ePKI Timestamping Certification Authority
Certification Practice Statement (eTSCA CPS)

Version 1.0

Chunghwa Telecom Co., Ltd.

October 09, 2019

Contents

CPS Version Control

Version	Date	Revision Summary
1.0	October 09, 2019	First Released.

1. Introduction

1.1 Overview

ePKI Timestamping CA (eTSCA) is a level-one Subordinate CA of ePKI Root Certification Authority (eCA) and is responsible for the issuance and management of time-stamp certificates. According to the Certificate Policy for the Chunghwa Telecom eCommerce Public Key Infrastructure (ePKI CP), eCA is a top-level CA and a trust anchor of ePKI that relying parties can directly trust its certificates. eCA and eTSCA are both established and operated by Chunghwa Telecom Co., Ltd (CHT).

1.1.1 Certification Practice Statement

This Certification Practice Statement (CPS) describes the practices used to comply with the Electronic Signatures Act, Regulations on Required Information for Certification Practice Statements, ePKI CP, eCA CPS and the official versions of related international standards, including

(1) the Internet Engineering Task Force (IETF) request for comments (RFC) 3647, RFC 5280, RFC 6960, RFC 5019, RFC 3161, RFC 5816 and RFC 3628;

(2) ITU-T X.509;

(3) the European Telecommunications Standards Institute (ETSI) TS 102 023, EN 319 421 and EN 319 422; and

(4) Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates published by CA/Browser Forum (http://www.cabforum.org).

1.1.2 CPS Applicability

The practice statement stipulated in this CPS applies to eTSCA, RAs, Subscribers, Relying parties, repository and other participants.

1.2 Document Name and Identification

This document is ePKI Timestamping Certification Authority Certification Practice Statement. This CPS is version 1.0 and was approved for publication on October 09, 2019. The current version of this CPS can be obtained at the website: https://eca.hinet.net/repository/ or https://tsaca.hinet.net/repository.htm.

eTSCA operates in accordance with the Identity Assurance Level (IAL) level 3 and Authenticator Assurance Level (AAL) level 3 under ePKI CP. The assurance level and the corresponding object identifier (OID) used by eTSCA is listed in the Table below:

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

Assurance Level	OID Name	OID Value
Level 3	id-pen-cht-ePKI-certpolicy-class3Assurance	id-pen-cht-ePKI-certpolicy 3

eTSCA and the time-stamp certificates issued by eTSCA use the following AAL and OIDs defined in the ePKI CP.

Authenticator Assurance Level	OID Name	OID Value
Level 3	id-cht-ePKI-tokenAssurance 3	1.3.6.1.4.1.23459.100.4.3

1.3 PKI Participants

The key members of eTSCA include:

(1) eTSCA

(2) Registration Authorities (RAs)

(3) Subscribers

(4) Relying Parties

1.3.1 Certification Authorities

eTSCA, established and operated by CHT, operates in accordance with the ePKI CP and issues time-stamp certificates.

1.3.2 Registration Authorities

The RA is responsible for collection and authentication of subscriber identity and certificate-related information. eTSCA RA, comprised of one or more RA counters authorized under the organization approved by eTSCA, is established and operated by CHT. Each RA counter has an RA officer (RAO) who is responsible for performing application, revocation and rekey of time-stamp certificates.

eTSCA does not permit any delegated third party to be the registration and verification authority of time-stamp certificates. The delegated third parties mean any natural person or legal entity that is not eTSCA but is delegated to assist the certificate management procedure, and is not covered by the external audit of eTSCA.

1.3.3 Subscribers

A Subscriber refers to the subject who has applied for and obtained a certificate issued by eTSCA. The relationship between the subscriber and certificate subject is listed in the following Table:

Certificate Subject	Subscriber
Time-stamping Authority (TSA) or Time-stamping Unit (TSU)	Owner of TSA

Generation of subscriber key pairs shall comply with the regulations in Section 6.1.1 of this CPS. The subscriber must have the right and

capability to control the private key that corresponds to its subscriber certificate. The subscriber is not capable of issuing certificates to other parties.

1.3.4 Relying Parties

A relying party is the entity that relies on the validity of the binding of the certificate subject name to a public key. 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, or

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

1.3.5 Other Participants

eTSCA and ePKI Time-Stamping Authority are collaborative partners. ePKI Time-Stamping Authority is operated in accordance with the ePKI Time-Stamp Authority policy and ePKI Time-Stamp Authority practice statement, which are approved by the Chunghwa Telecom Certificate Policy Management Authority (PMA) and published in the eCA reposity.

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

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

eTSCA issues time-stamp certificates as defined in the ePKI CP (including certificates for signature use) used to provide evidence that an electronic document existed before a particular time.

For the time-stamp certificates issued by eTSCA, the scope of applications is described as follows:

Cert. Type	Scope of Applications
Time-stamp certificates	• Provide evidence that an electronic document existed at or before a particular time. • Proof of signature time of electronic documents. • Electronic document storage and proof service. • The recipient verifies the correctness of the time-stamp of the electronic document. • Protection the evidence of digital asset generation time or issuance time. • Scope of application includes (but not limited to): e-policy, e-contract, electronic bill, business secret protection, intellectual property protection, e-bidding, e-voting, e-documents, e-certificate letter and code signing, etc.

Subscribers and Relying parties must carefully read, comply with this CPS and shall pay attention to the update of this CPS before using and trusting the certificate services provided by eTSCA.

1.4.2 Prohibited Certificate Uses

Certificates issued under this CPS may not be used in the scope of:

(1) Crime,

(2) Military command and nuclear, biological and chemical weapons control,

(3) Operation of nuclear equipment,

(4) Aviation flight and control systems, and

(5) The scope of prohibitions announced under the law.

1.5 Policy Administration

1.5.1 Organization Administering the Document

Chunghwa Telecom Co., Ltd.

1.5.2 Contact Person

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 Time-stamp 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://tsaca.hinet.net/repository.htm.

1.5.2.2 Certificate Problem Report

Subscribers, Relying parties, application software suppliers, and other third parties may report 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. eTSCA may or may not revoke in response to this request. See Sections 4.9.3 and 4.9.5 for detail of actions performed by eTSCA for making this decision.

1.5.3 Person Determining CPS Suitability for the Policy

eTSCA shall submit this CPS to the PMA for review and approval after checking whether this CPS conforms to the ePKI CP.

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).

eTSCA conducts regular self-audits to demonstrate that it has operated with the assurance level 3 under the ePKI CP. 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 ePKI Root Certification Authority (eCA), into their CA trust lists.

According to the criteria of each program, 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 eTSCA and eCA must conduct and eTSCA must submit the current CPS and audit report to each root certificate program annually. eTSCA shall also continue to maintain the audit seals published on the eTSCA website.

1.5.4 CPS Approval Procedures

This CPS is published by eTSCA following approval by the PMA or MOEA. This CPS must be revised in response to any revision of the ePKI CP, and the revised CPS must be submitted to the PMA and MOEA for approval.

After the revisions of this CPS take effect, if there is any inconsistency

between the original CPS and the revised CPS, then the revised CPS takes precedence unless stipulated otherwise. 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 eTSCA repository is responsible for the publication and storage of eTSCA issued certificates and certificate revocation lists (CRLs), this CPS and the ePKI CP and also provides inquiry services to Subscribers and Relying parties. The repository provides 24-hour round-the-clock service. The website of the eTSCA repository is at https://tsaca.hinet.net/repository.htm. The repository will resume normal operation within two calendar days if unable to operate normally for some reason.

2.2 Publication of Certification Information

eTSCA shall take responsibility for making the following information publicly accessible in its repository:

(1) The ePKI CP and this CPS,
(2) CRLs including issuance time and validity and certificate revocation time,
(3) Online Certificate Status Protocol (OCSP) service,
(4) eTSCA certificates (until the expiry of all certificates issued with private key corresponding to that certificate's public key),
(5) Privacy protection policy,
(6) Related latest news regarding eTSCA, and
(7) The last result of the external audit (as specified in Section 8.6).

2.3 Time or Frequency of Publication

(1) This CPS is assessed whether it is necessary to revise 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 eTSCA is published in the repository within seven calendar days upon the approval of the PMA;

(3) eTSCA issues CRLs at least twice a day and publishes CRLs in the repository; and

(4) eTSCA certificates issued by eCA are published in the repository within seven calendar days upon issuance and receipt of the certificates.

2.4 Access Controls on Repositories

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

The information published by eTSCA under Section 2.2 is primarily provided for browser inquiries by Subscribers and Relying parties. As a result, access control should be implemented when providing access for viewing to guarantee repository security and maintain accessibility and availability.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

eTSCA uses the X.500 Distinguished Name (DN) for the certificate subject name of issued time-stamp certificates.

3.1.2 Need for Names to be Meaningful

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

3.1.3 Anonymity or Psuedonymity of Subscribers

eTSCA does not issue anonymous certificates or pseudonymous certificates to any TSA.

3.1.4 Rules for Interpreting Various Name Forms

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

3.1.5 Uniqueness of Names

eTSCA's X.500 distinguished name for its CA certificates is:

C=TW,

O=Chunghwa Telecom Co., Ltd.,

CN= ePKI Timestamping CA – Gn, where n = 1, 2, 3…

eTSCA shall use the X.520 standard to define the various naming attributes for assembly to ensure the uniqueness of the X.500 naming space recognized by eTSCA for subject name of the subscriber certificate. The subject name of the subscriber certificate issued by eTSCA permits (but

not limited to) the use of the following naming attributes defined in the X.520 standard for assembly:

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

According to ETSI EN 319 422, the countryName attribute shall specify the country in which the TSA is established (which is not necessarily the name of the country where the TSU is located). The organizationName shall contain the full registered name of the TSA responsible for managing the TSU. That name should be an officially registered name of the TSA. The commonName specifies an identifier that the TSA can uniquely identify the TSU.

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

If the identification name used by the Subscriber is proven by relevant competent authorities (institutions) or the authority with the right of interpretation that the identification name is owned by other Applicant, that Subscriber shall assume relevant legal responsibility and eTSCA may revoke that Subscriber’s certificate.

3.1.6 Recognition, Authentication, and Role of Trademarks

The certificate subject name provided by Subscribers must comply with relevant regulations in our country's Trademark Act and Fair-Trade Act. eTSCA shall not bear the responsibility for reviewing whether the certificate subject name provided by the Subscriber complies with the above regulations. Related disputes and arbitration shall not be the obligation of eTSCA and the Subscriber shall handle matters in accordance with regular administrative and judicial remedies.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

eTSCA shall verify that the private key is possessed by the individual.

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

3.2.2 Authentication of Organization Identity

The identification required, identification and confirmation procedures, and whether the application shall be submitted at the counter in person for organization identification and authentication are described as follows according to different organization types:

(1) Identity authentication for private organization:

The private organization must submit copies of the correct certification documents (such as Registry List of Company, Alteration of Company Registry List, Certificate of Corporate

Registration, photocopies of Application Form for Registration of Withholding Entity Establishment (Alteration) (Notification for Tax ID Number Assignation)) which have been approved by the competent authority or a legally authorized body (such as a court) to the RAO. The copies of the certification documents shall be affixed with the seal of the organization and responsible person (must match the seal used at the time of company registration). The RAO shall check the authenticity of the application information submitted by the organization and representative identity and verify that the representative has the right to apply for the certificate in the organization's name. The representative shall submit the application at eTSCA or RA counter in person. If the representative is unable to submit the application at the counter in person, an agent may be appointed to submit the application at the counter of his/her behalf. The assurance level 3 regulations for authentication of the identity of representatives in Section 3.2.3 shall be followed.

(2) Identity authentication for government agency or authority:

The government agency or authority follows the above private organization identity authentication method or official public document to apply for the certificate. eTSCA or RA must verify that the agency or authority really exists and determine the authenticity of the official documents.

(3) Identity authentication for Organizations belonging to CHT:

Organizations belonging to CHT must apply for the certificate with official documents and the RA must check if the agency or authority really exists and determine the authenticity of the public documents.

Validation of the organization's legal existence, organization name,

registration number, business or operational existence, can be obtained from Qualified Government Information Sources (QGIS) such as the Ministry of Economic Affairs Bussiness & Factory Registration Databas and Qualified Government Tax Information Sources (Qualified Government Tax Information Source, QTIS) from public information of the Finance and Taxation Information Center of the Ministry of Finance, or contacted in person with the registration authority, or obtained from qualified government information sources and qualified government tax information sources, registration authorities or qualified independent sources via e-mail, email address, website or phone to contact to confirm the identity of the applicant.

3.2.3 Authentication of Individual Identity

The identification required, identification and confirmation procedures, and whether the application shall be submitted at the counter in person for individual identification and authentication are described as follows:

(1) Check written documentation:

The applicant shall provide information which includes name, ID number and birthdate and at least present one original approved photo ID (such as national ID card) during certificate application to the RAO to authenticate the applicant's identity.

(2) Personal information submitted by the applicant such as personal identification code (e.g., ID card number), name and address (e.g., household registration address) shall be checked against the information registered with the competent authority (e.g., household registration information) or other information

registered with a trusted third party recognized by the competent authority.

(3) Counter application:

The applicant must verify his / her identity in person at eTSCA or RA counter. If the applicant is unable to present the application in person at the counter, the applicant may submit a letter of appointment to appoint an agent to submit the application in person on their behalf but eTSCA or RA must verify the authenticity of the letter of appointment (such as the subscriber's seal on the letter of appointment) and authenticate the identity of the agent in accordance with the above regulations.

If an applicant has previously underwent the counter identification and authentication procedures performed by eTSCA, RA or CA trusted authority or individual (e.g., household registration office or notary) which conforms to the above regulations and the counter has kept the evidence material (e.g., seal certification), then the applicant does not need to apply in person. eTSCA or RA will verify the evidence material they kept instead.

3.2.4 Non-verified Subscriber Information

Not appliable.

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

(1) Confirming the organization legal existence through third-party

identity verification service or database, or documents issued by government or authorized organizations;

(2) Using telephone, postal letter, e-mail, SMS or fax 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

eTSCA is not a Root CA. Not appliable.

3.2.7 Data Source Accuracy

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

(1) The age of the information provided,

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

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

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

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

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

As stated in Section 3.2.

3.3.2 Identification and Authentication for Re-key after Revocation

If the Subscriber's private key needs to be re-keyed due to certificate revocation, the Subscriber shall re-apply for the certificate with eTSCA. The RA will identify and authenticate the Subscriber who re-apply for the certificate in accordance with the regulations in Section 3.2.

3.4 Identification and Authentication for Revocation Request

eTSCA or its RA must perform authentication of the certificate revocation application to verify that the Applicant has the right to submit the certificate revocation. The authentication procedure for certificate revocation applications is the same as the regulations in Section 3.2.

4. Certificate Life-cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

eTSCA currently only accepts organizations to submit certificate applications.

Because a TSA or the TSU of a TSA is not legally capable, the certificate applicant must be submitted by the owner of that TSA .

4.1.2 Enrollment Process and Responsibilities

eTSCA and its RA are responsible for ensuring that the identity of the certificate Applicant is verified in compliance with the ePKI CP and CPS before certificate issuance. The Applicant is responsible for providing enough and accurate information (e.g., filling out the organization legal name and code) and identification documents that eTSCA and its RA can perform the necessary identity identification and authentication prior to the certificate issuance. The Subscriber shall bear the following responsibilities:

(1) The Subscriber shall comply with the relevant application regulations in this CPS and the Subscriber Agreement and verify the accuracy of the information submitted for the application,

(2) The Subscriber shall accept the certificate in accordance with the regulations in Section 4.4 after eTSCA approves the certificate application and issues the certificate,

(3) After obtaining the certificate issued by eTSCA, the Subscriber shall check the accuracy of the information contained in the

certificate and use the certification in accordance with the regulations in section 1.4.1. If there is an error in the certificate information, the Subscriber shall notify the RA and refrain from using the certificate,

(4) The Subscriber shall properly safeguard and use their private key,

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

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

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

4.2 Certificate Application Processing

The certificate application procedures are as follows:

(1) The certificate Applicant fills out the information on the certification application form and agrees to the Subscriber Agreements,

(2) The Applicant sends the information for certificate application and relevant certification to the RA, and

(3) The Applicant shall self-generate the keys and a PKCS#10 certificate request file signed with the private key. The certificate

request file is submitted to the RA during the certificate application.

4.2.1 Performing Identification and Authentication Functions

eTSCA and its RA shall ensure that the system and procedure are sufficient to verify the Subscriber's identity that complies with the ePKI CP and this CPS. The initial registration procedure is implemented in accordance with the regulations in Section 3.2 of this CPS. The Applicant shall submit correct and complete factual information. The information required for the certificate application contain required and optional information, and only the information listed on the certificate profile is recorded in the certificate. The information submitted by the Applicant and contact records kept by eTSCA and its RA during the application process shall be properly kept in a secure, auditable manner in accordance with the ePKI CP and this CPS.

4.2.2 Approval or Rejection of Certificate Applications

If all identity authentication tasks can be successfully implemented under the relevant regulations and best practices, eTSCA and its RA may approve the certificate application.

If the above identity authentication tasks cannot be successfully completed, eTSCA and its RA may refuse the certificate application. Except for identity identification and authentication reason, eTSCA and its RA may also refuse to issue the certificate for other reasons. eTSCA and its RA may refuse the certificate application from Applicants who have previously been rejected or have previously violated the Subscriber Agreements.

4.2.3 Time to Process Certificate Applications

eTSCA and its RA shall complete the time-stamp certificate application within a reasonable period of time. Provided that the information submitted by the Applicant is complete and complies with the ePKI CP, this CPS and checking requirements, the RAO shall quickly complete the certificate application review. The time needed for the RA to process certificate applications and that for eTSCA to issue the certificates depends on the certificate group. These times may be disclosed in the Subscriber Agreements, contract or eTSCA website.

The review procedure for the applications of time-stamp certificates which are received and meet relevant regulations shall be completed within 5 working days by the RAOs and the Subscriber shall be asked to accept the certificate. After the certificate is accepted, eTSCA shall complete the certificate issuance within one working day or the date specified by the Subscriber on which the certificate is to be obtained by the Subscriber.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

Upon eTSCA and its RAs receive the certificate application, the relevant review procedures are enforced in accordance with Chapter 3 of this CPS to serve as a basis for determining whether approve the certificate issuance or not.

Certificate issuance steps are as follows:

(1) The RA submits the certificate application passed the review procedures to eTSCA,

(2) When eTSCA receives the certificate application submitted by the

RA, the authorization status of the RA is first checked, the authorized assurance level and scope is verified and then the certificate is issued according to the information of the certificate application submitted by the RA,

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

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

(5) eTSCA reserves the right to refuse certificate issuance to any entity. eTSCA shall not bear any liability for damages to the Applicant who has been refused to issue the certificate.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

After eTSCA completes certificate issuance, the Subscriber is notified to draw the certificate or notify the Subscriber to draw the certificate through the RA.

If eTSCA or its RA does not approve the certificate issuance, the Applicant is notified by e-mail or telephone and shall be informed of the reasons for the refusal.

If the information in the certificate is found to be incorrect or is inconsistent with the information provided at the time of application when

the Subscriber accepts the certificate, the RA should be notified immediately. Otherwise, it shall be deemed that the Subscriber consents to abide by the rights and obligations in this CPS and related contracts.

4.4 Certificate Acceptance

The Applicant shall check whether the information recorded in the certificate is correct and consistent with the information provided at the time of application. After the Applicant accepts the issued certificate, eTSCA must publish the certificate to its repository. If the Applicant reviews the content of the issued certificate and refuses to accept the certificate, eTSCA will revoke the certificate.

The above certificate Applicant shall review the certificate fields that should at least include the certificate subject name, certificatePolicies, keyUsage and extKeyUsage before deciding to accept the certificate.

Acceptance of the certificate is deemed the Applicant's consent to comply with the rights and obligations in this CPS, Subscriber Agreements or related contracts.

If there is a fee or refund matter involved with certificate refusal, the Applicant shall handle the matter in accordance with the provisions of the Consumer Protection Act and Fair-Trade Act.

4.4.1 Conduct Constituting Certificate Acceptance

The certificate Applicant pre-reviews the content of a subscriber certificate to be issued or reviews the content of an issued subscriber certificate is correct. The certificate is then published to the repository or delivered to the Applicant by eTSCA.

4.4.2 Publication of the Certificate by the CA

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

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers refer to the entities that request and obtain certificates approved by eTSCA. Their relationship with the certificate subject is shown in the table in Section 1.3.3 of this CPS. Scope of applications regarding time-stamp certificate is stipulated in Section 1.4.1 of this CPS. Key pairs of subscribers shall be generated in compliance with Section 6.1.1 of this CPS. Subscribers must be able to control the private keys and do not issue certificates to others. Subscribers must independently possess and control the right and capability to the private key corresponding to the certificate. Subscribers themselves do not issue certificates to others. Subscribers shall protect their private keys from unauthorized use or disclosure and shall use their private keys only for the correct key usage (i.e., the policy for key usage specified in the extension of the certificates), such as digitalsignature and contentCommitment. Subscribers must correctly use certificates adhering to the certificate policies listed in the certificates.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties refer to third parties who trust the connecting relationship between the certificate subject name and public key. Relying parties shall use software that is compliant with ITU-T X.509 and IETF RFCs.

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

(1) Verify the integrity of the electronic documents with digital signatures.
(2) Verify the identity of the document signature author.

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

For example, relying parties may only trust digital signatures that conform to the following conditions:

(1) Digital signature is generated through the corresponding valid certificate and the certificate accuracy can be verified through the certificate chain.
(2) Related CRL or OCSP response messages are checked for certificate and unrevoked certificates used by relying parties.
(3) Certificates are used according their CPS regulations and certificate usage.

4.6 Certificate Renewal

Certificate renewal refers to the reissue of one certificate with

unchanged subscriber identification information which has the same public key, the same certificate subject information and a different serial number from the original certificate but it is a certificate with a valid extension.

Since random extension of public keys could result in reduced private key security and increased probability of key compromise. eTSCA does not provide certificate renewal services. Key pair generation and certificate request submission is done in the same manner as the initial registration.

4.6.1 Circumstances for Certificate Renewal

Not appliable.

4.6.2 Who May Request Renewal

Not appliable.

4.6.3 Processing Certificate Renewal Requests

Not appliable.

4.6.4 Notification of New Certificate Issuance to Subscriber

Not appliable.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Not appliable.

4.6.6 Publication of the Renewal Certificate by the CA

Not appliable.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Not appliable.

4.7 Certificate Re-Key

4.7.1 Circumstance for Certificate Re-key

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

If the Subscriber's tims-stamp certificate has not been revoked, eTSCA or its RA may start to process the re-key and new certificate application two months before the expiry of the subscriber's private key usage period. The procedure for the new certificate shall be handled in accordance with Sections 4.1 and 4.2.

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

4.7.2 Who May Request Certification of a New Public Key

A subscriber or legally authorized third party (representative authorized by the organization) may submit a time-stamp certificate application to eTSCA.

4.7.3 Processing Certificate Re-keying Requests

For subscriber certificate re-keying, Subscribers shall submit a new application of time-stamp certificate to eTSCA. The related procedures must be implemented in accordance with Sections 3.1, 3.2, 3.3, 4.1 and 4.2.

4.7.4 Notification of New Certificate Issuance to Subscriber

As stated in Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

As stated in Section 4.4.1.

4.7.6 Publication of the Re-keyed Certificate by the CA

As stated in Section 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

The RA may receive notification of re-keyed certificate issuance.

4.8 Certificate Modification

4.8.1 Circumstance for Certificate Modification

eTSCA does not provide certificate modification service.

If there is any change to the information contained in the certificate, the Subscriber must submit a new certificate application in accordance with the procedures in Sections 4.1 and 4.2. After the Subscriber receives the new certificate, the old certificate shall be revoked.

4.8.2 Who May Request Certificate Modification

Not appliable.

4.8.3 Processing Certificate Modification Requests

Not appliable.

4.8.4 Notification of New Certificate Issuance to Subscriber

Not appliable.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not appliable.

4.8.6 Publication of the Modified Certificate by the CA

Not appliable.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not appliable.

4.9 Certificate Revocation and Suspension

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

4.9.1 Circumstances for Revocation

eTSCA shall revoke a certificate within 3 working days if one or more of the following occurs:

(1) The Subscriber requests in writing to eTSCA that they wish to revoke the certificate;
(2) The Subscriber notifies eTSCA that the original certificate request was not authorized and does not retroactively grant authorization; or
(3) eTSCA obtains evidence that the Subscriber's private key corresponding to the public key in the certificate suffered a key compromise.

eTSCA should revoke a certificate within 3 working days and must revoke a certificate within 7 working days if one or more of the following occurs:

(1) The certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6;

(2) eTSCA obtains evidence that the certificate was misused;
(3) eTSCA is made aware that a subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;
(4) eTSCA is made aware of a material change in the information contained in the certificate;
(5) eTSCA is made aware that the certificate was not issued in accordance with these requirements or the ePKI CP or this CPS;
(6) eTSCA determines or is made aware that any of the information appearing in the certificate is inaccurate;
(7) eTSCA's right to issue certificates under these requirements expires or is revoked or terminated, unless eTSCA has made arrangements to continue maintaining the CRL/OCSP Repository;
(8) Revocation is required by the ePKI CP and/or this CPS;
(9) eTSCA is made aware of a demonstrated or proven method that exposes the Subscriber's private key to compromise, methods have been developed that can easily calculate it based on the public key (such as a Debian weak key, see https://wiki.debian.org/SSLkeys), or if there is clear evidence that the specific method used to generate the private key was flawed; or
(10) Under the circumstance that the payment deadline has expired and the Subscriber has been notified, the Subscriber has still not paid the fee.

eTSCA may at its own discretion revoke subscriber certificaters under the aforementioned circumstances.

4.9.2 Who Can Request Revocation

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

In addition, a Subscriber, Relying party, application software supplier or other third parties may submit certificate problem report to advise eTSCA a reasonable reason to revoke the certificate.

4.9.3 Procedure for Revocation Request

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

(2) After the RA completes the review procesures, the RA submits the certificate revocation application to eTSCA;

(3) When eTSCA receives the certificate revocation application submitted by the RA, the authorization status of the RA is first checked to verify its authorized assurance level and scope. Afterward, the certificate is revoked based on the certificate revocation request submitted by the RA;

(4) If the application does not pass the above checking, eTSCA will send back the related erroneous message to the RA and refuse to perform related subsequent work. If there are any questions, the RA may directly contact eTSCA to understand where the problem is;

(5) In order to ensure the security, integrity and non-repudiability of the data transmitted between eTSCA and its RA, the data of the certificate application is encrypted with a digital signature and transmitted through the network by transport layer security (TLS) protocol;
(6) eTSCA uses the same CA private key issuing the certificate to publish the revoked certificate serial number and the reason for revocation to the CRL by the digital signature;
(7) Provide a timelier OCSP service (e.g. the status of being revoked, the status of being applied, or the status is valid); and
(8) eTSCA receives certificate problem reports and provides 24x7 availability of certificate problem response mechanism, as specified in Section 4.9.3.1.

4.9.3.1 Mechanism for Responding the Certificate Problems

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

4.9.4 Revocation Request Grace Period

The certificate revocation request grace period refers to the time to submit a certificate revocation request when the Subscriber has confirmed the certificate revocation circumstances. The RA shall report suspect RA private key compromise circumstances to eTSCA within one hour. When the Subscriber's private key is lost or suspect or known to be compromised

or the information appearing in the certificate has expired or is inaccurate, the Subscriber shall promptly submit a certificate revocation application to the RA. The certificate revocation request grace period is two working days. eTSCA may extend the certificate revocation grace period when deemed necessary.

4.9.5 Time within Which CA Must Process the Revocation Request

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

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

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

4.9.6 Revocation Checking Requirement for Relying Parties

Before using time-stamp certificates issued by eTSCA, the Relying parties shall first check the CRLs or OCSP responses published by eTSCA to verify the validity of certificates. The Relying parties shall verify the revoking time of certificates, the validity of signatures of the CRLs or OCSP responses, and certificate chains with their validity.

eTSCA publishes the information of revoked certificates to the repository for checking purposes. There are no restrictions for the checking of CRLs by Relying parties. The website is at: https://tsaca.hinet.net/repository.htm

4.9.7 CRL Issuance Frequency

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

4.9.8 Maximum Latency for CRLs

eTSCA shall publish the CRL no later than the time specified in the nextUpdate field of the previously issued CRL.

4.9.9 On-line Revocation/Status Checking Availability

eTSCA provides the inquiry to certificate revocation/status by CRL and OCSP responses.

eTSCA uses OCSP Responder to provide the OCSP responses

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

4.9.10 On-line Revocation Checking Requirements

Relying parties shall check the validity of certificates by using the CRLs or OCSP service in accordance with Section 4.9.6 or 4.9.9, respectively.

eTSCA uses SHA-256 Hash Function Algorithm to issue OCSP responses.

eTSCA supports the OCSP service such that Relying parties can use HTTP-based POST or GET method to execute the OCSP service.

Regarding the subscriber certificates, the updating frequency of OCSP shall be at least one update every four days; the maximum effective period of OCSP responses is 10 calendars days.

If the OCSP responders receive the status request of the un-issued certificates, it must not reply the status as “Good,” and eTSCA shall supervise whether the OCSP responders respond to such requests in compliance with the above security response procedures.

4.9.11 Other Forms of Revocation Advertisements Available

No other forms of revocation advertisements.

4.9.12 Special Requirements Related to Key Compromise

As stated in Sections 4.9.1, 4.9.2 and 4.9.3.

4.9.13 Circumstances for Suspension

eTSCA does not provide the service of certificate suspension.

4.9.14 Who Can Request Suspension

Not appliable.

4.9.15 Procedure for Suspension Request

Not appliable.

4.9.16 Limits on Suspension Period

Not appliable.

4.9.17 Procedure for Certificate Resumption

Not appliable.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

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

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

4.10.2 Service Availability

eTSCA maintains 24x7 availability of certificate status service.

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

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

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

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

eTSCA and subscriber's private signing keys shall not be escrowed.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

eTSCA does not currently support session key encapsulation and recovery.

5. Facility, Management, and Operation Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

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

5.1.2 Physical Access

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

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

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

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

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

The following checks and records need to be made when eTSCA 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 eTSCA 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 eTSCA facility has a constant temperature and humidity system to provide an optimal operation environment for the facility.

5.1.4 Water Exposures

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

5.1.5 Fire Prevention and Protection

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

5.1.6 Media Storage

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

5.1.7 Waste Disposal

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

5.1.8 Off-site Backup

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

5.2 Procedural Controls

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

5.2.1 Trusted Roles

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

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

The administrator is responsible for:

- Installation, configuration and maintenance of the eTSCA system
- Creation and maintenance of system user accounts
- Generation and backup of eTSCA keys

The CA officer is responsible for:

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

The internal auditor is responsible for:

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

The system operator is responsible for:

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

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

The physical security controller is responsible for:

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

The cyber security coordinator is responsible for:

- Maintenance of the network and network facilities
- Patches management for the vulnerabilities of the network facilities
- The cyber security of eTSCA
- Detection and report of the cyber security events

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

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

The RAO is responsible for:

- Processing certificate requests of issuance, revocation and re-key, including enrollment, identity identification and authentication

The RA system requiring two-factor authentication must handle certificate vetting process and certificate issuance by personnel in trusted roles.

5.2.2 Number of Persons Required per Task

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

- Administrator

  At least 3 qualified individuals are needed.

- CA Officer

  At least 2 qualified individuals are needed.

- Internal Auditor

  At least 2 qualified individuals are needed.

- System Operator

  At least 2 qualified individuals are needed.

- Physical security controller

  At least 2 qualified individuals are needed.

- Cyber security coordinator

  At least 1 qualified individual.

- Anti-virus and anti-hacking coordinator

  At least 1 qualified individual.

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

Assignments	Administrator	CA Officer	Internal Auditor	System Operator	Physical security controller	Cyber security coordinator	Anti-virus and anti-hacking coordinator
Installation, configuration, and maintenance of the eTSCA system	2				1		
Establishment and maintenance of system user accounts	2				1		
Generation and backup of eTSCA keys	2		1		1		

Assignments	Administrator	CA Officer	Internal Auditor	System Operator	Physical security controller	Cyber security coordinator	Anti-virus and anti-hacking coordinator
Activation / deactivation of certificate issuance services		2			1		
Activation / deactivation of certificate revocation services		2			1		
Activate/deactivate the issuance services of CRL		2			1		
Checking, maintenance and archiving of audit logs			1		1		
Daily operation and maintenance of system equipment				1	1		
System backup and recovery				1	1		
Storage media updating				1	1		
Hardware and software updates outside the eTSCA certificate management system				1	1		
Website maintenance				1	1		
Daily operation and maintenance of the network and network facilities				1	1	1	
Patching the vulnerabilities of the network facilities	1				1	1	
Reporting the threats and vulnerabilities of computer virus							1
keep the antivirus system's signatures update and patches for the vulnerabilities				1	1		

5.2.3 Identification and Authentication for Each Role

Use IC cards to identify and authenticate administrator, CA officer, internal auditor and system operator roles as well as central access system

to determine the authority to identify and authenticate physical security controller role.

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

Operating system account management by the eTSCA host uses login account numbers, passwords and groups to identify and authenticate administrator, CA officer, internal auditor, and system operator. eTSCA uses the user's account, password, and system account administration functions, or other security mechanisms to identify the role of the cyber security coordinator.

5.2.4 Roles Requiring Separation of Duties

Trusted roles of eTSCA requiring separation of duties are described as follows:

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

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

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

(1) Security evaluation for personnel selection

Personnel selection includes the following items:

(a) Personality evaluation,

(b) Applicant experience evaluation,

(c) Academic and professional skills and qualifications evaluation,

(d) Personal identity check, and

(e) Evaluation of personnel conduct.

(2) Management of Personnel Evaluation

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

(3) Appointment, Dismissal and Transfer

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

(4) Duty of Confidentiality Agreement

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

5.3.2 Background Check Procedures

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

5.3.3 Training Requirements

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

Trusted Role	Training Requirements
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 and vulnerabilities of computer virus. (2) Security mechanism for the operating system and the network.
RAO	(1) Basic knowledge of the PKI (2) Identity authorization and information verification policies and procedures (including ePKI CP and this CPS)

5.3.4 Retraining Frequency and Requirements

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

5.3.5 Job Rotation Frequency and Sequence

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

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

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

(4) Only personnel with a full two years of experience as a cyber security coordinator as well as the requisite training and clearance

may be reassigned to the position of administrator, CA officer, or internal auditor.

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

5.3.6 Sanctions for Unauthorized Actions

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

5.3.7 Independent Contractor Requirements

The security requirements of the independent contractor of eTSCA shall be in accordance with Section 5.3.

5.3.8 Documentation Supplied to Personnel

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

5.4 Audit Logging Procedures

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

5.4.1 Types of Events Recorded

(1) Key generation

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

(2) Private key loading and storage

- Loading the private key into a system component.
- All access to private keys kept by eTSCA for key recovery work.

(3) Certificate registration

- Certificate registration request procedure.

(4) Certificate revocation

- Certificate revocation request procedure.

(5) Account administration

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

(6) Certificate profile management

- Certificate profile changes.

(7) CRL profile management

- CRL profile changes.

(8) Physical access / site security

- Known or suspect violation of physical security regulations.

(9) Anomalies

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

5.4.2 Frequency of Processing Log

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

eTSCA shall check the audit logs monthly.

5.4.3 Retention Period for Audit Log

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

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

5.4.4 Protection of Audit Log

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

5.4.5 Audit Log Backup Procedures

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

(1) eTSCA shall routinely archive event logs.

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

5.4.6 Audit Collection System (Internal vs. External)

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

5.4.7 Notification to Event-causing Subject

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

5.4.8 Vulnerability Assessments

eTSCA shall follow the methods and frequency stipulated in the

WebTrust Principles and Criteria for Certification Authorities to conduct the vulnerability assessments at least once per quarter and the penetration testing at least once per year. eTSCA also must conduct penetration testing after it is determined that there is a significant upgrade or modification to the application program or infrastructure. eTSCA shall record the skills, tools, followed ethics, competitive relations and independence guidelines for those personnel or groups capable of implementing reliable vulnerability scanning, penetration testing, or information security diagnosis or security surveillance.

5.5 Records Archival

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

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

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

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

5.5.1 Types of Records Archived

eTSCA retains the following information in its archives:

(1) eTSCA accreditation information from competent authorities.

(2) CPS.

(3) Major contracts.

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

5.5.2 Retention Period for Archive

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

5.5.3 Protection of Archive

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

5.5.4 Archive Backup Procedures

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

5.5.5 Requirements for Time-stamping of Records

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

5.5.6 Archive Collection System (Internal or External)

There is currently no archive information collection system.

5.5.7 Procedures to Obtain and Verify Archive Information

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

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

5.6 Key Changeover

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

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

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

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

eTSCA establishes notifying and handling procedures in the event of security incident or system compromise. The procedures shall be reviewed, drilled, and updated at least annually.

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

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

If the eTSCA computer equipment is damaged or unable to operate, but the eTSCA signature key has not been destroyed, priority shall be given to restoring operation of the eTSCA repository and quickly reestablishing the generation of certificate status information.

5.7.3 Entity Private Key Compromise Procedures

eTSCA implements the following recovery procedures in the event of signature key compromise in order to restore the operation of certificate issuance and administration as soon as possible:

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

eTSCA shall conduct the drills at least once a year.

5.7.4 Business Continuity Capabilities after a Disaster

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

5.8 CA or RA Termination

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

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

(2) eTSCA shall take the following measures when terminating their service:

- For certificates which are valid at the time of termination, arrangements shall be made for other CA to take over the service. Matters regarding service termination and service acceptance by other CAs shall be notified to subscribers with valid certificates. This shall not apply if notification cannot be made.
- All records and files during the operation period shall be handed over to the other CA that is taking over this service.
- If there is no CA willing to take over the eTSCA service, a report shall be submitted to the competent authority to arrange for other CA to take over this service.
- If the competent authority arranges for other CA to take over

the service but no other CA takes over the service, eTSCA shall revoke the still valid certificates, publish the revoked certificates in the repository and notify all certificate-related persons 30 days prior to service termination. eTSCA shall refund the certificate issuance fees based on the propotion of the certificate validity.

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

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

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

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

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

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

6.1.1.1 Subscriber Key Pair Generation

Subscribers securely generate the key pairs and are responsible for the safekeeping of their private keys.

6.1.2 Private Keys Delivery to Subscriber

Not applicable.

6.1.3 Public Key Delivery to Certificate Issuer

If the subscriber self-generates a key pair and delivers the public key to the RA via a certificate signing request file with PKCS# 10 format. The RA shall delivery the public key to eTSCA via secure channels after it is verified that the subscriber is in possession of the corresponding private key in accordance with the regulations in Section 3.2.1.

Secure channels referred in this Chapter are the use of Transport Layer

Security (TLS) or other equivalent or higher level data encryption transmission methods.

6.1.4 CA Public Key Delivery to Relying Parties

The eTSCA public key is issued by eCA and published to the eTSCA repository for direct download and installation by subscribers and relying parties. Relying parties shall obtain eCA's public key or self-signed certificate via secure channels according to the eCA CPS before using the eTSCA public key certificate. Relying parties shall then validate the signature in the eTSCA public key certificate to ensure the trustworthiness of the public key in the public key certificate.

6.1.5 Key Sizes

eTSCA uses 2048-bit or the above RSA keys and SHA-256 hash function algorithm to issue certificates.

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

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

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

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

6.1.6 Public Key Parameters Generation and Quality Checking

The public key parameter of the RSA algorithm is null.

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

The subscriber key may generate the prime numbers needed for the RSA algorithm inside the hardware security module but this does not guarantee that this prime number is a strong prime.

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

If the certificates are issued with ECC algorithm, eTSCA shall 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 either the ECC Full Public Key Validation Routine or the ECC Partial Public Key Validation Routine.

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

eTSCA's private signing key is used to issue certificates and CRLs. eTSCA's own public key certificate is issued by eCA. The keyUsage bits used for the keyUsage extension are digitalSignature, keyCertSign and cRLSign. The extKeyUsage extension shall contain the value of id-kp-timeStamping (1.3.6.1.5.5.7.3.8).

The keyUsage extension of time-stamp certificates contains digitalSignature and contentCommitment. The extKeyUsage extension shall contain the value of id-kp-timeStamping (1.3.6.1.5.5.7.3.8).

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

eTSCA uses FIPS 140-2 Level 3 certified hardware security modules.

Storage media for subscriber key pairs shall be the hardware security

modules that meets the requirements of FIPS 140-2 Level 3, CEN Workshop Agreement 14167-2[CWA 14167-2], or ISO 15408 EAL 4.

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

eTSCA key splitting multi-person control uses n-out-of-m LaGrange Polynomial Interpolation. It is a perfect secret sharing method used for private key splitting and 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 eTSCA private key multi-person control. Therefore, it can be used as the activation method for private keys as well (see Section 6.2.8).

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

6.2.3 Private Key Escrow

eTSCA's private signing key is not escrowed. eTSCA shall not be responsible for the safekeeping of subscriber private keys.

6.2.4 Private Key Backup

Backups of eTSCA private keys are performed according to the key splitting multi-person controls in Section 6.2.2, and IC cards verified with FIPS 140-2 Level 2 or above are used as the storage media for key splitting.

6.2.5 Private Key Archival

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

6.2.6 Private Key Transfer into or from a Cryptographic Module

eTSCA transfers the private key into the cryptographic modules under

the following circumstances:

(1) Key generation,

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

(3) For the purpose of HSM transfer, the private keys are encrypted when transported between hardware security modules and never exist in plaintext form. After the private keys are imported, the related secret parameters generated during the transport process must be completely destroyed.

6.2.7 Private Key Storage on Cryptographic Module

As stated in Sections 6.1.1 and 6.2.1.

6.2.8 Method of Activating Private Key

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

Subscribers shall choose a secure computer environment and a trustworthy application system carefully, and keep and use the private keys properly. The subscriber private keys shall be kept in a hardware security module and can only be activated by the IC cards controlled by multiple people. The controlling IC cards for different purposes are maintained by different people.

6.2.9 Method of Deactivating Private Key

The multi-person controls in Section 6.2.2 are used to deactivate eTSCA private keys.

eTSCA does not provide subscriber private key deactivation service.

6.2.10 Method of Destroying Private Key

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

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

If a private key is no longer used, it must be deactived or deleted from its storage location. After deleting the key, the key management tools provided by this module must be used to verify that the above key no longer exists.

If services are permanent not provided by a hardware security module, all private keys stored in this module must be erased.

The destruction method for subscriber private keys is not stipulated.

6.2.11. Cryptographic Module Rating

See Section 6.2.1.

6.3 Other Aspects of Key Pair Management

Subscribers must manage their own key pairs. eTSCA is not responsible for safeguarding subscriber private keys.

6.3.1 Public Key Archival

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

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

6.3.2.1 eTSCA Certificate Operational Periods and Key Pair Usage Periods

eTSCA certificate operational periods and key pair usage periods are:

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

The new OCSP responder certificate is disclosed daily (given to the relying parties by the OCSP response signed by the new private key digital signature which contains that certificate).

6.3.2.2 Subscriber Certificate Operational Periods and Key Pair Usage Periods

The subscriber certificate operational periods and key pair usage periods are:

Type of Cert.	Private Key Usage	Certificate Term
Time-stamp Certificate	■ See Section 6.1.7: 15 months	135 months

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

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

6.4.2 Activation Data Protection

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

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

6.4.3 Other Aspects of Activation Data

The eTSCA private key activation data is not archived.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

eTSCA and related auxiliary systems provide the following security control functions through the operating system, or a combination of operating system, software and physical safeguards:

(1) Authenticate the identity of users before permitting access to the system or applications,

(2) Manage privileges of users to limit users to their assigned roles,

(3) Provide security audit capability, and

(4) Support protection of process integrity and security control.

The eTSCA equipment is established on work platforms which have undergone a security assessment and the CA-related systems (hardware, software, operating system) must be operated with configurations which have undergone a security assessment. eTSCA enforces multi-factor authentication for all accounts capable of directly causing certificate issuance.

6.5.2 Computer Security Rating

eTSCA servers use Common Criteria EAL 3 certified computer operating systems.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

Quality control for eTSCA system development complies with CMMI standards.

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

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

The system research and development department shall exercise the due care of a good administrator, sign a security warranty guaranteeing there are no back doors or malicious programs, and provide a product or program handover list, test report, system management manual, and source code scanning report to eTSCA as well as conduct program version control.

6.6.2 Security Management Controls

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

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

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

eTSCA references the methodologies and standards in the ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, ISO/IEC 31000 and WebTrust Principles and Criteria for Certification Authorities 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 eTSCA host and repository have firewalls and are connected to external networks. The repository is placed on the outside service area (de-militarized zone, DMZ) in the firewall and connected to the Internet. Except during required maintenance or backup, the repository provides uninterrupted certificate and CRL inquiry services.

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

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

6.8 Time-stamping

eTSCA regularly conducts system synchronization with a reliable time source to maintain the correctness of system time and ensure the

accuracy of the following times:

(1) Time of subscriber certificate issuance,

(2) Time of subscriber certificate revocation,

(3) Time of CRL issuance, and

(4) Time of system event occurrence.

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

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

The certificates issued by eTSCA conform to the official versions of the ITU-T X.509, RFC 3161, RFC 3628 and RFC 5280.

eTSCA 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)

eTSCA issues X.509 version 3 certificates.

7.1.2 Certificate Extensions

The extensions of the certificates issued by eTSCA are set in compliance with the official versions of the ITU-T X.509, RFC3161, RFC 3628 and RFC 5280.

7.1.2.1 Subordinate CA Certificate of eTSCA

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

a. certificatePolicies

This extension is required and marked as non-critical. It asserts the policy identifier.

b. cRLDistributionPoints

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

c. authorityInfoAccess

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

d. basicConstraints

This extension is required and marked as critical. The cA field

is set to true. As a result of eTSCA does not sign the subordinate CA certificates downwards, the pathLenConstraint field is set to zero (0).

e. keyUsage

This extension is required and marked as critical. This extension is used to mark keyUsage bits as digitalSignature, keyCertSign and cRLSign.

f. nameConstraints

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

g. extKeyUsage

This extension is optional and marked as non-critical. It asserts the value of id-kp-timeStamping (1.3.6.1.5.5.7.3.8).

7.1.2.2 Subscriber Certificate

a. certificatePolicies

This extension is required and marked as non-critical. It asserts the policy identifier.

b. cRLDistributionPoints

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

c. authorityInfoAccess

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

d. basicConstraints

This extension is optional and marked as non-critical. The cA field is set to false.

e. keyUsage

This extension is optional and marked as critical. The bits of both digitalSignature and contentCommitment must be set.

f. extKeyUsage

For the time-stamp certificates issued by eTSCA, this extension is required and marked as critical. It asserts the value of id-kp-timeStamping (1.3.6.1.5.5.7.3.8).

7.1.3 Algorithm Object Identifiers

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

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

(OID: 1.2.840.113549.1.1.11)

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

(OID: 1.2.840.113549.1.1.12)

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

(OID: 1.2.840.113549.1.1.13)

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

(OID: 1.2.840.10045.4.3.2)

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

(OID: 1.2.840.10045.4.3.3)

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

(OID: 1.2.840.10045.4.3.4)

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

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

(OID: 1.2.840.113549.1.1.1)

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

(OID: 1.2.840.10045.2.1)

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

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

(OID: 1.2.840.10045.3.1.7)

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

(OID: 1.3.132.0.34)

7.1.4 Name Forms

The subject and issuer fields of the certificate must use the X.500 distinguished name and the name attribute type shall comply with the official versions of the ITU-T X.509, RFC 3161, RFC 3628 and RFC 5280.

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

7.1.4.1 Issuer Information

According to RFC 5280 “Name Chaining”, the content of Issuer DN for the certificate issuer, shall be identical to the Subject DN of the CA issuing the certificate. Therefore, for the subscriber certificate issued by eTSCA, the Issuer DN has to be identical to the content of the Subject DN of eTSCA.

7.1.4.2 Subject Information–Subscriber Certificates

By issuing the subscriber certificates, eTSCA and RAs have complied with the procedures specified in the CP and/or the CPS, to ensure all the Subject information recorded in these certificates are accurate.

7.1.4.2.1 Subject Alternative Name Extension

The Subject Alternative Name Extensions for time-stamp certificates are as follows:

Certificate Extension	Required/Optional Extension
extension:subjectAltName	Optional

7.1.4.2.2 Subject Distinguished Name Fields

The Subject Distinguished Name Fields of time-stamp certificates issued by eTSCA are described as follows:

Certificate field	Time-stamp certificate
subject:commonName (OID 2.5.4.3)	○
subject:organizationName (OID 2.5.4.10)	○
subject:givenName (OID 2.5.4.42) and subject:surname (OID 2.5.4.4)	×
subject:streetAddress (OID 2.5.4.9)	×
subject:localityName (OID 2.5.4.7)	Δ
subject:stateOrProvinceName (OID 2.5.4.8)	Δ
subject:postalCode(OID 2.5.4.17)	×
subject:countryName(OID 2.5.4.6)	○
subject:organizationUnitName(OID 2.5.4.11)	Δ

Symbols' meaning:

Optional: Δ Required: ○ Prohibited: ×

7.1.4.3 Subject Information–CA Certificates

The CA certificates of eTSCA is validated and issued by eCA based on the procedures specified in the ePKI CP and/or eCA CPS. The Subject

Distinguished Name Fields are as follows:

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

7.1.5 Name Constraints

Name constraints are not used.

7.1.6 Certificate Policy Object Identifier

The ePKI CP object identifier is used for the certificate policy object identifier of the certificates issued by eTSCA.

Please refer to Section 1.2 for the certificate policy object identifier of time-stamp certificates issued by eTSCA.

7.1.7 Usage of Policy Constraints Extension

Certificates issued by eTSCA do not contain policy constraints extension.

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates issued by eTSCA do not contain policy qualifiers.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

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

7.2 CRL Profile

7.2.1 Version Number(s)

eTSCA issues ITU-T X.509 version 2 CRLs.

7.2.2 CRL and CRL Entry Extensions

The extensions of crlExtensions and crlEntryExtensions in the CRLs issued by eTSCA conform to the official versions of the official versions of the ITU-T X.509 and RFC 5280.

7.3 OCSP Profile

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

7.3.1 Version Number(s)

An OCSP request accepted by eTSCA shall contain the following information:

- Version number, and
- Target certificate identifier

The target certificate identifier includes: Hash function algorithm, hash value of certificate issuer name, hash value of certificate issuer public key and certificate serial number of the target certificate.

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

Field	Description
Status	Response status, includes success, request format error, internal error, try again later, request no signature or request no certificate authorization, the following items must be included when status is successful
Version number	v.1 (0x0)
OCSP responding server ID (Responder ID)	The subject DN of OCSP responder
Produced Time	OCSP Response sign time

Field	Description
Target certificate identifier	The contents of this field include the hash algorithm, the hash of the issuer's DN, the hash of the issuer's public key and the serial number of the target certificate.
Certificate Status	Certificate status code (0: valid /1: revoked /2: unknown)
ThisUpdate/NextUpdate	Recommended validity region for this response packet includes: ThisUpdate and NextUpdate
Signature Algorithm	OCSP Response signature algorithm, which can be either sha256WithRSAEncryption or ecdsaWithsha384
Signature	OCSP responder signature
Certificates	OCSP responder certificate

7.3.2 OCSP Extensions

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

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

7.3.3 Regulations for Operation of OCSP

The operation of OCSP in eTSCA includes:

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

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

8. Compliance Audit and Other Assessments

8.1 Frequency or Circumstances of Assessment

eTSCA 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 standard used for the audit is WebTrust Principles and Criteria for Certification Authorities.

8.2 Identity/Qualifications of Assessor

CHT retains a qualified auditor, who is familiar with the operations of eTSCA and is authorized by WebTrust for CA program as a licensed WebTrust practitioner to perform WebTrust Principles and Criteria for Certification Authorities audit standard in R.O.C., to provide impartial and objective audit services. Audit personnel shall be a certified information system auditor or a person who has equivalent qualification; and shall at least possess the experience of conducting a WebTrust for CA seal audit twice at 4 man-days or the experience of conducting a CA information security management audit twice at 8 man-days. eTSCA shall conduct identity identification of auditors during auditing.

8.3 Assessor’s Relationship to Assessed Entity

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

8.4 Topics Covered by Assessment

The assessment shall include the following topics:

(1) Whether eTSCA is operating in accordance with this CPS, including management and technical audit of the physical environment, personnel procedural controls, key control, certificate lifecycle control, and hardware cryptographic module control;
(2) Whether the RA of eTSCA complies with this CPS and related procedures; and
(3) Whether the requirements of this CPS are being implemented and enforced subject to the ePKI CP, and whether the requirements are suitable for the practical operations of eTSCA.

8.5 Actions Taken as a Result of Deficiency

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

(1) Note the discrepancy;
(2) Notify eTSCA about the discrepancy, and if the discrepancy is a critical fault, the PMA shall be notified as well; and
(3) eTSCA shall submit an improvement plan regarding the discrepancy items within 30 days and promptly implement it. The discrepancy items shall also be listed as follow-up audit tracking items. The RA is notified to make improvements to RA-related deficiencies.

8.6 Communications of Results

Except for any audit findings that could result in system attacks and the stipulations in Section 9.3, eTSCA shall make its audit report publicly available. Audit results are displayed with WebTrust for Certification Authorities seal on eTSCA’s homepage. The audit report and

management's assertions may be viewed by clicking on the seal. eTSCA should make its audit report and management's assertions publicly available no later than three months after the end of the audit period. In the event of a delay greater than three months, eTSCA shall provide an explanatory letter signed by the qualified auditor.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

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

9.1.2 Certificate Access Fees

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

9.1.3 Revocation or Status Information Access Fees

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

9.1.4 Fees for Other Services

No charge at the moment.

9.1.5 Refund Policy

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

9.2 Financial Responsibility

9.2.1 Insurance Coverage

eTSCA is owned and operated by CHT. Its financial responsibilities

are the responsibilities of CHT. If the competent authority has insurance regulations for the certification authority in the future, eTSCA will cooperate accordingly.

9.2.2 Other Assets

eTSCA finances are a part of the overall finances of CHT. CHT is a publicly listed company and a Republic of China company listed on the New York Stock Exchange. 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. eTSCA can provide self-insured asset prices based on CHT's financial reports. CHT's finances are sound and its ratio of current assets to current liabilities is no lower than 1.0 which meets the requirement of the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates.

9.2.3 Insurance or Warranty Coverage for End-Entities

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

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

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

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

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

9.3.2 Information Not Within the Scope of Confidential Information

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

9.3.3 Responsibility to Protect Confidential Information

eTSCA shall handle subscriber application information in accordance with the Electronic Signatures Act, WebTrust Principles and Criteria for Certification Authorities audit criteria and Personal Information Protection Act.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

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

9.4.2 Information Treated as Private

Private information includes:

(i) The personal information listed on any certificate application is deemed private information and may only be disclosed with the consent of the subscriber or in accordance with related law and regulation,

(ii) Information (or subscriber information) that cannot be obtained through certificates, CRLs or certificate catalog service,

(iii) Identifiable information of personnel in eTSCA, such as names together with palmprint or fingerprint biometrics, and

(iv) Personal information on confidentiality agreements or contracts.

eTSCA and its RA implement security control measures to prevent personally identifiable information from unauthorized disclosure, leakage or damage.

9.4.3 Information Not Deemed Private

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

Issued certificates, revoked certificates and CRLs published in the eTSCA repository are not deemed private information.

9.4.4 Responsibility to Protect Private Information

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

9.4.5 Notice and Consent to Use Private Information

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

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

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

9.4.7 Other Information Disclosure Circumstances

Subscriber personal information obtained during eTSCA operations is handled in accordance with related laws and regulations and may not be disclosed externally to ensure the personal privacy of subscribers. This shall not apply if stipulated otherwise under the law.

9.5 Intellectual Property Rights

The following is the intellectual property of eTSCA:

(1) Key pairs and split keys of eTSCA and RA;

(2) Related documents or system development for certificate management of eTSCA;

(3) Certificates and CRLs issued by eTSCA; and

(4) This CPS.

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

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

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

(1) Comply with the ePKI CP and this CPS;

(2) Perform certificate application identification and authentication;

(3) Provide certificate issuance and publication services;

(4) Revoke certificates;

(5) Issue and publish CRLs;

(6) Issue and provide OCSP response messages;

(7) Securely generate eTSCA and RA private keys;

(8) Secure management of private keys;

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

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

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

9.6.2 RA Representations and Warranties

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

RAs shall represent and warrant that:

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

(2) All information provided to eTSCA does not contain any false or misleading information,

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

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

(5) RA private keys are securely managed.

9.6.3 Subscriber Representations and Warranties

For the express benefit of eTSCA and the Certificate Beneficiaries, the Applicant shall warrant that, prior to the issuance of a certificate, eTSCA will obtain the Applicant's acknowledgement of the Terms of Use.

Applicant shall represent and warrant to eTSCA that it will:

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

(2) Provide accurate and complete information to eTSCA and RA,

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

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

(5) Promptly notify eTSCA, cease using a certificate, and request revocation of the certificate, if
   (i) any information in the certificate is or becomes incorrect or inaccurate, or
   (ii) there is any actual or suspected misuse or compromise of the Subscriber's private key associated with the public key included in the certificate (and cease using the private key),
(6) Use the certificate only for legal and authorized purposes, consistent with the ePKI CP, this CPS and Subscriber Agreement, and
(7) Promptly cease using the certificate and related private key after the certificate's expiration.

9.6.4 Relying Party Representations and Warranties

Each relying party represents and warrants that it:

(1) Complied with the provisions of this CPS when using a certificate or inquiring the eTSCA repository;
(2) Shall check the certificate assurance level during use of certificates;
(3) Checked the keyUsage field listed in the certificate during use of certificates;
(4) Validated a certificate (published by eTSCA) by using a CRL or OCSP published by eTSCA in accordance with the proper certificate path validation procedure;
(5) Shall carefully select secure computer environments and reliable application systems. If the rights of subscribers and relying parties are infringed due to the use of a untrusted computer environment or application system, relying parties shall bear the responsibility solely;

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

(7) Understood and agreed to eTSCA legal liability clauses and will use the certificate in accordance with Section 1.4.1 when accepting the certificate.

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

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

Except to the extent prohibited by law or as otherwise provided herein, eTSCA 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 eTSCA has issued and managed the certificate in accordance with this CPS, eTSCA shall not be liable to the subscribers or relying parties for any losses suffered as a result of use or reliance on such certificate. Otherwise, eTSCA 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 eTSCA

If subscribers or relying parties suffer damages due to the intentional or unintentional failure of eTSCA to follow the ePKI CP, this CPS, relevant laws and regulations or the provisions of contracts signed between eTSCA

and subscribers/relying parties when processing subscriber certificate-related work, CHT shall be held liable. Subscribers may claim compensation for damages based on the related provisions of the contract set down between eTSCA and subscribers. Relying parties shall request compensation in accordance with relevant laws and regulations. The total compensation limit of eTSCA for each subscriber or relying party is shown in the following Table. If subscribers or relying party has signed a contract with CHT, the certificate scope of use and transaction compensation limit shall be determined separately.

Certificate Assurance Level	Compensation Limit (NTD)
Level 3	3,000,000

This compensation limits is the maximum compensation amount. The actual compensation amount is based on the actual damages incurred by the subscribers or relying parties.

9.9.2 Indemnification by RA

The RA is set up by CHT. If subscribers or relying parties suffer damages due to the RA intentional or unintentional failure to follow this CPS, related laws and regulations or the provisions of contracts signed between the RA and subscribers/relying parties when processing subscriber certification registrations, CHT shall be held liable. Compensation limits for the RA are detailed in Section 9.9.1.

9.10 Term and Termination

9.10.1 Term

This CPS and any amendments are effective when approved by the Electronic Signatures Act competent authority and published to the eTSCA website and repository. This CPS remains effective 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

CHT will communicate the conditions and effect of this CPS's termination via the eTSCA website and repository. The communication will specify which provisions survive termination. At a minimum, responsibilities related to protecting confidential information will survive termination.

9.11 Individual Notices and Communications with Participants

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

9.12 Amendments

9.12.1 Procedure for Amendment

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

9.12.2 Notification Mechanism and Period

eTSCA will post appropriate notice on its websites of any major or significant changes to this CPS as well as any appropriate period by when

the revised CPS becomes effective. If subscribers or relying parties have any comment on the change items, they can submit the comment within the comment period. Reassess to the changes and response may or may not be made by eTSCA according to these comments.

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

9.12.3 Circumstances under which OID Must Be Changed

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

9.13 Dispute Resolution Provisions

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

9.14 Governing Law

For disputes involving eTSCA issued certificates, the applicable 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 this CPS.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

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

and supersedes all prior verbal or written representations between the parties on the same matters.

9.16.2 Assignment

The participants, including eTSCA, RAs, subscribers, and relying parties, may not assign or delegate their rights or obligations under this CPS to other parties in any form without a prior written notice to eTSCA.

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.

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

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

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

9.16.5 Force Majeure

eTSCA is not liable for any delay or failure to perform an obligation under this CPS to the extent that the delay or failure is caused by a force majeure or other circumstances not attributable to eTSCA, including but not limited to natural disasters, wars, terrorism or failures of the Internet. eTSCA has set clear limitations for certificate usage and is not bear any legal responsibility for damages caused by exceeding these usage limitations.

9.17 Other Provisions

No stipulation.

Appendix 1: Acronyms and Definitions

Acronyms	Full Name	Definition
CA	Certification Authority	See Appendix 2.
CMMI	Capability Maturity Model Integration	See Appendix 2.
CP	Certificate Policy	See Appendix 2.
CP OID	CP Object Identifier	
CPS	Certification Practice Statement	See Appendix 2.
CDN	Content Delivery Network	See Appendix 2.
CRL	Certificate Revocation List	See Appendix 2.
DN	Distinguished Name	
eCA	ePKI Root Certification Authority	See Appendix 2.
EE	End Entities	See Appendix 2.
ePKI	Chunghwa Telecom ecommerce Public Key Infrastructure	See Appendix 2.
FIPS	(US Government) Federal Information Processing Standard	See Appendix 2.
IETF	Internet Engineering Task Force	See Appendix 2.
NIST	(US Government) National Institute of Standards and Technology	See Appendix 2.
OCSP	Online Certificate Status Protocol	See Appendix 2.
OID	Object Identifier	See Appendix 2.
PIN	Personal Identification Number	
PKCS	Public-Key Cryptography	See Appendix 2.

Acronyms	Full Name	Definition
	Standard	
PKI	Public Key Infrastructure	See Appendix 2.
QGIS	Qualified Government Information Source	See Appendix 2.
QTIS	Qualified Government Tax Information Source	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.
TSA	Time-stamping Authority	See Appendix 2.
TST	Time-stamp Token	See Appendix 2.
TSU	Time-stamping Unit	See Appendix 2.
UPS	Uninterrupted Power System	See Appendix 2.
UTC	Coordinated Universal Time	See Appendix 2.

Appendix 2: Glossary

Access	Use the information processing capabilities of system resources
Access Control	Authorization procedure for access to information system resources given to subscribers, programs, procedures and other systems.
Activation Data	Private data, other than keys, that are required to access cryptographic modules and that need to be protected (i.e., unlock private keys for signing or decryption events).
Applicant	Subscribers who request certificates from a CA and have not yet completed the certificate procedure.
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 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.
Backup	Information or program copying that can be used for recovery purposes when needed.
Baseline Requirements	"The Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" issued by CA/Browser Forum, and all the amendments.
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 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.
Certificate Policy (CP)	(1) Refers to a named set of rules that indicates the applicability to a certain community or class of application with common security requirements [Article 2-3, Chapter 1, Regulations on Required Information for Certification Practice Statements] (2) Certificate policy refers to the dedicated profile administration policy established for the electronic transactions performed through certificate administration. Certificate policy covers a variety of issues including the formation, generation, delivery, auditing, administration and restoration after compromise. Certificate policy indirectly controls the use and operation of certificate security systems to protect the transactions performed by the communication systems. The security services required for certain application are provided through control of the certificate extension methods, certificate policy and related technology.
Certification Practice Statement	(1) External notification by the certificate authority used to describe the practice

(CPS)	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)	(1) The certificate revocation list digitally signed by the certification authority provided for relying party use. [Article 2-8, Chapter 1, Regulations on Required Information for Certification Practice Statements] (2) List maintained by the certificate authority. The expiry dates of the above revoked certificates issued by the certification authority are recorded on the list.
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.
Cryptographic Module	A set of hardware, software, firmware or combination of the above used to run cryptologic or programs (including crypto algorithms) and included within the cryptographic boundaries of the module.
Data Integrity	Information that has been subjected to unauthorized access or accidental modification, damage or loss.
Digital Signature	An electronic signature generated by use of mathematic algorithm or other means to create a certain length of digital data encrypted by the

	signatory's private key and capable of being verified by the public key. [Article 2-3, Electronic Signatures Act]
Domain Name	A node label assigned by the domain name system. Converts the IP address into a text name that is easily remembered by humans.
Duration	A certificate field made up of two subfields "start time of the validity period" (notBefore) and "end time of the validity period" (notAfter).
E-commerce	Provision of goods for sale and other services through the use of network technology (specifically the Internet).
End Entity	The PKI includes the following two types of entities: (1) Those responsible for the safeguarding and use of certificate public keys. (2) Third parties who trust the certificates issued by the PKI (not holders of private keys and not a certificate authority). The end entities are subscribers and relying parties including personnel, organizations, accounts, devices and sites.
Chunghwa Telecom ecommerce Public Key Infrastructure (ePKI)	A hierarchical PKI established by CHT in compliance with ITU-T X.509 to promote electronic services. It can be used within various applications in e-commerce and e-government.
Certificate Policy Management Authority (PMA)	An organization which was established for electronic certificate management matters, such as (i) discussion and review of the CP and the electronic certificate framework of the PKI owned by CHT and (ii) review of interoperation requests submitted by subordinate CAs and cross-certified CAs and that of CPS.
ePKI Root CA (eCA)	The Root CA and top-level CA in ePKI, and its public key is the trust anchor of ePKI.
Federal Information Processing	Except for military organizations in the US Federal Government System, information processing standard for all government organizations and

Standard (FIPS)	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.
Identification	A statement of who the user is. [A Guide to Understanding Identification and Authentication in Trusted Systems] A way that can be used to describe or claim the identity of an individual or entity, e.g., user account, name or e-mail.
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.
Issuing CA	For a particular certificate, the CA that issues the certificate is the issuing CA.
Key Escrow	Storage of related information using the subscriber's private key and according to the terms of the mandatory subscriber escrow agreement (or similar contract). The terms of this escrow agreement requires that one or more than one agencies have possession of the subscriber key provided it is beneficial to the subscriber, employer or another party in accordance with the provisions of the agreement.
Key Pair	Two mathematically related keys having the

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

	repository to process the certificate status request.
Private Key	(1) The key in the signature key pair used to generate digital signatures. (2) The key in the encryption key pair used to decrypt secret information. This key must be kept secret under these two circumstances.
Public Key	(1) The key in the signature key pair used to verify the validity of the digital signature. (2) The key in the encryption key pair used for encrypting secret information. These keys must be made public (usually in a digital certificate form) under these two circumstances.
Public-Key Cryptography Standard (PKCS)	In order to promote the use of public key technology, the RSA laboratory under the RSA Information Security Company has developed a series of public key cryptography standards that are widely used by the industry.
Public Key Infrastructure (PKI)	A set of law, policy, standards, personnel, equipment, facilities, technology, processes, audits and services developed on a broad scale and management of asymmetric cryptography and public key certificates.
Qualified Auditor	Accountant firms, entities, or individuals that satisfy the auditor qualification requirements specified in Section 8.2 of the Baseline Requirements, as well as independent from the audited parties.
Qualified Government Information Source (QGIS)	A regularly-updated and current, publicly available, database designed for the purpose of accurately providing the information for which it is consulted, and which is generally recognized as a dependable source of such information provided that it is maintained by a Government Entity, such as Ministry of Economic Affairs Bussiness & Factory Registration Database, the reporting of data is required by law, and false or misleading

	reporting is punishable with criminal or civil penalties. Nothing in the EV SSL Certificate Guidelines shall prohibit the use of third-party vendors to obtain the information from the Government Entity provided that the third party obtains the information directly from the Government Entity.
Qualified Government Tax Information Source (QTIS)	A Qualified Governmental Information Source that specifically contains tax information relating to Private Organizations, Business Entities, or Individuals. Such as Fiscal Information Agency, Ministry of Finance in Taiwan and IFS in USA.
Registration Authority (RA)	(1) Responsible for checking the identity and other attributes of the certificate applicant but does not issue or administer certificates. The nature and scope of obligations borne by the registration authority are set down in the applicable certificate policy or agreement. (2) An entity responsible for the identity identification and authentication of the certificate subject which does not issue certificates.
Re-key (a certificate)	Changing the key values used in the cryptographic system application program. It is commonly achieved by issuing a new certificate for the new public key.
Relying Party	(1) Recipient of a certificate who acts in reliance of that certificate or a digital signature to verify the public key listed in the certificate, or the counterpart to identify (or its attributes) of the subject named in a trusted certificate and public key listed in the certificate. [Article 2-6, Chapter 1, 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 system for storing and retrieving certificates or other information relevant to certificates. [Article 2-7, Chapter 1, Regulations on Required Information for Certificate Practice Statements] (2) A database that contains information and data relating to certificates as specified in the CP/CPS.
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 Layer	Protocol issued by Netscape through introduction of their web browser which can encrypt network communication in the transport layer and ensure the integrity of transmitted information and perform identity authentication on the server and client. The advantage of the secure socket layer protocol is it is independent and separate from the application layer protocol. High level application layer protocol (such as: HTTP, FTP and Telnet) may be established on top of SSL. The SSL protocol completes encryption algorithm, communication secret key agreement and server authentication work before the application layer protocol communication. This protocol is a successor to the Transport Layer Security (TLS) protocol.
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).
Subordinate CA	In a hierarchical PKI, a CA whose certificate

	signature key is certified by another CA, and whose activities are constrained by that other CA.
Subscriber	An entity that (1) is the subject named or identified in a certificate issued to that entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual, an organization, an application or network device.
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	A digitally signed assertion by a trusted authority that a specific digital object existed at a certain time.
Time-stamping Authority (TSA)	Authority which issues time-stamp tokens.
Time-stamp Token (TST)	Data object that binds a representation of a datum to a particular time, thus establishing evidence that the datum existed before that time.
Time-stamping Unit (TSU)	Set of hardware and software which is managed as a unit and has a single time-stamp token signing key active at a time.
Transport Layer	TLS 1.0 was first defined in RFC 2246 by the IETF

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.