ePKI Root Certification Authority

Certification Practice Statement

Version 1.4

Chunghwa Telecom Co., Ltd.

March 14, 2018

Contents

ABSTRACT

Important matters regarding the ePKI Root Certification Authority Certification Practice Statement (eCA CPS) are as follows: (in accordance with Article 11 of the Electronic Signatures Act and Regulations on Required Information for Certification Practice Statements announced by the Ministry of Economic Affairs (MOEA))

1. Competent Authority Approval No.: Chin-Shang-Tzu No. 10702216460
2. Certificates issued:
   (1) Types: Self-signed certificates, self-issued certificates, subordinate Certification Authority (CA) certificates issued to subordinate CAs and cross-certificates issued to cross-certified CAs by the eCA.
   (2) Assurance level: Certificates with five levels of assurance are issued in accordance with the Certificate Policy (CP) of the Chunghwa Telecom ecommerce Public Key Infrastructure (ePKI).
   (3) Applicability:

   The issuance subject of the self-signed certificate is the eCA itself. The self-signed certificate contains the public key of the eCA which can be used to verify the digital signatures on subordinate CA certificates, cross-certificates, self-issued certificates and certification authority revocation lists (CARLs) issued by the eCA.

   Self-issued certificates are certificates issued by the eCA for CP or eCA re-key requirements. They are used to construct the trusted certificate path between the old and new keys or the exchange of the CP.

The issuance subject of subordinate CA certificates is subordinate CAs established under the ePKI. Subordinate CA certificates contain the subordinate CA public key which can used to verify the digital signatures on certificates and certification revocation lists (CRLs) issued by the subordinate CA.

The issuance subject of cross-certificates is a root certification authority (Root CA) which is established under another public key infrastructure (PKI) and cross-certified with the eCA. In other words, it is a CA outside the ePKI. Cross-certificates contain cross-certified CA public keys which can be used to verify the digital signatures on certificates and CARLs issued by the CA.

3. Liability and Important Notices:

(1) For subordinate CAs, cross-certified CAs or relying parties by not abiding by the applicability of certificate utilization provided in this CPS, the eCA shall not bear any legal responsibility.

(2) The liability of the eCA for damages arising from the issuance or use of certificates by cross-certified CAs cross-certified by the eCA is limited to the scope of liability set down in this CPS and contracts entered into between the cross-certified CAs and the eCA.

(3) The eCA shall not bear any legal responsibility for damages arising from a force majeure or other events not attributable to the eCA.

(4) If some certification services have to be suspended temporarily because of system maintenance, replacement or expansion of the eCA, the eCA will announce the

information in the repository and notify CAs. Relying parties, subordinate CAs or cross-certified CAs may not request compensation for damages based on the above-mentioned reasons from the eCA.

4. Other Important Circumstances:

(1) The eCA directly accepts certificate registration and revocation requests so there is no need to set up a registration authority (RA).

(2) The applicability of certificates issued by the eCA varies depending on their assurance levels, subordinate CAs and cross-certified CAs must clearly state the assurance level of the requested certificate when the subordinate CA applies for subordinate CA certificates or the cross-certified CA applies for cross-certificates.

(3) Private keys must be self-generated, kept, and used properly by the CAs applying for subordinate CA certificates or the cross-certificates..

(4) Acceptance of a certificate, which is issued by the eCA, by a CA indicates that the CA has verified the correctness of the certificate information.

(5) If a subordinate CA or cross-certified CA needs to revoke a certificate, the eCA shall be promptly notified and the rules and procedures of the CPS shall be followed. However, the subordinate CA or cross-certified CA shall first take appropriate action before announcing the certificate revocation status to reduce the impact on the subordinate CA, the cross-certified CA or relying parties and bear the legal responsibility arising from the use of the certificate.

(6) Relying parties shall first check the correctness, validity,

assurance level and use restrictions of the certificate when using certificates issued by the eCA.

(7) The Company will designate an impartial third party to conduct an audit for operations for the eCA and subordinate CAs based on the Trust Service Principles and Criteria for Certification Authorities and WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security.

CPS Version Control

Version	Date	Revision Summary
1.2	August 21, 2015	RFC 3647 Version of eCA CPS released.
1.3	February 4, 2016	1. Add IV/EV CP OID. 2. Amend Description of Appropriate Certificate Uses of EV、DV、OV、IV SSL Certificate. 3. Adopt Microsoft Root Certificate Program Requirement，amend name form of self-signed certificate of the eCA from the second generation. 4. Minor change of Chapter 8. 5. Minor change of Indemnities.
1.4(20170714)	July 14, 2017	1. Minor Change such as Summary, Section 1.2, Section 1.4.1, Section 2.1, Section 2.3, Section 4.2, Section 4.7, Section 4.8, Section 4.9, Section 5.1 to Section 5.4, Chapter 6 & Chapter 7, Chapter 8 & Chapter 9. 2. Add some acronyms, definition and glossary.
1.4(20171023)	October 23, 2017	Minor Change such as Section 4.5.2、Section 7.1.1, Section 7.3, Section 9.12.1 and so on.
1.4(20180126)	January 26, 2018	Minor revisions of section 3.3.1 & 6.2.2.
1.4(20180214)	February 14, 2018	Add Version Control.
1.4	March 14, 2018	Add Competent Authority Approval No.: Chin-Shang-Tzu No. 10702216460 in Abstract.

1. Introduction

1.1 Overview

1.1.1 Certification Practice Statement

The name of this document is ePKI Root Certification Authority Certification Practice Statement (eCA CPS) of Chunghwa Telecom. The eCA CPS is stipulated to follow the Certificate Policy (CP) for the Chunghwa Telecom ecommerce Public Key Infrastructure (ePKI) and complies with the Regulations on Required Information for Certification Practice Statements, which is the relevant rules and regulations of the Electronic Signatures Act, and related international standards such as the Internet Engineering Task Force (IETF) RFC 3647, ITU-T X.509, IETF PKIX Working Group RFC 5280, CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates and CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates. The eCA CPS mainly describes how the ePKI Root Certification Authority (eCA) proceeds according to the assurance level 4 defined in the CP to issue and manage self-signed certificates, self-issued certificates, subordinate certification authority (CA) certificates, and cross-certificates.

According to the regulations of the ePKI CP, the eCA is the highest CA and the trust anchor of the ePKI and has the highest assurance level. Relying parties can directly trust the certificates of the eCA itself.

1.1.2 CPS Applicability

The practice statement stipulated in this CPS applies to eCA related entities such as the eCA, subordinate CAs, cross-certified

CAs, relying parties and the repository.

Regarding use of this CPS by CAs which is not authorized by the eCA, any problems arising from use of this CPS by other CAs shall be borne by the CAs themselves.

1.2 Document Name and Identification

This version is 1.4. The issue date of this version was March 21, 2018. The latest version of this CPS can be obtained from http://eca.hinet.net or http://ePKI.com.tw.

This CPS was stipulated based on the CP. The operation of the eCA is based upon the provisions of the assurance level 4 defined in the CP. There are a total of five assurance levels for issued certificates. The following are the CP object identifiers (OIDs) registered under the id-cht arc:

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

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

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

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

Assurance Level	OID Name	OID Value
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 OID registered as private enterprise number (PEN) with the Internet Assigned Numbers Authority (IANA) from December 2014 in accordance with the CP v1.1.

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}

If the SSL server certificates issued by subordinate CAs conform to the requirements defined in the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates and pass the external audit of AICPA/CPA WebTrust for Certification Authorities - SSL Baseline Requirements and Network Security, the subordinate CAs and the SSL server certificates issued by the former will be allowed to use Organization Validation (OV) SSL CP OID({joint-iso-itu-t(2) international-organizations(23)

ca-browser-forum(140) certificate policies(1) baseline requirements(2) organization-validated(2)} (2.23.140.1.2.2)), Domain Validation (DV) SSL CP OID ({joint-iso-itu-t(2) international-organizations(23) ca-browser-forum (140) certificate policies(1) baseline requirements(2) domain- validated(1)} (2.23.140.1.2.1)) and Individual Validation (IV) SSL CP OID ({joint-iso-itu-t(2) international-organizations(23) ca-browser -forum(140) certificate policies(1) baseline requirements(2) individual -validated(3)} (2.23.140.1.2.3)) of the CA/Browser Forum.

The SSL server certificates issued by subordinate CA conform to the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates and the subordinate CAs and the application software suppliers (such as browsers or operating system providers) shall negotiate with each other regarding their certificate handling methods. Subordinate CA certificate and SSL Server certificates can use CA/Browser Forum Extended Validation (EV) SSL CP OID ({joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate policies(1) certificate – policies(1) ev-guidelines(1)} (2.23.140.1.1)).

This CPS conforms to the current version of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates and Guidelines for the Issuance and Management of Extended Validation Certificates published at http://www.cabforum.org. In the event of any inconsistency between this CPS and the current official version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates and Guidelines for the Issuance and Management of Extended Validation Certificates, the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates and Guidelines for the Issuance and Management of Extended Validation Certificates take

precedence over this CPS.

The subordinate CAs' certificates and the certificates applied to PDF document signatures (certificate that issued to organizations and/or individuals with assurance Level 1, 2, or 3) may use OID 1.3.6.1.4.1.23459.100.0.9. This OID is trusted by Adobe Approved Trust List (AATL).

1.3 PKI Participants

The key members of the CPS include:

(1) eCA

(2) Subordinate CA

(3) Cross-Certified CA

(4) Relying Parties

1.3.1 Certification Authorities

1.3.1.1 eCA

The eCA is the trust anchor of the ePKI. In addition to the issuance and management of eCA certificates and subordinate CA certificates at the first level of the ePKI, the eCA is also responsible for performing the cross-certification with a root CA established for other public key infrastructure (PKI) outside the ePKI and issuing and managing cross-certificates issued to CAs outside the ePKI.

The eCA directly accepts certificate registration and revocation requests and is responsible for collecting and verifying the identity and the certificate-related information of subordinate CAs and cross-certified CAs. There is no need to set up a registration authority (RA).

1.3.1.2 Subordinate CA

The subordinate CA, another type of CA in the ePKI, is

mainly responsible for the issuance and management 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 establish a multi-level hierarchy of PKI. However, the subordinate CA cannot directly cross-certify with the CA outside the ePKI.

The establishment of a subordinate CA shall be done in accordance with related CP regulations. A contact window which is responsible for the interoperability work with the eCA and other subordinate CAs shall be set up.

The first level of the subordinate CAs under this ePKI include Public Certification Authority and ePKI EV SSL Certification Authority; both of them are operated by the Company.

1.3.1.3 Cross-Certified CA

The cross-certified CA refers to a CA which is a root CA outside the ePKI that performs cross-certification with the eCA. The root CA, which wishes to apply for cross-certification with the eCA, must first conform to the security regulations of the CP assurance level used, possess the establishment and management capabilities of the PKI, digital signature, and certificate issuance technology, determine related responsibilities and obligations for CA, RA, and relying parties, and pass external audits equivalent in strength to the ePKI.

1.3.2 Registration Authorities

The eCA directly accepts certificate registration and revocation

requests and is responsible for collecting and verifying the identity and certificate-related information of subordinate CAs and cross-certified CAs. There is no need to set up a RA.

1.3.3 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 certificates according to the certificate policies listed on the certificates. In addition, for property categories such as application processes and devices, 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.

1.3.4 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 used based on the corresponding CA certificate and certificate status information. The certificate may be used for the following work after checking the validity of the certificate:

(1) To verify the integrity of a digitally signed electronic document,

(2) To identify the creator of a digitally signed electronic document

(3) To establish a safe communications channel with the certificate subject.

1.3.5 Other Participants

If the eCA selects other authorities, which provide related trust services, such as a bridge CA, time stamp authority (TSA), or data archiving service as collaborative partners, the related information shall be disclosed on the website and the collaboration mechanism and mutual rights and obligations shall be set down in the CPS to ensure the efficiency and reliability of the eCA service quality.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The eCA issues four kinds of certificates: self-signed certificates, self-issued certificates, subordinate CA certificates and cross-certificates.

The self-signed certificate is used to establish the trust anchor of the ePKI. The self-issued certificate is used for the eCA re-key or the exchange of the CP. The subordinate CA certificate is used to establish interoperable trust relationships between CAs to construct the certificate trust path needed for the interoperability for CAs. The cross-certificate is used to establish a mutual trust relationship between two CAs under different PKI to construct the certificate trust path needed for the interoperability for CAs.

The issuance subject of the self-signed certificate is the eCA itself. The self-signed certificate contains the eCA public key which can be used to verify the digital signatures on subordinate CA certificates, cross-certificates, self-issued certificates and certification authority revocation lists (CARLs) issued by the eCA.

The issuance subject of the subordinate CA certificate is subordinate CAs established under the ePKI. The subordinate CA

certificate contains the subordinate CA public key which can be used to verify the digital signatures on certificates and CRLs issued by the subordinate CA.

The issuance subject of the cross-certificate is a root CA which is established under another PKI and cross-certifies with the eCA. The cross-certificate contains the cross-certified CA public key which can be used to verify the digital signatures on certificates and CARLs issued by the CA.

The certificates issued by the eCA are divided in the five levels of assurance in accordance with CP regulations. The recommended applicability of each assurance level is as follows:

Assurance Level	Applicability
Test Level	Only provided for test use and does not bear any legal responsibility for the transmitted data.
Level 1	Use e-mail notification to verify that the applicant can operate the e-mail account. Suitable for use in an Internet environment in which the risk of malicious activity is considered to be low or unable to provide a higher assurance level. When used for digital signatures, it can identify that the subscriber comes from a certain e-mail account or guarantee the integrity of the signed document. When used for encryption, the relying party can use the subscriber's certificate public key to encrypt and transmit the message or the symmetric key to guarantee its confidentiality but it is not suitable for on-line transactions when identity authentication and non-repudiation are required.
Level 2	Suitable for use with information which may be tampered with but the Internet environment has no malicious tampering (data interception is possible but likelihood is not high). Not suitable for the signing of important documents (life essential and high value transaction documents). Suitable for data encryption and identity verification of small value e-commerce transactions.
Level 3	Suitable for use in an Internet environment in which there are malicious users, which intercept or tamper with information, and

Assurance Level	Applicability
	risks, which are greater than the environment of Level 2. Transmitted information may include on-line cash transactions.
Level 4	Suitable for use in an Internet environment where potential threats to data are high or the cost to restore tampered data is high. Transmitted information includes high value on-line transactions or highly confidential documents.

The assurance level, authentication method, scope of application, and reducible risks of the SSL certificates shall comply with the aforesaid table, and their descriptions are as the following:

Assurance Level and Certificate Type	Authentication Method	Scope of Application	Risk Description of Reducible Risks
Level 2 DV SSL certificate	Follow CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates and assurance level 2 regulations to authenticate remote domain names and webpage services.	Provide communication channel encryption (communication channel encryption refers to facilitate encryption key exchange to achieve information transmission encryption between the subscriber's browser and website'). Suitable for use with protected network communications.	Provide an encryption protection to the non-monetary or non-property transactions where the probability of existence of malicious acts (e.g. online fraud, personal information breach, leakage of confidential information, etc.) is low.
Level 3 OV SSL certificate	Follow CA/Browser Forum Baseline Requirements for the Issuance and	Provide communication channel encryption and must authenticate which	Provide a robust authentication and high-level security to the following environments

Assurance Level and Certificate Type	Authentication Method	Scope of Application	Risk Description of Reducible Risks
	Management of Publicly-Trusted Certificates and assurance level 3 regulations to authenticate the remote domain name and the webpage services controlled by the applicant and authenticate which organization owns the domain name.	organization owns the domain name. Suitable for use with protected network communications.	(included but not limited to): (1) the important monetary or property transactions; (2) internet transactions where the probability of existence of malicious acts (e.g. online fraud, personal information breach, leakage of confidential information, etc.) is moderate.
Level 3 IV SSL certificate	Follow CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates and assurance level 3 regulations to authenticate the remote domain name and the webpage services controlled by the applicant and authenticate which natural person owns the domain name.	Provide communication channel encryption and must authenticate which natural person owns the domain name. Suitable for use with protected network communications.	Provide a robust authentication and high-level security to the following environments (included but not limited to): (1) the important monetary or property transactions ; (2) internet transactions where the probability of existence of malicious acts (e.g. online fraud, personal information breach, leakage of confidential information, etc.) is moderate.

Assurance Level and Certificate Type	Authentication Method	Scope of Application	Risk Description of Reducible Risks
Level 3 EV SSL certificate	Follow CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates to authenticate which organization owns the remote domain name and webpage service, verify that that organization truly exists in its legal jurisdiction, and participate in certificate transparency to prevent any misissuance of certificates.	Provide communication channel encryption and must authenticate which organization owns the domain name. Suitable for use with protected network communications. Browser will show the green address bar and directly display the organization information of EV SSL certificate subject to facilitate subscriber to identify the certificate holder.	Provide a robust authentication and extremely high-level security to the following environments (included but not limited to): (1) transactions with high monetary or property value; (2) internet transactions where the probability of existence of malicious acts (e.g. online fraud, personal information breach, leakage of confidential information, etc.) is very high.

1.4.2 Restricted Certificate Use

Relying parties shall obtain the trusted eCA public key or self-signed certificates via a self-signed certificate secure channel as described in section 6.1.4 which can be used to verify the digital signatures of self-issued certificates, subordinate CA certificates, cross-certificates and CARLs issued by the eCA.

Relying parties shall carefully select secure computer environments and trusted application systems to prevent the eCA public keys and self-issued certificates from being damaged or replaced so to ensure use of the correct eCA public key or

self-signed certificate to verify the digital signatures of eCA issued self-issued certificates, subordinate CA certificates, cross-certificates or CARLs.

The type of assurance level certificates which can be issued by the subordinate CA is recorded on the certificates issued to subordinate CA by the eCA so relying parties can decide whether or not to trust the subordinate CA and certificates issued by that.

The type of assurance level of certificates which can be issued by the CA and how many cross-certification levels can be performed by the CA with other CA are recorded on the cross-certificates issued by the eCA to the root CA outside the ePKI so relying parties can decide whether or not to trust the CA and certificates issued by that. In addition, the cross-certificate contains the certificate policy mapping relation used by the CA so the relying party can decide based on the corresponding relations whether to trust that CA and its issued certificates.

The relying parties must properly use the key in accordance with the regulations of key usage purposes described in section 6.1.7 and use certificate validation methods which conform to international standard (such as the ITU-T X.509 standard or IETF RFC5280) definitions to verify the validity of certificates.

Relying parties must carefully read the CPS before using the certificate service provided by the eCA, follow the CPS regulations and watch for CPS updates.

1.4.3 Prohibited Certificate Uses

(1) Crime.

(2) Control for military orders and war situations as well as nuclear, biological, and chemical weapons.

(3) Operation of nuclear equipment.

(4) Aviation flight and control systems.

(5) Scope of prohibitions announced under the law

1.5 Policy Administration

1.5.1 Organization Administering the Document

Chunghwa Telecom Co., Ltd. (the Company).

1.5.2 Contact Person

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

Phone: 0800080365

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

E-mail: caservice@cht.com.tw

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

1.5.3 Person determining CPS suitability for the policy

The eCA shall first check whether the CPS conforms to relevant CP regulations and then submit the CPS to the Policy Management Committee for review and approval.

In accordance with the 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 eCA conducts regular self-audits to prove operations

comply with the assurance level used with the CP. In order to ensure the smooth operation of certificates issued by the CAs under the ePKI by operating systems, browsers and software platforms, the ePKI has already applied to participate in the root certificate programs for operating systems, browsers and software platforms. The self-issued certificates issued by the eCA are widely deployed in the CA trust lists of software platforms. According to regulations of the root certificate program, the audit should be conducted by qualified auditors for the full PKI hierarchy. The period during which the CA issues certificates shall be divided into an unbroken sequence of audit periods. An audit period must not exceed one year in duration. External audits for the eCA and subordinate CAs are conducted annually and the latest CPS and external audit results are submitted to the root certificate program. The eCA also continues to maintain the audit seal published in the eCA website.

1.5.4 CPS Approval Procedures

The CPS is published by the eCA following approval by the MOEA, the competent authority of the Electronic Signatures Act. If the CPS must be revised together with the posted CPS revisions, the revised CPS is first submitted to the ePKI Policy Management Committee for review and then forwarded to the MOEA for approval.

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

1.6 Definitions and Acronyms

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

2. Publication and Repository Responsibilities

2.1 Repository Responsibility

The repository, under the management of the eCA, publishes the eCA issued certificates, CARLs and other certificate-related information and provides 24-hour round-the-clock service. The website address of the eCA repository is http://eca.hinet.net or http://ePKI.com.tw. The repository will resume normal operation within two calendar days if unable to operate normally for some reason.

The responsibility of the repository includes:

(1) Regularly publish issued certificates, CARLs and other certificate related information in accordance with section 2.2.

(2) Publish the latest CP and CPS information.

(3) Access control of the repository shall comply with the provisions in section 2.4.

(4) Guarantee the accessibility status and availability of the repository information.

(5) Publish the results from the external compliance audits (as outlined in Section 8.6).

2.2 Publication of Certification Information of eCA

The eCA publishes the following in its repository:

(1) Certificate policy.

(2) This CPS.

(3) CARLs.

(4) Online Certificate Status Protocol (OCSP) inquiry service

(5) Self-signed certificates by the eCA.

(6) Self-issued certificates cross-signed with the eCA's old and new keys.

(7) Subordinate CA certificates.

(8) Cross-Certificates.

(9) Privacy protection policy.

(10) The results of last external compliance audit. (as outlined in Section 8.6)

(11) The latest related news.

Furthermore, if the subordinate CAs under the eCA or the cross-certified CAs which cross certify with the eCA provide the SSL certificates issuance service, the eCA will require the SSL certificate issuing CAs to publish three SSL certificate website URLs to the application software providers which are used for valid, revoked, and expired SSL certificates respectively, for the application software providers to test whether their software is able to use that SSL certificates to chain up to the self-signed certificate of the eCA.

2.3 Timing or Frequency of Publication

(1) The eCA shall publish CPS in the repository within seven calendar days upon receiving the competent authority’s approval letter.

(2) The CP complied with by the eCA shall be published within seven calendar days upon the approval of ePKI Certificate

Policy Management Committee.

(3) The eCA issues CARL at least twice per day and publishes in the repository.

(4) Self-signed certificates, self-issued certificates, cross-certificates and subordinate CA certificates, are published in the repository within seven calendar days upon issuance and receipt of the certificates.

2.4 Access Controls on Repositories

There is no network connection between the eCA server and repository server. Therefore, the certificates and CARLs issued by the eCA server cannot be transmitted directly to the repository server via network. When the eCA wants to publish the issued certificates and CARLs, related eCA personnel store the certificates and CARLs that need to be published on portable media and then copy the files to the repository server offline manually for publication.

The information published by the eCA under section 2.2 is primarily provided for subordinate CA, cross-certified CA and relying party inquiries, and thus is accessible for viewing and downloading. As a result, access control should be implemented when providing access to viewing to guarantee repository security and maintain accessibility and availability.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

The subject name of the certificate issued by the eCA conforms to the distinguished name (DN) of X.500. Self-signed certificates, self-issued certificates, subordinate CA certificates issued to subordinate CAs, and cross-certificates issued to cross-certified CAs use the distinguished name format.

3.1.2 Need for Names to be Meaningful

The Subjects of organizations applying to become subordinate CAs or cross-certified CAs shall comply with the requirements of CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates and the related requirements for naming the Subjects in the domestic laws; moreover, the name should be sufficient to represent and identify the CA.

3.1.3 Anonymity or Pseudonymity of Subscribers

Not applicable for CA certificates issued by eCA.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting various name forms should comply with the name attribute definition of ITU-T X.520.

3.1.5 Uniqueness of Names

eCA examines the uniqueness of the CA names applying to become subordinate CA and cross-certified CA. If a duplicate name is found, the applying CA is required to change the name.

In favor of international interoperability, the first generation self-signed certificate of the eCA uses the following name form:

C = TW,

O = Chunghwa Telecom Co., Ltd.,

OU = ePKI Root Certification Authority

In favor of international interoperability, the second generation self-signed certificate of the eCA uses the following name form:

C = TW,

O = Chunghwa Telecom Co., Ltd.,

CN = ePKI Root Certification Authority - Gn

Where n = 2, 3….,

Moreover, in the self-signed certificate issued by the eCA, the certificate issuer name is identical to the certificate subject name.

3.1.6 Recognition, Authentication and Role of Trademarks

The certificate subject name provided by subordinate CAs and cross-certified CAs includes the trademark or any legally protected name, trade name, business name or symbol, the eCA is not responsible for their examination but their names must conform to the Trademark Act, Fair Trade Act and other relevant regulations in Taiwan. The eCA does not guarantee the approval, verification, legality or uniqueness of the trademark including in the certificate subject name. Relevant disputes or arbitrations related to the trademark shall not be the obligation of the eCA and the subordinate CA and cross-certified CA shall submit applications to relevant competent authorities or courts.

3.1.7 Resolution Procedure for Naming Disputes

The Company shall handle disputes regarding naming rights.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

When the CA applies for a certificate, eCA checks if the CA's private key and public key listed on the certificate form a pair. One PKCS#10 Certificate Signing Request file is generated by the CA and the eCA uses the CA's public key to check the signature to prove the CA possesses the corresponding private key.

3.2.2 Authentication of Organization Identity

The eCA identity authentication is reviewed at a Policy Management Committee meeting convened by the Company.

When a CA self-established by the Company becomes a subordinate CA (for example: Public Certification Authority), the identity authentication is reviewed by a Policy Management Committee meeting convened by the Company.

For cross-certificate application submitted by CA not self-established by the Company, the application shall include the organization name, locality, representative and other information which is sufficient to identify the organization. The eCA shall confirm the existence of the organization as well as the authenticity of the application, representative identity and the representative's authority to represent the organization. The representative is required to apply for the certificate in person.

If the usage of the certificate issued by a subordinate CA is e-mail signature and encryption, the subordinate CA shall authenticate the organization's identity and validate if the organization is in possession or is authorized to use the e-mail address recorded on the certificate.

If the usage of the certificate issued by a subordinate CA is encrypted transmission by SSL server, the subordinate CA shall follow the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates and the subordinate CA shall authenticate that the certificate applicant has domain name control. If the SSL server certificate is for organization validation (OV), the subordinate CA shall authenticate the organization identity and validate that the organization is in possession or is authorized to use the full qualified domain name (FQDN) recorded on the certificate. The subordinate CA must be cross-checked against the registration information in the trusted database. If the SSL server certificate is for individual validation (IV), the subordinate CA shall authenticate the natural person's identity and validate that the natural person is in possession of or is authorized to use the FQDN recorded in the certificate. The subordinate CA may compare this information against the information stored in the trusted database. If the SSL server certificate is for extended validation (EV), the subordinate CA shall authenticate the organization’s identity and validate that the organization is in possession of or is authorized to use the FQDN recorded in the certificate in accordance with the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates. The subordinate CA may compare this information against the information stored in the trusted database.

If the usage of the certificate issued by a subordinate CA is dedicated server signature and encryption, the subordinate CA shall authenticate the organization identity and validate whether or not the dedicated software name recorded in the certificate by the organization is appropriate.

If the usage of the certificate issued by a subordinate CA is timestamp server signature and encryption, the subordinate CA shall authenticate the organization identity and validate whether or not the software name used with the timestamp server recorded on the certificate by the organization is appropriate.

If the usage of certificate issued by a subordinate CA is code signing, the subordinate CA shall authenticate the organization identity and validate that the organization matches the organization name recorded on the certificate.

3.2.3 Authentication of Individual Identity

Not applicable for CA established by the Company.

For CA not established by the Company, CA certificates must be applied for by representatives appointed by official document (individuals authorized to submit cross-certificate applications). The authentication procedure is as follows:

(1) Cross-checking written documentation:

When applying for a certificate, the representative shall present the original copy of a ROC identity card or passport so the eCA can authenticate the identity of the representative. The representative's ID number, name and household address information must be cross-checked together against the application information submitted by the CA.

(2) Submit representative's letter of authorization.

The representative must authenticate his/her identity in person.

3.2.4 Non-Validated Subscriber Information

Not applicable for CAs with issuance assurance level levels 4, 3 and 2.

The CA does not need to validate if the common name on assurance level 1 or test level individual certificates is the legal name of the certificate applicant.

3.2.5 Validation of Authority

When there is a connection between a certain individual (certificate applicant) and the certificate subject name and the individual applies for a certificate lifecycle activity such as a certificate application or revocation request, the eCA or subordinate CA or its RA shall perform a validation of authority and verify that the individual can represent the certificate subject such as:

(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 a position at the certificate subject (organization or company) and is authorized to represent the certificate subject through telephone, mail, e-mail or other equivalent procedures.

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

3.2.6 Criteria for Interoperation

Not specified.

3.3 Identification and Authentication for Re-key Requests

Certificate rekey is the issue of a new certificate of equivalent characteristics and assurance level as the old certificate and the new

certificate not only has a new and different public key (corresponding to the new and different private key) and different serial numbers but also may be assigned a different validity period.

The subordinate CA or cross-certified CA should reapply for a certificate from the eCA when making a rekey request, eCA shall follow the rules in 3.2.2 to identify and authenticate the CA reapplying for the certificate.

3.3.1 Certificate Renewal Rekey

The eCA is not allowed to renew self-signed certificates, self-issued certificates, subordinate CAs certificates, or cross-certificates.

3.3.2 Identification and Authentication for Re-key after Revocation

After a certificate is revoked by the CA, the procedure for new certificate application identification and authentication in section 3.2 is followed to perform initial registration again.

3.4 Identification and Authentication for Certificate Revocation Request

The authentication procedure for eCA self-signed certificates, subordinate CA certificates and cross-certificates revocation requests is the same as the rules in section 3.2.2.

4. Certificate Lifecycle Operational Requirements

4.1 Certificate Application

4.1.1 Who can Submit a Certificate Application

Certificate applicants include the eCA, subordinate CA and root CA outside the infrastructure.

4.1.2 Enrollment Process and Responsibilities

4.1.2.1 ePKI eCA Obligations

(1) Operate in accordance with CP assurance level 4 regulations and the CPS.

(2) Establish subordinate CA application and CA cross-certification request procedures.

(3) Perform the identification and authentication procedures for applications made by subordinate CAs and the cross-certification application between CAs.

(4) Issue and publish certificates.

(5) Revoke certificates.

(6) Issue and public CARLs.

(7) Perform CA personnel identification and authentication procedures.

(8) Securely generate eCA private keys.

(9) Safeguard the eCA private keys.

(10) Perform eCA self-signed certificate rekey and self-issued certification issuance.

(11) Accept subordinate CA certificate registration and revocation requests.

(12) Accept the Cross-Certified CA's cross-certificate

registration and revocation requests.

4.1.2.2 Subordinate CA Obligations

(1) Follow CPS regulations. Shall be liable for compensation if damages suffered by relying party due to failure to follow regulations.

(2) eCA issued certificates have different assurance levels and applications based upon the CP standards. The subordinate CA must clearly state the assurance level of the certificate applied for when submitting a certificate application.

(3) The subordinate CA shall follow the procedure in section 4.2 when applying for a certificate and check the accuracy of the information on the application.

(4) After the subordinate CA application is approved and the eCA issues the certificate, the subordinate CA shall follow section 4.4 when accepting the certificate.

(5) Acceptance of the certificate issued by the eCA by the subordinate CA indicates that the subordinate CA has checked the accuracy of the information on the certificate and may use the certificate in accordance with section 4.5.

(6) The subordinate CA shall self-generate private keys in accordance with the regulations in Chapter 6.

(7) The subordinate CA shall properly safeguard and use the private keys.

(8) The digital signature signed using the private key which corresponds to the certificate public key is the subordinate CA's digital signature. When generating a digital signature, the subordinate CA must make sure the subordinate CA certificate has been accepted and the certificate is still valid and has not yet been revoked.

(9) If the certificate revocation circumstances in section 4.9.1 occur (such as disclosure or loss of private key information) and the subordinate CA must revoke the certificate, the eCA shall be promptly notified and the regulations in section 4.9 followed to suspend or revoke the certificate. However, the subordinate CA shall bear the legal liability of certificate use prior to the publication of the certificate revocation status.

(10) If the eCA is unable to operate normally for some reason, the subordinate CA shall speedily seek other ways for completion of legal acts and may not use the inability of eCA to provide normal operations as grounds of defense to others.

4.1.2.3 Cross-Certified CA Obligations

(1) Follow the CPS and provisions of the Cross-Certification Agreement (CCA). Shall be liable for compensation if damages suffered by relying party due to failure to follow regulations.

(2) eCA issued certificates have different assurance levels and applications based upon the CP standards. The CA must clearly state the assurance level of the certificate applied for when submitting a cross-certificate application.

(3) The procedures in section 4.2 shall be followed for the cross-certificate applications when the CA applies for certificates and the accuracy of the application information is checked.

(4) The CA shall follow the regulations in section 4.4 when accepting the certificate after the CA cross-certificate application is approved and the eCA issues the certificate.

(5) Acceptance of the certificates issued by the eCA by the CA indicates that the information contained in the certificate has

been checked for accuracy and the regulations in section 4.5 shall be followed during certificate use.

(6) The CA shall follow the regulations in Chapter 6 when applying for cross-certification and self-generate the private key.

(7) The Cross-Certified CA shall properly safeguard and use the private key.

(8) The digital signature signed with the private key which corresponds with the certificate's public key is the CA's digital signature. When creating a digital signature, the CA must check the accepted certificate and the certificate must be valid and unrevoked.

(9) If the certificate revocation circumstances in section 4.9.1 occur (such as disclosure or loss of the private key information), the CA must revoke the certificate and promptly notify the eCA. The certificate is suspended or revoked in accordance with the regulations in section 4.9. However, the CA shall bear the legal liability of certificate use prior to the publication of the certificate revocation status.

(10) When the eCA is unable to operate normally for some reason, the CA shall speedily seek other ways for completion of legal acts and may not use the inability of eCA to provide normal operations as grounds of defense to others.

4.2 Certificate Application Processing

If the intermediate level of the ePKI is the subordinate CAs, unless agreed by the CA of the upper-level, the subordinate CAs shall not accept other CA to become their subordinate CAs.

Before the eCA issue the cross-certificates to the CAs other than these one of the ePKI, a negotiation between the ePKI Policy Management Committee and that CA shall be conducted to determine if the cross-certificates issue by the CA to other CAs will be acknowledged.

4.2.1 Performing Identification and Authentication Functions

4.2.1.1 Initiation

(1) Initiation application

For CA established by the Company, the Company convenes a Policy Management Committee meeting to review the PKCS#10 certificate application file and the validity period, the certificate subject name and other related information for the certificate to be issued. For CA not established by the Company, the cross-certificate application, CPS and PKCS#10 certificate application file must be submitted. If the CA follows a certificate policy other than the Certificate Policy for the Chunghwa Telecom ecommerce Public Key Architecture, the certificate policy followed should be attached.

(2) Identity identification and authentication

Follow the regulations in section 3.2.2 to perform the mutual authentication procedures for the applications between eCA, subordinate CA or Cross-Certified CA.

(3) Perform the following checking procedure

Check the application to make sure there are no technical compatibility issues between the subordinate CA, the cross-certified CA and the eCA for cross-certification.

If the CA applying for the cross-certificate follows a certificate policy other than the Certificate Policy for the Chunghwa Telecom ecommerce Public Key Infrastructure, check the corresponding relations between its certificate policy and the

ePKI CP.

Check if the CPS of the CA follows the certificate policy used by the CA.

Check the PKCS#10 application file submitted for the initialization application to make sure actual cross-certification work can be completed.

4.2.2 Approval or Rejection of Certificate Applications

4.2.2.1 Examination

A Policy Management Committee meeting is convened to review the application when the eCA submits a self-signed certificate application.

A Policy Management Committee meeting is convened to review the application when a CA submits a subordinate CA certificate application.

A Policy Management Committee meeting is convened to review the related document information submitted by the CA and eCA checking results when the CA submits a cross-certification application in order to determine the appropriateness of the CA and eCA cross-certification. The committee ultimately decides whether the application enters the next stage, supplemental information is required or the application is rejected.

4.2.2.2 Arrangement

CAs established by the Company does not need to sign a Cross-Certification Agreement (CCA).

When a CA not established by the Company submits the cross-certificate application, a meeting is convened and the CA

applying for cross-certification is notified to attend. The following steps are followed:

(1) Identity identification and authentication

Follow the regulations in section 3.2.3 before the meeting starts to perform the identity identification and authentication procedure for the representative of the CA applying for cross-certification.

(2) The negotiations with the CA applying for the cross-certification must follow the terms and conditions.

(3) Determine if cross-certification is approved for CA applying for cross-certification. If approved, the CA applying for cross-certification signs the CCA.

(4) Enter the certificate issuance procedure.

4.2.3Time to Process Certificate Applications

After the information submitted by the CA for the certificate application is determined to be complete, conforming to the certificate policy and eCA CPS, technically compatible, eCA compatible and passes the Policy Management Committee meeting review, the eCA shall complete the certificate issuance within seven calendar days.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

The eCA follows the resolution of the Policy Management Committee (meeting minutes) when issuing self-signed certificates and self-issued certificates.

The eCA issues one self-signed certificate. This certificate is sent to relying parties in accordance with section 6.1.4 regulations.

eCA follows the Policy Management Committee meeting approval results (meeting minutes) when deciding whether or not to issue subordinate CA certificates or cross-certified CA certificates.

4.3.2 Notification to the Certificate Applicant by the CA of Issuance of the Certificate

If the certificate application is approved, the subordinate CA or the cross-certified CA is notified and the eCA performs the work related to certificate issuance. After the certificate is issued, the Company shall notify the CA by letter and attach the issued certificate.

If certificate application is not approved, the subordinate CA or cross-certified CA which submitted the application is notified by letter and the reasons why the application was not approved are stated within.

4.4 Certificate Acceptance

After the eCA determines that the self-signed certificate and self-issued certificate is free of errors, the internal issuance procedures are followed to publish the self-signed certificate and self-issued certificate in the repository.

After receiving notification of approval of their certificate application, the subordinate CA or the cross-certified CA must check the attached certificate to make sure the certificate contents are accurate. If there are no errors on the certificate, the eCA shall be notified. CA not established by the Company must sign a certificate acceptance confirmation document and reply by letter to the Company to complete the certificate acceptance procedure. Internal issuance procedures are followed for subordinate CA established by the

Company to publish the self-signed certificate and the self-issued certificate in the repository.

After the eCA receives the certificate acceptance confirmation document, the subordinate CA's CA certificates or cross-certificates issued to the CA are published in the repository.

If the CA does not return the certificate acceptance confirmation document within 30 calendar days, it shall be deemed as refusal of certificate acceptance. The eCA revokes that certificate and no publication is made.

4.4.1 Conduct Constituting Certificate Acceptance

After the eCA confirms the information on the self-signed certificate and self-issued certificate is free of errors, the internal issuance procedures are followed to publish the self-signed certificate and self-issued certificate in the repository.

After receiving notification of approval of their certificate application, the subordinate CA or the cross-certified CA must check the attached certificate to make sure the certificate contents are accurate. If there are no errors on the certificate, the eCA shall be notified. CA not established by the Company must sign a certificate acceptance confirmation document and reply by letter to the Company to complete the certificate acceptance procedure.

If the CA does not return the certificate acceptance confirmation document within 30 calendar days, it shall be deemed as refusal of certificate acceptance. The eCA revokes that certificate and no publication is made.

4.4.2 Publication of the Certificate by the eCA

After receiving the certificate acceptance confirmation document, the eCA issues the subordinate CA’s CA certificates or

cross-certificates issued to the CA are published in the repository.

Subordinate CA established by the Company follow the internal issuance procedure to publish the subordinate CA certificate in the repository.

4.4.3 Notification of Certificate Issuance by the eCA to Other Entities

If there are newly issued self-signed certificates, the eCA follows the root certificate program of operating system, browser and software platform to submit the application to enter the self-signed certificate into the CA trust list.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers refer to the entities that request and obtain certificates. For organizations, it is the name recorded as the certificate subject and the entity that possesses the private key corresponding to certificate public key. With regard to types of property (such as application programs, hardware and equipment), the certificate subscriber is the individual or organization requesting the certificate since property has no capacity to act. The generation of subscriber key pairs shall comply with the regulations in section 6.1.1. Subscribers must solely control the rights and capabilities to the private keys corresponding to the certificates. The subscriber does not issue certificates to other parties. Subscribers shall protect their private keys against unauthorized use or disclosure by third parties and shall use their private keys only for their intended

purpose (the key usage listed in the certificate extension field). Subscribers shall correctly use certificates in accordance with the CP listed on the certificate.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties refers to third parties who trust the connecting relationship between the certificate subject name and public key. Relying parties shall use software that is compliant with ITU-T X.509, Internet Engineering Task Force (IETF) RFC, CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates or CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates related standards or standard software.

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

(1) Verify the integrity of the electronic documents with digital signatures.
(2) Verify the identity of document signature author.
(3) Establish secure communication channels with the subscriber.

The above certificate status information can be obtained from the CARL, CRL, or OCSP services. The CARL and CRL download URLs can be obtained in the extension field at the CRL distribution point (CDP); the service URL of OCSP inquiry can be obtained from the extension field at the Authority Information Access (AIA). In addition, the relying parties shall check the CA issuer and subscriber

certificate CP to verify the assurance level of the certificate.

4.6 Certificate Usage

CA certificates are not allowed to be renewed. Only subscriber certificates can be renewed.

4.6.1 Circumstances for Certificate Renewal

Not applicable.

4.6.2 Who May Request Renewal

Not applicable.

4.6.3 Certificate Renewal Procedure

Not applicable.

4.6.4 Notification of New certificate Issuance to Subscriber

Not applicable.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Not applicable.

4.6.6 Publication of the Renewal Certificate by the CA

Not applicable.

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

Not applicable.

4.7 Certificate Re-Key

4.7.1 Circumstances for CA Certificate Re-Key

Under the following two circumstances, the eCA will renew the key and issue a new self-signed certificate:

(1) The lifecycle of currently used keys has ended.

(2) Security issues exist for currently used keys (such as suspected or confirmed key compromise).

Under the following three circumstances, the subordinate CA will renew the key and issue a new subordinate CA certificate:

(1) The lifecycle of currently used keys has ended.

(2) Security issues exist for currently used keys (such as suspected or confirmed key compromise).

(3) Security issues regarding the cryptographic algorithm or international protective measures eliminated in advance (such as the CA/Browser Forum's decision to phase out the use of the SHA-1 hash function algorithm in October 2014).

Under the following two circumstances, the Cross-Certified CA will renew the key and a new cross-certificate shall be issued by the eCA:

(1) The lifecycle of currently used keys has ended.

(2) Security issues exist for currently used keys (such as suspected or confirmed key compromise).

4.7.2 Who May Request Certificate Re-Key

Applications may be submitted by the eCA, subordinate CA or root CA outside the ePKI.

4.7.3 Processing certificate re-keying requests

For certificate re-keys, the CA submits a new certificate

application to the eCA. The regulations in section 3.1, 3.2, 3.3, 4.1 and 4.2 must be followed for the procedures used by eCA to perform certificate re-key.

4.7.4 Notification for Issuing Replacement of Certificate Keys to CAs

The regulations in section 6.3.2 must be followed for routine re-key of CA private keys.

After a CA certificate is revoked, its private key should be suspended. Besides, after issuing a new key, the CA should follow the regulations specified in section 4.2 to apply for a new certification from the eCA.

For the CA which issue assurance level 2, 3 and 4 certificates, if its certificate has not been revoked, the eCA can start to accept its rekey and apply for a new certificate one month before the CA private key usage period expires. Follow the regulations in section 4.2 for the new certificate application procedure.

For CA certificates where there are international protective security measures such as the SHA-1 hash function algorithm being phased out, follow the regulations in section 4.2 to submit a new certificate application prior to the expiry of the CA private key usage period.

For the notifications for replacement of certificate keys to CA from the eCA, please refer to Section 4.3.2.

4.7.5 Circumstances Constituting Acceptance of Certificate Re-Key

Same as section 4.4.1.

4.7.6 Publication of the Re-Keyed Certificate by

the CA

Same as section 4.4.2.

4.7.7 Notification of Certificate Issuance by the eCA to Other Entities

Same as section 4.4.3.

4.8 Certificate Modification

4.8.1 Circumstances for Certificate Modification

Certificate modification refers to provide a new certificate for the same subject that has few differences with the old certificate on the authentication information (for example a new e-mail address or other relatively unimportant attribute information) and conforms to relevant regulations in the CP and CPS. In the new certificate, it may use a new certificate subject public key or keep using the original subject public key but the certificate expiry date and the original certificate expiry date are the same. After the certificate is modified, the old certificate should be scrapped.

4.8.2 Who May Request Certificate Modification

Certificate applicants include the eCA, subordinate CA or root CA outside the ePKI.

4.8.3 Processing Certificate Modification Requests

See the regulations in section 4.2 for the certificate modification application procedure.

4.8.4 Notification for Issuing Modification of Certificates to CAs

After the eCA issues the modified certificate, the subordinate CA established by the eCA or the Company is notified with the meeting minutes or through internal issuance procedures. The eCA notifies subordinate CA not established under the Company and Cross-Certified CAs by letter.

If the eCA does not approve the issuance of the modified certificate, the subordinate CA established by the eCA or the Company is notified with the meeting minutes or through internal issuance procedures. The eCA notifies subordinate CA not established under the Company and Cross-Certified CAs by letter. The eCA clearly states the reasons for not approving the certificate issuance. The eCA may refuse to issue the certificate for reasons other than applicant identity identification and authentication.

4.8.5 Circumstances Constituting Acceptance of Certificate Modification

The certificate applicant first examines the content of the issued certificate or examines the certificate content for errors. The certificate is then posted by the CA in the repository or sent to the certificate applicant.

4.8.6 Publication of the Modified Certificate by the CA

The CA repository services shall routinely publish all modified certificates. The RA may make an agreement with the CA to send the certificate through the RA to the subscriber.

4.8.7 Notification of Certificate Issuance by the

CA to Other Entities

Not specified.

4.9 Certificate Suspension and Termination

The eCA does not provide certificate suspension and resumption services. Certificate revocation information is published in the eCA repository.

4.9.1 Circumstances for Revocation

The eCA must submit a certificate revocation request under (but not limited to) the following circumstances:

(1) Suspected or confirmed private key compromise including disclosure or loss of private key information.

(2) Certificate is no longer needed for use including termination of eCA services.

Subordinate CAs or Cross-Certified CAs must submit a certificate revocation request under (but not limited to) the following circumstances:

(1) Suspected or confirmed private key compromise including disclosure of loss of private key information.

(2) Certificate is no longer needed for use including termination of CA services or termination of the subordinate or Cross-Certification relationship with the eCA.

(3) The original request for certificate has not been authorized nor able to obtain the authorization afterwards.

In addition, the eCA may revoke certificates without prior approval from the subordinate CA and Cross-Certified CA under the following circumstances:

(1) Incorrectness of any part of the certificate content.

(2) Confirmed case of unauthorized use, forgery or compromised of the private key used for subordinate CA or Cross-Certified CA signatures, or failure to meet the requirements specified in Section 6.1.5 and 6.1.6.

(3) In case of confirmed unauthorized use, forgery or compromise of the eCA's private key or system, all of the certificates issued by the eCA to Subordinate CAs or Cross-Certified CAs are revoked.

(4) The certificates of the eCA, subordinate CA or Cross-Certified CA are not issued in accordance with CPS procedures.

(5) Confirmed case of violation of the CPS, CCA or other related laws and regulations by the eCA, subordinate CA or Cross-Certified CA.

(6) Notification by the competent authority of the eCA, subordinate CA or Cross-Certified CA or in accordance with relevant laws and regulations.

(7) The eCA, subordinate CAs or cross-certificate CAs terminate the services, nor delegate other CAs to provide the certificate revocation service.

(8) Confirmation of the abuse of the certificates issued by the eCA, subordinate CA or Cross-Certified CA.

(9) The subordinate CAs or Cross-Certified CAs fail to reply in writing to accept the confirmation document before the deadline.

(10) The rights under the certificates issued by the eCA, subordinate CA or Cross-Certified CA has been expired, revoked, or terminated, and the eCA does not maintain and

operate the repository, publish the CARL, or provide the OCSP inquiry services.

(11) Revocations required by the certificate policies of the eCA or the CPS.

(12) The technical contents or formats may incur unacceptable risks to the application software suppliers or the relying parties. For example, the certificate is cracked, or confirmed as the non-applicable encryption algorithm, signature algorithm, or length of keys after being assessed by CA/Browser Forum.

If the certificate subject information on a certificate must be changed, the eCA shall review and determine if the certificate should be revoked.

4.9.2 Who Can Request Certificate Revocation

(1) The competent authorities of the eCA, subordinate CA or Cross-Certified CA (e.g. the competent authority to the Electronic Signature Act in Taiwan is MOE).

(2) Subordinate CAs which request revocation of its certificate.

(3) Cross-Certified CAs which request revocation of its certificate.

(4) The eCA. The eCA may request the certificate revocation or revoke the certificate sole upon its discretion by the reasons to revoke certificate specified in Section 4.9.1.

In addition, the subscribers, the application software suppliers, and other third parties may provide the certificate problem reports, to request the revocation to the eCA. After receiving the certificate problem reports, the eCA will confirm if the request accepted or not by the requirement of Section 4.9.5.

4.9.3 Certificate Revocation Procedure

4.9.3.1 Initiation

(1) Initiation request

Request shall be made by letter with the certificate revocation request form attached.

(2) Identity identification and authentication

Identity identification and authentication of the eCA, subordinate CA or Cross-Certified CA shall be carried out in accordance with section 3.2.2.

(3) Request review

The related information on submitted document is reviewed to determine the appropriateness of the certificate revocation request.

(4) Determination

Determine whether to enter the next stage, ask for supporting documents or notify the subordinate CA or Cross-Certified CA by official letter of the denial of the revocation request. The reasons for the denial shall be stated.

4.9.3.2 Certificate Revocation

The eCA adds the revoked certificate to the CARL and posts the CARL in the repository before the next CARL posting at the latest. The subordinate CA or Cross-Certified CA is notified by letter after the certificate revocation. The certificate status information posted in the repository includes revoked certificates until the certificates expire.

4.9.3.3 Responding Mechanism to Certificate Problems

The eCA provides the instruction and guidelines for certificate problem reporting, for the subscribers, the application

software suppliers, the relying parties, and other third-party organizations to report the certificate problem reports when they observe the possible events of private key cracked, certificate abusing, or the certificates are forged, cracked, abused, or used inappropriately.

The subscribers, the application software suppliers, the relying parties, and other third-party organizations may visit the website of the eCA to obtain the instructions/guidelines for certificate problem reporting, and report the certificate problems to the eCA accordingly.

4.9.4 Revocation Request Grace Period

If any of the circumstances described in section 4.9.1 occur, the eCA, subordinate CA or Cross-Certified CA shall submit the certificate revocation request within 10 calendar days and, if possible, before the eCA publishes the following CARL.

Shall the events that allow the eCA revoke the certificates on its discretion without the prior consents from the subordinate CAs or cross-certified CAs, as specified in Section 4.9.1, the eCA may request the revocation of the certificate once the reason of revocation is confirmed, and then inform the subordinate CAs or cross-certified CAs.

4.9.5 Time Within Which CA must Process the Revocation Request

The eCA shall investigate and confirm if the request of certificate revocation is accepted by the following principles in 24 hours upon receiving the certificate problem reports. If the request of certificate revocation is accepted after the confirmation, the

operation of certificate revocation will be proceeded by the requirements of Section 4.9.3.

(1) The claimed problematic content.

(2) The quantity of the certificate problem reports submitted by the certificate or the subscriber.

(3) The entity submits the certificate problem report.

(4) The related laws and regulations.

The eCA shall complete the certificate revocation in seven calendar days upon receiving the certificate revocation request.

4.9.6 Revocation Checking Requirements for Relying Parties

The relying parties shall check the CARL published by the eCA or the responses from the Online Certificate Status Protocol (OCSP) to verify the validity of certificates before using the subordinate CA certificates or self-issued certificates issued by the eCA.

The relying parties shall check the revocation time of the certificate, the authenticity, integrity and validity of the signatures of the CARL or OCSP responses. For example, if the CARL is applied, the relying parties shall check if the DN of the issuer of the CARL matches the DN of Subject of the self-signed certificate in the eCA. Furthermore, the recorded public keys of the self-signed certificate in the eCA shall be applied to verify the CARL.

The relying parties shall check if the CARL is the latest version. The update time of the CARL is recoreded in the “thisUpdate” field on the CARL, and the “nextUpdate” field specifies the expected time for the next update by the eCA. When the relying parties validate the CARL, if they find the system time (which shall be calibrated

regularly) is later than the next update time of the CARL, it means the CARL is not the most updated one. The relying parties shall download the latest CARL in the repository.

In case of verifying the old data (e.g. the filed data), the relying parties shall check if the CARL used at the time the data were generated was valid at that time.

4.9.7 CARL Issuance Frequency

CARLs are issued at least twice per day, and the CARL shall expire within 36 hours. The updated CARLs are published in the repository. Because the eCA may issue the new CARL before the old one expires, the effective period of new CARL may overlap with the old one. During the overlapped period, the new CARL is available at the eCA's repository before the old one expires, for the relying parties to obtain the most updated CA revocation information.

If any certificate is revoked, the eCA will issue the new CARL within 24 hours upon completing the revocation, and add information of the revoked certificate to the CARL and pulished in the repository.

4.9.8 Maximum Latency for eCA Revocation List Publishing

The eCA shall publish the CARL at the latest before the next update (nextUpdate) listed on the CARL.

4.9.9 Online Revocation/Status Checking Availability

The eCA provides the Online Certificate Revocation/Status Verification Services by CARL, web format certificate download,

and OCSP inquiry service.

The eCA uses the OCSP responses complying with RFC 6960 and RFC 5019 standard specifications provided by OCSP responders, and use the private key for signature to issue the RSA 2048 w/SHA-256 certificate of OCSP responder, for the relying parties to validate the digital signature of the OCSP responses, in order to verify the integrity and reliability of the information source. The server certificate of the OCSP responders shall include the extension field "id-pkix-ocsp-nocheck" meeting the specification of RFC 6960.

4.9.10 On-Line Revocation Checking Requirements

If the relying party is unable to check the CARL in accordance with section 4.9.6, Online Certificate Status Protocol (OCSP) services in section 4.9.9 shall be used to check if the certificate used is valid or not.

The eCA supports relying parties to use HTTP POST and GET to execute the OCSP inquiry service. The provided OCSP inquiry service updates and confirms the status of the self-issued certificate, the subordinate CA certificates, and the cross-certificates at least every 12 months. The maximum effective period of the OCSP response is 36 hours. If the self-issued certificate, the certificates of subordinate CA, or the cross-certificates are revoked, the status of the certificate shall be updated within 24 hours upon the revocation, allowing the OCSP inquiry service to provide the most updated and correct status of the certificates.

In case the OCSP responders receives the status request of the un-issued certificates, the status shall not be replied as "Good," and the eCA shall supervise if the OCSP responders reply such request

complying with the above-mentioned secure responding procedure.

4.9.11 Other Forms of Revocation Advertisements Available

For the purpose of quickening the validation of the SSL certificate of high traffic websites to accomplish the validation of the real-time online SSL certificate status, the eCA supports the operation of OCSP stapling.

4.9.12 Special Requirements Related to Key Compromise

The eCA shall state key compromise as the reason for certification revocation in the CARL posted by the eCA if a private key of a subordinate CA or Cross-Certified CA has been compromised.

4.9.13 Circumstances for Suspension

Certificate suspension services are not provided.

4.9.14 Who Can Request Certificate Suspension

Not applicable because certificate suspension services are not provided.

4.9.15 Procedure for Certificate Suspension

Not applicable because certificate suspension services are not provided.

4.9.16 Limits on Suspension Period

Not applicable because certificate suspension services are not provided.

4.9.17 Procedure for Certificate Resumption

Not applicable because certificate suspension services are not

provided.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The eCA shall provide CARLs and a CRL distribution point noted in the subordinate CA certificate. The eCA has been providing OCSP inquiry services starting from May 22, 2015.

The information of certificate revocation in the CARL or OCSP responses can only be removed when the revoked certificate expires.

4.10.2 Service Availability

The eCA shall maintain 24x7 uninterrupted repository system to provide the CARL and the OCSP inquiry service. Under the normal working conditions, the aforesaid certificate status inquiry services shall reply in ten seconds.

The eCA has 27x7 responding mechanism, to adapt the High-Priority Certificate Problem Report. The eCA may report to the law enforcement and revoke the problematic certificate upon its discretion.

4.10.3 Optional features

Not stipulated.

4.11 End of subscription

End of subscription refers to the subordinate CAs or cross-certified CAs cease to use the services of the eCA, including the termination of the services to the subordinate CAs or cross-certified CAs by the eCA when the certificates expire, or the services terminated when the certificates of the subordinate CAs or cross-certified CAs revoked.

The eCA shall allow the subordinate CAs or cross-certified CAs terminate the agreement of the certificate services by revoking certificates, certificate expiring, or invalidate the agreed terms of the Cross-Certification agreement.

4.12 Private Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

The private keys used for signatures by the eCA shall not be escrowed. The eCA does not support the escrowing and recovery of the private keys of subordinate CAs, cross-certified CAs, or subscribers.

4.12.2 Session Key Encapsulation and Recovery Policy and Practice

The eCA does not currently support session key encapsulation and recovery.

5. Facility, Management, and Operation Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

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

5.1.2 Physical Access

Physical control regulations and operation of the eCA meets level 4 assurance level standards. There are four guarding levels in the eCA facility housing. On the first and second levels, there are year-round entrance and building security controls in place. On the third level, access is controlled to this floor using a card access control system. On the fourth level, a fingerprint recognition control system is used to control access for facility personnel. The fingerprint scanner uses 3D sampling technology which is capable of detecting whether the fingerprint is from a live object by fingerprint depth and color.

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

Portable storage devices that are brought into the facility

housing are checked for computer viruses or other types of software that could damage the eCA system.

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

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

(1) Check if system equipment is operating normally.

(2) Check if the computer racks are locked.

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

5.1.3 Power and Air Conditioning

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

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

5.1.4 Water Exposures

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

5.1.5 Fire Prevention and Protection

The eCA facility has an automatic fire detection, alarm and protection system with self-activating extinguishing equipment. Switches are installed at every major entrance / exit of the facility to

allow manual activation by personnel on-site during emergencies.

5.1.6 Media Storage

Audit records, archives and backups are kept in storage media for one year at the eCA facility. After one year, the data shall be moved offsite for storage at a separate location.

5.1.7 Waste Disposal

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

5.1.8 Off-site Backup

The off-site backup location is over 30 km away from the eCA facility. One backup of the all information including data and system programs shall be made at least once per week. Backups of modified data shall be done on the same day of the modification. The non-technical security control of backup site has an equivalent security level as the eCA.

5.2 Procedural Controls

In order to protect the security of system procedures, the eCA uses procedural controls to specify the trusted roles of related system tasks, the number of people required for each task and how each role is identified and authenticated.

5.2.1 Trusted Roles

In order to properly distinguish the duties of each system task and to prevent undetected malicious use of the system, the trusted role authorized to perform each system access task is clearly defined.

The seven trusted roles at the eCA are administrator, officer, auditor, operator, controller, cyber security coordinator and anti-virus and anti-hacking coordinator. Each trusted role is administrated according to section 5.3 to prevent damage caused internal operations. Each trusted role may be performed by multiple persons but one person shall be assigned the chief role. The tasks performed by each role are as follows:

(1) The administrator is responsible for:
- Installation, configuration and maintenance of the eCA system.
- Creation and maintenance of eCA system user accounts.
- Setting of audit parameters.
- Generation and backup of eCA keys.
- Publishing of CARLs in the repository.

(2) The officer is responsible for:
- Activate/deactivate the issuance services of certificate.
- Activate/deactivate the revocation services of certificate.
- Activate/deactivate the issuance services of CARL.

(3) The auditor is responsible for:
- Checking, maintenance and archiving of audit logs.
- Perform or supervise internal audits to ensure the eCA is operating in accordance with CPS regulations.

(4) The operator is responsible for:
- Daily operation and maintenance of system equipment.
- System backup and recovery.
- Storage media updating.
- Hardware and software updates outside the eCA system.
- Maintenance of the website(s)
- Protecting mechanism such as system security or

defending the threats of virus or malicious software.

(5) The physical controller is responsible for:

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

(6) The cyber security coordinator is responsible for:

- Maintenance of the network and network facilities.
- Patches management for the vulnerability of the network facilities
- The cyber security of the eCA.
- The detection and report of the cyber security events.

(7) The anti-virus and anti-hacking coordinator is responsible for:

- Researching, applying, or providing the anti-virus, anti-hacking, and anti-malicious software technologies or measures to ensure the security of the system and the internet.
- Reporting the collected threats of computer virus or vulnerability to the administrator or the cyber security coordinator for enhancement.

5.2.2 Role Assignment

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

(1) The administrator, the officer, the auditor, and the cyber security coordinator cannot assume any other roles among these four at the same time, but the administrator, the officer, and the auditor can be the operator as well.

(2) The physical controller shall not concurrently assume any

role of the administrator, the officer, the auditor, and the operator.

(3) A person serving a trusted role is not allowed to perform self-audits.

5.2.3 Number of Persons Required Per Task

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

(1) Administrator: at least 3 qualified individuals

(2) Officer: at least 3 qualified individuals

(3) Auditor: at least 2 qualified individuals

(4) Operator: at least 2 qualified individuals

(5) Physical Security Controller: at least 2 qualified individuals

(6) Cyber security coordinator: at least 1 qualified individual

(7) Anti-virus and anti-hacking coordinator: at least 1 qualified individual

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

Assignments	Administrator	Officer	Auditor	Operator	Physical Security Controller	Cyber security coordinator	Anti-virus and anti-hacking coordinator
Installation, configuration, and maintenance of the eCA certificate management system	2				1		

Assignments	Administrator	Officer	Auditor	Operator	Physical Security Controller	Cyber security coordinator	Anti-virus and anti-hacking coordinator
Establishment and maintenance of eCA certificate management system user accounts	2				1		
Configuring audit parameters	2				1		
Generation and backup of eCA keys	2		1		1		
Issuing certificates		2			1		
Revoking certificates		2			1		
Publishing CARL in repository	1				1		
Activate/deactivate the issuance services of certificate		2			1		
Activate/deactivate the revocation services of certificate		2			1		
Activate/deactivate the issuance services of CARL		2			1		
Review, maintenance and archiving of audit logs			1		1		

Assignments	Administrator	Officer	Auditor	Operator	Physical Security Controller	Cyber security coordinator	Anti-virus and anti-hacking coordinator
Daily routine operation of system equipment				1	1		
System backup and recovery				1	1		
Updating storage media				1	1		
Software and hardware updates outside of eCA system				1	1		
Website maintenance				1	1		
Daily operation and maintenance of the network and network facilities				1	1	1	
Patching the vulnerabilities of the network facilities	1				1	1	
Reporting the threats of computer virus or vulnerability							1
keep the antivirus system’s signatures update and patches for the vulnerabilities				1	1		

5.2.4 Identification and Authentication for each Role

The eCA utilized system account, password and group management functions and IC cards to identify and authenticate administrator, officer, auditor, operator and controller roles as well as central access control system authorization setting function to identify and authenticate physical security controllers. The eCA uses the user's account, password, and system account administration functions, or other security mechanism to identify the role of the cyber security coordinators.

5.3 Personnel Controls

5.3.1 Background, Qualifications, Experience and Clearance Requirements

(1) Personnel selection and security clearance items

- Personality
- Experiences
- Academic and professional skills and qualifications
- Personal identity check
- Trustworthiness

(2) Management of personnel evaluation

All eCA personnel shall have their qualifications checked before employment to verify their qualifications and work abilities. After formal employment, personnel shall receive appropriate training and sign a document accepting responsibility to perform certain duties. All personnel shall have their qualifications rechecked each year. If personnel do not pass the qualification check, a qualified individual shall be

assigned to serve in this position.

(3) Appointment, dismissal and transfer

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

(4) Duty of confidentiality agreement

All eCA related personnel shall sign an agreement to fulfill the duty of confidentiality and sign a non-disclosure agreement stating that business confidential information may not be disclosed verbally or by photocopy, loan, delivery, article or other methods.

5.3.2 Background Check Procedures

The eCA shall check the related documents that verify the identity and certify the qualifications of the personnel performing the trusted roles defined in section 5.2.1.

5.3.3 Training Requirements

Trusted Roles	Training Requirements
Administrator	1. eCA security clearance system. 2. Installation, configuration, and maintenance of the eCA operation procedures. 3. Establishment and maintenance Cross-Certified CA account operation procedures. 4. Set up audit parameter configuration operation procedures. 5. eCA key generation and backup operation procedures. 6. Operative procedure to publish CARLs in the repository 7. Disaster recovery and continuous operation procedure.
Officer	1. eCA security clearance system. 2. eCA software and hardware use and operation

Trusted Roles	Training Requirements
	procedures 3. Activate/deactivate the issuance services of certificate. 4. Activate/deactivate the revocation services of certificate. 5. Activate/deactivate the issuance services of CARL. 6. Disaster recovery and continuous operation procedure.
Auditor	1. eCA security clearance system. 2. eCA software and hardware use and operation procedures 3. eCA key generation and backup operation procedures. 4. Audit log check, upkeep and archiving procedures. 5. Disaster recovery and continuous operation procedure.
Operator	1. eCA security clearance system. 2. Daily operation and maintenance procedures for system equipment. 3. Upgrading of storage media procedure. 4. Disaster recovery and continuous operation procedure. 5. Network and website maintenance procedure.
Controller	1. Physical access authorization setting procedure. 2. Disaster recovery and continuous operation procedure.
Cyber security coordinator	1. Maintenance of the network and network facilities. 2. Security mechanism for the network.
Anti-virus and anti-hacking coordinator	1. Prevention and control to the threats of computer virus and vulnerability 2. Security mechanism for the operating system and the network.

5.3.4 Retraining Frequency and Requirements

For hardware / software upgrades, work procedure changes, equipment replacement and amendments to related regulations, the eCA will schedule retraining for related personnel and record the

training status to ensure that work procedures and regulatory changes are understood.

5.3.5 Job Rotation Frequency and Sequence

A full year of service at the original position is needed before an administrator can be reassigned to the position of operator or auditor.

A full year of service at the original position is needed before an officer can be reassigned to the position of administrator or an auditor.

A full year of service at the original position is needed before an auditor can be can be reassigned to the position of administrator or an officer.

Only personnel with a full two years of experience as an operator as well as the requisite training and clearance may be reassigned to the position of operator, administrator, or auditor.

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

Only personnel with a full two years of experience as an anti-virus and anti-hacking coordinator as well as the requisite training and clearance may be reassigned to the position of administrator, officer, or auditor.

5.3.6 Sanctions for Unauthorized Actions

The eCA shall take appropriate administrative and disciplinary actions against personnel who violated the CP, CPS or other procedures announced by other eCA. In the event of serious cases that result in damages, appropriate legal action shall be taken.

5.3.7 Independent Contractor Requirement

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

5.3.8 Documentation Supplied to Personnel

The eCA shall make available to related personnel relevant documentation pertaining to the ePKI CP, technical specifications, the CPS, system operation manuals and the Electronic Signatures Act.

5.4 Security Audit Procedure

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

5.4.1 Types of Audited Events

(1) Security audits

- Any change to major audit parameters such as audit frequency, audit event type and new / old parameter content.
- Any attempt to delete or modify audit log files.

(2) Identification and authentication

- Attempt to set up a new role no matter whether successful or not
- Change in the maximum allowable time for identity authentication attempts
- Maximum of identity authentication attempt failure times

when the user logs in the system

- Locked account number unlocked by administrator and the account number is locked due to the number of failed identity authentication attempts
- Administrator changes system identity authentication system such as change from password to biometrics.

(3) Key generation

- eCA key generation times

(4) Private key load and storage

- Loading the private key into a system component
- All access to certificate subject private keys kept by the CA

(5) Trusted public key addition, deletion and saving

- Trusted public key modification including addition, deletion and saving

(6) Private key export

- Export of private keys (does not include single session keys or keys limited to one use)

(7) Certificate registration

- Certificate registration request process

(8) Certificate revocation

- Certificate revocation request process

(9) Certificate status change approval

- Approve or deny certificate status change requests

(10) eCA configuration

- eCA security related configuration setting changes

(11) Account administration

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

(12) Certificate profile management

- Certificate profile changes

(13) CARL profile management

- CARL profile changes

(14) Miscellaneous

- Installation of operating systems.
- Installation of eCA systems.
- Installation of hardware security modules.
- Removal of hardware security modules.
- Destruction of hardware security modules.
- System startup.
- Logon attempts to the eCA certificate management system.
- Hardware and software receipt.
- Attempts to set passwords.
- Attempts to modify passwords.
- eCA internal data backups.
- eCA internal data recovery.
- File manipulation (such as creation, renaming, moving)
- Posting of any information to the repository
- Access to the eCA internal database.
- Any certificate compromise complaints.
- Certificate loading into token.
- Token transmission process.
- Token zeroization.
- eCA or Cross-Certified CA rekey

(15) eCA service configuration changes

- Hardware
- Software

- Operating system
- Patches
- Security profile

(16) Physical access / site security

- Personnel access to the eCA facility.
- Access to the eCA servers.
- Known or suspect violation of physical security regulations

(17) Anomalies

- Software defect
- Software integrity check failure
- Acceptance of unsuitable information
- Irregular routing information
- Network attack (suspect or confirmed)
- Equipment failure
- Power anomalies
- UPS failure
- Clear and significant network service or access failure
- Certificate policy violation
- CPS violation
- Reset system clock

5.4.2 Audit File Processing Frequency

The eCA shall review audit logs once every month and track and investigate major events. Review work includes verifying that the audit logs have not been tampered with, examining all log entries and check them for any warnings or anomalies. The CA shall examine any significant set of security audit records generated since the last audit review and check further for any evidence of malicious

activity. Check if audit log results are documented.

5.4.3 Retention Period for Audit Logs

Audit logs shall be retained on-site for two months and the log retention management system shall be operated in accordance with the regulations in sections 5.4.4, 5.4.5, 5.4.6 and 5.5.

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

5.4.4 Protection of Audit Log Files

Signature and encryption technology shall be used to protect the current and archived audit logs. CD-R or other unmodifiable media shall be used to save the audit logs.

The private keys used to sign event logs may not be used for other purposes. It is prohibited to use audit system private keys for other purposes. The private keys used for the audit system may not be disclosed.

Manual audit logs shall be stored is a secure location.

5.4.5 Audit Log Backup Procedures

Electronic audit logs are backed up once a month.

The eCA shall routinely make backups of the event logs. The audit system shall automatically archive audit trail information regularly on a daily, weekly and monthly basis.

The eCA shall keep the event log files in a secure location.

5.4.6 Security Audit System

Audit systems are built in the eCA system. Audit procedures are activated when the eCA system is activated and only stops when the eCA system is shut down.

If the automated audit system cannot operate normally, the eCA

shall suspend certificate issuance services until the issue is resolved before resuming service again to protect system information integrity and confidentiality when the security system is in a high risk state.

5.4.7 Notification to Event-Causing Subject

If an event occurs which is recorded by the audit system, the audit system does not need to notify the event-causing subject that the event has been recorded by the system.

5.4.8 Vulnerability Assessments

The eCA follows the approaches and frequency required by AICPA/CPA WebTrust $^{SM/TM}$ for Certification Authorities Trust Services Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.0 and CA/Browser Forum NETWORK AND CERTIFICATE SYSTEM SECURITY REQUIREMENTS Version 1.0 to assess the vulnerability at least once per season, and conducts the penetration test once per year. After acknowledging the material change or update for the applications or infrastructures, the eCA must conduct the penetration test as well. The remedy and correction measures are taken after the penetration test and the vulnerability assessment by the eCA. The eCA shall record the skills, tools, ethic codes to be complied with, competing relationship and independence of the personnel and organization that are trustworthy to execute the vulnerability scanning, the penetration test, the health check of information security, or security monitor.

5.5 Records Archival Method

5.5.1 Types of Recorded Events

- eCA accreditation information from competent authorities (hypothetical use)
- CPS
- CCA (hypothetical use)
- System and equipment configuration setting
- System and configuration setting modifications and updates
- Certificate request information
- Revocation request information
- Certificate acceptance confirmation documents
- Issued or announced certificates
- eCA rekey records
- Issued or announced CARLs
- Audit logs
- Used to verify and validate the content of files and other explanatory information or application programs.
- Audit personnel requirement documents
- Organization and personal identity authentication information as stipulated in sections 3.2.2 and 3.2.3

5.5.2 Retention Period for Archive

The retention period for eCA file information is 20 years. The application programs used to process file data are kept for 20 years.

After the file data retention period, written information is destroyed in a safe manner. Backups of information in electronic form shall be backed up separately to other storage media which is given adequate protection or destroyed in a safe manner.

5.5.3 Protection of Archive

Additions, modifications or deletion of archive information is not allowed.

The eCA may transfer the archive information to another storage media which is given adequate protection. The protection level may not be lower than the original protection level.

Archive information is stored in a safe location.

5.5.4 Archive Backup Procedures

Archive information is backed up at an offsite backup center. See section 5.1.8 for the offsite backup location.

5.5.5 Requirements for Record Timestamping

Archived electronic records (such as certificates, CARLs and audit logs) include data and time information and some of these records have appropriate digital signature protection which can be used to check the date and time information on the records for alteration. However, the date and time information on these electronic records are not electronic timestamp information provided by an accredited third party. The date and time are from a computer operating system. All eCA computer systems are regularly calibrated to ensure the accuracy and trustworthiness of the date and time information on electronic records.

Date information is recorded on written archive records. If necessary, time information is also recorded on written archive records. The date and time records on written records may not be arbitrarily changed. If it is necessary to make changes, the changes must be signed by audit personnel.

5.5.6 Archive Information Collection System

The eCA does not have an archive information collection

system.

5.5.7 Procedures to Obtain and Verify Archive Information

Archive information may be obtained after a written request for formal authorization is approved.

Audit personnel are responsible for verification of archive information. The authenticity of document signatures and dates on written documents must be verified. The digital signatures on archive information must be verified for electronic files.

5.6 Key Changeover

The eCA shall renew the key pair for certificate issue before the usage period for the private key issued certificate expires at the latest and issue one new self-signed certificate and two self-issued certificates. The newly issued self-signed certificate is delivered to the relying party in accordance with the regulations in section 6.1.4. The self-issued certificate is published in the repository for relying party download.

The subordinate CA shall renew the key pair for certificate issue before the usage period for the certificate issued with CA's own private key expires at the latest. After the key renewal, the subordinate CA shall apply for a new certificate from the eCA in accordance with the regulations in sections 4.1 and 4.2.

The Cross-Certified CA shall renew the key pair for certificate issue before the usage period for the certificate issued with CA's own private key expires at the latest. After the key renewal, the Cross-Certified CA shall apply for a new certificate from the eCA in accordance with the regulations in sections 4.1 and 4.2.

5.7 Key Compromise and Disaster Recovery Procedures

5.7.1 Emergency and System Compromise Handling Procedures

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

5.7.2 Computing Resources, Software and Data Corruption Recovery Procedure

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

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

5.7.3 eCA Signature Key Compromise Recovery Procedure

The eCA establishes recovery procedures in the event of signature key compromise and conducts annual drills.

5.7.4 eCA Security Facilities Disaster Recovery Procedure

The eCA conducts annual security facility disaster recovery drills.

5.7.5 eCA Signature Key Certificate Revocation Recovery Procedure

The eCA establishes recovery signature key certificate revocation procedures and conducts annual drills.

5.8 eCA Termination Service

The eCA follows the regulations of the Electronic Signatures Act in the event of service termination.

The eCA shall follow the items below to ensure that service termination has a minimal effect on subordinate CAs, Cross-Certified CAs and relying parties:

(1) The eCA shall notify subordinate CAs and Cross-Certified CAs (does not apply if unable to notify), and the application software suppliers (e.g. browers or operating system supplier) in the trust list of the self-issued certificate root CA of the eCA, of the service termination three months in advance and post the notification in the repository.

(2) The eCA shall revoke all unrevoked and unexpired certification when terminating their service as well as safeguard and transfer the related files and records in accordance with Electronic Signatures Act regulations.

6.Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

According to section 6.2.1, the eCA generates key pairs using the NIST FIPS 140-2 algorithm within the hardware security module. The private keys are input and output in accordance with sections 6.2.2 and 6.2.6.

eCA key generation is witnessed and video taped by those related personnel who have signed key initiation witness document (the public key of the generated key pair is listed on it). This public key of the key pairs of the eCA is distributed via trusted channels. The related personnel shall include the members of the ePKI policy management committee, CHT and the qualified auditors.

Subordinate CA and cross-certified CA must generate key pairs in accordance with CP regulations.

When issuing certificates to subordinate CA and cross-certified CA, the eCA checks the public key in each certificate request file to ensure that the CA public key in the certificate issued by the eCA are unique.

The eCA uses a hardware secure module to generate random numbers, public keys and corresponding keys.

Subordinate CAs must follow CP regulations and select suitable software and hardware for key generation. Before subordinate CA certificates are issued, the eCA shall review the suitability of the software or hardware selected by the subordinate CA.

Cross-certified CA must follow CP regulations and select suitable software and hardware for key generation. Before cross-certificates are issued, the eCA shall review the suitability of the software or hardware selected by the CA.

The eCA only provides the self-signed certificate, self-issued certificate, the certificates of the subordinate CAs and the cross-certificate, but not the certificate of subscriber (including SSL certificate). For the related requirements for generating keys of the certificate of subscriber (including SSL certificate) please refer to the CPS of the subordinate CAs under the ePKI or the CPS for the cross-certified CAs.

6.1.2 Private Key Delivery to Subscriber

The subordinate CA must self-generate private keys. Therefore, the eCA does not need to deliver the private key to the subordinate CA.

Any cross-certified CA cross certified with the eCA must self-generate the private key. Therefore, the eCA does not need to deliver the private key to the cross-certified CA.

6.1.3 Public Key Delivery to Certificate Issuer

The PKCS#10 certificate request file is submitted when the CA requests the certificate.

6.1.4 CA Public Key Delivery to Relying Parties

The eCA self-signed certificate contains the eCA public key. There are the following secure distribution channels:

(1) After the eCA has issued a certificate to the subordinate CA, it will delivery this certificate of the subordinate CA along with eCA self-signed certificate or public key to the CA. This subordinate CA stores the eCA self-signed certificate or

public key into the token (such as IC card). The CA distributes this token securely to the subscriber or relying party.

(2) After the eCA has issued a cross-certificate to the cross-certified CA, it will delivery this cross-certificate along with eCA self-signed certificate or public key to the cross-certified CA. This cross-certified CA stores the eCA self-signed certificate or public key into the token (such as IC card). The cross-certified CA distributes this token securely to the subscriber or relying party.

(3) The eCA self-signed certificate is built in the software issued by a trusted third party. Subscribers obtain this software via secure channel (for example purchase software installation CD-ROM from trusted distributor or install from major operating system or browser) from which the eCA self-signed certificate can be obtained.

(4) For eCA self-signed public key certificates stored in mass circulation CD-ROMs, the subscriber obtains these CD-ROMs via secure channels from which the eCA self-signed certificate can be obtained.

(5) When activated by the eCA, the eCA public key is published on-site and the eCA public key certificate signed by related personnel is delivered to the media for announcement (such as published in newspaper or saved in library). The relying party can compare the eCA public key announced by the media with the one contained in the eCA self-signed public key certificate downloaded from the Internet.

6.1.5 Key Sizes

The eCA uses key size of 4096 bit RSA keys and SHA-256, SHA-384, or SHA-512 hash function algorithms to issue certificates.

The subordinate CA and cross-certified CA must follow CP regulations to determine a proper key size, in other words:

(1) Before December 31st, 2030, the subordinate CAs and the cross-certified CAs must use the 2048 bit RSA keys or other keys with equivalent security strength;

(2) From January 1st, 2031, the subordinate CAs and the cross-certified CAs shall use the 3072 bit RSA keys or other keys with equivalent security strength

The eCA shall examine whether the CA has chosen an appropriate key size before the subordinate CA certificate or cross-certificate is issued by the eCA.

6.1.6 Public Key Parameters Generation and Quality Checking

The public key parameter of the RSA algorithm is null.

The eCA and subordinate CA use an ANSI X9.31 algorithm or NIST FIPS 186-4 standard to generate the prime numbers needed for the RSA algorithm and ensure that the prime number is a strong prime.

The cross-certified CA must perform appropriate key parameter quality checking based on the selected algorithm.

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

In the future, if certificates are issued with ECC algorithm, the eCA will comply with the requirements of Section 5.6.2.3.2 and 5.6.2.3.3, NIST SP 56A Revision 2, to verify all the effective periods of keys using ECC Full Public Key Validation Routine and ECC Partial Public Key Validation Routine.

6.1.7 Key Usage Purposes (as per X.509 v3 key usage field)

The private key corresponding to the eCA self-signed certificate can only be used for issuing self-signed certificates, self-issued certificates, certificates of subordinate CAs, cross-certificates, CARLs, certificates of OCSP responders or OCSP responses. The first-generation eCA self-signed certificate does not contain a key usage extension field. From the second generation, the self-signed certificates shall contain a key usage extension field, and marked as "critical" field. The bits of key usage is keyCertSign and cRLSign.

For subordinate CA certificates issued by eCA, the key usage bits used for the certificate's usage extension field setting are keyCertSign and cRLSign.

For cross-certified CA certificates issued by the eCA, the key usage bits used for the certificate's usage extension field setting are keyCertSign and cRLSign.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and

Controls

The eCA uses hardware secure modules complying with FIPS 140-2 Level 3 in accordance with CP regulations.

The subordinate CA must follow CP regulations when choosing an appropriate cryptographic module. The eCA shall examine whether the CA has chosen an appropriate cryptographic module assurance level before the subordinate CA certificate is issued by the eCA.

The cross-certified CA must follow CP regulations when choosing an appropriate cryptographic module. The eCA shall examine whether the CA has chosen an appropriate cryptographic module assurance level before the cross-certificate is issued by the eCA.

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

Control

eCA key splitting multi-person control uses n-out-of-m LaGrange Polynomial Interpolation. It is a perfect secret sharing method which can used for private key splitting and recovery. Besides, n and m must be values greater than or equal to 2, and n must be less than or equal to m. Use of this method can provide the highest security level for eCA private key multi-person control. Therefore, it can be used as the activation method for private keys (see section 6.2.8).

If the signature private key for an assurance level 3 or 4 certificate is to be issued, CP regulations must be followed when using the multi-person procedures. The eCA shall examine whether the CA is using appropriate multi-person control procedures before the subordinate CA certificate and cross-certificate are issued by the

eCA.

6.2.3 Private Key Escrow

eCA private keys used for signatures cannot be escrowed. The eCA is not responsible for safekeeping the signature private keys from subordinate CAs and cross-certified CAs.

6.2.4 Private Key Backup

Backups of private keys are made according to the key splitting multi-person control methods in section 6.2.2 and highly secure IC cards are used for as the secret sharing storage media.

The subordinate CA and cross-certified CA must follow CP regulations when choosing an appropriate private key backup method. The eCA shall examine whether the CA has chosen an appropriate private key backup method before the subordinate CA certificate or cross-certificate is issued by the eCA.

The eCA is not responsible for the safekeeping of the private key backups made by the subordinate CA and cross-certified CA.

6.2.5 Private Key Archival

The eCA signature private key cannot be archived, but the corresponding public key will be archived in a file format according to the requirements of Section 5.5. The eCA does not archive the signature private keys of subordinate CAs and cross-certified CAs.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

The eCA can only transfer private keys into a cryptographic module when conduct key backup recovery or cryptographic module replacement and shall follow the multi-person control method in the section 6.2.2 regulations when transferring private keys into the

cryptographic modules. Encryption or key splitting may be used as the private key transfer method to ensure that the importation process does expose the key code outside the cryptographic module. After the private key importation is completed, the secret parameters related to the importation process generation are completely destroyed.

The subordinate CA and cross-certified CA must follow CP regulations to choose an appropriate private key importation method when it needs to import a private key into a cryptographic module, the eCA shall examine whether the CA has chosen an appropriate private key importation method before the subordinate CA certificate or cross-certificate is issued by the eCA.

6.2.7 Private Key Storage on Cryptographic Modules

Follow the regulations in sections 6.1.1 and 6.2.1.

6.2.8 Method of Activating Private Key

eCA RSA private key activation is controlled by multi-person control IC cards. Different usage control IC cards are kept separately by the administrator and officer.

The subordinate CA and cross-certified CA must follow CP regulations when choosing an appropriate private key activation method. The eCA shall examine whether the CA has chosen an appropriate private key activation method before the subordinate CA certificate or cross-certificate is issued by the eCA.

6.2.9 Method of Deactivating Private Key

As the eCA utilizes an offline operation mode, the eCA keys are normally in a deactivated state in order to prevent illegal use of the private key.

Once certificate issuance and other related administrative work is completed, the eCA uses the n-out-of-m method to deactivate the private key. The subordinate CA and cross-certified CA must follow CP regulations when choosing an appropriate private key deactivation method. The eCA shall examine whether the CA has chosen an appropriate private key deactivation method before the subordinate CA certificate or cross-certificate is issued by the eCA.

6.2.10 Method of Destroying Private Key

In order to prevent the theft of old eCA private keys which influences the correctness of issued certificates, eCA private keys are destroyed at the end of their lifecycle. Therefore, after the eCA completes key renewal and issuance of a new eCA self-signed certificate and no other certificates or CARL will be issued, zeroization of the memory locations of the old eCA private key stored in the hardware secure module is conducted to destroy the old private key in the hardware secure module. Split old private keys are also physically destroyed.

If a hardware secure module will cease to provide the demanded services to the eCA but still is accessible, all the private keys (including these used or probably used private keys) stored in this hardware secure module shall be destroyed. After destroying all the private keys in this hardware secure module, it is necessary to verify that all the aforesaid private key do not exist anymore with the key management tools provided by the hardware secure module.

The subordinate CA and cross-certified CA must follow CP regulations when choosing an appropriate private key destruction method. The eCA shall examine whether the CA has chosen an appropriate private key destruction method before the subordinate

CA certificate or cross-certificate is issued by the eCA.

6.2.11 Cryptographic Module Rating

See section 6.2.1.

6.3 Other Aspects of Key Pair Management

Subordinate CA and cross-certified CA must manage their own key pairs. The eCA is not responsible for safeguarding the private keys of subordinate CA and cross-certified CA.

6.3.1 Public Key Archival

The eCA shall conduct certificate archiving and follow the regulations in section 5.5 to perform security control for the archival system. No addition archiving is done for public keys because certificate archiving can replace public key archiving.

6.3.2 Certificate Operational Periods And Key Pair Usage Periods

The eCA only provides the self-signed certificate, self-issued certificate, the certificates of subordinate CAs and cross-certificate, but not the certificate of subscriber (including SSL certificate). For the related requirements for issuing subscriber certificates (including SSL certificate) please refer to the CPS of the subordinate CAs under the ePKI or the CPS of the cross-certified CAs.

6.3.2.1 eCA Public and Private Key Usage Periods

The RSA key size for eCA public and private keys is 4096 bits. The maximum usage period is 30 years. The maximum usage period for certificates issued with private keys in 10 years, but the usage of certificate issuing authority’s CARLs,

certificates of OCSP responders, or OCSP responses will expire when the issued certificates of subordinate CAs, self-issued certificate or cross-certificate, certificates of OCSP responders, or OCSP responses expire. In addition, as the modification of CP may need to have the self-issued certificate re-issued, and thus the usage period of private key of the eCA is 30 years at maximum.

The usage period for certificates for the private keys and public keys of OCSP responders is one and half days. The new certificates for OCSP responders are published every day (the OCSP responses that uses the new private key to sign digitally contain this OCSP responder certificate, for relying parties to validate the signature of an OCSP response.

The coverage and the expiry dates of all certificates issued with the private key corresponding to the certificate public key shall be considered for the validity of eCA self-signed certificates.

The validity of self-issued certificates cross-signed with old or new eCA keys shall extend until self-signed certificate issued with the old eCA key and all of the certificates issued with the private key corresponding with the public key for its issued certificate expire.

6.3.2.2 Subordinate CA and Cross-Certified CA Public and Private Key Usage Periods

For the public and private key of subordinate CAs and cross-certified CAs, the minimum key size is RSA 2048 bytes, and the maximum usage period is 20 years. For the usage of subscriber certificates issued by private key, the maximum

usage period is 10 years but usage to issue CRLs, OCSP responder certificates or OCSP response is not subject to these restrictions.

The total lifecycle of subordinate CA and cross-certified CA certificates issued by the eCA plus the lifecycle of the signature private key used by the eCA to sign certificates may not exceed the lifecycle of the eCA self-signed certificate.

6.3.2.3 SHA-1 Hash Function Algorithm Validity Period

According to the regulations of CA/Browser Forum's Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v.1.2.1, certification authorities may continue to use the certificates from SHA-1 root certificate CA which have existed before October 2014 (such as the first-generation self-signed certificate of the eCA). The reason is that this kind of public trusted certificates from the root CA are distributed through the safe distribution channels as specified in section 6.1.4.

The eCA uses SHA-256 Hash Function Algorithm to issue self-signed certificates of a new generation eCA from December 2014, and fully utilizes SHA-256 Hash Function Algorithm to issue self-issued certificates, certificates of subordinate CAs and cross-certificates from November 2015.

The first-generation eCA provides the CARLs complying with SHA-1 and SHA-256 Hash Function Algorithm, for the relying parties to validate the status of their certificates of subordinate CAs and cross-certificates issued under SHA-1 and SHA-256 Hash Function Algorithm. The CARLs of SHA-1 Hash Function Algorithm are provided until all the certificates of subordinate CAs and cross-certificates issued

under SHA-1 Hash Function Algorithm by the first-generation eCA expire, or the subordinate CAs and cross-certified CAs no longer provide the issuance service of certifications and CRLs. The second-generation eCA use SHA-256 Hash Function Algorithm to issue CARLs.

The OCSP responders of the eCA use RSA 2048 w/SHA-256 to issue OCSP responses.

The subordinate CAs under the ePKI shall apply SHA-256 or other Hash Function Algorithm with higher security level to issue subscriber certificates, CRL, and OCSP responses. All the SHA-1 SSL certificates under the PKI with valid period over 2017 have been fully revoked. If there is any other SHA-1 subscriber certificates belong to other valid categories, the subordinate CA shall recommend them to choose the appropriate application software, to transfer to SHA-256 or certificates issued by the Hash Function Algorithm with higher security level, otherwise the subscribers shall bear the risks solely.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The eCA activation data is generated by the hardware secure module and then written in the n-out-of-m control IC cards. The activation data within the IC cards is directly accessed by the built-in card readers inside the hardware secure module. The IC card personal identification number (PIN) is directly input from the built-in keyboard in the hardware secure module.

The subordinate CA and cross-certified CA must follow CP regulations when choosing an appropriate activation data generation method. The eCA shall examine whether the CA has chosen an appropriate activation data generation method before the subordinate CA certificate or cross-certificate is issued by the eCA.

6.4.2 Activation Data Protection

The eCA activation data is protected by the n-out-of-m control IC cards. Administrators are responsible for safekeeping of the IC card PINs. The PIN may not be stored in any media. If there are over three failed login attempts, the controlled IC card is locked. During IC card handover, a new PIN is set by the new administrator.

The subordinate CA and cross-certified CA must follow CP regulations when choosing an appropriate activation data protection method. The eCA shall examine whether the CA has chosen an appropriate activation data protection method before the subordinate CA certificate or cross-certificate is issued by the eCA.

6.4.3 Other Aspects of Activation Data

The eCA private key activation data is not archived.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

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

- Identity authentication login.
- Provide discretionary access control.
- Provide security audit capability.
- Access control restrictions for certificate services and trusted roles.
- Offer trusted role and identity identification and authentication.
- Ensure the security of each communication and database through cryptographic technology.
- Offer secure and reliable channels for trusted roles and related identity identification.
- Offer process integrity and security control protection.

6.5.2 Computer Security Rating

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

6.6 Lifecycle Technical Controls

6.6.1 System Development Controls

Quality control for eCA system development complies with CMMI standards.

System development environments, testing environments and on-line operation environments must be segregated to prevent unauthorized access and changes.

The products or programs handed over by the eCA should sign a security warranty guaranteeing there are no back doors or malicious programs and provide a product or program handover list, testing report and system management manuals, and source code scanning report to the

eCA as well as conduct program version controls.

6.6.2 Security Management Controls

The eCA hardware and software is dedicated and only the components which have obtained security authorization can be used. Hardware devices, network connection or software components irrelevant to the operation shall not be installed and the checks for malicious code should be conducted during each use.

When software is installed for the first time, the eCA shall check if the provider has supplied the correct and unmodified version. After system installation, the eCA shall check software integrity during each use and regular use tools include anti-virus software, malware removal tool to scan.

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

The eCA shall reference the methodologies and standards in ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, ISO/IEC 31000 and AICPA/CPA Trust Service Principles and Criteria for Certification Authorities and CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates for risk assessment, risk management and security management and control measures.

6.6.3 Life Cycle Security Controls

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

6.7 Network Security Controls

The eCA servers are not connected to external networks. The repository is connected to the Internet to provide uninterrupted certificate and CARL inquiry services (except during required maintenance or backup).

The certificates and CARLs issued by the eCA servers are protected with digital signature, and sent to the repository from the eCA manually.

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

6.8 Time Stamping

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 issuance times.

(4) System event occurrence times.

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

7.Certificate, CRL and OCSP Service Profiles

7.1 Certificate Profile

The profiles of eCA issued certificates are in compliance with related regulations 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, or the latest version of the related regulations.

The eCA generates the certificate serial number for issued certificates with Cryptographically secure pseudorandom number generator (CSPRNG), and the size of certificate serial number is at least 64 bytes and is non-sequential positive integers.

7.1.1 Version Number

The eCA issues certificates are in compliance with RFC5280 and ITU-T X.509 v3 version.

7.1.2 Certificate Extensions

The extensions of certificates issued by eCA are in compliance with regulations 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.

There are four kinds of certificates issued by the eCA, namely self-signed certificate, self-issued certificate, subordinate CA certificate and cross-certificate. The necessary extension fields and the criticality of that extension field are described below. Other optional extension fields may be used as applicable, and the methods shall comply with the aforesaid regulations.

(1) Self-signed Certificate

Name of the extension field	Criticality	Description
Subject Key Identifier	FALSE	The SHA-1 Hash value of the Subject Public Key
Basic Constraints	TRUE	Subject Type=CA Path Length Constraint=None
Key Usage	TRUE	KeyCertSign and cRLSign

(2) Self-issued Certificate

Name of the extension field	Criticality	Description
Authority Key Identifier	FALSE	The SHA-1 Hash value of the Issuer Public Key
Subject Key Identifier	FALSE	The SHA-1 Hash value of the Subject Public Key
CRL Distribution Points	FALSE	CARL's url announced by the eCA
Authority Information Access	FALSE	Two items included in this extension field: ■ The urls of self-signed certificate and self-issued certificate announced by the eCA ■ The url of OCSP services for the eCA
Certificate Policies	FALSE	Two items shall be included in this extension field: ■ All OIDs defined by the certificate policies of the ePKI, CHT ■ All OIDs defined by CA/Browser Forum, as the following. If the EV SSL OID is applied, the policy qualifier shall be used to marke the

Name of the extension field	Criticality	Description
		announcement of the CPS. ➢ DV SSL OID "2.23.140.1.2.1" ➢ OV SSL OID" 2.23.140.1.2.2" ➢ IV SSL OID "2.23.140.1.2.3" ➢ EV SSL OID "2.23.140.1.1"
Key Usage	TRUE	KeyCertSign and cRLSign
Basic Constraints)	TRUE	Subject Type=CA Path Length Constraint=None

(3) Subordinate CA Certificate

Name of the extension field	Criticality	Description
Authority Key Identifier	FALSE	The SHA-1 Hash value of the Issuer Public Key
Subject Key Identifier	FALSE	The SHA-1 Hash value of the Subject Public Key
CRL Distribution Points	FALSE	CARL's url announced by the eCA
Authority Information Access	FALSE	Two items included in this extension field: ■ The urls of self-signed certificate and self-issued certificate announced by the eCA ■ The url of OCSP services for the eCA
Certificate Policies	FALSE	This extension field used to mark the subordinate CA certificate policies that approved and permitted to use by the eCA; one or more of the following OIDs

Name of the extension field	Criticality	Description
		may be contained. ■ OIDs defined by the certificate policies of the ePKI, CHT ■ OIDs defined by CA/Browser Forum, as the following. If the EV SSL OID is applied, the policy qualifier shall be used to marke the announcement of the CPS. ➢ DV SSL OID "2.23.140.1.2.1" ➢ OV SSL OID" 2.23.140.1.2.2" ➢ IV SSL OID "2.23.140.1.2.3" ➢ EV SSL OID "2.23.140.1.1"
Key Usage	TRUE	KeyCertSign and cRLSign
Basic Constraints	TRUE	Subject Type=CA Path Length Constraint=Setup by the needed certificate path length of the subordinate CA.

(4) Cross-Certificate

Name of the extension field	Criticality	Description
Authority Key Identifier	FALSE	The SHA-1 Hash value of the Issuer Public Key
Subject Key Identifier	FALSE	The SHA-1 Hash value of the Subject Public Key
CRL Distribution Points	FALSE	CARL's url announced by the eCA
Authority Information Access	FALSE	Two items included in this extension field: ■ The urls of self-signed

Name of the extension field	Criticality	Description
		certificate and self-issued certificate announced by the eCA ■ The url of OCSP services for the eCA
Certificate Policies	FALSE	This extension field used to mark the cross-certified CA certificate policies that approved and permitted to use by the eCA; one or more of the following OIDs may be contained. ■ OIDs defined by the certificate policies of the ePKI, CHT ■ OIDs defined by CA/Browser Forum, as the following. If the EV SSL OID is applied, the policy qualifier shall be used to mark the announcement of the CPS. ➢ DV SSL OID "2.23.140.1.2.1" ➢ OV SSL OID" 2.23.140.1.2.2" ➢ IV SSL OID "2.23.140.1.2.3" ➢ EV SSL OID "2.23.140.1.1"
Key Usage	TRUE	KeyCertSign and cRLSign
Basic Constraints	TRUE	Subject Type=CA Path Length Constraint= Setup by the needed certificate path length of the subordinate CA.

In addition to, the eCA is not allowed to issue certificates in the following environments:

(1) The extension fields of the certificates contain the

configurations not applicable to the public internet, such as: in the field of Extended Key Usage, only the configurations applicable to the private internet services.

(2) The information contained in content of certificates may mislead the trusted certificate user to believe this certificate information been verified by the eCA.

The eCA does not issue subscriber certificates. In other words, the eCA does not implement the issuance of precertificates defined by RFC 6962.

7.1.3 Algorithm Object Identifiers

The algorithms indicted by the following OIDs are used for signatures on eCA issued certificates:

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

(OID：1.2.840.113549.1.1.11)

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

(OID：1.2.840.113549.1.1.12)

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

(OID：1.2.840.113549.1.1.13)

The algorithms used with the subject public key on eCA issued certificates must use the following OIDs:

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

(OID：1.2.840.113549.1.1.1)

7.1.4 Name Forms

The subject and issuer fields of the certificate comply with X.500 distinguished name and the attribute type shall comply with

related regulations 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, or the latest version of the regulations.

The issuer field of self-issued certificates, subordinate CA certificates and cross-certificates issued by the eCA shall be identical as the subject field of their self-signed certificates.

From the second-generation of the eCA, the distinguished name of the subject including three attributes, namely "common name" (commonName), "organization name" (organizatioName), and "country Name" (countryName), described as the following:

(1) commonName

To record the name used to identify the eCA. This name is the only one identifier of the certificate, to distinguish from other certificates.

(2) organizationName

The organization name may be a little bit different from the name used to verify identity. Take the abbreviation as an example, part of the text of the organization name can be adjusted by the abbreviation recognized domestically, such as changing "Chunghwa Telecom Company Limited" to "Chunghwa Telecom Co., Ltd."

(3) countryName

To record the country where the place of business of the eCA locates, and shall be represented by the country codes specified in ISO 3166-1.

By issuing the self-issued certificates, subordinate CA certificates and cross-certificates of Cross-Certified CAs, the

eCA has complied with the procedures specified in the certificate policies and/or the CPS, to ensure all the values recorded in the subject of these certificates are accurate.

7.1.5 Name Constraints

No name constraints are used.

7.1.6 Certificate Policy Object Identifier

The self-signed certificates of the eCA does not include any extension field of certificate policies.

For the self-issued certificates, subordinate CA certificates and cross-certificates issued by the eCA, the extension field of certificate policies may use the OID defined by the ePKI, as well as contain the OID defined by CA/Browser Forum, including: DV SSL OID "2.23.140.1.2.1," OV SSL OID" 2.23.140.1.2.2," IV SSL OID "2.23.140.1.2.3," and EV SSL OID "2.23.140.1.1."

7.1.7 Usage of Policy Constraints Extension

Policy constraints extensions are used as required for subordinate CA certificates and cross-certificates issued by the eCA.

7.1.8 Policy Qualifiers Syntax and Semantics

The self-issued certificates, subordinate CA certificates and cross-certificates issued by the eCA may use policy qualifiers in the extension field of certificate policies if needed. Currently, only the self-issued certificates and the subordinate CA certificates that issue EV SSL certificates use policy qualifier, to mark the CPS of the eCA and the url of the announcement.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

The certificate policies extension contained on eCA issued

certificates are not recorded as critical extensions.

7.2 CARL Profile

7.2.1 Version Numbers

The eCA issues CARLs complying with RFC5280 and ITU-T X.509 v 2 version.

7.2.2 CARL and the CARL Entry Extensions

The CARL, crlExtensions and crlEntryExtensions, and crlEntryExtensions issued by eCA complies with the regulations in ITU-T X.509, CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates and IETF PKIX Working Group 5280 or latest versions.

7.3 OCSP Profile

The eCA provides OCSP service in compliance with IETF PKIX Working Group RFC 6960 and RFC 5019 standards and Authority Information Access (AIA) extension in the self-issued certificates, subordinate CA certificates and cross-certificates contain the eCA OCSP service URL.

7.3.1 Version Numbers

The fields in OCSPRequest for the eCA OCSP service include the following data:

- Version number
- The requested certificate identifier

  The requested certificate identifier includes: Hash function algorithm, the Hash value of the CA issuer name, the Hash value of the CA issuer key and the requested certificate serial

number.

The basic fields in OCSPResponse issued by the eCA shall include the following data:

Field	Description
Version number	v.1 (0x0)
OCSP server ID (Responder ID)	OCSP server subject DN)
Produced Time	OCSPResponse sign time
Target certificate identifier	Includes: Hash algorithm, the Hash value of the certificate issuer name, the Hash value of the certificate issuer key and the requested certificate serial number
Certificate Status	Certificate status code： 0: valid 1: revoked 2: unknown
ThisUpdate/NextUpdate	This recommended validity region for this response includes: ThisUpdate and NextUpdate
Signature Algorithm	OCSPResponse signature algorithm, is sha256WithRSAEncryption
Signature	OCSP server signature
Certificates	OCSP server certificate

7.3.2 OCSP Extensions

The eCA OCSPResponse includes the following extensions:

- Authority key identifier of OCSP server.
- If OCSPRequest contains a nonce field, the OCSPResponse also must contain the same nonce field.

8. Compliance Audit and Other Assessments

8.1 Frequency or circumstances of assessment

The eCA accepts a one-time annual compliance audit of the infrastructure (the audit period may not exceed 12 months) and non-scheduled internal audits to verify that related operations conform to the security regulations and procedures of the work standards. Since Chunghwa Telecom ePKI provides publicly trusted SSL certificate issuance services, Trust Service Principles and Criteria for Certification Authorities standards have been adopted and WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security standards are used to conduct eCA audits.

8.2 Identity / Qualifications of Assessor

The Company shall employs an auditor to perform the eCA compliance audit work which is familiar with eCA and subordinate CA operations and has been authorized by WebTrust for CA Seal administration authorities (AICPA/CPA） to perform Trust Service Principles and Criteria for Certification Authorities in Taiwan to provide fair and impartial audit services. Audit personnel shall be qualified and authorized Certified Information System Audit (CISA)

auditors or have equivalent qualifications and shall at least possess the experience of conducting a WebTrust for CA audit twice at 4 man-days or the experience of conducting a CA information security management audit twice at 8 man-days. The eCA shall conduct identity identification of audit personnel during audits.

8.3 Assessor's relationship to assessed entity

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

8.4 Topics Covered by Assessment

(1) Whether or not eCA operations follow the CPS.

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

8.5 Action Taken as a Result of Deficiency

The following actions shall be taken if the establishment or operation of the eCA is found not to conform to CPS regulations:

(1) Record non-conformities.

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

Regarding the non-conforming items, the eCA shall submit an improvement plan within 30 days and promptly implement it. The non-conforming items shall also be listed as follow-up audit tracking items.

8.6 Communications of Results

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

9. Other Business and Legal Matters

9.1 Fees

The eCA reserves the right to collect fees from subordinate CAs and CAs which request cross-certificates. These fees are limited to fees which apply to eCA operation fees.

If the eCA collects fees from subordinate CAs and CAs which request cross-certificates, the CPS will be revised and related fee inquiry methods and fee request procedures shall be established.

9.1.1 Certificate Issuance or Renewal Fees

Not collected at this time.

9.1.2 Certificate Access Fees

Not collected at this time.

9.1.3 Certificate Revocation or Status Information Access Fees

Not collected at this time.

9.1.4 Fees for Other Services

Not collected at this time.

9.1.5 Refund Policy

No fees collected at this time because there is no refund request procedure.

9.2 Financial Responsibility

The eCA is operated by the Company. Its financial responsibilities are the responsibilities of the Company.

9.2.1 Insurance Coverage

The eCA is operated by the Company. Its financial responsibilities are the responsibilities of the Company. No insurance policies have been taken out yet for the eCA certificate business. Insurance will be added in the future as required by competent authority regulations.

9.2.2 Other Assets

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

9.2.3 Insurance or Warranty Coverage for End-Entities

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

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

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

(1) Private keys and passwords used in eCA operations.

(2) eCA key splitting safekeeping information.

(3) Subordinate CA request information may only be disclosed with the permission of the subordinate CA or in compliance with relevant laws and regulations.

(4) Cross-Certified CA request information may only be disclosed with the permission of the Cross-Certified CA or in compliance with relevant laws and regulations.

(5) Audit and tracking logs generated and kept by the eCA.

(6) The audit logs and reports made by audit personnel by during the audit process may not be fully disclosed.

(7) Documents listed as confidential level operations.

9.3.2 Information Not Within the Scope of

Confidential Information

Issued certificates, revoked certificates and CARLs published in the eCA repository are not deemed confidential information.

Identity information and information listed on certificate unless stipulated otherwise are not deemed confidential information.

9.3.3 Responsibility to Protect Confidential Information

The eCA shall handle eCA application information, subordinate CA application information and Cross-Certified CA's cross-certificate application information in accordance with the Electronic Signatures Act, Trust Service Principles and Criteria for Certification Authorities standards and the Personal Information Protection Act.

eCA implements security measures to prevent confidential information against disclosure and damage.

9.4 Privacy of Personal Information

9.4.1 Privacy Protection Plan

The eCA has posted its personal information statement and privacy declaration on its website. The eCA implements privacy impact analysis, personal information risk assessments and related measures for its privacy protection plan.

9.4.2 Information treated as private

The personal information listed on any certificate application is deemed private information and only may be disclosed with the consent of the subscriber or in accordance with related laws and regulations. Information that cannot be obtained through the

certificate and CARL or subscriber information obtained through certificate catalog and personally identifiable 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. The eCA implements security control measures to prevent personally identifiable information from unauthorized disclosure, leakage and damage.

9.4.3 Information Not Deemed Private

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

9.4.4 Responsibility to Protect Private Information

The personal information required for the operation of the eCA, in either paper or digital form, must be securely stored and protected in accordance with the personal information protection and privacy rights declaration posted on the website and comply with related regulations in the Electronic Signatures Act, Trust Service Principles and Criteria for Certification Authorities standards and Personal Information Protection Act.

9.4.5 Notice and Consent to Use Private Information

Follow the Personal Information Protection Act. Personal information shall not be used in other areas without the consent of the CA and the party involved or unless stipulated otherwise in the personal information protection and privacy rights declaration

posted on the eCA website and CPS.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

If judicial, supervisory or law enforcement authorities need to check private information under section 9.4.2 for investigation or evidence collection requirements, the matter shall be handled in accordance with Personal Information Protection Act. However, the eCA reserves the right to collect a reasonable fee from the authorities requesting access to the information.

9.4.7 Other Information Disclosure Circumstances

Subordinate CA may check the application information under section 9.3.1 paragraph (3). However, the eCA reserves the right to collect a reasonable fee from the subordinate CA requesting access to the information.

Cross-Certified CA may check the application information under section 9.3.1 paragraph (4). However, the eCA reserves the right to collect a reasonable fee from the CA requesting access to the information.

Other information disclosure circumstances are handled in accordance with related laws and regulations.

9.5 Intellectual Property Rights

The eCA retains ownership of the eCA key pairs and split keys. Subordinate CA or Cross-Certified CA keys belong to their certificates. However, the certificate is the property of the eCA when the public key is issued as a certificate by the eCA.

The eCA retains ownership of eCA issued certificates and

CARLs.

The eCA retains ownership of the certificate subject names on eCA issued self-signed certificates and self-issued certificates.

The eCA shall do its best to ensure the correctness of subordinate CA and Cross-Certified CA names. However, the eCA does not guarantee trademark ownership of subordinate CA and Cross-Certified CA names. If there is a trademark dispute over a subordinate CA or Cross-Certified CA name, the subordinate CA and Cross-Certified CA shall handle the matter in accordance with legal procedures and submit the results to the eCA to protect their rights.

The CPS may be freely downloaded from the repository or copied and distributed in accordance with the Copyright Act but it must be copied in full and the copyright noted as being owned by the Company. Fees may not be collected from others for the copying and distribution of the CPS. The Company shall prosecute improper use or distribution of the CPS in accordance with the law.

9.6 Representations and Warranties

9.6.1 eCA representations and warranties

(1) Follow CP assurance level 4 regulations and CPS in operations.

(2) Establish subordinate CA application and CA cross-certification application procedures.

(3) Implement subordinate CA application and CA cross-certification application identification and authentication procedures.

(4) Issue and publish certificates.

(5) Revoke certificates.

(6) Issue and publish CARLs.

(7) Issue and provide OCSP response messages.

(8) Implement CA personnel identification and authentication procedures.

(9) Securely generate eCA private keys.

(10) Protect eCA private keys.

(11) Conduct eCA self-signed certificate re-key and self-issued certificate issuance.

(12) Accept subordinate CA certificate registration and revocation applications.

(13) Accept Cross-Certified CA cross-certificate registration and revocation applications.

9.6.2 Registration Authority Representations and Warranties

The eCA does not establish registration authorities. See section 9.6.1.

9.6.3 Subordinate CA and Cross-Certified CA Representations and Warranties

9.6.3.1 Subordinate CA Representations and Warranties

Subordinate CA shall bear the following obligations:

(1) Follow CPS regulations. Liable for damages if relying parties suffer damages due to failure to follow regulations.

(2) eCA issued certificates have different assurance levels and different usages as stipulated in CP regulations. When a certificate application is submitted, the subordinate CA must state the assurance level of the requested certificate.

(3) The subordinate CA handles certificate applications in accordance with the procedures in section 4.2 and checks the correctness of the application information.

(4) After the subordinate CA application is approved and the eCA issues the certificate, the subordinate CA shall accept the certification in accordance with the regulations in section 4.3.

(5) Acceptance of the eCA issued certificate by the subordinate CA indicates that the information contained in the certificate has been checked for accuracy and the certificate shall be used in accordance with section 1.4.1.

(6) The subordinate CA shall self-generate private keys in accordance with the regulations in chapter 6.

(7) The subordinate CA shall properly safeguard and use private keys.

(8) The digital signatures signed with private keys that correspond with certificate public key are subordinate CA digital signatures. When a digital signature is generated, the subordinate CA must check if the certificate has been accepted and the certificate is within the validity period and unrevoked.

(9) If a certificate revocation event of subordinate CA occurs as described in section 4.9.1 (such as the disclosure or loss of private key information) and the subordinate CA needs to revoke the subordinate CA certificate, the eCA shall be notified immediately. However, subscribers shall bear legal responsibility for use of the subordinate CA certificate prior to the notification before the transaction has been taking effect.

(10) IF the eCA is unable to operate normally for some reason, the subordinate CA shall speedily seek other ways for completion of legal acts and may not use the inability of eCA

to provide normal operations as grounds of defense to others.

9.6.3.2 Cross-Certified CA Representations and Warranties

Cross-Certified CA shall bear the following obligations:

(1) Follow CPS regulations and CCA terms and conditions. Liable for damages if relying parties suffer damages due to failure to follow regulations.

(2) eCA issued certificates have different assurance levels and different usages as stipulated in CP regulations. When a certificate application is submitted, the CA must state the assurance level of the requested certificate.

(3) The CA certificate applications are handled in accordance with the procedures in section 4.2 and the CA checks the correctness of the application information.

(4) After the CA cross-certificate application is approved and the eCA issues the certificate, the CA shall accept the certificate in accordance with the regulations in section 4.4.

(5) Acceptance of the eCA issued certificate by the CA indicates that the information contained in the certificate has been checked for accuracy and the certificate shall be used in accordance with the regulations in section 1.4.1.

(6) The CA requesting the cross-certificate shall self-generate private keys in accordance with the regulations in chapter 6.

(7) The Cross-Certified CA shall properly safeguard and use private keys.

(8) The digital signatures signed with private keys that correspond with certificate public key are CA digital signatures. When a digital signature is generated, the CA must check if the certificate has been accepted and the certificate is within the validity period and unrevoked.

(9) If a certificate revocation event occurs as described in section 4.9.1 (such as the disclosure or loss of private key information) and the CA needs to revoke the certificate, the eCA shall be notified immediately and the certificate shall be suspended or revoked in accordance with the regulations in section 4.9. However, the CA shall bear legal responsibility for use of the certificate prior to the publication of certificate revocation status.

(10) If the eCA is unable to operate normally for some reason, the CA shall speedily seek other ways for completion of legal acts and may not use the inability of eCA to provide normal operations as grounds of defense to others.

9.6.4 Relying Parties Representations and Warranties

Relying parties using certificates issued by the eCA shall undertake and guarantee for the following obligations. If there is a violation, relying parties shall be liable for any loss or damages within the scope of attribution:

(1) The relying party must follow CPS regulations when using eCA issuance certificates or checking the eCA repository.

(2) The relying parties shall obtain the trusted eCA public keys or self-signed certificates through secure distribution channels according to the self-signed certificate described in section 6.1.4.

(3) Relying parties shall first check the certificate assurance level when using eCA issued certificates to ensure their rights.

(4) Relying parties shall first check the usage restrictions when

using eCA issued certificates to confirm that certificate use conforms to usage restrictions set down by the eCA.

(5) Relying parties shall first check the CARL when using eCA issued certificates or OCSP response messages to check if the certificate is valid or not.

(6) Relying parties shall obtain the self-issued certificate from the eCA repository when using the self-issued certificates after eCA rekey to establish a certificate trust path between the eCA and CA.

(7) Relying parties shall first check the digital signature when using eCA certificates, CARLs or OCSP response messages to verify that the certificate, CARL or OCSP response messages is correct.

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

(9) If the eCA is unable to operate normally for some reason, the relying parties shall speedily seek other ways for completion of legal acts.

(10) The relying parties shall understand and agree to the eCA liability terms and conditions and also accept and use the eCA issued certificate within the certificate trust scope defined in section 1.4.1.

9.6.5 Other Participant Representations and Warranties

Not stipulated.

9.7 Disclaimer of Warranties

If a portion of certificate service must be temporarily suspended due to eCA system maintenance, conversion or expansion requirements, the eCA shall post an announcement in the repository three days in advance and notify the subordinate CAs, Cross-Certified CAs and relying parties. Subordinate CAs and Cross-Certified CAs may not use this as a reason to claim compensation from the eCA.

If subordinate CAs and Cross-Certified CAs submit a certificate revocation request to the eCA due to certificate revocation circumstances in section 4.9.1. After receiving the certificate revocation application, the eCA shall complete the certificate revocation work in 10 working days at the latest and post the issued CARL in the repository. Cross-Certified CAs shall take appropriate actions to limit the effect on relying parties and bear the responsibility of use of the certificate by the CA prior to the publishing of the certificate revocation status.

9.8 Limitations of Liability

The eCA operates in accordance with CP assurance level 4 and follows CPS procedures for certificate issuance and revocation, CARL issuance and publication, provide OCSP services and maintain regular repository operation.

The eCA shall not be liable for consequences arising from the failure of subordinate CA, Cross-Certified CA or relying parties to use certificates which the scope of use set down in section 1.4.1.

9.9 Indemnities

9.9.1 eCA Liability

(1) If subordinate CAs, Cross-Certified CAs or relying parties suffer damages due to intentional or accidental failure of eCA work personnel to follow CPS regulations when performing self-signed certificate, self-issued certificate, CA certificate, and cross-certificate issuance and revocation work or violation of related laws and regulations which caused the eCA, subordinate CAs, Cross-Certified CAs or relying parties to suffer damages, the eCA shall compensate for the direct damages in accordance with regulations.

(2)In the event of damages caused by certificates issued by the eCA due to force majeure factors under section 9.16.5, the eCA shall not bear any liability.

(3) If the CA's certificate is used for illegal transactions during the period from after a CA or another entitled party submits a certificate termination request to until the eCA actually completes the termination of that CA's certificate, the eCA shall not bear any liability provided the eCA a performs the processing work in accordance with the CPS and related work regulations.

(4) If damages are incurred due to the failure of the subordinate CA, Cross-Certified CA or relying party to use the certificate in accordance with the usage regulations in section 1.4.1, the eCA shall not bear any liability.

(5) The limitation period for damage claims is set in accordance with the provisions of the Electronic Signatures Act and related laws and regulations.

9.9.2 Subordinate CA and Cross-Certified CA Liability

Under legal standards, the eCA may request that the subordinate CA and Cross-Certified CA be liable for the direct damages which were caused by the following circumstances:

(1) False or fraudulent reporting during certificate application by the subordinate CA or the Cross-Certified CA results in the issuance of inaccurate CA certificates or cross-certificates by the eCA.

（2) Improper safekeeping of the private key by the subordinate CA or Cross-Certified CA results in the compromise, disclosure, alteration or unauthorized use of the private key.

(3) The subordinate CA or Cross-Certified CA violates the law, CP or CPS (such as failure to issue proper certificates according to the assurance level in CPS regulations) or cross-certificate agreement regulations.

(4) The subordinate CA or Cross-Certified CA violates the agreements signed with the eCA for participation in the root certification programs of operation systems, browsers and software applications which could affect the trusted CA list that the eCA has built in or applied for built in the above application software suppliers.

eCA may stipulate the liability of subordinate CAs or Cross-Certified CAs in the Cross-Certification Agreement,

9.10 Term and Termination

9.10.1 Term

The CPS and any attachments shall take effect when approved by the Electronic Signatures Act competent authority and published on the eCA website and repository. The CPS and any attachments remain in effect until replaced with a newer version.

9.10.2 Termination

The old version of the CPS and any attachments shall be terminated when a newer version is approved by the Electronic Signatures Act competent authority and published.

9.10.3 Effect of Termination and Survival

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

9.11 Individual Notices and Communication with Participants

The eCA, subordinate CAs, Cross-Certified CAs, subscribers and relying parties shall adopt suitable methods for establishing mutual notification and communication channels including but not limited to official document, letter, telephone, fax, e-mail or secure e-mail.

9.12 Amendments

9.12.1 Procedure for Amendment

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

The eCA conducts annual reviews of the terms specified in the official version of Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates and Guidelines for the Issuance and Management of Extended Validation Certificates issued by CA/Browser Forum (http://www.cabforum.org), to evaluate if the CPS needs any amendment. If there is any contradiction between the CPS and the regulations of that Forum, the regulations of the Forum prevails, and the CPS is amended accordingly.

9.12.2 Notification Mechanism and Period

9.12.2.1 Notification Mechanism

All change items are posted in the eCA repository. Where the impact of Section 9.12.2.2 (1) is significant, letters are issued to notify subordinate CA and Cross-Certified CA not established by the Company.

No additional notification is made for non-material changes to the CPS.

9.12.2.2 Modification Items

Assess the level on impact of change items on subordinate CA, Cross-Certified CA and relying parties:

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

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

9.12.2.3 Comment Reply Period

The reply period for comments on change items is:

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

Where the impact of section 9.12.2.2 (2) is less significant, the reply period is within 7 calendar days of the posting date.

9.12.2.4 Comment Handling Mechanism

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

9.12.2.5 Final Notification Period

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

9.12.3 Circumstances Under which the OID Must Be Changed

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

9.13 Dispute Resolution Provisions

In the event of a dispute between CA belonging to the Company and the eCA, the dispute shall be jointly resolved between the Company's organization and management system and higher level competent authorities. If there is a dispute between the Cross-Certified CA not established by the Company and the eCA, a consensus shall first be reached through negotiation. If negotiation fails, the parties shall handle the dispute according to the dispute resolution procedures provided in the contract. In the event of litigation, the Taiwan Taichung District Court shall be the court of first instance.

9.14 Governing Law

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

9.15 Compliance with 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 and CPS.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

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

9.16.2 Assignment

The rights and obligations of key participants (eCA, RA, subscribers and relying parties) described in the CPS may not be assigned in any form to other parties without notifying the Public CA.

9.16.3 Severability

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

The CPS complies with the requirements to the root CAs in the official version of Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates and Guidelines for the Issuance and Management of Extended Validation Certificates issued by CA/Browser Forum

(http://www.cabforum.org); however, if the related requirements of the Baseline Requirements and EV SSL Certificate Guidelines conflict with the related domestic laws and regulations complied by the CPS, the CPS may be adjusted to satisfy the requirements of the laws and regulations. If the domestic laws and regulations are not applicable anymore, or the Baseline Requirements and EV SSL Certificate Guidelines revised their contents to be compatible with the domestic laws and regulations, the CPS will delete and amend the adjusted contents. The aforesaid actions shall be completed in 90 days.

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 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 do 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 CA or a relying party suffers damages due to a force majeure or other circumstances not attributable to eCA including but not limited to natural disasters, war or terrorist attack, the eCA shall not bear any legal liability.

9.17 Other Provisions

Not stipulated

Appendix 1: Acronyms and Definitions

Acronyms	Full Name	Definition
AATL	Adobe Approved Trust List	
AIA	Authority Information 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.
CRL	Certificate Revocation List	See Appendix 2.
CT	Certificate Transparency	See Appendix 2.
DN	Distinguished Name	
DNS	Domain Name System	See Appendix 2.
DV	Domain Validation	See Appendix 2.
eCA	ePKI Root Certification Authority	See Appendix 2.
EE	End Entities	See Appendix 2.
ePKI	Chunghwa Telecom ecommerce Public Key Infrastructure	See Appendix 2.
EV	Extended Validation	See Appendix 2.

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

Term	Definition
Access	Use the information processing capabilities of system resources.
Access Control	Authorization procedure for access to information system resources given to subscribers, programs, procedures and other systems.
Activation Data	The private data required besides keys to access the cryptographic module (such as data used to activate the private key for signatures or encryption).
American Institute of Certified Public Accountants (AICPA)	Institution which jointly drafted The Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy system standards with the Chartered Professional Accountants Canada and the management organization for WebTrust for CA and SSL Baseline Requirement & Network Security mark.
Applicant	Subscribers who request certificates from a CA and have not yet completed the certificate procedure.
Archive	A physically separate storage site for long-term information (storage site for important information) which can be used to support audit, usage and integrity services.
Assurance	A reliable basis to determine that an entity conforms to certain security requirements (the

Term	Definition
	standards in Chapter 1 and Chapter 2 Item 1 in the CPS.
Assurance Level	A level possessing a relative assurance level (standards in Chapter 1 and Chapter 2 item 2 in the CPS)
Audit	Assessment of whether system controls are adequate and ensure conformance with existing policy and operation procedures, and independent checking and review of recommended required improvements to existing controls, policies and procedures.
Audit Data	Activity logs of a system organized in the order of time of occurrence that can be used to reconstruct or investigate the time sequence or changes that occurred during a certain event.
Authenticate	(1) Authentication is the process by which a claimed identity is verified. (A Guide to Understanding Identification and Authentication in Trusted Systems, National Computer Security Center) (2)Determination of identity authenticity when an identity of a certain entity is shown.
Authentication	(1)The process of establishing confidence in the identity of users or information systems. (2)Security measures used for information transmission, messages and ways to authorize individuals to receive certain types of information.

Term	Definition
	(3) "authentication" is proof of identification. Mutual authentication refers to authentication mutually conducted between two parties during communication activities.
Authority Information Access (AIA)	Records extensions related to certificate authority information access. The content may include: OCSP service sites and certificate issuance authority certificate verification path downloading site.
Backup	Information or program copying that can be used for recovery purposes when needed.
Binding	The process for binding (connecting) two related information elements.
Biometric	The physical or behavioral attributes of a person.
CA Certificate	Certificates issued by CAs.
Capability Maturity Model (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:

Term	Definition
	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 time stamped list. The list contains the serial numbers of revoked CA The list contains the serial numbers of revoked CA public key certificates (including subordinate CA certificates and cross-certificates).
Certificate Policy (CP)	(1) Refers to a named set of rules that indicates the applicability to a certain community or class of application with common security requirements (Article 2.3 Chapter 1, in the Regulations on the Required Information for

Term	Definition
	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

Term	Definition
	certificate policy or other service contracts).
Certificate Problem Reports	The complaints regarding suspected cracking of keys, certificate misused, or other types of fraud, cracks, abuse, or inappropriate behaviors related to certificates.
Certificate Revocation List (CRL)	(1) The certificate revocation list digitally signed by the certification authority provided for relying party use. (Article 2.8, Chapter 11 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.
Certificate Transparency (CT)	Certificate transparency is an open platform for the public monitoring and auditing of all certificates on the Internet (SSL certificate is the priority objective at the current stage). The information is given to domain name owners, CA and domain name subscribers on issued and existing public certificates is provided to judge if the certificate has been misissued or maliciously issued. In other words, the purpose is to provide a public monitoring and information disclosure environment which can be used to monitor TLS/SSL certificate systems and review specific TLS/SSL certificates to lessen certificate-related risks. Certificate transparency is mainly comprised of certificate journals, certificate monitors and certificate auditors.
Chartered Professional Accountants Canada (CPA)	Institution which jointly drafted The Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality

Term	Definition
	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 certificate used to establish a trust relationship between two root CAs. This certificate is a type of a CA certificate and not a subscriber certificate.
Cross-Certificate 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.
Cryptographic Module	A set of hardware, software, firmware or combination of the above used to run cryptologic or programs (including crypto algorithms) and included within the cryptographic boundaries of

Term	Definition
	the module.
Crypto period	The validity period set for each key.
Data Integrity	Information that has been subjected to unauthorized access or accidental modification, damage or loss.
Digital Signature	An electronic signature generated by use of mathematic algorithm or other means to create a certain length of digital data encrypted by the signatory's private key and capable of being verified by the public key. (Article 2.3 Electronic Signatures Act)
Domain Name	A node label assigned by the domain name system. Converts the IP address into a text name that is easily remembered by humans.
Domain Name System (DNS)	A distributed database used to automatically convert the IP address to domain name.
Domain Validation (DV)	Before SSL certificate approval and issuance, authentication of subscriber domain name control rights but no authentication of subscriber organization or individual identity, so the connection to a domain validation SSL certificate installed websites are able to provide SSL encryption channels but are unable to know who the owner of the website is.
Dual-Use Certificate	Certificates that may be used for digital signatures or data encryption.
Duration	A certificate field made up of two subfields "start time of the validity period" (not Before) and "end

Term	Definition
	time of the validity period" (not Before).
E-commerce	Provision of goods for sale and other services through the use of network technology (specifically the Internet).
Encryption Certificate	A certificate including a public key used for encryption of electronic messages, files, documents or other information. This key can also be used to establish or exchange a variety of short-term secret keys for encryption.
End Entity	The PKI includes the following two types of entities: (1) Those responsible for the safeguarding and use of certificate public keys. (2) Third parties who trust the certificates issued by the PKI (not holders of private keys and not a certificate authority). The end entities are subscribers and relying parties including personnel, organizations, accounts, devices and sites.
End-Entity Certificate	Certificates issued to end-entities.
Chunghwa Telecom ecommerce Public Key Infrastructure (ePKI)	In order to promote Electronic Policy and create a sound e-commerce infrastructure, the Chunghwa Telecom Co., Ltd. shall follow the ITU-T X.509 standards to establish the public key infrastructure for use with various applications in e-commerce and e-government.
Chunghwa Telecom	An organization which was established for the

Term	Definition
ecommerce Public Key Infrastructure Policy Management Committee (ePKI Policy Management Committee)	purpose of: Discuss and review the ePKI CP and electronic certificate system framework, accept subordinate CA and cross-certified CA interoperation applications and other matters such as review and study of CPS and electronic certificate management matters.
ePKI Root CA (eCA)	The Chunghwa Telecom Public Key Infrastructure Root Certification Authority (Root CA) is the top level certificate authority in this hierarchical public key infrastructure. Their public keys are the trust anchor.
Extended Validation (EV)	Validation process defined in the Guidelines for the Issuance and Management of Extended Validation Certificates issued by the CA/Browser Forum.
EV Certificate	Certificate subject information including the information validated in accordance with CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates regulations.
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

Term	Definition
	module into 11 types of security requirements. Each security requirement type is then divided into 4 security levels.
Firewall	An access restriction gateway between networks which complies with near-end (local area) security policy.
Fully Qualified Domain Name (FQDN)	An unambiguous domain name that specifies the exact location of a computer within the domain's hierarchy. The fully qualified domain name consists of two parts: the host name (service name) and domain name. For example, ourserver.ourdomain.com.tw. "ourserver" is the host name and "ourdomain.com.tw" is the domain name. In this name, ourdomain is the second-level domain, .com is the generic top-level domain, (gTLD) and .tw is the country code top-level domain (ccTLD). A fully qualified domain name always starts with a host name.
Identification	A statement of who the user is (globally known)(A Guide to Understanding Identification and Authentication in Trusted Systems) "identification" is a statement of who the user is (globally known)
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

Term	Definition
	of high quality technical documents affects how man designs, uses and manages the Internet and allows the Internet to operate smoothly.
Individual Validation (IV)	Except for identification and authentication of natural person subscriber's domain control rights, identification and authentication of subscriber personal identity according to the certificate's assurance level during the SSL certificate approval process. Therefore, connection to an IV SSL certificate installed website can provide a TLS encryption channel. It is known which individual is the owner of that website to ensure the integrity of data transmission.
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

Term	Definition
	following attributes: (1) One of the keys is used for encryption. This encrypted data may only be decrypted by the other key. (2) It is impossible to determine one key from another (from a mathematical calculation standpoint).
Internet Assigned Numbers Authority (IANA)	Internet site assignment organization responsible for managing the IP addresses, domain names and many other parameters used for the Internet.
Issuing CA	For a particular certificate, the CA that issues the certificate is called 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.
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.

Term	Definition
Object Identifier (OID)	(1) One type of unique alphanumeric / numeric identified registered under the International Standard Organization registration standard which could be used to identify the uniquely corresponding certificate policy; where the certificate policy is modified, the OID is not changed accordingly. (Article 2.4 Chapter 1 in the Regulations on Required Information for Certification Practice Statements) (2) When a special form of code, object or object type is registered with the International Standard Organization (ISO), the unique code may be used as an identified. For example, this code can be used in the public key infrastructure to indicate what certificate policy and cryptographic algorithms are used.
Online Certificate Status Protocol (OCSP)	Online Certificate Status Protocol is a type of online certificate checking protocol which lets the application software of relying parties to determine the status (such as revoked or valid) of a certain certificate.
OCSP Responder	An online server authorized by a CA to operate, and connected to the repository to process the certificate status requests.
OCSP Stapling	This is a form of TLS Certificate Status Request extension, which may replace the OCSP to check X.509 certificate status.

Term	Definition
	In practice, a website may obtain a “time limited (e.g. two hours)” OCSP response from the OCSP responder and cache it. Next, this cached OCSP response will be sent to the subscriber (typically a browser) whenever initiating the TLS Handshake. The subscriber only needs to verify the validity of that OCSP response without sending the OCSP request to the CA. In that way, the subscriber will not need to request the SSL certificate status from the CA when connecting to a high traffic TLS website, and thus to decrease the burden of the CA. This mechanism also prevents the privacy concern that the OCSP responder knows which subscribers attempting to browsing that SSL website by having the TLS website transferring the OCSP Response, including the information related to the validity of the SSL certificate, issued by the OCSP responder of the CA.
Out-of-Band	Delivery method other than ordinary information delivery channels. If the delivery method is by electric cable, a special secure channel may be the use of physical registered mail.
Organization Validation, (OV)	In the SSL certificate approval process, except for identification and authentication of subscriber domain name control rights, following the certificate assurance level to identify and

Term	Definition
	authenticate the identity of subscriber organizations and individuals. So connection to an Organization Validation SSL certificate installed websites is able to provide SSL encryption channels, know who the owner of the website is and ensure the integrity of the transmitted information.
Private Key	(1) The key in the signature key pair used to generate digital signatures. (2) The key in the encryption key pair used to decrypt secret information. This key must be kept secret under these two circumstances.
Public Key	(1) Key used to verify the validity of digital signature in a pair of signature keys. (2) Key used to encrypt the classified information in a pair of encryption/decryption keys. (3) In the both environment, the key must be public accessible (in digital certificate format generally).
Public Key Infrastructure (PKI)	A set of roles, policies, standards, personnel, equipment, facilities, technology, audits , services and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.
Public-Key Cryptography Standard,	In order to promote the use of public key technology, the RSA laboratory under the RSA

Term	Definition
(PKCS)	Information Security Company has developed a series of public key cryptography standards that are widely used by the industry.
Qualified Auditor	Accountant firms, entities, or individuals that satisfy the auditor qualification specified in Section 17.6 of Guidelines for the Issuance and Management of Extended Validation Certificates, and Section 8.2 of the Baseline Requirements, as well as independent from the audited parties.
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

Term	Definition
	subject named in a trusted certificate and public key listed in the certificate. (Article 2.6, Chapter 1 in the Regulations on Required Information for Certification Practice Statements) (2) The individual or agency which receives information including a certificate and digital signature (the public key listed on the certificate may be used to verify the digital signature) and may rely on this information.
Renew (a certificate)	The procedure for issuing a new certificate to renew the validity of information bound together with the public key.
Repository	(1) A trustworthy system used to store and retrieve certificates and other information relevant to certification. (Article 2.7, Chapter 1 in the Regulations on Required Information for Certificate Practice Statements) (2) The database containing the certificate policy and certificate-related information.
Reserved IP Addresses	IPv4 and IPv6 addresses 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
Root Certification	The highest level certificate authority in a public

Term	Definition
Authority (Root CA)	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.
Revoke a Certificate	Termination of a certificate prior to its expiry date.
Request for Comments, (RFC)	A series of memos issued by the Internet Engineer Task Force that include Internet, UNIX and Internet community standards, protocols and procedures for number assignment.
Secure Socket Layer	Protocol issued by Netscape through 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)

Term	Definition
	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.
Self-Issued Certificate	Self-issued certificate is the certificate issued when the root CA replacing keys or when the certificate policy needing. It is issued by the root CAs of two generations to each other by using the private keys, to establish the certificate-trusted path between the old and new keys or the interconnection of the certificate policies.
Self-Signed Certificate	Self-signed certificate means the certificate whose name of the issuer is identical to the name of the certificate subject. In other words, it is a certificate issued by using the private key of a pair of keys to focusing the paring public key and other information. A self-signed certificate under a PKI may be used as the trust anchor of a certificate path. The subject of certificate issuance is the eCA itself. This certificate contains the public key of the eCA and

Term	Definition
	the name of the issuer is identical to the name of the certificate subject. It may be used by the relying parties to verify the digital signature of self-issued certificates, subordinate CA certificates, cross-certificates and CARLs issued by the eCA.
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

Term	Definition
	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

Term	Definition
	to authenticate certificates.
Trusted Certificate	Certificate trusted by relying party obtained through a secure and reliable transmission method. The public key contained in this type of certificate comes from a trusted path. Also called a trust anchor.
Trustworthy System	Computer hardware, software and programs which possess the following attributes: (1) Functions that protect again intrusion and misuse. (2) Provides reasonably accessible, reliable and accurate operations. (3) Appropriate implementation of preset function. (4) Security procedures uniformly accepted by the general public.
Uninterrupted Power System (UPS)	Provide uninterrupted backup power to loading equipment in the event of abnormal power conditions (such as power outage, interference or power surge) to allow uninterrupted operation of servers, switches and other critical equipment and precision instruments to prevent loss of calculation data, communication network interruption and loss of instrument control.
Validation	The process of identification of certificate applicants. Validation is a subset of identification and refers to identification in the context of establishment of the identity of certificate applicants. (RFC 3647)
Zeroize	Method to delete electronically stored information.

Term	Definition
	Storage of changed information to prevent information recovery.