ePKI Root Certification Authority

Certification Practice Statement

Version 1.7

Chunghwa Telecom Co., Ltd.

April 22, 2020

Contents

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 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.
1.5	May 28, 2018	(1) Based on the audit criteria information announced in CPA Canada's website (http://www.webtrust.org) to amend Abstract, Section 5.4.8, Section 6.6.2, Section 8.2、Section 8.6, Section 9.3.3 and Section 9.4.4. (2) Add the information of CAA issuer Domain Names of ePKI into Section 2.2 based on Baseline Requirements.

Version	Date	Revision Summary
1.6	April 30, 2019	(1) Section title revision to meet RFC 3647. (2) Add assurance assurance level definitions to Section 1.4.1. (3) Amendments are made in Sections 1.5.2, 4.9 and 9.12 in compliant with the Baseline Requirements. (4) Revision of Sections 2.3, 3.2.6, 4.2, 4.5, 4.8.4, 4.8.5, 4.10, 5.6, 6.1, 6.2, 6.3, 6.6.2, 6.8, 7.1, 7.2, 7.3, 8.1, 9.7, 9.8, 9.16.3 and 9.16.4.
1.65	Aug 30, 2019	Add the information of GTLSCA in Section 1.3.1.2.
1.67	Nov 18, 2019	(1) Add the information of eTSCA in Section 1.3.1.2. (2) Remove the description regarding the validity of OCSP responses in Section 4.9.10. (3) Amendments are made in Section 7.1.2 on the Certificate Policies extensions of self-issued certificate, subordinate CA certificate and cross-certificate. (4) Amendments are made in Section 7.1.8 on the description that eCA may use policy qualifier to mark the URL of the eCA CPS.
1.7	Apr 22, 2020	(1) Amendments is made in Section 4.9.10 in accordance with CA/B Forum Ballot SC23. (2) Amendments is made in Section 7.1.2 in accordance with the Baseline Requirements and the operation status of CA. (3) Revision of Sections 1.3.4, 1.5.3, 1.5.4, 3.2.5, 4.1.2 4.9.9, 5.3.7, 6.3.2.1, 7.3, 8.5, 9.5, 9.6.3 and 9.16.

1. Introduction

1.1 Overview

1.1.1 Certification Practice Statement

The ePKI Root Certification Authority (eCA) Certification Practice Statement (CPS) conforms to 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 sub-law of the Electronic Signatures Act, and the official versions of related international standards such as the Internet Engineering Task Force (IETF) RFC 3647, RFC 5280, ITU-T X.509, CA/Browser Forum (http://www.cabforum.org) Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (Baseline Requirements) and Guidelines for the Issuance and Management of Extended Validation Certificates (EV SSL Certificate Guidelines). This CPS mainly describes how eCA performs the issuance and management of self-signed certificates, self-issued certificates, subordinate CA certificates, and cross-certificates in accordance with the identity assurance level 4 defined in the ePKI CP.

According to the ePKI CP, eCA is a top-level CA and a trust anchor of ePKI. eCA must maintain a high level of credibility that relying parties can directly trust its certificates.

1.1.2 CPS Applicability

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

Any problems arising from the reference of this CPS by any CA which is not authorized by eCA shall be the responsibility of that CA.

1.2 Document Name and Identification

This document is ePKI Root Certification Authority Certification Practice Statement of Chunghwa Telecom and was approved for publication on April 22, 2020. This CPS is version 1.7. The current version of this CPS can be obtained at the website: https://eca.hinet.net or https://epki.com.tw/.

This CPS was stipulated based on the ePKI CP. The operation of 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}
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 ePKI 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 Baseline Requirements 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.

If the SSL server certificates issued by subordinate CA conform to the EV SSL Certificate Guidelines 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)).

If there is any inconsistency between this CPS and the official versions of the Baseline Requirements and EV SSL Certificate Guidelines, then the Baseline Requirements and EV SSL Certificate Guidelines take precedence.

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 this CPS include:

(1) eCA
(2) Subordinate CA
(3) Cross-Certified CA
(4) Relying Parties

1.3.1 Certification Authorities

1.3.1.1 eCA

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, 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.

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 eCA and other subordinate CAs shall be set up.

The first level subordinate CAs under ePKI has three Subordinate CAs, including Public Certification Authority (PublicCA), ePKI Timestamping Certification Authority (eTSCA) and Government TLS Certification Authority (GTLSCA), where PublicCA and eTSCA are formed by Chunghwa Telecom Co., Ltd. (CHT) and GTLSCA is entrusted by National Development Council (NDC) with the task of operation.

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 eCA. The root CA, which wishes to apply for cross-certification with eCA, must first conform to the security regulations of the assurance levels defined in the ePKI CP, 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

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, a Subordinate CA is not called the subscriber because the Subordinate CA is capable of issuing certificates.

1.3.4 Relying Parties

A relying party is the entity that relies on the validity of the binding of the certificate subject name to a public key, that is, the relying party is a third party (not a private key holder or a CA) trusting

certificates issued by CAs in ePKI. The relying party must check the validity of the received certificate by checking the CA certificate and the appropriate certificate status information. The certificate may be used for the following work after checking the validity of the certificate:

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

(2) Identify the creator of a signature of an electronic document, or

(3) Establish confidential communications with the certificate subject.

1.3.5 Other Participants

If 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 mutual operation mechanism and the rights and obligations of each other shall be specified in this CPS to ensure the efficiency and reliability of the service quality provided by eCA.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

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

A self-signed certificate is used to establish the trust anchor of the ePKI. A self-issued certificate is used for the eCA re-key or the exchange of the ePKI 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 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 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 that CA.

The certificates issued by eCA are divided in the five levels of assurance in accordance with the ePKI CP. 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

Assurance Level	Applicability
	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 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 1 DV SSL certificate	Follow the Baseline Requirements and assurance level 2 regulations to authenticate remote domain	Provide communication channel encryption (communication channel encryption refers	Provide an encryption protection to the non-monetary or non-property transactions where the probability of

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

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

Assurance Level and Certificate Type	Authentication Method	Scope of Application	Risk Description of Reducible Risks
		information of EV SSL certificate subject to facilitate subscriber to identify the certificate holder.	information breach, leakage of confidential information, etc.) is very high.

Subordinate CAs can use the following three OIDs for each authenticator assurance level defined in the ePKI CP according to their needs:

Authenticator Assurance Level	OID Name	OID Value
Level 1	id-cht-ePKI-tokenAssurance 1	1.3.6.1.4.1.23459.100.4.1
Level 2	id-cht-ePKI-tokenAssurance 2	1.3.6.1.4.1.23459.100.4.2
Level 3	id-cht-ePKI-tokenAssurance 3	1.3.6.1.4.1.23459.100.4.3

Relying parties shall obtain the trusted eCA public key or self-signed certificates via a secure distribution 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 eCA.

Relying parties shall carefully select secure computer environments and trusted application systems to prevent the eCA public keys or self-issued certificates from being damaged or replaced. This can ensure use of the correct eCA public key or self-signed certificate to verify the digital signatures of self-issued certificates, subordinate CA certificates, cross-certificates and CARLs issued by eCA.

The type of assurance level that a subordinate CA can issue is

recorded in the subordinate CA certificates issued by eCA. Relying parties can decide whether to trust the subordinate CA and its certificates.

The type of assurance level and cross-certification levels that a root CA outside ePKI can issue and perform with other root CAs are recorded in the cross-certificate issued by eCA. In addition, the cross-certificate contains the certificate policy mapping enforced by the root CA. Relying parties can decide whether to trust the root CA and its certificate.

Relying parties must use the keys in compliance with Section 6.1.7 and use the certificate validation methods in accordance with international standards (such as ITU-T X.509 or RFC 5280) to verify the validity of certificates.

Relying parties must carefully read this CPS before using the certificate service provided by eCA, comply with this CPS and pay attention to the update of this CPS.

1.4.2 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. (CHT).

1.5.2 Contact Person

1.5.2.1 CPS Related Issues

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

E-mail: caservice@cht.com.tw

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

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

1.5.2.2 Certificate Problem Report

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

eCA may or may not revoke in response to this request. See Sections 4.9.3.3 and 4.9.5 for detail of actions performed by eCA for making this decision.

1.5.3 Person Determining CPS suitability for the Policy

eCA shall first check whether this CPS conforms to relevant ePKI CP regulations and then submit the CPS to the Chunghwa Telecom Certificate Policy Management Authority (PMA) for review and approval.

In addition, according to the Electronic Signatures Act, CAs can provide the service of certificate issuance after the CPS has been approved by the competent authority, the Ministry of Economic Affairs (MOEA).

eCA conducts regular self-audits to demonstrate that it has

operated with the assurance level under the ePKI CP. In order to ensure the smooth operation of certificates issued by the CAs under the ePKI in most operating systems, browsers and software platforms, ePKI has applied to the root certificate programs of most operating systems, browsers, and software platforms to include our root certificate, the self-signed certificate of eCA, into their CA trust list. According to the criteria of root programs, full-surveillance period-of-time audits must be conducted and updated audit information provided no less frequently than annually. That is, successive audits must be contiguous (no gaps). In addition, external audits for eCA and subordinate CAs must conducted and eCA must submit the current CPS and audit report to each root certificate program annually. eCA shall also continue to maintain the audit seals published on the eCA website.

1.5.4 CPS Approval Procedures

This CPS is published by eCA following approval by the MOEA, the competent authority of the Electronic Signatures Act. This CPS must be revised in response to any revision of the ePKI CP, and the revised CPS is first submitted to the PMA for review and then forwarded to the MOEA for approval.

After the revisions of this CPS take effect, if there is any inconsistency between the original CPS and the revised CPS, then the revised CPS takes precedence unless stipulated otherwise. If the revisions are made by attached documents, the attached documents shall take precedence if there is a discrepancy between the attached documents and original CPS.

1.6 Definitions and Acronyms

See Appendix 1 for the abbreviations and definitions and Appendix 2 for the glossary.

2. Publication and Repository Responsibilities

2.1 Repositories

The repository, under the management of eCA, publishes the certificates issued by eCA, CARLs and other certificate-related information and provides 24-hour round-the-clock service. The website address of the eCA repository is at 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

eCA publishes the following information in its repository:

(1) The ePKI CP.

(2) This CPS.

(3) CARLs.

(4) Online Certificate Status Protocol (OCSP) service

(5) Self-signed certificates by eCA.

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

The CAA Issuer Domain Names of ePKI include pki.hinet.net, publicca.hinet.net, eca.hinet.net and epki.com.tw.

2.3 Timing or Frequency of Publication

(1) This CPS is reviewed and updated annually. New or modified version of this CPS is published in the repository within seven calendar days upon receiving the approval letter from the competent authority;

(2) New or modified version of the ePKI CP complied with by eCA is published in the repository within seven calendar days upon the approval of the PMA;

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

(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 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 eCA under Section 2.2 is primarily provided for inquiring for subordinate CA, cross-certified CA and relying party, 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 eCA conforms to the distinguished name (DN) of ITU-T 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 Baseline Requirements 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 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 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 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, 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. 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 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

CHT 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 are paired. One PKCS#10 Certificate Signing Request file is generated by the CA and 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

Identity authentication of the root CA (e.g., eCA) is reviewed at a PMA meeting convened by CHT.

When a CA established by CHT becomes a subordinate CA (for example: Public Certification Authority), the identity authentication is reviewed by a PMA meeting convened by CHT.

When a CA (not established by CHT) apply to eCA for a subordinate CA certificate or cross-certificate, the application shall include the organization name, locality, representative and other information which is sufficient to identify the organization. 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 comply with the Baseline Requirements 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 EV SSL Certificate Guidelines. 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 proprietary server signature and encryption, the subordinate CA shall authenticate the organization identity and validate whether or not the proprietary 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 CHT.

For CA not established by CHT, applications of CA certificates (subordinate CA certificate or cross-certificate) must be submitted by representatives (individuals who is authorized) appointed by official

document. 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 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 a certificate lifecycle activity such as a certificate application or revocation request is submitted by an individual (an authorized representative) related to the certificate subject, eCA or subordinate CA or its RA shall perform a validation of authority to verify that the individual can represent the certificate subject, such as:

(1) Confirming the organization legal existence through third-party identity verification service or database, documents issued by government or authorized organizations, or an attestation letter written by a government official, lawyer, or accountant;

(2) Using telephone, postal letter, e-mail not provided by the

representative or any equivalent way to confirm that the individual affiliated with the certificate subject (organization or company) and is authorized to represent the certificate subject; or

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

3.2.6 Criteria for Interoperation

eCA allows another root CA to interoperate with, the terms and criteria of which are set forth in the applicable agreement. The root CA wishing to interoperate with shall provide the PMA at least the following information:

(1) The CPS of that root CA

(2) A description of certificate types that the root CA will issue

(3) The root CA shall provide the audit report indicating that all CAs under that root CA have conducted a compliance audit in accordance with WebTrust for CA and, please refer to Audit Applicability Matrix of CPA Canada (http://www.webtrust.org/principles-and-criteria/docs/item85436.pdf) for the audit standards on which the report is based.

(4) The issuing CA that issues SSL certificates shall also provide Baseline Requirements Assessment.

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 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 Identification and Authentication for Routine Re-key

When a CA make a routine re-key request, the issuing CA shall re-verify the CA's identity in accordance with Section 3.2.

3.3.2 Identification and Authentication for Re-key after Revocation

After a certificate is revoked by the CA, the identification and authentication procedure for new certificate application shall comply with Section 3.2 to perform identity validation again.

3.4 Identification and Authentication for Revocation Request

The authentication procedure for eCA self-signed certificates, self-issued certificates, subordinate CA certificates, and cross-certificates revocation requests is the same as the rules in Section 3.2.

4. Certificate Life-cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

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

4.1.2 Enrollment Process and Responsibilities

4.1.2.1 ePKI eCA Obligations

(1) Procedures are implemented in accordance with the ePKI CP assurance level 4 and this CPS
(2) Establish subordinate CA and cross-certified CA application procedures,
(3) Perform the identification and authentication procedures for applications made by subordinate CAs and cross-certified CAs,
(4) Issue and publish certificates,
(5) Revoke certificates,
(6) Issue and publish CARLs,
(7) Perform CA personnel identification and authentication procedures,
(8) Securely generate eCA private keys,
(9) Safeguard the eCA private keys,
(10) Conduct re-key of the eCA self-signed certificate and issuance of the eCA self-issued certificate,
(11) Accept certificate registration and revocation applications of subordinate CAs, and
(12) Accept cross-certificate registration and revocation applications of cross-certified CAs.

4.1.2.2 Subordinate CA Obligations

(1) Subordinate CAs shall comply with the provisions of this CPS, and will be liable for relying parties' damages due to the violation,

(2) Subordinate CAs must state the assurance level of the requested certificate when submitting a certificate application, because the certificates issued by eCA have different assurance levels and different usages as stipulated in the ePKI CP,

(3) Subordinate CAs shall perform subordinate CA certificate applications in accordance with Section 4.2 of this CPS and must confirm the accuracy of the application information,

(4) Subordinate CAs shall accept the certification in accordance with Section 4.4, after a subordinate CA certificate application is approved and eCA has issued the certificate,

(5) Acceptance of a subordinate CA certificate issued by eCA indicates that the subordinate CA has checked the accuracy of the information contained in the certificate and may use the certificate in accordance with Section 4.5,

(6) Subordinate CAs shall self-generate private keys in accordance with Chapter 6,

(7) Subordinate CAs shall properly safeguard and use their private keys,

(8) Check whether the certificate has been accepted and the certificate is within the validity period and is unrevoked when a digital signature signed with private keys that correspond with subordinate CA certificate public key is generated,

(9) Revoke a subordinate CA certificate if a certificate revocation event of subordinate CA occurred as described in Section

4.9.1 (such as the disclosure or loss of private key information), and eCA shall be notified immediately. However, the subordinate CA shall bear legal responsibility for use of that certificate prior to the notification or before the change has been made, and

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

4.1.2.3 Cross-Certified CA Obligations

(1) Cross-certified CAs shall comply with the provisions of this CPS and the CCA terms and conditions, and will be liable for relying parties' damages due to the violation,

(2) Cross-certified CAs must state the assurance level of the requested certificate when submitting a cross-certificate application, because the certificates issued by eCA have different assurance levels and different usages as stipulated in the ePKI CP,

(3) Cross-certified CAs shall perform cross-certificate applications in accordance with Section 4.2 of this CPS and must confirm the accuracy of the application information,

(4) Cross-certified CAs shall accept the certification in accordance with Section 4.4, after a cross-certificate application is approved and eCA has issued the certificate,

(5) Acceptance of a cross-certificate issued by eCA indicates that the cross-certified CA has checked the accuracy of the information contained in the certificate and may use the certificate in accordance with Section 4.5,

(6) Cross-certified CAs shall self-generate private keys in

accordance with Chapter 6,

(7) Cross-certified CAs shall properly safeguard and use their private keys,

(8) Check whether the certificate has been accepted and the certificate is within the validity period and is unrevoked when a digital signature signed with private keys that correspond with cross-certificate public key is generated,

(9) Revoke a cross-certificate if a certificate revocation event of cross-certified CA occurred as described in Section 4.9.1 (such as the disclosure or loss of private key information), and eCA shall be notified immediately to perform certificate suspension or revocation in accordance with Section 4.9. However, the cross-certified CA shall bear legal responsibility for use of that certificate prior to the notification or before the change has been made, and

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

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 eCA issue the cross-certificates to the CAs other than these one of the ePKI, a negotiation between the PMA 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 CHT, CHT convenes a PMA 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 CHT, the subordinate CA certificate or 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. External operated subordinate CA or root CA outside ePKI shall provide an up to date point-in-time or period of time audit report. The issuing CA that issues SSL certificates shall also provide a Baseline Requirements Assessment.

(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 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 PMA meeting is convened when eCA submits a self-signed or self-issued certificate application.

A PMA meeting is convened when a CA submits a subordinate CA certificate application. The PMA will review the related documents provided by the CA to evaluate the appropriateness for becoming a subordinate CA of eCA. The PMA may decide that the application enters the next stage, supplemental information is required, or the application is rejected.

A PMA meeting is convened to review the related documents submitted by the CA and eCA's checking results when the CA submits a cross-certification application in order to determine the appropriateness of the application. The PMA ultimately decides that the application enters the next stage, supplemental information is required, or the application is rejected.

4.2.2.2 Arrangement

For root CA established by CHT, it is not required to sign a Cross-Certification Agreement (CCA).

When a CA not established by CHT submits an application of subordinate CA certificate, a meeting will be notified to the CA (External operated subordinate CA) applying for subordinate CA certificate and the following steps are followed:

(1) Identity identification and authentication

The external operated subordinate CA shall review and agree to comply with the ePKI CP, this CPS, and the terms and criteria of the (external) subordinate CA certificate application. The CA shall then prepare relevant application materials and notify eCA through official letter. During the meeting, eCA shall first perform the identity identification and authentication procedure for the representative of the external operated subordinate CA in accordance with Section 3.2.3.

(2) eCA provides review comments to the PMA prior to the meeting

(3) The PMA determines whether to approve the application regarding the external operated subordinate CA joins ePKI. If approved, the PMA then authorize eCA to perform the procedure of certificate issuance.

When a root CA not established by CHT submits the cross-certificate application, a meeting will be notified to the root CA applying for cross-certification and the following steps are followed:

(1) Identity identification and authentication

During the meeting, eCA shall first perform the identity identification and authentication procedure for the representative of the root CA in accordance with Section 3.2.3

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

(3) Determine whether to approve the application. If approved, eCA signs a CCA with the root CA.

(4) Proceed to the certificate issuance procedure.

4.2.3 Time 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 PMA meeting review, eCA shall complete the certificate issuance within seven calendar days.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

eCA follows the resolution of the PMA (meeting minutes) when issuing self-signed certificates and self-issued certificates.

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

eCA follows the PMA 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 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 eCA performs the work related to certificate issuance. After the certificate is issued, CHT 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 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, eCA shall be notified. CA not established by CHT must sign a certificate acceptance confirmation document and reply by letter to CHT to complete the certificate acceptance procedure. Internal issuance procedures are followed for subordinate CA established by CHT to publish the self-signed certificate and the self-issued certificate in the repository.

After receiving the certificate acceptance confirmation document, eCA publishes the CA certificates issued to subordinate CAs or cross-certificates issued to root CAs 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. eCA revokes that certificate and no publication is made.

4.4.1 Conduct Constituting Certificate Acceptance

After 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, eCA shall be notified. CA not established by CHT must sign a certificate acceptance confirmation document and reply by letter to CHT 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. eCA revokes that certificate and no publication is made.

4.4.2 Publication of the Certificate by the CA

After receiving the certificate acceptance confirmation document, eCA publishes the CA certificates issued to subordinate CAs or cross-certificates issued to root CAs in the repository.

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

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

If there are newly issued self-signed certificates, 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

Key pairs of subscribers shall be generated in compliance with Section 6.1.1 of the ePKI CP. Subscribers must be able to control the private keys corresponding to the public key of their certificates and do not issue certificates to others. Subscribers shall protect their private keys from unauthorized use or disclosure and shall use their private keys for the correct key usage (i.e., the policy for key usage specified in the extension of the certificates). Subscribers shall correctly use their certificates adhering to the certificate policies listed in the certificates.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties shall use software that is compliant with the ITU-T X.509, IETF RFC, Baseline Requirements and EV SSL Certificate

Guidelines.

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 generator, and
(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 CRL distribution points extension of certificates; the URL of OCSP service can be obtained from the authority information access extension of certificates. In addition, the relying parties shall check the content of the certificate policies extension of the issuing CA and subscriber certificates to confirm the assurance level of the certificates.

4.6 Certificate Renewal

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

4.6.1 Circumstance for Certificate Renewal

Not applicable.

4.6.2 Who May Request Renewal

Not applicable.

4.6.3 Processing Certificate Renewal Requests

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 Certificate Issuance by the CA to Other Entities

Not applicable.

4.7 Certificate Re-key

4.7.1 Circumstance for CA Certificate Re-key

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 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).

For the CA that issues assurance levels 2, 3 and 4 certificates, if its certificate has not been revoked, eCA may start to process the re-key and new CA certificate application one month before the expiry of the CA private key usage period. The procedure for applying a new CA certificate is performed in accordance with Section 4.2.

4.7.2 Who May Request Certificate of a New Public Key

Applications may be submitted by the 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 eCA. The regulations in Sections 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 of New Certificate Issuance to CAs

For the notification to the CA who submits the certificate re-keying request, please refer to Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

As stated in Section 4.4.1.

4.7.6 Publication of the Re-keyed Certificate by the CA

As stated in Section 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

As stated in Section 4.4.3.

4.8 Certificate Modification

4.8.1 Circumstance for Certificate Modification

Certificate modification means creating a new certificate for the

same subject, where authenticated information that slightly differs from the old certificate (e.g., add certificate policy OIDs to the CertificatePolicies extension of Subordinate CA certificates or self-issued certificates). The new certificate has a new certificate serial number but with the same subject public key and 'NotAfter' date.

4.8.2 Who May Request Certificate Modification

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

4.8.3 Processing Certificate Modification Requests

As stated in Section 4.2.

4.8.4 Notification of New Certificate Issuance to Subscriber

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

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

4.8.5 Conduct Constituting Acceptance of Modified Certificate

The CA applying for certificate modification must check the modified certificate to make sure the certificate contents are accurate. If there are no errors in the certificate, eCA shall be notified. CAs not established by CHT must send a reply letter indicating acceptance of

the modified certificate; CAs that is established by CHT must ask eCA to announce its new certificate through internal procedures.

4.8.6 Publication of the Modified Certificate by the CA

eCA shall publish the modified CA certificates to its repository.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.9 Certificate Revocation and Suspension

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

For expired certificates, eCA may not accept certificate revocation requests. For revoked certificates prior to expiry, eCA shall list the information of revocation on the CARLs. After that, the information shall be removed.

4.9.1 Circumstances for Revocation

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.

eCA shall revoke a Subordinate CA certificate or cross-certificate within seven (7) days if one or more of the following occurs:

(1) The Subordinate CA or cross-certified CA requests revocation in writing;

(2) The Subordinate CA or cross-certified CA notifies the issuing CA that the original certificate request was not authorized and does not retroactively grant authorization;

(3) eCA obtains evidence that the Subordinate CA or cross-certified CA's private key corresponding to the public key in the certificate suffered a key compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6;
(4) eCA obtains evidence that the certificate was misused;
(5) eCA is made aware that the certificate was not issued in accordance with or that Subordinate CA or cross-certified CA has not complied with the ePKI CP or this CPS;
(6) eCA determines that any of the information appearing in the certificate is inaccurate or misleading;
(7) The Subordinate CA or cross-certified CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the certificate;
(8) The Subordinate CA or cross-certified CA's right to issue certificates under these requirements expires or is revoked or terminated, unless eCA has made arrangements to continue maintaining the CRL/OCSP Repository; or
(9) Revocation is required by the ePKI CP and/or this CPS.

If the certificate subject information on a certificate must be changed, eCA shall review and determine if the certificate should be revoked. eCA may at its own discretion revoke certificates, including Subordinate CA certificates or cross-certificates, under the aforementioned circumstances.

4.9.2 Who Can Request Revocation

(1) The competent authorities of eCA, subordinate CA or Cross-Certified CA (e.g. the competent authority to the Electronic Signature Act in Taiwan is MOE),
(2) Subordinate CAs that wants to revoke its certificate,

(3) Cross-Certified CAs that wants to revoke its certificate, or

(4) eCA.

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

4.9.3 Procedure for Revocation Request

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 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

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

eCA provides the instruction and guidelines for certificate problem report with which CAs, application software suppliers, relying parties, and other third parties can submit to eCA when they observe the possible events of private key cracked, certificate abusing, or the certificates are forged, cracked, abused, or used inappropriately.

CAs, application software suppliers, relying parties, and other third parties may visit the eCA website to obtain the instructions/guidelines for certificate problem reporting, and report the certificate problems to eCA accordingly.

4.9.4 Revocation Request Grace Period

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

Shall the events that allow 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, 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

Within 24 hours after receiving a Certificate Problem Report, eCA shall investigate the facts and circumstances related to a Certificate

Problem Report and provide a preliminary report on its findings to both CAs and the entity who filed the Certificate Problem Report.

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

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

4.9.6 Revocation Checking Requirement for Relying Parties

Before using subordinate CA certificates, cross-certificates, or self-issued certificates issued by eCA, the relying parties shall verify the validity of the certificates using the CARLs or OCSP responses published by eCA.

The relying parties shall check the revocation time of the certificate as well as 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 content of Issuer DN field of the CARL matches the Subject DN of the self-signed certificate of eCA. Furthermore, the recorded public keys of the self-signed

certificate in eCA shall be applied to verify the signature of 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 eCA. When the relying parties verify 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 archived 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 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 repository before the old one expires, for the relying parties to obtain the most updated CA revocation information.

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

4.9.8 Maximum Latency for CRLs

eCA shall publish the CARL no later than the time specified in the nextUpdate field of the previously issued CARL.

4.9.9 On-line Revocation/Status Checking Availability

eCA provides CARLs, certificate download service (via websites),

and OCSP services for certificate status checking.

eCA provides the OCSP responses, complying with RFC 6960 and RFC 5019, by OCSP responders. eCA uses the private signing key to issue the OCSP responder certificates with the security strength at least RSA 2048 w/SHA-256 with which the relying parties can verify the digital signature of the OCSP responses and confirm the integrity and reliability of the information sources. The certificates of the OCSP responders shall include the extension “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 use the CARL in accordance with Section 4.9.6 to check if the certificate used is valid or not, OCSP services as described in Section 4.9.9 shall be used.

eCA provides the OCSP service, and the OCSP responder operated by eCA supports the HTTP-based POST and GET methods, as described in RFC 6960 and RFC 5019. eCA updates the status of self-issued certificates, subordinate CA certificates and cross-certificates provided via its OCSP service at least every twelve months and within 24 hours after any of these certificates is revoked in order to allow the OCSP service to provide the most updated and correct status of the certificates.

A certificate serial number within an OCSP request may be one of three options, which are "assigned", "reserved" and "unused". The “assigned” certificate serial number means the serial number of the certificate issued by eCA; the “reserved” certificate serial number is the serial number of precertificates required for issuing TLS/SSL certificates; and the certificate serial number that does not meet the aforementioned conditions is the "unused" certificate serial number. Since eCA does not provide the issuance of subscriber certificates, it

does not issue precertificates. In other words, the OCSP responder of eCA may provide response for OCSP requests with “assigned” or “unused” certificate serial numbers.

If the OCSP responder receives a request for the status of a certificate serial number that is “assigned”, the responder shall respond with the status at that time of the certificate assigned with that serial number. If the OCSP responder receives a request for the status of a certificate serial number that is “unused”, the responder shall not respond with a "good" status. eCA shall monitor the responder for such requests as part of its security response procedures.

4.9.11 Other Forms of Revocation Advertisements Available

In order to speed up and instantly complete the verification of the SSL certificates status of high-traffic websites, eCA supports the operation of OCSP stapling.

4.9.12 Special Requirements Related to Key Compromise

eCA shall state key compromise as the reason for certification revocation in the CARL posted by 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 Suspension

Not applicable because certificate suspension services are not provided.

4.9.15 Procedure for Suspension Request

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.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

eCA provides CARLs. The CARL download URL is noted in the CRL distribution points extension of self-issued certificates, subordinate CA certificates, and cross-certificates. eCA has been providing OCSP services starting from May 22, 2015.

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

4.10.2 Service Availability

eCA maintains 24x7 uninterrupted repository system to provide CARLs and the OCSP services. Under the normal operating conditions, the aforesaid certificate status inquiry services shall reply in ten seconds.

eCA maintains a continuous 24x7 ability to respond to a high-priority Certificate Problem Report. eCA may report such a complaint to the law enforcement and revoke the problematic certificate upon its discretion.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

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

subordinate CAs or cross-certified CAs revoked.

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 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

The private keys used for signatures by eCA shall not be escrowed. 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

eCA does not currently support session key encapsulation and recovery.

5. Facility, Management, and Operational 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 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 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 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 eCA.

5.2 Procedural Controls

In order to protect the security of system procedures, 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 eCA are administrator, CA officer, internal auditor, system operator, physical security 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 CA 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 internal auditor is responsible for:
- Checking, maintenance and archiving of audit logs.
- Perform or supervise internal audits to ensure eCA is operating in accordance with CPS regulations.

(4) The system 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 security 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 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 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) CA Officer: at least 3 qualified individuals
(3) Internal Auditor: at least 2 qualified individuals
(4) System 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	CA Officer	Internal Auditor	System 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		
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		
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		
Daily routine operation of system equipment				1	1		
System backup and recovery				1	1		
Updating storage media				1	1		
Software and hardware updates				1	1		

Assignments	Administrator	CA Officer	Internal Auditor	System Operator	Physical Security Controller	Cyber security coordinator	Anti-virus and anti-hacking coordinator
outside of eCA system							
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		

5.2.3 Identification and Authentication for Each Role

eCA utilized system account, password and group management functions and IC cards to identify and authenticate administrator, CA officer, internal auditor, and system operator as well as central access control system authorization setting function to identify and authenticate physical security controllers. 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.

5.2.4 Roles Requiring Separation of Duties

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

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

(2) The physical controller shall not concurrently assume any role of the administrator, CA officer, internal auditor, and system operator.

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

5.3 Personnel Controls

5.3.1 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

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.
CA Officer	(1) eCA security clearance system. (2) eCA software and hardware use and operation 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.

Trusted Roles	Training Requirements
Internal 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.
System 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.
Physical Security Controller	(1) Physical access authorization setting procedure. (2) Disaster recovery and continuous operation procedure.
Cyber security coordinator	(1) Maintenance of the network and network facilities. (2) Security mechanism for the network.
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, 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 system operator or internal auditor.

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

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

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

5.3.6 Sanctions for Unauthorized Actions

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 Requirements

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

5.3.8 Documentation Supplied to Personnel

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

5.4 Audit Logging Procedures

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 Events Recorded

(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 Frequency of Processing Log

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. 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 Log

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

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.

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.

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

5.4.6 Audit Collection System (Internal vs. External)

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, 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

eCA follows the approaches and frequency required by WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security and CA/Browser Forum Network and Certification System Security Requirements 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, eCA must conduct the penetration test as well. The remedy and correction measures are taken after the penetration test and the vulnerability assessment by eCA. 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

5.5.1 Types of Records Archived

- 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.

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 Time-stamping of Records

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 Collection System (Internal or External)

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

eCA changes its private keys and signs a new self-signed certificate under the following two circumstances:

(1) The usage period of its private key has expired, and
(2) Security concerns, e.g., suspected or confirmed private key compromise.

eCA shall periodically change its private keys in accordance with Section 6.3.2.1 and shall change its key pair before the usage period of its private key has expired. After key changeover, eCA shall sign a new self-signed certificate (by using the new private key) and mutually sign a new self-issued certificate (by using the new and old private keys, separately). The issuance procedures for these three new certificates need to comply with Section 4.3. The new self-signed certificate shall be delivered to relying parties in accordance with Section 6.1.4 while the

new self-issued certificates shall be published in eCA repository for download.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

eCA establishes incident and compromise reporting and handling procedures, and conducts annual drills.

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

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

If eCA's computer equipment is damaged or unable to operation, but the eCA private signing 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 Entity Private Key Compromise Procedures

eCA establishes recovery procedures in the event of private signing key compromise and conducts annual drills.

5.7.4 Business Continuity Capabilities after a Disaster

eCA conducts annual security facility disaster recovery drills.

5.8 CA or RA Termination

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

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) 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 eCA, of the service termination three months in advance and post the notification in the repository.

(2) 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, eCA generates key pairs within the hardware cryptographic module by using the algorithm that meets NIST FIPS 140-2 standard. The private keys are input and output in accordance with Sections 6.2.2 and 6.2.6.

eCA key generation is witnessed and videotaped by those related personnel who have signed key initiation witness document (the public key of the generated key pair is listed on it). This public key of the key pairs of eCA is distributed via trusted channels. The related personnel shall include the members of the PMA and qualified auditors. The qualified auditors shall then issue a witness report of the key generation ceremony which indicates that eCA was generated the key pair and certificate in accordance with the Key Generation Script and control measures to ensure the integrity and confidentiality of the key pairs.

Subordinate CA and cross-certified CA must generate key pairs in accordance with the ePKI CP and follow the procedures specified in the Key Generation Script which shall be witnessed or videotaped by the qualified auditors. In addition, the qualified auditors shall then issue a witness report of the key generation ceremony for cross-certified CA and external operated subordinate CA.

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

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

Subordinate CAs must follow CP regulations and select suitable

software and hardware for key generation. Before subordinate CA certificates are issued, 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, eCA shall review the suitability of the software or hardware selected by the CA.

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 of the cross-certified CAs.

6.1.2 Private Key Delivery to Subscriber

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

Any cross-certified CA cross certified with eCA must self-generate the private key. Therefore, 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 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 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 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

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

Subordinate CAs and cross-certified CAs must use proper key size of RSA keys and SHA-256, SHA-384, or SHA-512 hash function algorithms to issue certificates in accordance with the ePKI CP, the regulations of the key size are as follows:

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

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

eCA shall examine whether the subordinate CAs and cross-certified CAs have chosen an appropriate key size before their certificates are issued by eCA.

6.1.6 Public Key Parameters Generation and Quality Checking

The public key parameter of the RSA algorithm is null.

eCA and its subordinate CAs 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.

Cross-certified CAs must perform appropriate key parameter quality checking based on the selected algorithm.

According to Section 5.3.3, NIST SP 800-89, eCA confirms that the value of the public exponent is an odd number greater than 3 and is in the range between $2^{16}+1$ and $2^{256}-1$. In addition, the modulus shall be 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, eCA will comply with the requirements of Sections 5.6.2.3.2 and 5.6.2.3.3 in NIST SP 800-56A Revision 2 to confirm the validity of all keys using 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, subordinate CA certificates, cross-certificates, CARLs, OCSP responder certificates or OCSP responses.

The first-generation eCA self-signed certificate does not contain the key usage extension. From the second generation, the self-signed certificates shall contain the key usage extension which is marked as critical. Bit positions for keyCertSign and cRLSign are set. If the eCA private signing key is used for signing OCSP responses, then the digitalSignature bit will be set.

For subordinate CA certificates issued by eCA, the key usage extension is present and bit positions for keyCertSign and cRLSign are set. If the subordinate CA private signing key is used for signing OCSP responses, then the digitalSignature bit will be set.

For cross-certified CA certificates issued by eCA, the key usage extension is present and bit positions for keyCertSign and cRLSign are set. If the cross-certified CA private signing key is used for signing OCSP responses, then the digitalSignature bit will be set.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

eCA uses hardware cryptographic 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. eCA shall examine whether the CA has chosen an appropriate cryptographic module security level before the subordinate CA certificate is issued by eCA.

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

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

The multi-person control for eCA key splitting uses n-out-of-m LaGrange Polynomial Interpolation. It is a perfect secret sharing method used for private key splitting backup/recovery, where 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).

The CA private signing keys for issuing certificates at assurance levels 3 and 4 must be controlled complying with the multi-person control specified in the ePKI CP. eCA shall examine whether CAs use appropriate multi-person control procedures prior to the issuance of the subordinate CA certificates or cross-certificates.

6.2.3 Private Key Escrow

eCA’s private signing keys cannot be escrowed. eCA is not

responsible for safekeeping the private signing keys from subordinate CAs and cross-certified CAs.

6.2.4 Private Key Backup

Backups of private keys are made by eCA according to the key splitting multi-person control methods in Section 6.2.2 and highly secure IC cards are used 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. 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 eCA.

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

6.2.6 Private Key Transfer into or from a Cryptographic Module

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

The subordinate CA and cross-certified CA must follow CP

regulations to choose an appropriate private key importation method when they need to transfer a private key into a cryptographic module, eCA shall examine whether the CA has chosen an appropriate private key importation method prior to the issuance of the subordinate CA certificates or cross-certificates.

If eCA becomes aware that a subordinate CA or cross-certified CA private key has been communicated to an unauthorized person or an organization not affiliated with the subordinate CA or cross-certified CA, then eCA will revoke all certificates that include the public key corresponding to the communicated private key.

6.2.7 Private Key Storage on Cryptographic Module

As stated in Sections 6.1.1 and 6.2.1.

6.2.8 Method of Activating Private Key

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 CA officer.

The subordinate CA and cross-certified CA must follow CP regulations when choosing an appropriate private key activation method. 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 eCA.

6.2.9 Method of Deactivating Private Key

As 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, 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. 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 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 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 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. 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 eCA.

6.2.11 Cryptographic Module Rating

See Section 6.2.1.

6.3 Other Aspects of Key Pair Management

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

6.3.1 Public Key Archival

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

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

6.3.2.1 eCA Certificate Operational Periods and Key Usage Periods

The eCA public keys and private keys have the key size of RSA 4096 bit and the maximum operational period of 30 years. The maximum usage period of using private keys to issue subordinate CA certificates or cross-certificates is 15 years, but the usage period of using private keys to issue CARLs, OCSP responder certificates or OCSP responses is valid until subordinate CA certificates, self-issued certificates or cross-certificates expired. In addition, as the modification of the ePKI CP may need to have the self-issued certificate re-issued, and thus the usage period of private keys of eCA

to issue self-issued certificates is 30 years at maximum.

The usage period for certificates and private keys of OCSP responders is 36 hours. The new certificates for OCSP responders are published daily (the OCSP responses that uses the new private key to sign digitally contain this OCSP responder certificate, for relying parties to verify the signature of an OCSP response.

The validity of the eCA self-signed certificate shall cover the expiry dates of all certificates signed with the private key corresponding to the public key of the eCA self-signed certificate.

The validity of eCA self-issued certificates cross-signed with old and new eCA keys shall extend until the eCA self-signed certificate issued with the old eCA key expired.

6.3.2.2 Subordinate CA and Cross-Certified CA Certificate Operational Periods and Key Usage Periods

The public keys and private keys of subordinate CAs and cross-certified CAs have the key size of RSA 2048 bit at least and the maximum operational period of 20 years. The maximum usage period of using private keys to issue subscriber certificates is 10 years, but the usage period of using private keys to issue CRLs, OCSP responder certificates or OCSP responses is not subject to these restrictions.

The validity of subordinate CA certificates or cross-certificates issued by eCA shall not exceed the validity of the eCA self-signed certificate.

6.3.2.3 SHA-1 Hash Function Algorithm Validity Period

According to Baseline Requirements v.1.2.1, CAs may continue to use the SHA-1 root CA certificates which have existed before October 2014 (such as the first-generation self-signed certificate of 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.

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, subordinate CA certificates and cross-certificates from November 2015.

The first-generation eCA provides the CARLs complying with SHA-1 and SHA-256 Hash Function Algorithm, such that the relying parties can verify the status of subordinate CA certificates and cross-certificates issued by eCA and issued with SHA-1 and SHA-256 Hash Function Algorithms. The CARLs with SHA-1 Hash Function Algorithm are provided until all the subordinate CA certificates and cross-certificates issued with SHA-1 Hash Function Algorithm by the first-generation eCA expire, or the subordinate CAs and cross-certified CAs no longer provide the issuance of certificates and CRLs. The second-generation eCA use SHA-256 Hash Function Algorithm to issue CARLs.

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

Subordinate CAs under ePKI or cross-certified CAs 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 ePKI with valid period over 2017 have been fully revoked. Subordinate CAs under ePKI has stopped issuing non-SSL subscriber certificates with SHA-1 algorithm according to the ePKI CP version 1.5 from December 1, 2018.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The eCA activation data is generated by the hardware cryptographic 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 cryptographic module. The IC card personal identification number (PIN) is directly input from the built-in keyboard in the hardware cryptographic module.

The subordinate CA and cross-certified CA must follow CP regulations when choosing an appropriate activation data generation method. 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 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 shall 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. 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 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

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 Life Cycle 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 delivered to 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 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. There must be no other hardware devices, network connection or component software irrelevant to the operation installed and the checks for malicious code should be conducted during each use.

When software is installed for the first time, eCA shall check if the provider has supplied the correct and unmodified version. After system installation, eCA shall check the integrity of CA software during each use and shall be regularly scanned by using tools including anti-virus software and malware removal tool.

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

eCA references the methodologies and standards in the ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, ISO/IEC 31000, WebTrust Principles and Criteria for Certification Authorities, and Baseline Requirements for risk assessment, risk management and security management and control measures.

6.6.3 Life Cycle Security Controls

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

6.7 Network Security Controls

The 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 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

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) Time of certificate issuance,

(2) Time of certificate revocation,

(3) Time of CARL issuance, and

(4) Time of system event occurrence.

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

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

eCA issues certificates in compliance with the official versions of the ITU-T X.509, Baseline Requirements and RFC 5280.

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

7.1.1 Version Number(s)

eCA issues certificates in compliance with RFC 5280 and ITU-T X.509 version 3.

7.1.2 Certificate Extensions

The extensions of certificates issued by eCA are in compliance with the official versions of the ITU-T X.509, Baseline Requirements and RFC 5280.

There are four kinds of certificates issued by eCA, namely the self-signed certificate, self-issued certificate, subordinate CA certificate and cross-certificate. The necessary extensions and their criticality are described below.

(1) Self-signed Certificate

Extension Fields	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	The content in this extension can be one of the following: ■ keyCertSign and cRLSign. (Default) ■ digitalSignature, keyCertSign and cRLSign. (If eCA uses the private signing key to issue OCSP Responses, the bits of digitalSignature,

Extension Fields	Criticality	Description
		keyCertSign, and cRLSign are asserted.)

(2) Self-issued Certificate

Extension Fields	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	The URL of CARLs announced by eCA
Authority Information Access	FALSE	Two items included in this extension: ■ The URL to download the self-signed certificate of eCA ■ The URL of OCSP services provided by eCA
Certificate Policies	FALSE	The following two items shall be included in this extension. The policy qualifier in this extension may be used to mark the published URL of this CPS as needed: ■ All CP OIDs defined in the ePKI CP. ■ All CP OIDs defined by CA/Browser Forum referenced in the ePKI CP.
Key Usage	TRUE	The content in this extension shall be identical to the content of key usage extension in the self-signed certificate.
Basic Constraints	TRUE	Subject Type=CA Path Length Constraint=None

(3) Subordinate CA Certificate

Extension Fields	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	The URL of CARLs announced by eCA
Authority Information Access	FALSE	Two items included in this extension: ■ The URL to download the self-signed certificate of eCA ■ The URL of OCSP services provided by eCA

Extension Fields	Criticality	Description
Certificate Policies	FALSE	This extension is used to indicate the certificate policies that used by the subordinate CA and approved and permitted to use by eCA. The policy qualifier in this extension may be used to mark the published URL of this CPS as needed. One or more of the following OIDs may be contained in this extension: ■ CP OIDs defined in the ePKI CP. ■ CP OIDs defined by CA/Browser Forum referenced in the ePKI CP.
Key Usage	TRUE	The content in this extension can be one of the following: ■ keyCertSign and cRLSign. (Default) ■ digitalSignature, keyCertSign and cRLSign. (If the subordinate CA uses the private signing key to issue OCSP Responses, the bits of digitalSignature, keyCertSign, and cRLSign are asserted)
Basic Constraints	TRUE	Subject Type=CA Path Length Constraint=Set according to the needed certificate path length of the subordinate CA.

(4) Cross-Certificate

Extension Fields	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	The URL of CARLs announced by eCA
Authority Information Access	FALSE	Two items included in this extension field: ■ The URL to download the self-signed certificate of eCA ■ The URL of OCSP services provided by eCA
Certificate Policies	FALSE	This extension is used to indicate the certificate policies that used by the cross-certified CA and approved and permitted to use by eCA. The policy qualifier in this extension may be used to mark the published URL of this CPS as

Extension Fields	Criticality	Description
		needed. One or more of the following OIDs may be contained in this extension: ■ CP OIDs defined in the ePKI CP. ■ CP OIDs defined by CA/Browser Forum referenced in the ePKI CP.
Policy Mappings	FALSE	This extension is used to indicate the correspondences between the certificate policies of the cross-certified CA and the ones of eCA. It lists one or more pairs of CP OIDs. The pairing indicates eCA considers its CP OID equivalent to the cross-certified CA's CP OID.
Key Usage	TRUE	The content in this extension can be one of the following: ■ keyCertSign and cRLSign. (Default) ■ digitalSignature, keyCertSign and cRLSign. (If the cross-certified CA uses the private signing key to issue OCSP Responses, the bits of digitalSignature, keyCertSign, and cRLSign are asserted.)
Basic Constraints	TRUE	Subject Type=CA Path Length Constraint= Set according to the needed certificate path length of the subordinate CA.

Other extensions are optional. They may be used as applicable, and the methods shall comply with the aforesaid regulations. Among them, if the subscriber certificate issued by the subordinate CA is to be used for secure e-mail or establishing a secure channel between the browser and the website server, the certificate of that subordinate CA must include an extended key usage extension specifying the extended key usages that the subordinate CA is authorized to issue certificates for. However, the anyExtendedKeyUsage KeyPurposeId must not appear within this extension. Both the id-kp-serverAuth and id-kp-emailProtection KeyPurposeIds also must not be included in the same certificate.

In addition, eCA is not allowed to issue a certificate with:

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

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

eCA does not issue subscriber certificates. That is, eCA does not implement the issuance of pre-certificates 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) sha256WithRSAEncryption(11)}

(OID：1.2.840.113549.1.1.11)

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

(OID：1.2.840.113549.1.1.12)

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

(OID：1.2.840.113549.1.1.13)

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) rsaEncryption(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 the official versions of the ITU-T X.509, Baseline Requirements and RFC 5280.

The content of Issuer DN field of self-signed certificates, self-issued certificates, subordinate CA certificates and cross-certificates issued by eCA shall be identical as the Subject DN of the self-signed certificates.

From the second-generation of eCA self-signed certificates, the Subject DN includes three attributes, namely “commonName”, “organizationName”, and “countryName”, described as follows:

(1) commonName

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

(2) organizationName

To record the official name of the organization to which eCA belongs. The authentication of this organization identify shall be implemented in accordance with Section 3.2.2.

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 that 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, eCA represents that it followed the procedure set forth in the ePKI CP and/or this CPS to verify that, as of the certificate’s issuance date, all of the subject information was accurate.

7.1.5 Name Constraints

No name constraints are used in eCA. Self-signed certificates, self-issued certificates, subordinate CA certificates and cross-certificates, which are not technically constrained as described in this Section, will be disclosed publicly, such as being disclosed in the Common CA Database (CCADB) of Mozilla.

7.1.6 Certificate Policy Object Identifier

The self-signed certificates of eCA do not include the certificate policies extension.

For the self-issued certificates, subordinate CA certificates and cross-certificates issued by eCA, the certificate policies extension may contain the CP OIDs defined in the ePKI CP or the ones defined by CA/Browser Forum referenced in the ePKI CP. With regard to the related statement of the CP OIDs, please refer to Section 1.2.

7.1.7 Usage of Policy Constraints Extension

The policy constraints extension may be used as required for subordinate CA certificates and cross-certificates issued by eCA.

7.1.8 Policy Qualifiers Syntax and Semantics

The self-issued certificates, subordinate CA certificates and cross-certificates issued by eCA may use the policy qualifier in the certificate policies extension to mark the published URL of this CPS if needed.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

The certificate policies extension of the certificates issued by eCA are not marked as critical.

7.2 CARL Profile

7.2.1 Version Number(s)

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

7.2.2 CRL and the CRL Entry Extensions

The CRL extensions and CRL entry extensions in the CARL issued by eCA comply with the official versions of the ITU-T X.509, Baseline Requirements and RFC 5280.

7.3 OCSP Profile

eCA provides OCSP service in compliance with RFC 6960 and RFC 5019, and the URL of the eCA OCSP service is contained in the authority information access extension of the self-issued certificates, subordinate CA certificates and cross-certificates.

7.3.1 Version Number(s)

An OCSP request in eCA shall contain the following information:

- Protocol version, and
- Target certificate identifier

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

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

Field	Description
Version	v.1 (0x0)
OCSP Responder ID	The subject DN of OCSP responder
Produced Time	OCSP response sign time
Target Certificate Identifier	The contents of this field include the hash algorithm, the hash of the

Field	Description
	issuer's DN, the hash of the issuer's public key and the serial number of the target certificate.
Certificate Status	Certificate status code (0: valid /1: revoked /2: unknown)
ThisUpdate/NextUpdate	This recommended validity period for this response, including ThisUpdate and NextUpdate
Signature Algorithm	OCSP response signature algorithm, which can be sha256WithRSAEncryption
Signature	OCSP responder signature
Certificates	OCSP responder certificate

7.3.2 OCSP Extensions

The eCA OCSP response includes the following extensions:

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

8. Compliance Audit and Other Assessments

8.1 Frequency or Circumstances of Assessment

eCA shall undergo routine external audits at least once per year (the audited period may not exceed 12 months) and non-routine internal audits to confirm that the security regulations and procedures of the ePKI CP and this CPS are being implemented and enforced. The standards used for the audit are WebTrust Principles and Criteria for Certification Authorities and WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security.

8.2 Identity/Qualifications of Assessor

CHT retains a qualified auditor, who is familiar with the operations of eCA and its subordinate CAs and is authorized by WebTrust for CA program as a licensed WebTrust practitioner to perform WebTrust 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. eCA shall conduct identity identification of audit personnel during audits.

8.3 Assessor’s Relationship to Assessed Entity

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

8.4 Topics Covered by Assessment

(1) Whether eCA is operating in accordance with this CPS, and

(2) Whether the regulations of this CPS comply with the ePKI CP.

8.5 Actions Taken as a Result of Deficiency

The following actions shall be taken if audit personnel find a discrepancy between the requirements of this CPS and the establishment or operation of eCA:

(1) Note the discrepancy, and

(2) Notify eCA about the discrepancy.

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

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, WebTrust for Certification Authorities – Extended Validation SSL and WebTrust for Certification Authorities – SSL Baseline Requirements seals. 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

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 eCA collects fees from subordinate CAs and CAs which request cross-certificates, this 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 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

eCA is operated by CHT. Its financial responsibilities are the responsibilities of CHT.

9.2.1 Insurance Coverage

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

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The information generated, received and kept by eCA is deemed as confidential information. Personnel currently and previously employed by 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 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

eCA shall handle the application information of Subordinate CAs and Cross-Certified CAs in accordance with the Electronic Signatures Act, the audit scheme of WebTrust Principles and Criteria for Certification Authorities 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 Plan

eCA has posted its personal information statement and privacy declaration on its website. 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. 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 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 must comply with the Electronic Signatures Act, the audit scheme of WebTrust Principles and Criteria for Certification Authorities and the 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, 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, 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, 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

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 eCA when the public key is issued as a certificate by eCA.

eCA retains ownership of eCA issued certificates and CARLs.

eCA retains ownership of the certificate subject names on eCA

issued self-signed certificates and self-issued certificates.

eCA shall do its best to ensure the correctness of subordinate CA and Cross-Certified CA names. However, 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 eCA to protect their rights.

This CPS may be freely downloaded from the repository. CHT grants permission to copy (in full) and distribute this CPS on a free basis according to the Copyright Act of our country, which need to be indicated that the copyright is owned by CHT. CHT reserves the right to pursue legal action for any violation of the use or dissemination of this CPS.

9.6 Representations and Warranties

9.6.1 eCA Representations and Warranties

eCA represents and warranties that it will:

(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 RA Representations and Warranties

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 CAs represent and warrant that they will:

(1) Comply with the provisions of this CPS, and will be liable for relying parties' damages due to the violation;

(2) State the assurance level of the requested certificate when submitting a certificate application, because the certificates issued by eCA have different assurance levels and different usages as stipulated in the ePKI CP;

(3) Perform subordinate CA certificate applications in accordance with Section 4.2 of this CPS and must confirm the accuracy of the application information;

(4) Accept the certification in accordance with Section 4.4, after a subordinate CA certificate application is approved and eCA has issued the certificate;

(5) Check the accuracy of the information contained in the certificate prior to the acceptance of a subordinate CA certificate issued by eCA, and the certificate shall be used in

accordance with Section 1.4.1;

(6) Self-generate private keys in accordance with Chapter 6;

(7) Properly safeguard and use their private keys;

(8) Check whether the certificate has been accepted and the certificate is within the validity period and is unrevoked when a digital signature signed with private keys that correspond with subordinate CA certificate public key is generated;

(9) Promptly notify eCA if a certificate revocation event of subordinate CA occurred as described in Section 4.9.1 (such as the disclosure or loss of private key). However, the subordinate CA shall bear legal responsibility for use of that certificate prior to the notification or before the change has been made; and

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

9.6.3.2 Cross-certified CA Representations and Warranties

Cross-Certified CA represent and warrant that they will:

(1) Comply with the provisions of this CPS and the CCA terms and conditions, and will be liable for relying parties' damages due to the violation;

(2) State the assurance level of the requested certificate when submitting a cross-certificate application, because the certificates issued by eCA have different assurance levels and different usages as stipulated in the CP;

(3) Perform cross-certificate applications in accordance with Section 4.2 of this CPS and must confirm the accuracy of the application information;

(4) Accept the certification in accordance with Section 4.4, after a cross-certificate application is approved and eCA has issued the certificate;

(5) Check the accuracy of the information contained in the certificate prior to the acceptance of a cross-certificate issued by eCA, and the certificate shall be used in accordance with Section 1.4.1;

(6) Self-generate private keys in accordance with Chapter 6;

(7) Properly safeguard and use their private keys;

(8) Check whether the certificate has been accepted and the certificate is within the validity period and is unrevoked when a digital signature signed with private keys that correspond with cross-certificate public key is generated;

(9) Promptly notify eCA to perform certificate suspension or revocation in accordance with Section 4.9, if a certificate revocation event of cross-certified CA occurred as described in Section 4.9.1 (such as the disclosure or loss of private key). However, the cross-certified CA shall bear legal responsibility for use of that certificate prior to the notification or before the change has been made; and

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

9.6.4 Relying Party Representations and Warranties

Relying parties using certificates issued by 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 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 eCA and CAs.
(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 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 legal liability clauses of eCA and also accept and use the eCA issued certificate within the certificate trust scope defined in Section 1.4.1.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

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

9.8 Limitations of Liability

Except to the extent ePKI has issued and managed the certificate in accordance with the Baseline Requirements and this CPS, ePKI shall not be liable to the subordinate CAs, cross-certified CAs or relying parties for any losses suffered as a result of use or reliance on such certificate. Otherwise, ePKI will assume the compensation liability no more than the amount stipulated in the CPS Section 9.9.

9.9 Indemnities

9.9.1 Indemnification by eCA

(1) If subordinate CAs, Cross-Certified CAs or relying parties suffer damages due to intentional or accidental failure of eCA personnel to follow the ePKI CP and/or 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 eCA, subordinate CAs, Cross-Certified CAs or relying parties to suffer damages, eCA shall compensate for the direct damages in accordance with the regulations.

(2) In the event of damages caused by certificates issued by eCA due to force majeure factors under Section 9.16.5, 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 eCA actually completes the termination of that CA's certificate, eCA shall not bear any liability provided eCA a performs the processing work in accordance with this 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, 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 Indemnification by Subordinate CAs and Cross-certified CAs

Under legal standards, 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

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 eCA for participation in the root certification programs of operation systems, browsers and software applications which could affect the trusted CA list that 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

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

9.10.2 Termination

This CPS and any amendments remain effective until replaced by a newer version approved by the Electronic Signatures Act competent authority.

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

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

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

9.12.2 Notification Mechanism and Period

eCA will post appropriate notice on its websites of any major or significant changes to this CPS as well as any appropriate period by when the revised CPS becomes effective. eCA will notify subordinate CAs and cross-certified CAs not owned by CHT through official letter or email to provide notice of proposed amendments. If CAs or relying parties have any comment on the change items, they can submit the comment within the comment period. Reassess to the changes and

response may or may not be made by eCA according to these comments.

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

9.12.3 Circumstances under which OID Must Be Changed

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

9.13 Dispute Resolution Provisions

In the event of a dispute between CA belonging to CHT and eCA, the dispute shall be jointly resolved between CHT's organization and management system and higher level competent authorities. If there is a dispute between the Cross-Certified CA not established by CHT and 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 regarding the interpretation and legality of any agreement signed based on the ePKI CP and CPS.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

The commitments set forth in this CPS constitute the entire agreement between the participants and supersedes all prior verbal or written representations between the parties on the same matters.

9.16.2 Assignment

The participants, including PublicCA, Subordinate CAs, cross-certified CAs, and relying parties, may not assign or delegate their rights or obligations under this CPS to other parties in any form without a prior written notice to PublicCA.

9.16.3 Severability

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

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

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

In the event that eCA suffers damages attributable to an intentional or unintentional violation of this CPS by a CA or relying party, eCA

may seek compensation for damages and indemnification and attorneys' fees related to the dispute or litigation from the responsible party.

eCA's failure to assert rights with regard to the violation of this CPS to the party does not waive eCA's right to pursue the violation of this CPS later 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, eCA shall not bear any legal liability.

9.17 Other Provisions

No stipulation.

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.
CMMI	Capability Maturity Model Integration	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.
FIPS	(US Government) Federal Information Processing Standard	
FQDN	Fully Qualified Domain Name	See Appendix 2.
IANA	Internet Assigned Numbers Authority	See Appendix 2.

Acronyms	Full Name	Definition
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	Secure Sockets 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	Private data, other than keys, that are required to access cryptographic modules and that need to be protected (i.e., unlock private keys for signing or decryption events).
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 WebTrust for CA-SSL Baseline Requirement and Network Security seals.
Applicant	Subscribers who request certificates from a CA and have not yet completed the certificate procedure.
Archive	A physically separate storage site for long-term information (storage site for important information) which can be used to support audit, usage and integrity services.
Assurance	A basis that the trusted entity has complied with certain security requirements. [Article 2-1, Chapter 1, Regulations on Required Information for Certification Practice Statements]
Assurance Level	A certain level in a relative assurance tier. [Article 2-2, Chapter 1, Regulations on Required Information for Certification Practice Statements]
Audit	Assessment of whether system controls are adequate and ensure conformance with existing policy and operation procedures, and independent checking and review of recommended required improvements to existing controls, policies and procedures.
Audit Data	Activity logs of a system organized in the order of time

Term	Definition
	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 user identities electronically presented to an information system. [NIST.SP.800-63-2 Electronic Authentication Guideline] (2) Safety measures used to secure data transmission or ways to authorize the privilege of individuals upon receiving certain types of information. (3) Authentication is the process by which a claimed identity is verified. [A Guide to Understanding Identification and Authentication in Trusted Systems] Mutual authentication means that the authentication is performed between two parties during communication.
Authority Information Access (AIA)	Records extensions related to certificate authority information access. The content may include: OCSP service sites and certificate issuance authority certificate verification path downloading site.
Backup	Information or program copying that can be used for recovery purposes when needed.
Binding	The process for binding (connecting) two related information elements.
Biometric	The physical or behavioral attributes of a person.
CA Certificate	Certificates issued by CAs.
Capability Maturity Model Integration (CMMI)	CMMI is the successor of the Capability Maturity Model (CMM) and was developed by the Software Engineering Institute at Carnegie Mellon University. CMMI models provide guidance for developing or

Term	Definition
	improving processes that meet the business goals of an organization. Its purpose is to help improve organizational performance.
Certificate	(1) Refers to verification information carrying a digital signature used to verify the identity and qualifications of the signer in electronic form. [Article 2-6, Electronic Signatures Act] (2) Digital presentation of information. The contents include: A. Issuing certificate authority B. Subscriber name or identity C. Subscriber public key D. Certificate validity period E. Certification authority digital signature The term 'certificate' referred to in the certificate policy specifically refers to ITU-T X.509 v.3 format certificates which states the certificate policy object identifier in the 'certificate policy' field.
Certification Authority (CA)	(1) The agency or natural person that issues certificate. [Article 2-5, Electronic Signatures Act] (2) The competent body trusted by the subscriber. Its functions are the issuance and administration of ITU-T X.509 format public key certificates, CARLs and CRLs.
Certification Authority 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, Regulations on Required Information for Certification Practice Statements] (2) Certificate policy refers to the dedicated profile administration policy established for the electronic transactions performed through certificate

Term	Definition
	administration. Certificate policy covers a variety of issues including the formation, generation, delivery, auditing, administration and restoration after compromise. Certificate policy indirectly controls the use and operation of certificate security systems to protect the transactions performed by the communication systems. The security services required for certain application are provided through control of the certificate extension field methods, certificate policy and related technology.
Certification Practice Statement (CPS)	(1) External notification by the certificate authority used to describe the practice statement of the certificate authority governing certificate issuance and processing of other certification work. [Article 2-7, Electronic Signatures Act] (2) Announcement of a statement that certain procedures of the certificate authority for certificate work (including issuance, suspension, revocation, renewal and access) comply with certain requirements (listed in the certificate policy or other service contracts).
Certificate 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)	A regularly updated list of revoked certificates that is created and digitally signed by the CA that issued the certificates. The list contains the certificates that the issuing CA has issued that are revoked prior to their stated expiration date.
Certificate Transparency (CT)	CT is an open platform for the public monitoring and auditing of all certificates on the Internet (TLS/SSL certificate is the priority objective at the current stage). It provides related information of issued certificates to domain owners, CA, and domain subscribers to determine whether any certificate has been issued improperly. In other words, CT provides a public monitoring and information disclosure environment which can be used to monitor all issuance mechanisms of CAs that issue TLS/SSL certificates and to review

Term	Definition
	any specific TLS/SSL certificate to lessen any risk that caused by mis-issued certificates. CT comprises 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 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 and Network Security seals. Canadian Institute of Chartered Accountants is abbreviated as CICA.
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 the module.
Data Integrity	Information that has been subjected to unauthorized access or accidental modification, damage or loss.
Digital Signature	An electronic signature generated by use of mathematic algorithm or other means to create a certain length of digital data encrypted by the signatory's private key and capable of being verified by the public key. [Article 2-3, Electronic Signatures Act]

Term	Definition
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.
Duration	A certificate field that contains two subfields, a start time "notBefore" and an end time "notAfter."
E-commerce	Provision of goods for sale and other services through the use of network technology (specifically the Internet).
End Entity	The PKI includes the following two types of entities: (1) Those responsible for the safeguarding and use of certificate public keys. (2) Third parties who trust the certificates issued by the PKI (not holders of private keys and not a certificate authority). The end entities are subscribers and relying parties including personnel, organizations, accounts, devices and sites.
End-Entity Certificate	Certificates issued to end-entities.
Chunghwa Telecom ecommerce Public Key Infrastructure (ePKI)	In order to promote Electronic Policy and create a sound e-commerce infrastructure, the Chunghwa Telecom Co., Ltd. shall follow the ITU-T X.509 standards to establish the public key infrastructure for use with various applications in e-commerce and e-government.
Chunghwa Telecom Certificate Policy Management Authority (PMA)	An organization which was established for electronic certificate management matters, such as (i) discussion and review of the CP and the electronic certificate framework of the PKI owned by CHT and (ii) review of interoperation requests submitted by subordinate

Term	Definition
	CAs and cross-certified CAs and that of CPS.
ePKI Root CA (eCA)	The Chunghwa Telecom Public Key Infrastructure Root Certification Authority (Root CA) is the top level certificate authority in this hierarchical public key infrastructure. Their public keys are the trust anchor.
Extended Validation (EV)	Validation process defined in the EV SSL Certificate Guidelines.
EV Certificate	Certificate subject information including the information validated in accordance with the EV SSL Certificate Guidelines.
Federal Information Processing Standard (FIPS)	Except for military organizations in the US Federal Government System, information processing standard for all government organizations and government subcontractors. The security requirement standard for the cryptographic module is FIPS no. 140 standard (FIPS 140). FIPS 140-2 divides the cryptographic module into 11 types of security requirements. Each security requirement type is then divided into 4 security levels.
Firewall	An access restriction gateway between networks which complies with near-end (local area) security policy.
Fully Qualified Domain Name (FQDN)	An absolute domain name that specifies its exact location in the DNS hierarchy. A FQDN consists of two parts, a host name (service name) and a domain name. For example, a website with the hostname *ourserver* in the parent domain *ourdomain.com.tw* has the FQDN *ourserver.ourdomain.com.tw*, where *ourdomain* is the third-level domain, *.com* is the second-level domain and *.tw* is the country code top-level domain (ccTLD). In addition, a website with the hostname *www* in the parent domain *ourdomain.com* has the FQDN *www.ourdomain.com*, where *ourdomain* is the second-level domain and *.com* is the generic top-level domain (gTLD). A FQDN always starts with a host name.
Identification	A statement of who the user is. [A Guide to Understanding Identification and Authentication in Trusted Systems] A way that can be used to describe or claim the

Term	Definition
	identity of an individual or entity, e.g., user account, name or e-mail.
Integrity	Protecting information so that it is not subject to unauthorized modification or damage. Preserve information in an untampered state during transmission and storage following generation at its source until receipt by the final recipient.
Internet Engineering Task Force (IETF)	Responsible for the development and promotion of Internet standards. Official website is at: https://www.ietf.org/ . Its vision is the generation of high quality technical documents affects how man designs, uses and manages the Internet and allows the Internet to operate smoothly.
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 Pair	Two mathematically linked keys possessing the following attributes: (1) One of the keys is used for encryption. This encrypted data may only be decrypted by the other key. (2) It is impossible to determine one key from another (from a mathematical calculation standpoint).

Term	Definition
Internet Assigned Numbers Authority (IANA)	An organization that oversees the allocation of global IP address, domain names and many other parameters used for Internet.
Issuing CA	For a particular certificate, the CA that issues the certificate is called the issuing CA.
Non-Repudiation	Provide proof of delivery to the information sender and proof of sender identity to the receiver so neither party may repudiate the processing of this information after the fact. Technically speaking, non-repudiation refers to the guarantee that this signature must be signed by the corresponding private key if a certain public key can be used to verify a certain digital signature for a trusting party. Legally speaking, non-repudiation refers to the establishment of a possession and control system for private signature keys.
Object Identifier (OID)	(1) One type of unique alphanumeric / numeric identified registered under the International Standard Organization registration standard which could be used to identify the uniquely corresponding certificate policy; where the certificate policy is modified, the OID is not changed accordingly. [Article 2-4, Chapter 1, Regulations on Required Information for Certification Practice Statements] (2) When a special form of code, object or object type is registered with the International Standard Organization (ISO), the unique code may be used as an identified. For example, this code can be used in the public key infrastructure to indicate what certificate policy and cryptographic algorithms are used.
Online Certificate Status Protocol (OCSP)	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

Term	Definition
	extension, which may replace the OCSP to check X.509 certificate status. In practice, a website may obtain a “time limited (e.g. two hours)” OCSP response from the OCSP responder and cache it. Next, this cached OCSP response will be sent to the subscriber (typically a browser) whenever initiating the TLS Handshake. The subscriber only needs to verify the validity of that OCSP response without sending the 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 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.

Term	Definition
	This key must be kept secret under these two circumstances.
Public Key	(11) Key used to verify the validity of digital signature in a pair of signature keys. (12) Key used to encrypt the classified information in a pair of encryption/decryption keys. (13) In the both environment, the key must be public accessible (in digital certificate format generally).
Public-Key Cryptography Standard, (PKCS)	In order to promote the use of public key technology, the RSA laboratory under the RSA Information Security Company has developed a series of public key cryptography standards that are widely used by the industry.
Public Key Infrastructure (PKI)	A set of 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.
Qualified Auditor	Accountant firms, entities, or individuals that satisfy the auditor qualification specified in Section 17.6 of the EV SSL Certificate Guidelines, 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

Term	Definition
	public key listed in the certificate, or the counterpart to identify (or its attributes) of the subject named in a trusted certificate and public key listed in the certificate. [Article 2-6, Chapter 1, Regulations on Required Information for Certification Practice Statements] (2) The individual or agency which receives information including a certificate and digital signature (the public key listed on the certificate may be used to verify the digital signature) and may rely on this information.
Renew (a certificate)	The procedure for issuing a new certificate to renew the validity of information bound together with the public key.
Repository	(1) A trustworthy system used to store and retrieve certificates and other information relevant to certification. [Article 2-7, Chapter 1, Regulations on Required Information for Certification Practice Statements] (2) The database containing the certificate policy and certificate-related information.
Reserved IP Addresses	IPv4 and IPv6 addresses are reserved in the IANA setting. See http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml and http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml
Root Certification Authority (Root CA)	The top-level certification authority in a hierarchical PKI that issues subordinate CA certificates and self-signed certificates, and the self-signed certificates are distributed by the application software suppliers.
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 Sockets	Protocol issued by Netscape through promotion of

Term	Definition
Layer	their web browser which can encrypt network communication in the transport layer and ensure the integrity of transmitted information and perform identity authentication on the server and client. The advantage of the secure socket layer protocol is it is independent and separate from the application layer protocol. High level application layer protocol (such as: HTTP, FTP and Telnet) may be established on top of SSL. The SSL protocol completes encryption algorithm, communication secret key agreement and server authentication work before the application layer protocol communication. This protocol is a successor to the Transport Layer Security (TLS) protocol.
Secret Key	Shared secret in the symmetric cryptosystem, identity authentication of the subscriber is performed by sharing other secrets through passwords, PIN or remote hose (or service). The single key is jointly held by two parties. The sender uses it to encrypt the transmitted information and the receiver uses it to decrypt the information. This jointly held key is generated with previously agreed upon algorithms.
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-issued certificates are CA certificates in which the issuer and subject are the same entity. In other words, it is a certificate containing the corresponding public key or other information signed with the same private key. A self-signed certificate in a PKI may serve as a trust anchor for a certification path. The subject of certificate is the root CA itself. Self-issued certificates can be used by relying parties to validate the self-issued certificates, subordinate CA

Term	Definition
	certificates, cross-certificates and CARLs issued by a root CA.
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 a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA. A CA that is not owned and operated by CHT is called External Operated Subordinate CA.
Subscriber	An entity that (1) is the subject named or identified in a certificate issued to that entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual, an organization, an application or network device.
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	TLS 1.0 was first defined in RFC 2246 by the IETF

Term	Definition
Security (TLS)	based on the SSL 3.0 and updated in RFC 5246 and RFC 6176 as TLS 1.2. The current version is TLS 1.3 defined in RFC 8446 by the IETF in 2018.
Trust List	List of trusted certificates used by relying parties to authenticate certificates.
Trusted Certificate	Certificate trusted by relying party obtained through a secure and reliable transmission method. The public key contained in this type of certificate comes from a trusted path. Also called a trust anchor.
Trustworthy System	Computer hardware, software and programs which possess the following attributes: (1) Functions that protect again intrusion and misuse. (2) Provides reasonably accessible, reliable and accurate operations. (3) Appropriate implementation of preset function. (4) Security procedures uniformly accepted by the general public.
Uninterrupted Power System (UPS)	Provide uninterrupted backup power to loading equipment in the event of abnormal power conditions (such as power outage, interference or power surge) to allow uninterrupted operation of servers, switches and other critical equipment and precision instruments to prevent loss of calculation data, communication network interruption and loss of instrument control.
Validation	The process of identification of certificate applicants. Validation is a subset of identification and refers to identification in the context of establishment of the identity of certificate applicants. [RFC 3647]
Zeroize	Method to delete electronically stored information. Storage of changed information to prevent information recovery.