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

CA or certificate subscriber private key activation data and other related access control systems shall be adequately protected. For CAs operating at assurance levels 1, 2 and 3, activation data is selected by subscriber themselves. For CAs operating at assurance level 4, the CA must be able to accept subscriber biometric data or enhanced security systems from the cryptographic module. If the activation data must be delivered, it should be delivered via proper secure channels.

6.4.2 Activation Data Protection

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

6.4.3 Other Aspects of Activation Data

Not stipulated

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

CAs operating at assurance levels 3 and 4 and its other related auxiliary systems shall include the follow functions. These company security functions may be provided by an operating system or a combination of operating system, software and physical protection measures.

(1) Identity authentication login.

(2) Provide discretionary access control.

(3) Provide security audit capability.

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

(5) There are ePKI trusted role and identity identification and authentication.

(6) Ensure the security of each communication and database through cryptographic technology.

(7) Offer secure and reliable channels for ePKI trusted roles and related identity identification.

(8) Process integrity and security control protection.

CA equipment must be established on work platforms which have undergone a security assessment and the CA-related systems (hardware, software, operating system) must be operated with configurations which have undergone a security assessment.

6.5.2 Computer Security Rating

Not stipulated

6.6 Lifecycle Technical Controls

6.6.1 System Development Controls

CA system development controls are as follows:

Assurance Level	System Development Controls
Test level	Not stipulated
Level 1	Not stipulated
Level 2 Level 3 Level 4	(1) The software used by CAs shall be developed with good software engineering development methods such as the Capability Maturity Model (CMM). (2) Must prevent installation of malicious software in CA equipment. Only components authorized by security policy may be used for CA operations. (3) For RA hardware and software, check for malicious code at initial use and perform routine scanning regularly. (4) System development environment and test environment shall be separated from the on-line environment. (5) System development departments shall exercise the due care of a good administrator such as the signing of certificates of security compliance to ensure that there are no back doors or malicious programs, provision of program or hardware handover lists, test reports and administration manuals, version control and certificate management centers.

6.6.2 Security Management Controls

Assurance Level	Security Management Controls
Test level	(1) CAs may not install or operate other unrelated systems (including hardware devices, network connections and component software). (2) Must record and control CA-related system configurations, any revisions and function upgrades and be able to detect unauthorized modifications of CA software or configuration systems. Must check if software is the correct and unmodified version provided by the supplier when the CA installs the software for the first time.
Level 1	
Level 2	
Level 3	

Level 4	(1) CA hardware and software must be dedicated and may not be installed and operated on other unrelated application systems (including hardware devives, network connections and component software). (2) Must record and control CA-related system configurations, any revisions and function upgrades and be able to detect unauthorized modifications of CA software or configuration systems. (3) Must check if software is the correct and unmodified version provided by the supplier when the CA installs the software for the first time. (4) CA must check CA software integrity at least once a month. (5) Complies with the security measures in AICPA/CPA Trust Service Principles and Criteria for Certification Authorities regulations.

6.6.3 Life Cycle Security Controls

CAs shall disclose the key lifecycle security rating frequency in the CPS.

6.7 Network Security Controls

The eCA servers are not connected to external networks. The repository is connected to the Internet to provide uninterrupted services (except during required maintenance or backup). The certificates and CARLs issued by the eCA servers are manually delivered from the eCA server physically segregated from the external Internet to the repository

and all information (certificates and CARLs) have digital signature protection. The eCA repository protects against denial of service and intrusion attacks by system patch updates, system vulnerability scanning, intrusion detection system firewall systems and filtering routers.

6.8 Timestamping

The eCA 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) CARL/CRL issuance times.

(4) System event occurrence times.

CA clock synchronizations are auditable events.

7. Certificate, CRL and OCSP Service Profiles

7.1 Certificate Profile

7.1.1 Version Numbers

CAs must sign ITU-T X.509 v3 version certificates. The Version Numbers field value is 3.

7.1.2 Certificate Extensions

eCA and subordinate CA issued certificates shall conform to the requirements defined in the latest versions of ITU-T X.509, CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates amd IETF PKIX Working Group 5280 or other related standards. If it is necessary to use a private extension, it shall be stated in the CPS. It shall also be stated which belong to critical private extensions. It must be able to achieve interoperability with its community in application services.

7.1.3 Algorithm Object Identifiers

eCA subordinate CA issued certificates shall use the following algorithm object identifiers (OID) during signing:

sha-1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12}
sha512WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13}

eCA subordinate CA issued certificates shall use the following OID to identify and generate subject key algorithm:

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

7.1.4 Name Forms

eCA subordinate CA issued certificate subject and issuer field values shall use a ITU-T X.500 distinguished name. This name attribute type shall conform to the requirements defined in the latest versions of ITU-T X.509, CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, IETF PKIX Working Group RFC 5280.

7.1.5 Name Constraints

Not stipulated

7.1.6 Certificate Policy Object Identifier

eCA subordinate CA issued certificates shall use certificate policy object identifier. In addition, the CP OID shall conform to the certificate assurance level.

7.1.7 Usage of Policy Constraint Extension

Not stipulated

7.1.8 Policy Qualifiers Syntax and Semantics

eCA subordinate CA issued certificates may not include policy qualifiers.

7.1.9 Processing Semantics for Critical Certificate Policies Extension

The processing semantics for critical certificate policies extension used for eCA subordinate CA issued certificates shall conform to the requirements in the latest versions of ITU-T X.509, CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, IETF PKIX Working Group RFC 5280.

7.2 CARL and CRL Profiles

7.2.1 Version Numbers

eCA issued CARL and eCA subordinate CA issued CRL shall comply with ITU-T X.509 v2 standards.

7.2.2 CARL and CRL Extension

For CA CARL / CRL profiles inside the ePKI, each extension field shall conform to the requirements defined in the latest versions of 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.

7.3 OCSP Service Profile

If OCSP services are provided, the CA shall disclose the OCSP service version number and standards used for the extension fields.

7.3.1 Version Numbers

CA OCSP services shall comply with IETF PKIX Working Group RFC 5019 / RFC 6960 standards and guidelines.

7.3.2 OCSP Service Extensions

The extensions for OCSP services provided by CA shall comply with the requirements in the latest versions of ITU-T X.509, CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, and IETF PKIX Working Group RFC 5019 / RFC 6960.

8. Compliance Audit Methods

CAs that issue assurance level 2, 3 and 4 certificates shall establish an impartial compliance audit system to ensure that their operations comply with CPS and CP regulations.

8.1 Frequency of Audits

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

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

8.2 Identity / Qualification of Audit Personnel

Audit personnel shall be independent from the audited CA and may be performed by the following entities:

(1) Impartial third party personnel.

(2) Independent entity separate in organization division from the audited CA.

Audit personnel shall submit an impartial and independent assessment. The Company retains auditors familiar with CA operations and Trust Service Principles and Criteria for Certification Authorities Version 2.0 authorized for practice in the ROC by the WebTrust for CA

seal management authorities to provide impartial and objective audit services. Audit personnel shall have Certified Information System Audit (CISA) or equivalent qualifications and and shall at least possess the experience of conducting a WebTrust for CA seal audit twice at 4 man-days or the experience of conducting a CA information security management audit twice at 8 man-days and be familiar with CA certificate issuance and administration regulations. CAs shall conduct identity identification of audit personnel during audits.

8.3 Audit Personnel Relationship to Audited Party

Audit personnel shall be independent of the audited CA in accordance with section 8.2 regulations.

8.4 Scope of Audit

The scope of audit is stipulated as follows:

(1) Whether or not CA operations comply with the CPS.

(2) Whether or not the CA CPS comply with CP regulations.

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

If a CCA is signed between the CA and its subordinate CA, the scope of the audit shall cover whether or not its subordinate CA is compliant with the regulations in the CCA.

8.5 Actions Taken as a Result of a Deficiency

If the establishment or operation of the CA does not comply with the CP or CCA regulations, audit personnel shall take the following actions:

(1) Audit personnel shall record non-conformities.

(2) Audit personnel shall notify the CA operation and management

department where the non-conformity occurred. If the non-conformity is a serious deficiency, the audit personnel shall also notify the Policy Management Committee.

The CA where the non-conformity occurred shall make improvements based on the audit report and CP / CCA regulations.

8.6 Scope of Audit Result Disclosure

Except for systems where attacks could occur and the scope defined in section 9.3, CAs shall announce the latest audit results relevant to relying parties who rely on the CA.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance and Renewal Fees

Not stipulated

9.1.2 Certificate Access Fees

Not stipulated

9.1.3 Certificate Revocation or Status Information Access Fees

Not stipulated

9.1.4 Fees for Other Services

Not stipulated

9.1.5 Refund Procedure

Not stipulated

9.2 Financial Responsibility

9.2.1 Scope of Insurance Coverage

Not stipulated

9.2.2 Other Assets

Not stipulated

9.2.3 End Entities Liability

End entities (subscriber and relying parties) liability is not

stipulated.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

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

(1) Any personal or organization information provided during the certificate application may not be disclosed without subscriber permission and in accordance with laws and regulations.
(2) The private keys and passwords used for CA operation are deemed confidential information and may not be disclosed.
(3) Audit logs may not be fully disclosed unless under the circumstances specified in section 8.6.

CAs shall state the types of confidential information in CPS.

9.3.2 Information Not Within the Scope of Confidential Information

(1) Certificates, CRLs, revoked and suspended certificates are not deemed confidential information. Certificate revocation and suspension information is non-confidential information and may not be externally disclosed.
(2) Identification information or information recorded on certifications is not deemed confidential information or private information unless specified otherwise.

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

9.3.3 Responsibility to Protect Confidential Information

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

9.4 Privacy of Personal Information

9.4.1 Privacy Protection Plan

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

9.4.2 Types of Private Information

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

9.4.3 Information Not Deemed Private

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

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

9.4.4 Responsibility to Protect Private Information

The personal information required for CA operation shall be securely stored and protected in accordance with the Electronic Signatures Act, Trust Service Principles and Criteria for Certification Authorities standards and relevant regulations of the Personal Information Protection Act. CAs must negotiate private information protection obligations with RAs.

9.4.5 Notice and Consent to Use Private Information

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

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

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

9.4.7 Other Information Disclosure Circumstances

Follow relevant laws and regulations. Regulations regarding provision of confidential information to subscribers stipulated in section

9.3.1 shall be established in the CA CPS.

9.5 Intellectual Property Rights

This CP is the intellectual property of the Company. The CP may be copied and distributed in accordance with the Copyright Act but it must be copied in whole and the copyright noted as being owned by the Company. Fees may not be collected from others for the copying and distribution of the CP. The Company shall prosecute improper use oe distribution of the CP in accordance with the law.

9.6 Legal Obligations

9.6.1 CA Obligations

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

9.6.2 RA Obligations

CAs shall bear all obligations arising from the RA work performed by the RAs acting as an agent on behalf of the CA. The RA obligations shall be determined based on the rights and obligations between the RAs and CAs. CAs shall state RA obligations in the CPS or RA contracts or agreements.

9.6.3 Subscriber Obligations

Subscribers shall bear the following obligations:

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

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

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

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

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

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

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

(8) Correctly use certificates. Only use for legal and authorized use purposes in the CPS and subscriber acceptance clauses including installation only in servers which completely match the domain names recorded in the SSL certificates and no use of private keys corresponding to program code signed certificates to sign malicious software.

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

9.6.4 Relying Parties Obligations

Relying parties using certificates issued by the CA shall bear the following obligations:

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

(2) Use certificates in accordance with certificate usage.

(3) Correctly examine digital signatures.

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

(5) Check key usage recorded on certificates.

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

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

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

9.6.5 Other Participant Obligations

Not specified

9.7 Disclaimer

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

9.8 Limitations of Liability

CAs shall state the limitations of liability in the CPS.

9.9 Compensation

CAs shall state the compensation responsibility to subscribers and

relying parties in the CPS.

9.10 Term and Termination

9.10.1 Term

The CP and any attachments are effective when published on the eCA website and repository and remain in effect until replaced with a newer version.

9.10.2 Termination

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

9.10.3 Effect of Termination and Survival

The conditions and effect of the CP termination shall be communicated via the eCA website and repository. This communication shall emphasize which provisions survive CP termination. At the minimum, the responsibilities related to protecting confidential information shall survive CP 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 listed in section 1.5.2 of the CPS. It is deemed valid only after sender receives a reply slip with a valid digital signature. If the reply slip is not received in 5 days, the comments may be sent in writing by express or registered mail.

9.12 Amendments

9.12.1 Procedure for Amendment

The Policy Management Committee shall examine the CP once a year. CAs shall examine the CPS once a year to maintain its assurance level.

9.12.2 Notification Mechanism and Period

9.12.2.1 Notification Mechanism

The Policy Management Committee and CA shall post those change items that could have a significant impact on subscribers to the eCA and CA repositories. CA shall state the notification mechanism for change items in the CPS.

9.12.2.2 Modification Items

The Policy Management Committee assesses the level on impact of CP change items on subscribers and relying parties:

(1) Significant impact: First post 15 calendar days in eCA repository before making the revision.

(2) Less significant impact: First post 7 calendar days in eCA repository before making the revision.

9.12.2.3 Comment Reply Period

The reply period for those with comments regarding section 9.12.2.2 change items is:

(1) The reply period is within 7 calendar days from announcement date for (1) comments with significant impact in accordance with section 9.12.2.2.

(2) The reply period is within 3 calendar days from announcement date for (2) comments with less significant impact in accordance with section 9.12.2.2.

The CA shall state the comment reply period in the CPS.

9.12.2.4 Comment Handling Mechanism

For comments on CP change items, the reply method posted in the eCA repository is transmitted to the eCA. The eCA shall consider related comments when evaluating the change items.

The CA shall state the comment handling mechanism in the CPS.

9.12.2.5 Final Notification Period

The revisions for the change items announced for the CP shall be made in accordance with sections 9.12.1 and 9.12.2. The notification period shall be at least 15 calendar days in accordance with regulations in 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 use purpose and assurance level stated in the CP, the CP OID does not require revision. Corresponding changes shall be made to the CPS in response to CP OID changes.

9.13 Dispute Resolution

In the event of a dispute regarding the interpretation of the CP content, the parties to the dispute shall strive in their negotiations to reach a concensus. If negotiation fails, Chunghwa Telecom may establish dispute settlement procedures to secure an interpretation. The CA shall clearly state the dispute resolution procedure in the CPS.

9.14 Governing Law

For disputes involving PKI 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 and legality of any agreement signed based on the CP.

9.16 General Provisions

9.16.1 Entire Agreement

The CAs shall obligate RAs by contract or agreement to comply with the CP and applicable industry standards and guidelines.

The CA shall obligate subscribers or relying parties by contract or agreement to provide CP-related provisions.

9.16.2 Assignment

Entities described in the CP may not assign their rights or obligations without prior written consent. The Company does not provide notification of rights and obligations assignment unless stated otherwise

in the Contract.

9.16.3 Severability

If any chapter of the CP is deemed incorrect or invalid, the remaining chapters will remain valid.

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

In the event that the eCA suffers damages attributable to an intentional or unintentional violation of related CPS regulations by a subscriber or relying party, the eCA may seek compensation for damages and request payment of the attorney's fees from responsible party related to the dispute or litigation. The eCA's failure to assert rights with regard to the violation of the CPS regulations does not waive the eCA'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 a CA including but not limited to natural disasters, war, terrorist attack or interruption in telecommunications network service, the CA shall not bear any legal liability. The CA may state other exemption provisions in the CPS but may not exclude mistakes arising from self-negligence.

9.17 Miscellaneous

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.
CCA	Cross Certification Agreement	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 Authorty Revocation List	See Appendix 2.
CRL	Certificate Revocation List	See Appendix 2.
DN	Distinguished Name	
DV	Domain Validation	See Appendix 2.
eCA	ePKI Root Certification Authority	See Appendix 2.
EE	End Entities	See Appendix 2.
ePKI	Chunghwa Telecom ecommerce Public Key Infrastructure	See Appendix 2.
FIPS	(US Government) Federal Information Processing Standard	See Appendix 2.
IANA	Internet Assigned Numbers Authority, IANA	See Appendix 2.
IETF	Internet Engineering Task Force	See Appendix 2.
NIST	(US Government) National Institute of Standards and Technology	See Appendix 2.
OCSP	Online Certificate Status Protocol	
OID	Object Identifier	See Appendix 2.

OV	Organization Validation	See Appendix 2.
PIN	Personal Identification Number	
PKCS	Public-Key Cryptography Standard	See Appendix 2.
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 of information processing capabilities of system resources.
Access Control	Authorization processing procedure for access to information system resources given to subscribers, programs, procedures and other systems.
Activation Data	The private data required besides keys to access the cryptographic module (such as data used to activate the private key for signatures or encryption).
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.
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	Determination of identity authenticity when an identity of a certain entity is shown. Mutual authentication refers to authentication mutually conducted between two parties during communication activities.
Authentication	Security measures used for information transmission, messages and ways to authorize individuals to receive certain types of information.
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.
Biometrics	The physical or behavioral attributes of a person.
CA Certificate	Certificates issued by CAs
Capability Maturity Model (CMM)	Software Process Assessment (SPA) and Software 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 Revocation List (CARL)	A signed and timestamped 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 Canda (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.
Cross-Certificate	A type of certificate used to establish a trust relationship between two root CAs. This certificate is a type of CA certificates and not a subscriber certificate.
Cryptographic Module	A set of hardware, software, firmware or combination of the above used to run cryptologic or programs (including cryptoalgorithms) and included within the cryptographic boundaries of the module.
Cryptoperiod	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)
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).
Domain Valiadition (DV)	SSL certificate approval and authentication of subscriber network control rights but no authentication of subscriber organization or individual identity, So connection and installation of domain validation SSL certificate websites are able to provide SSL encryption channels but are unable to know who the owner of the website is.
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.
ePKI Policy Managemet 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.
Integrity	Protecting information so that it is not subject to unauthorized modification or damage. Preserve

	information in an untampered state during transmission and storage following generation at its source until receipt by the final recipient.
Internet Engineering Task Force (IETF)	Responsible for the development and promotion of Internet standards. Official website is at: https://www.ietf.org/ . Its vision is the generation of high quality technical documents affects how man designs, uses and manages the Internet and allows the Internet to operate smoothly.
Key Escrow	Storage of related information using the subscriber’ s private key and according to the terms of the mandatory subscriber escrow agreement (or similar contract). The terms of this escrow agreement requires that one or more than one agencies have possession of the subscriber key provided it is beneficial to the subscriber, employer or another party in accordance with the provisions of the agreement.
Key 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).
Cross Certification Agreement (CCA)	The agreement containing the terms and individual liability and obligations that must be followed when the root CA and subordinate certification authorities apply to join the ePKI. The items and individual obligations and authority agreement that must be followed by the eCA and subject CA when the subjectCA joins the ePKI.

Internet Assigned Numbers Authority (IANA)	Internet site assignment organization responsible for managing the IP addresses, domain names and many other parameters used for the Internet.
Issuing CA	For an individual certificate, the CA that issues a certain certificate is the issuing CA.
Naming Authority	A competent authority responsible for assigning a unique identifying name and ensuring that each unique identifying name is meaningful and unique within its field.
National Institute of Standards and Technology (NIST)	Official website is at: http://www.nist.gov/ Similar to our Bureau of Standards, Metrology and Inspection. Its mission is to promote American innovation and industry competitiveness, encourage metrology, standards and technology to increase economic security and improve quality of life. NIST hardware cryptographic module standards and certification, key security assessment and federal government civil servant and contractor identity card standard are widely referenced and used.
Non-Repudiation	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 trusting 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 identifier registered under the International Standard Organization registration standard which could be used to identify the uniquely

	corresponding certificate policy; where the certificate policy is modified, the OID is not changed accordingly. (Article 2.4 Chapter 1 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.
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 control rights, following the certificate assurance level to identify and authenticate the identity of subscriber organizations and individuals. So connection and installation of domain validation SSL certificate websites are able to provide SSL encryption channels, 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.
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 Certification Practice Statements) (2) The database containing the certificate policy and certificate-related information.
Reserved IP Addresses	IPv4 and IPv6 addresses are reserved in the IANA setting. See http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml and http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml
Revoke a Certificate	Termination of certificate operations prior to its expiry date.
Request for Comments (RFC)	A series of memos issued by the Internet Engineer Task Force that include Internet, UNIX and Internet community standards, protocols and procedures for number assignment.
Root Certification Authority (Root CA)	The highest level certificate authority in a public key infrastructure. In addition to issuing subordinate CA and self-signed certificates, the application software provider is responsible for dissemination of self-signed certificates. Chinese is the language of the eCA and highest level certificate authority.
Secure Socket Layer	Protocol issued by Netscape through promotion 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 hose (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) Entity 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	Computer hardware, software and programs

System	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.
Zeroize	Method to delete electronically stored information. Storage of changed information to prevent information recovery.