Public Certification Authority Certification Practice Statement of Chunghwa Telecom

(PublicCA CPS)

Version 2.06

Chunghwa Telecom Co., Ltd.

May 28, 2021

Contents

CPS Version Control

Version	Date	Revision Summary
1.5	August 21, 2015	RFC 3647 Version CPS Released.
1.6	February 4, 2016	(1) Add IV CP OID. (2) Amend Description of Appropriate Certificate Uses of DV、OV、IV SSL Certificate. (3) Check of CAA DNS Record (4) Validity of OV/DV SSLCertificates should not exceed 39months. (5) Minor change of Chapter 8. (6) Add some glossaries in Appendix 2.
1.7 (20170714)	July 14, 2017	(1) Amendment of Section 3.2.5 about Domain Name Validation, Appendix 2. (2) Minor Change such as Summary, Section 1.3.2, Section 1.4.1, Section 2.2, Section 2.3, Section 4.2, Section 4.9, Section 6.3.2.2, Section 7.1, Section 9.1.3, Sction 9.12.1.
1.7 (20171023)	October 23, 2017	Minor Change such as Section 3.1,3、Section 3.1.5、Section 5.1、Sction 5.2、Section 6.2、Section 6.3、Chapter 7 and so on.
1.7 (20180126)	January 26, 2018	Minor change such as Section 6.2.2, section 4.2.2 & Sectioon 9.16.3.
1.7 (20180214)	February 14, 2018	Add Version Control.
1.7	March 21, 2018	Add Competent Authority Approval No.: Chin-Shang-Tzu No. 10702216460 in Abstract.
1.8	May 28, 2018	(1) Review CA/Browser Forum Baseline Requirements and operation staus to amend Section 3.2.5 about method of validation of Domain Names. (2) Amend Section 2.2 and Section 4.2.1 about CAA Issuer Domain Names & CAA. (3) Amend Section 7.1.2 about supporting of Certificate Transparency. (4) Based on the audit criteria naming information announced in CPA Canada's website (http://www.webtrust.org) to amend Abstract, Section 8.1, Section 8.2, Section 9.3.3 and section 9.4.4. (5) Add glossary such as WHOIS.

Version	Date	Revision Summary
1.9	April 30, 2019	(1) Section title revision to meet RFC 3647. (2) Remove domain validation method “Phone Contact with Domain Contact” to comply with CABF Ballot SC14. (3) Add authenticator assurance level definitions to Section 1.4.1. (4) Amendments are made in Sections 1.5.2, 4.9.1, 4.9.3, 4.9.5 and 9.12 in compliant with the Baseline Requirements. (5) Revision of Sections 1.1, 1.2, 1.3.3, 1.4.1, 2.2, 2.3, 3.1.2, 3.2.5, 3.2.6, 3.2.7, 4.5, 4.7, 4.9, 4.10, 4.11, 4.12, 5.2, 5.3.3, 5.3.5, 5.6, 5.8, 6.1.5, 6.1.7, 6.3.2, 6.6.2, 7.1, 7.2, 7.3, 8.4, 8.5, 8.6, 9.4.4, 9.6, 9.7, 9.8, 9.10.2 and 9.16.3.
2.0	April 22, 2020	(1) Add Sections 3.2.5.6 and 3.2.5.7 about domain validation methods to comply with CABF Ballot SC13. (2) Amendments are made in Section 4.9.10 to comply with CABF Ballot SC23. (3) Amendments are made in Section 7.1.4.2 to comply with CABF Ballot SC16. (4) Amendments are made in Section 7.1.2 in accordance with the Baseline Requirements and the operation status of CA. (5) Revision of Sections 1.5.3, 4.5.1, 4.8.1, 5.3.7, 5.7.1, 6.2.5, 6.2.6, 6.2.10, 7.3.1, 9.2.1 and 9.6.4.
2.05	April 22, 2021	(1) Amendments is made in Section 5.5.2 in accordance with the BR and the operation status of CA. (2) Revision of Sections 1.1.1, 1.3.5, 1.4.1, 1.4.2, 2.2, 2.3, 2.4, 3.1.1, 3.2.1, 3.2.2, 3.2.3, 3.2.5, 3.2.5.4, 3.2.5.6, 3.3.1, 4.2.2, 4.2.3, 4.9.8, 4.9.10, 5.7.3, 6.1.1.1, 6.1.2, 6.1.3, 6.1.6, 6.2.1, 6.3.2.1, 6.3.2.2, 7.1.2.1, 7.1.2.2, 7.1.4.2, 7.1.6, 8.1, 8.4, 9.4.2, 9.10.1, 9.10.2, 9.10.3 and 9.16.1.
2.06	May 28, 2021	Revision of Sections 1.1.1, 1.2, 1.4.1, 3.1.2, 3.1.3, 3.1.5, 3.2.1, 3.2.2, 3.2.3, 3.2.4, 3.2.5.4, 3.2.5.7, 4.3.1, 4.9.1, 4.9.12, 6.2.1, 6.7 and 7.1.4.2.

1. Introduction

1.1 Overview

According to the ePKI CP, ePKI Root Certification Authority (eCA) is a top-level CA and a trust anchor of ePKI. eCA must maintain a high level of credibility that relying parties can directly trust its certificates. Public Certification Authority (PublicCA) is a level-one Subordinate CA of eCA that obtains certificates from eCA and is responsible for the issuance and management of certificates for natural person, organization, equipment, and application software.

1.1.1 Certification Practice Statement

This Certification Practice Statement (CPS) describes the practices used to comply with the Electronic Signatures Act and its sub-law "Regulations on Required Information for Certification Practice Statements" of R.O.C., ePKI CP and the official versions of related international standards such as the Internet Engineering Task Force (IETF) request for comments (RFC) 3647, RFC 5280, RFC 6960, RFC 6962, RFC 5019, RFC 8659, ITU-T X.509, and CA/Browser Forum (http://www.cabforum.org) Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (Baseline Requirements), and Network and Certificate System Security Requirements.

1.1.2 CPS Applicability

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

1.2 Document Name and Identification

This document is Public Certification Authority Certification Practice Statement of Chunghwa Telecom and was approved for publication on May 28, 2021. This CPS is version 2.06. The current version of this CPS can be obtained at the website: https://publicca.hinet.net.

The identity assurance level and the CP object identifiers (OIDs) are listed in the Table below:

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

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

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

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

The SSL server software certificates issued by PublicCA conform to the requirements defined in the Baseline Requirements and pass the

external audit of AICPA/CPA WebTrust Principles and Criteria for Certification Authorities – SSL Baseline Requirements Audit Criteria Version 1.1 in November 2014 and shall be allowed to use for organization validation (OV) SSL CP OID ({joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate- policies(1) baseline-requirements(2) organization-validated(2)} (2.23.140.1.2.2)) and domain validation (DV) SSL CP OID ({joint-iso-itu-t(2) international-organizations(23) ca-browser- forum(140) certificate-policies(1) baseline-requirements(2) domain- validated(1)} (2.23.140.1.2.1)) and individual validation (IV) SSL CP OID ({joint-iso-itu-t(2) international-organizations(23) ca-browser- forum(140) certificate-policies(1) baseline-requirements(2) individual- validated(3)} (2.23.140.1.2.3)) of the CA/Browser Forum.

If there is any inconsistency between this CPS and the official version of the Baseline Requirements, then the Baseline Requirements takes precedence.

The CA certificate and PDF signing certificates (assurance level 2 or 3 certificates issued to organizations or individuals) of PublicCA may use the OID 1.3.6.1.4.1.23459.100.0.9, which is approved by the Adobe Approved Trust List (AATL).

1.3 PKI Participants

The key members of PublicCA include:

(1) PublicCA

(2) RAs

(3) Subscribers

(4) Relying Parties

1.3.1 Certification Authorities

PublicCA, established and operated by Chunghwa Telecom Co., Ltd. (CHT), operates and issues natural person, organization, equipment and application software certificates in accordance with the ePKI CP.

1.3.2 Registration Authorities

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

PublicCA RA is divided into two major categories: general RA and dedicated RA. General RA is established and operated by CHT while dedicated RA are set up and operated independently by customers that is recognized by CHT or have signed contracts with CHT.

PublicCA does not permit any delegated third party to be the SSL certificate registration authority to verify the ownership or control of domain names or IP addresses. The delegated third parties mean any natural person or legal entity that is not PublicCA but is delegated to assist the certificate management procedure and is not covered by the external audit of PublicCA.

1.3.3 Subscribers

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

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

Generation of subscriber key pairs shall comply with 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

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

(1) Verify the integrity of a digitally signed electronic document.
(2) Identify the creator of a digitally signed electronic document.
(3) Establish a secure communication channel with the subscriber.

1.3.5 Other Participants

Other authorities include time stamp authority (TSA) and card management center (responsible for the production and management of tokens).

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

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

Equipment and application software certificates can be used for the transport layer security (TLS) protocols and the dedicated applications servers.

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

Assurance Level	Applicable Type of Certificates	Authtication Method	Applicable Scope
Level 1	Natural person, organization, equipment or application software	Use e-mail methods to verify that the applicant can operate the e-mail account.	Use e-mail notification to verify that the applicant can control the e-mail account. Suitable for use in network environments in which the risk of malicious activity is considered to be low or a higher assurance level cannot be provided. When used for digital signatures, it can identify that the subscriber originates from a certain e-mail account or guarantee the integrity of the signed document. When used for encryption, the relying party can use the subscriber's certificate public key to encrypt and transmit the message or the symmetric key to guarantee its confidentiality but it is not suitable for on-line transactions that require

Assurance Level	Applicable Type of Certificates	Authtication Method	Applicable Scope
			certification. For example, information encryption and signatures required for e-mails.
Level 2	Natural person, organization, equipment or application software	Applicant does not need to apply in person at counter but must provide legal and proper documentation proving personal or organization identity. After the registration authority officers (RAO) cross checks the information provided by the applicant or the system automatically compares with a reliable database to make sure the applicant information is correct.	Suitable for use with information which may be tampered with but the network environment has no malicious tampering (data interception is possible but likelihood is not high). Not suitable for the signing of important documents (life essential and high value transaction documents). For example, information encryption and identity authentication for small value e-commerce transactions.
Level 3	Natural person, organization, equipment or application software	Applicant needs to apply in person at counter. The RAO checks the accuracy of application information or uses digital signature of applicant's private key corresponding to assurance level 3 certificate issued by government public key infrastructure or ePKI to submit the application. The system automatically compares the applicant's information to verify its accuracy.	Suitable for use in network environments in which there are malicious users, which intercept or tamper with information, and risks, which are greater than the environment of level 2. Transmitted information may include on-line cash or property transactions on keys. Suitable for e-commerce application, Internet tax filing, e-government, e-mail application, TLS encryption channel or identity identifying service.

Regarding the SSL certificates issued by PublicCA, assurance level, authentication method, scope of application, and reducible risks shall comply with the aforesaid table, and their descriptions are as follows:

Assurance Level and Cert. Type	Authentication Method	Scope of Usage	Risk Description of Reducible Risks
Level 1 DV SSL certificate	Follow the Baseline Requirements and assurance level 1 regulations to authenticate remote domain names and webpage services.	Provides communication channel encryption (communication channel encryption refers to 'facilitate encryption key exchange to achieve information transmission encryption between the subscriber's browser and website'). Suitable for use with protected network communications.	Provide an encryption protection to the non-monetary or non-property transactions, and/or transactions unlikely compromised by fraud or malicious access.
Level 3 OV SSL certificate	Follow the Baseline Requirements and assurance level 3 regulations to authenticate that the applicant can control which group is in possession of the remote domain name, webpage services and which organization owns the domain name.	Provides communication channel encryption and must authenticate which organization owns the domain name. Suitable for use with protected network communications.	Provide a robust authentication and high-level security to the important monetary or property transactions, and/or environment where the probability of fraud risk or malicious access involving personal information is moderate.
Level 3 IV SSL certificate	Follow the Baseline Requirements and assurance level 3 regulations to authenticate that the applicant can control which group is in possession of the remote domain name, webpage services and which natural person owns the domain name.	Provides communication channel encryption and must authenticate which natural person owns the domain name. Suitable for use with protected network communications.	Provide a robust authentication and high-level security to the important monetary or property transactions, and/or environment where the probability of fraud risk or malicious access involving personal information is moderate.

If PublicCA can confirm that the subscriber private key is stored in a

secure cryptographic hardware device (e.g., eID smart card), the authenticator assurance levels defined in the ePKI CP can be included in the device. The authenticator assurance levels are described as follows:

Authenticator Assurance Level	Descriptions
Level 1	Providing only partial assurance as to whether or not the token controller truly binded the Subscribers' accounts. Its successful single-factor or multi-factor authentication via the use of any available verification technique shall, via a secure authentication protocol, be able to confirm that the subscriber truly have possession of and control over that token. (1) Permitted token type: can use any one of the following types. ■ Memorable secret code, such as: password or personal identification number; ■ Single-factor encryption software; ■ Single-factor encryption equipment; ■ Multi-factor encryption software; ■ Multi-factor encryption equipment. (2) Requirements of the token and validator: ■ The encryption token shall use the approved encryption technology. The software token can also try to detect the possible of malicious attack to the terminal equipment (such as: installed with malicious software). If it is found, the certification in question shall be terminated. ■ The token owner and validator shall communicate with each other via authorized and securely encrypted channel to avoid man-in-the-middle attack.
Level 2	Providing reliable assurance as to whether or not the token controller truly binded the Subscribers' accounts. Its authentication carried out under the secure environment of authentication protocol via the use of two authentication factors shall include the approved encryption technology. (1) Permitted token type: The verify operation shall be performed via multi-factor authentication or two-factor authentication. ■ If multi-factor authentication is taken, the available types of token include: ➢ Multi-factor encryption software; ➢ Multi-factor encryption equipment. ■ If the authentication mechanism is only two-factor, it shall

Authenticator Assurance Level	Descriptions
	include a memorable secret code token and any one-time token described below: ➢ Single-factor encryption software; ➢ Single-factor encryption equipment. (2) Requirements of the token and validator: ■ Encryption token shall use the approved encryption technology. The token for government procurement shall pass FIPS 140 level 1 certification. The software token can also try to detect the possible of malicious attack to the terminal equipment (such as: installed with malicious software). If it is found, the certification in question shall be terminated. In addition, at least one type of token with replay attacks prevention capacity, such as dynamic passwords, shall be used. ■ The token owner and validator shall communicate with each other via authorized and securely encrypted channel to avoid man-in-the-middle attack. ■ If equipment such as mobile device is used in the verification process, the equipment's original unlocking function (such as: fingerprint recognition or personal identification number verification) shall not be regarded as a verification factor.
Level 3	Providing highly reliable assurance as to whether or not the token controller truly binded the Subscribers' accounts. It verifies ownership of the subscriber's key via encryption protocol. The verification operation requires hardware password token and token capable of blocking from hacked validator (can also simultaneously use equipment with the aforesaid functions) and shall be carried out under the secure environment of authentication protocol via the use of two authentication factors, which shall include the approved encryption technology. (1) Permitted token type: can use a combination of any one of the following tokens. ■ Multi-factor encryption equipment; ■ A combination of single-factor encryption equipment and memorable secret code. (2) Requirements of the token and validator: ■ The token owner and validator shall communicate with each other via authorized and securely encrypted channel to avoid man-in-the-middle attack. All encryption equipment token shall be equipped with validator capable of anti-hacking and replay attacks prevention.

Authenticator Assurance Level	Descriptions
	■ The token shall be cryptographic module which passed FIPS 140 level 2 (or up) or is in compliance with Global Platform Trusted Execution Environment. ■ If equipment such as mobile device is used in the verification process, the equipment's original unlocking function (such as: fingerprint recognition or personal identification number verification) shall not be regarded as a verification factor.

Below are the OIDs for each authenticator assurance level defined in the ePKI CP:

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

Subscribers and relying parties must carefully read and comply with this CPS before using and trusting the certificate service provided by PublicCA, and pay attention to the update of this CPS.

Subscribers shall choose suitable assurance level and type of certificates based on actual requirements and applications. Different certificates are applicable for different cases. When using a private key, subscribers shall choose a secure and trusted computer environment and application systems to prevent theft of the private key which could harm one's interests.

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

Relying parties shall appropriately use the individual keys in

compliance with the keyUsage field included in the certificate stipulated in Section 6.1.7 and correctly process the certificate attribute information listed in the certificate extension marked as critical.

1.4.2 Prohibited Certificate Uses

Certificates issued under this CPS are prohibited from being 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) Man-in-the-middle TLS traffic interception.

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 Public 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://publicca.hinet.net.

1.5.2.2 Certificate Problem Report

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

PublicCA 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 PublicCA for making this decision.

1.5.3 Person Determining CPS Suitability for the Policy

PublicCA shall first check whether this CPS conforms to the ePKI CP regulations and then submit the CPS to the Chunghwa Telecom Certificate Policy Management Authority (PMA) for review and approval. After approval, PublicCA is able to officially reference 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).

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

1.5.4 CPS Approval Procedures

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

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 document, the attached documents shall take precedence in the event of discrepancy between the attached documents and the original CPS.

1.6 Definitions and Acronyms

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

2. Publication and Repository Responsibilities

2.1 Repositories

The PublicCA repository is responsible for the publication and storage of certificates and certificate revocation lists (CRLs) issued by PublicCA and this CPS and provides inquiry services to subscribers and relying parties. The repository provides 24-hour round-the-clock service. The website of the PublicCA repository is at http://publicca.hinet.net. The repository will resume normal operation within two working days if unable to operate normally for some reason.

2.2 Publication of Certification Information

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

(1) This CPS and the ePKI CP.

(2) CRLs and Online Certificate Status Protocol (OCSP) service.

(3) PublicCA certificates (until the expiry of all certificates issued with private key corresponding to that certificate's public key).

(4) Issued certificates.

(5) Privacy protection policy.

(6) Related latest news regarding PublicCA.

(7) The latest external audit report (as specified in Section 8.6).

(8) The URLs of the test websites (valid, expired, revoked) which install SSL certificates issued by PublicCA for application software suppliers to test.

(9) CAA (Certification Authority Authorization) issuer domain names (as specified in Section 4.2.1) include 'pki.hinet.net', 'publicca.hinet.net', 'eca.hinet.net' and 'epki.com.tw'.

2.3 Time or Frequency of Publication

(1) This CPS is reviewed and updated annually, and a dated changelog is state in the “Document History” section even if no other changes are make to this document. New or modified version of this CPS is published in the repository as soon as possible upon receiving the approval letter from the competent authority,

(2) New or modified version of the ePKI CP complied with by PublicCA is published in the repository as soon as possible upon the approval of the PMA,

(3) PublicCA issues CRLs at least twice a day and publishes CRLs in the repository, and

(4) PublicCA certificates are published in the repository within seven calendar days after accepting issuance by an upper level CA.

2.4 Access Controls on Repositories

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

The information published by PublicCA under Section 2.2 is primarily provided for inquiring by subscribers and relying parties. PublicCA implements access control where it provides read-only access to prevent anyone from unauthorized writing operation, which would put repository security in risk.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

PublicCA certificates are issued with subject Distinguished Names (DNs) which meet the requirements of X.500 naming.

3.1.2 Need for Names to be Meaningful

The naming of the certificate subject should comply with the law of the country under the jurisdiction of the applicant.

PublicCA and its RA may abridge the prefix or suffix of the organization name, e.g., change the official name “Company Name Incorporated” to its abbreviated version “Company Name, Inc.”, and the abbreviation must be made on the basis that the certificate subject is easily identifiable in the jurisdiction in which it is established or registered. If the organization name is longer than 64 characters, PublicCA and its RA may abbreviate the organization name or delete the unimportant text in the organization name.

The Baseline Requirements shall be followed for the certificate subject name and subject alternate name in the SSL server software certificate. Internal names or reserved IP addresses shall not be used.

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

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

The DN for individual validation (IV) SSL server software certificate shall include the individual identity information of surname and given

name fields that is verified in Section 3.2.3.

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

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

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

3.1.3 Anonymity or Psuedonymity of Subscribers

DV SSL certificate can be regarded as an anonymous certificate (in which the identity of the individual or organization is not available from the certificate itself). PublicCA does not issue end entity pseudonymous certificates.

For requests of internationalized domain names (IDNs) applying for SSL certificates, its decoded hostname will undergo additional review to mitigate the risk for phishing and other fraudulent usage as stated in Section 4.2.1, e.g., homographic spoofing of IDNs; and the decoded hostname may be compared with previously rejected certificate requests or revoked certificates.

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

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

C=TW,

O=Chunghwa Telecom Co., Ltd.,

OU=Public Certification Authority

From the second generation, PublicCA's X.500 distinguished name for CA certificates are:

C=TW,

O=Chunghwa Telecom Co., Ltd.,

OU=Public Certification Authority - G2

In favor of facilitating international interoperability, the Baseline Requirements version 1.4.8 is referred. From the third generation, PublicCA's X.500 distinguished name for CA certificates uses the following formats:

C=TW,

O=Chunghwa Telecom Co., Ltd.,

CN=Public Certification Authority - Gn, where n = 3, 4…….

PublicCA applies various naming attributes defined in X.520 standard for assembly to ensure the uniqueness of each subject name in a certificate and the compliance of the X.500 naming space. The uniqueness of subject name in subscriber certificates is enforced by (but not limit to) assembling the following naming attributes defined in the X.520 standard:

- 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

The organizationName field must not be present in certificate subject for SSL certificates issued on or after Auguest 1, 2021.

3.1.6 Recognition, Authentication, and Role of Trademarks

The certificate subject name, including trademark or any name, business or company name or representation protected by law, provided by subscribers must comply with relevant regulations in our country's Trademark Act and Fair-Trade Act. PublicCA 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 PublicCA and the subscriber shall handle matters in accordance with regular administrative and judicial remedies.

3.1.7 Resolution Procedure for Naming Disputes

When subscribers have identical identification names, the subscriber who submitted the application first shall be given priority for use. Relevant disputes or arbitration shall not be the obligation of PublicCA 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 PublicCA may revoke that subscriber's certificate.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

PublicCA shall verify that the individual possesses the private key,

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

3.2.2 Authentication of Organization Identity

The certification document required for organization identification and authentication, and the authentication and verification procedures whether need to be performed at the counter are determined based on various assurance levels as shown in the following Table.

Assurance Level	Procedures for Authentication of Organization Identity
Level 1	(1) No identity verification required. (2) The applicant is required to demonstrate control of their e-mail address or domain name to which the certificate relates. (3) In-person identity proofing at counter is not required.
Level 2	(1) No identity verification required. (2) The applicant is required to provide organization information such as organization ID number (i.e. withholding tax ID number) and organization name. PublicCA may additionally cross-check the information provided by the applicant for consistency with available government or third-party data sources. (3) In-person identity proofing at counter is not required.
Level 3	PublicCA allows the following methods for authentication of organization identity: (1) In-person (physically-present) identity proofing at counter, which can be one of the following means: a. A certification document or official document issued by government agency in the jurisdiction of the applicant;

Assurance Level	Procedures for Authentication of Organization Identity
	b. Public information obtained from a qualified government information source (QGIS) such as the MOEA industry and business registration database or a qualified government tax information source (QTIS) such as the Fiscal Information Agency of MOF; or c. Organizations belonging to CHT apply for the certificate with written application. (2) Remote identity proofing, which can be one of the following means and the detailed operating procedures are formulated in the internal control system of each RA: a. Application through an identity assurance level 3 organization certificate issued by the GPKI or ePKI; b. For those organization who has complete registration procedure with the competent authority, like (1)-a or (1)-b, mailing the copies of the certification documents is acceptable; c. A letter attesting that subject information is correct written by an accountant, lawyer, or notary; d. A site visit by CA personnel or a third party who is acting as an agent for the CA; or e. Organizations belonging to CHT apply for the certificate with e-form.
DV SSL certificates	In compliance with the Baseline Requirements and the provisions for assurance level 1.
OV SSL certificates	In compliance with the Baseline Requirements and the provisions for assurance level 3.

3.2.3 Authentication of Individual Identity

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

Assurance Level	Procedures for Authentication of Individual Identity
Level 1	There is no requirement to link the applicant to a specific real-life identity. Any attributes provided in conjunction with the authentication process are self-asserted. (1) No identity verification required. (2) No identity verification other than control of the email address listed in the certificate. (3) In-person identity proofing at counter is not required.
Level 2	Evidence supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity. (1) No identity verification required. (2) The applicant is required to provide a legible copy of a valid government issued national identity document or photo ID (such as National ID, passport or health insurance card), and PublicCA will verify the information through reliable communications. (3) In-person identity proofing at counter is not required
Level 3	PublicCA allows the following methods for authentication of individual identity: (1) In-person (physically-present) identity proofing at counter, which can be one of the following means: The applicant must in-person proofing his / her identity at the CA or RA counter, at least present a national government-issued photo ID (such as National ID card, passport or health insurance card) to the RAO to examine whether they are authentic and unexpired. 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. When the applicant is not the citizen of Taiwan, the verification should be conducted according to the relevant regulations, where the detailed operating procedures are formulated in the internal control system of each RA. If an applicant (such as minor under 18 years old) is unable to submit the above photo ID, government-issued credentials (such as household

Assurance Level	Procedures for Authentication of Individual Identity
	registration) sufficient to prove the identity of the applicant and one adult with legal capacity to guarantee the applicant's identity in writing may be used in its place. The identity of the adult providing the guarantee must pass through the above authentication. (2) Remote identity proofing, which can be one of the following means and the detailed operating procedures are formulated in the internal control system of each RA: a. Application through a Citizen Digital Certificate IC Card; b. Delegate the duty of individual's identity examination to a financial institution who has business with the applicant; c. A declaration of applicant's identity that is witnessed and signed by a notary, lawyer, accountant, or any entity certified by a State or National Government as authorized to confirm identities; d. Other identity proofing mechanisms for remote account opening recognized by the competent authority of the relying party; e. Application through an identity assurance level 3 individual certificate issued by ePKI; f. A site visit by CA personnel or a third party who is acting as an agent for the CA; or g. Application through a telecommunications authentication where the related information is obtained from a telecommunications service provider under the applicant's consent. This method, where Subscriber Identity Module (SIM) authentication is used, provides the witness that the applicant and the number hirer have the same National ID number and the applicant had made identity proofing at the counter of Regular Chain stores at the time of dealing telecommunications business.

3.2.4 Non-verified Subscriber Information

The common name of an assurance level 1 individual certificate is not verified as the legal name of the subscriber. For SSL certificates, all information provided by the subscriber to be listed in the certificates must be verified.

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

(1) Using telephone, postal letter, e-mail, SMS or fax obtained from the reliable methods specified in Section 3.2.2.1 of the Baseline Requirements 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

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

PublicCA verifies an individual's or organization's right to use or control an email address to be contained in a certificate that will have the "Secure Email" EKU by doing one of the following:

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

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

(3) Applicants are required to verify that they do have control of the FQDN in accordance with one of the methods of domain name ownership or control verification in this section to confirm that the applicants indeed owns the e-mail account.

For DV SSL certificate applications, one or serveral methods (please refer to Section 3.2.5.1 to Section 3.2.5.7) recommended in the Baseline Requirements shall be choosed to validate the subscriber's right to use or control the domain name. For OV and IV SSL certificate applications, except for the validation of the subscriber's right to use or control the domain name, organization or individual's identity authentication must still be done in accordance with Sections 3.2.2 or 3.2.3.

3.2.5.1 Validating the Applicant as a Domain Contact

Confirming the Applicant's control over the FQDN by validating the Applicant is the Domain Contact. This method may only be used if PublicCA or RA is also the Domain Name Registrar, or an Affiliate of the Registrar, of the Base Domain Name. For example, Data Communications Business Group, Chunghwa Telecom Co., Ltd. is also the Domain Name Registrar of .tw.

Once the FQDN has been validated using this method, PublicCA MAY also issue SSL Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names. This method of validation confirms to Section 3.2.2.4.12 of the Baseline Requirements.

3.2.5.2 Email, Fax, SMS, or Postal Mail to Domain Contact

Confirming the Applicant's control over the FQDN by sending a Random Value to the Domain Contact via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to an email address, fax/SMS number, or postal mail address identified as a Domain Contact.

Each email, fax, SMS, or postal mail MAY confirm control of multiple Authorization Domain Names.

PublicCA or RA MAY send the email, fax, SMS, or postal mail identified under this section to one or more recipients, provided that every recipient is identified by the Domain Name Registrar as representing the Domain Name Registrant for every FQDN being verified via email, fax, SMS, or postal mail.

The Random Value SHALL be unique in each email, fax, SMS, or postal mail.

PublicCA or RA MAY resend the email, fax, SMS, or postal mail in its entirety, including reuse of the Random Value, provided that the communication's entire contents and recipient(s) remain unchanged.

The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation.

Once the FQDN has been validated using this method, PublicCA MAY also issue SSL Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names. This method of validation confirms to Section 3.2.2.4.2 of the Baseline Requirements.

3.2.5.3 Constructed Email to Domain Contact

Confirm the Applicant’s control over the FQDN by (i) sending an email to one or more addresses created by using 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at-sign ("@"), followed by an Authorization Domain Name, (For example, applicant’s Authorization Domain Name is abc.com，an RAO sends an email to webmaster@abc.com, hostmaster@abc.com or postmaster@abc.com) (ii) including a Random Value in the email, and (iii) receiving a confirming response utilizing the Random Value.

Each email MAY confirm control of multiple FQDNs, provided the Authorization Domain Name used in the email is an Authorization Domain Name for each FQDN being confirmed.

The Random Value SHALL be unique in each email.

The email MAY be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient SHALL remain unchanged.

The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation.

Once the FQDN has been validated using this method, PublicCA MAY also issue SSL Certificates for other FQDNs that end with all the labels of the validated FQDN. This method of validation confirms to Section 3.2.2.4.4 of the Baseline Requirements.

3.2.5.4 Agreed-Upon Change to Website

Confirming the Applicant's control over the FQDN by verifying that the Request Token or Random Value is contained in the contents of a file.

(1) The entire Request Token or Random Value must not appear in the request used to retrieve the file, and

(2) PublicCA MUST receive a successful HTTP response from the request (meaning a 2xx HTTP status code must be received).

The file containing the Request Token or Random Number:

(1) MUST be located on the Authorization Domain Name, and

(2) MUST be located under the "/.well-known/pki-validation" directory, and

(3) MUST be retrieved via either the "http" or "https" scheme, and

(4) MUST be accessed over an Authorized Port.

If the applicant adopts domain name redirects (also known as URL redirects), the following apply:

(1) Redirects MUST be initiated at the HTTP protocol layer.

A. For validations performed on or after July 1, 2021, redirects MUST be the result of a 301, 302, or 307 HTTP status code response, as defined in RFC 7231, Section 6.4, or a 308 HTTP status code response, as defined in RFC 7538, Section 3.

Redirects MUST be to the final value of the Location HTTP response header, as defined in RFC 7231, Section 7.1.2.

B. For validations performed prior to July 1, 2021, redirects MUST be the result of an HTTP status code result within the 3xx Redirection class of status codes, as defined in RFC 7231, Section 6.4. PublicCA limits the accepted status codes and resource URLs to those defined within (1).A.

(2) Redirects MUST be to resource URLs with either via the “http” or “https” scheme.

(3) Redirects MUST be to resource URLs accessed via Authorized Ports.

If a Random Value is used, PublicCA or RA SHALL provide a Random Value unique to the certificate request and SHALL not use the Random Value after 30 days from its creation. Once the FQDN has been validated using this method, PublicCA may also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method of validation confirms to Section 3.2.2.4.18 of the Baseline Requirements.

3.2.5.5 DNS Change

Confirming the Applicant's control over the requested FQDN by confirming the presence of a Random Value or Request Token in a DNS TXT or CAA record for an Authorization Domain Name or an Authorization Domain Name that is prefixed with a label that begins with an underscore character.

If a Random Value is used, PublicCA or RA SHALL provide a Random Value unique to the certificate request and SHALL not use the Random Value after (i) 30 days or (ii) if the Applicant submitted the certificate request, the timeframe permitted for reuse of validated information relevant to the certificate (such as in Section 4.2.1 of Baseline Requirement).

Once the FQDN has been validated using this method, PublicCA

MAY also issue SSL Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names. This method of validation confirms to Section 3.2.2.4.7 of the Baseline Requirements.

3.2.5.6 Email to DNS CAA Contact

Confirming the Applicant's control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to a DNS CAA Email Contact. The relevant CAA Resource Record Set MUST be found using the search algorithm defined in RFC 8659, Section 3.

Each email MAY confirm control of multiple FQDNs, provided that each email address is a DNS CAA Email Contact for each Authorization Domain Name being validated. The same email MAY be sent to multiple recipients as long as all recipients are DNS CAA Email Contacts for each Authorization Domain Name being validated.

The Random Value SHALL be unique in each email. The email MAY be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient(s) SHALL remain unchanged. The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation.

Once the FQDN has been validated using this method, PublicCA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names. This method of validation confirms to Section 3.2.2.4.13 of the Baseline Requirements.

3.2.5.7 Email to DNS TXT Contact

Confirming the Applicant's control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to a DNS TXT Record Email Contact for the Authorization Domain Name selected to

validate the FQDN.

Each email MAY confirm control of multiple FQDNs, provided that each email address is DNS TXT Record Email Contact for each Authorization Domain Name being validated. The same email MAY be sent to multiple recipients as long as all recipients are DNS TXT Record Email Contacts for each Authorization Domain Name being validated.

The Random Value SHALL be unique in each email. The email MAY be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient(s) SHALL remain unchanged. The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation.

Once the FQDN has been validated using this method, PublicCA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names. This method of validation confirms to Section 3.2.2.4.14 of the Baseline Requirements.

If a wildcard would fall within the label immediately to the left of a registry-controlled or public suffix, PublicCA refuses issuance unless the applicant proves its rightful control of the entire Domain Namespace. (e.g. PublicCA will NOT issue “*.com.tw” or “*.local”). If using the PSL, PublicCA consults the “ICANN DOMAINS” section only, not the “PRIVATE DOMAINS” section. PublicCA is not prohibited from issuing a Wildcard Certificate to the Registrant of an entire gTLD, provided that control of the entire namespace is demonstrated in an appropriate way.

3.2.6 Criteria for Interoperation

PublicCA is not a Root CA. Not appliable.

3.2.7 Data Source Accuracy

Prior to using any data source as a Reliable Data Source, PublicCA SHALL evaluate the source for its reliability, accuracy, and resistance to

alteration or falsification. PublicCA 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.

Databases maintained by PublicCA, its owner, or its affiliated companies do not qualify as a Reliable Data Source, if the primary purpose of the database is to collect information according to the validation requirements in Section 3.2 of the Baseline Requirements.

3.3 Identification and Authentication for Re-key Requests

If the subscriber's private key needs to be renewed upon expiry of the certificate usage period, certificate rekey work may be performed and the subscriber may re-apply for certification. Identification and authentication shall be performed in accordance with the regulations in Section 3.2.

3.3.1 Identification and Authentication for Routine Re-key

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

3.3.2 Identification and Authentication for Re-key after Revocation

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

3.4 Identification and Authentication for Revocation Request

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

4. Certificate Life-cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Organizations and individuals may submit certificate applications.

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

4.1.2 Enrollment Process and Responsibilities

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

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

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

(3) After obtaining the certificate issued by PublicCA, the subscriber shall check the accuracy of the information contained on the certificate and use the certification in accordance with the regulations in section 1.4.1. If there is an error in the certificate information, the subscriber shall notify the RA and refrain from using the certificate.

(4) The subscriber shall properly safeguard and use their private key.

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

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

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

4.2 Certificate Application Processing

The certificate application procedures are as follows:

(1) The certificate applicant fills out the information on the certification request and agrees to the subscriber agreements.

(2) The certificate applicant sends the certificate request information and related certification information to the RA.

(3) If the certificate applicant self-generates the keys, a PKCS#10 Certificate signing request is created and signed with the private

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

4.2.1 Performing Identification and Authentication Functions

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

PublicCA and RAs confirm and implement additional checks for the high-risk certificate requests before issuing the certificates. In the RAs, the system checks against the FQDNs with higher risks for phishing or other fraud activities; the phishing website addresses disclosed by Anti-Phishing Work Group (APWG) and similar organizations that are collected by PublicCA and RAs; the FQDNs which whose certificate requests were denied, or FQDNs provided by the browsers suppliers which owned by the suppliers and prohibited to issue SSL certificates, the blacklist which alerts the RA officers, or the suspicious FQDNs marked with Subject Alternative Name attribution that are entered by the RA officers in Google Safe Browsing List or Miller Smiles Phishing List, in order to prevent mistakenly issuing SSL certificates.

Before issuing SSL certificates, the SSL certificates to be issued will

be marked in every dNSName in the subjectAltName extension (i.e. the applicant provides every FQDN contained in the certificate request). The RA officers will access to Domain Name System (DNS) to check the Certification Authority Authorization (CAA) record based on RFC 6844 as amended by Errata 5065, and the certificates are only issued after passing the check. That is, if a FQDN's "issue" or "issuewild" tag contains "pki.hinet.net", "publicca.hinet.net", "eca.hinet.net" or "epki.com.tw", PublicCA will issue the SSL certificate of that FQDN. In case of the property tag "iodef" is present in the CAA records, PublicCA will determine wheather to issue SSL certificate after communicating with the applicant.

PublicCA or the RA checks DNS to see if the FQDN will be marked for the application of the SSL certificate has the DNS resource record of CAA. If the DNS resource record of CAA exists, and has not named PublicCA as the CA to authorize the issuance of the SSL certificate, PublicCA will deem that the certificate application agrees to authorize PublicCA to issue the SSL certificate for that complete domain name, and require the subscriber to visit the DNS for updating the DNS resource record of CAA, in order to have PublicCA included in the record, and the SSL certificate will be issued afterwards.

PublicCA or RA is permitted to treat a record lookup failure as permission PublicCA to issue if: (1) the failure is outside PublicCA's infrastructure; (2) the lookup has been retried at least once; and (3) the domain's zone does not have a DNSSEC validation chain to the ICANN root.

4.2.2 Approval or Rejection of Certificate Applications

If all identity authentication work follows relevant regulations and best practices can be successfully implemented, PublicCA and its RA may

approve the certificate application.

If the various identity authentication works cannot be successfully completed, PublicCA may reject the certificate application. Except for applicant identity identification and authentication reasons, PublicCA and its RA may refuse to use the certificate for other reasons. PublicCA and its RA may also reject certificate application from applicants who have previously been rejected or have previously violated the subscriber agreements.

PublicCA does not issue publicly trusted SSL certificates to internal server name or reserved IP addresses. The validation of authorized domain names and the basic domain names shall comply with the regulations. The related validation mechanisms are specified in Section 3.2.5, and please refer to the glossaries in Appendix 2.

4.2.3 Time to Process Certificate Applications

PublicCA and RAs shall complete the certificate application within a reasonable period of time. Provided that the information submitted by the applicant is complete and complies with CP, CPS and checking requirements, the RAO shall quickly complete the certificate application review. The time needed by RA to process certificate applications and PublicCA to issue the certificates depends on the certificate group and type. These times may be disclosed in the subscriber agreements, contract or RA website.

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

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

Upon PublicCA and its RA 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.

Certificate issuance steps are follows:

(1) The RA submits the certificate application passed the review procedures to PublicCA.

(2) When PublicCA 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, PublicCA 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 PublicCA to understand where the problem is.

(4) PublicCA provides the function of pre-issuance linting, which can check whether the format of the certificate to be issued complies with the Baseline Requirements/RFC 5280. If it does not meet the requirements, it will be rejected to prevent mis-issuance or false of the certificate.

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

(6) PublicCA reserves the right to refuse certificate issuance to any entity. PublicCA shall not bear any liability for damages to the applicant who is refused to issue the certificate.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

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

If PublicCA or RA does not approve the certificate issuance, the certificate applicant is notified by e-mail or telephone and shall be informed of the reasons for the refusal. Besides applicant identity identification and authentication reason, certificate issuance may be refused due to other reasons.

4.4 Certificate Acceptance

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

(1) The certificate applicant pre-reviews the content of the certificate to be issued. The certificate applicant reviews the information recorded on the certificate for accuracy and provides consistent information for the application. If the certificate applicant refuses to accept the information recorded on the certificate after reviewing the certificate content, the certificate is not issued. For example, if a SSL server software certificate applicant finds the fully qualified domain on other required TLS encrypted channels have not been applied for registration when pre-reviewing the certificate subject name field on the issued SSL certificate, issuance of that SSL certificate may be refused. A new certificate application may be submitted in accordance with Section 4.2.

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

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

Acceptance of the certificate is deemed as the certificate applicant's consent to comply with the rights and obligations in this CPS or related contracts.

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

4.4.1 Conduct Constituting Certificate Acceptance

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

4.4.2 Publication of the Certificate by the CA

The PublicCA repository service regularly publishes the issued certificates or delivers the certificate to the certificate applicant to achieve certificate publication. The RA may negotiate with PublicCA about certificate delivery by the RA to the certificate 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 PublicCA. Their relationship with the certificate subject is shown in the table in Section 1.3.3 of this CPS. Scope of applications regarding different assurance level certificates 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 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 digitalsignatures or keyEncryption. Subscribers shall correctly use their certificates adhering to the certificate policies listed in the certificates.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties 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, IETF RFCs and Baseline Requirements.

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

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

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

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

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

4.6 Certificate Renewal

Expired, suspended and revoked certificate shall not be renewed. The certificate shall be renewed up to the upper limit of the subscriber public key validity period specified in Section 6.3.2.2 to keep the security of the key pair.

4.6.1 Circumstances for Certificate Renewal

Unrevoked certificates which are about to expire may be renewed under the following circumstances:

(1) The public key listed on the certificate has not reached the usage limit stipulated in Section 6.3.2.2.
(2) The subscriber and its attribute information remain consistent.
(3) The private key corresponding to the public key listed on the certificate is still valid and has not been lost or compromised.

4.6.2 Who May Request Renewal

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

4.6.3 Processing Certificate Renewal Requests

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

4.6.4 Notification of New Certificate Issuance to Subscriber

According to the regulations in Section 4.3.2, PublicCA shall issue a notification to the subscriber whose certificate has been renewed, to download the renewed certificate. If PublicCA denies the renewal, the reason of denial shall be communicated to the subscriber.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

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

4.6.6 Publication of the Renewal Certificate by the CA

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

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

The RA may receive notification of renewal certificate issuance.

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.

For subscribers which hold assurance level 1, 2 and 3 certificates, if the certificate has not been revoked, PublicCA 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 Section 4.2.

After the subscriber's 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 PublicCA 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 (e.g., a representative authorized by the organization).

4.7.3 Processing Certificate Re-keying Requests

For subscriber certificate re-keying, subscribers shall submit a new

certificate application to PublicCA. 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

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

4.7.6 Publication of the Re-keyed Certificate by the CA

The PublicCA repository service regularly publishes the new certificates that undergo certificate re-keying or delivers the new certificate to the certificate applicant to achieve re-keyed certificate publication. The RA may negotiate with PublicCA about certificate delivery by the RA to the certificate applicant.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

RA may receive notification of re-keyed certificate issuance.

4.8 Certificate Modification

4.8.1 Circumstance for Certificate Modification

Certificate modification means creating a new certificate for the same subject, where authenticated information that slightly differs from the old certificate (e.g., changes to e-mail address or other relatively unimportant attribute information) which conforms to relevant regulations in the ePKI

CP and this CPS. The new certificate has a new certificate serial number but with the same subject public key and 'NotAfter' date. After the certificate is modified, the old certificate shall be revoked.

If there is any change to the important identity information such as the organization name, individual name or national ID number, the original certificate must be revoked. The subscriber must submit a new certificate application with the modified organization name, individual name or national ID number to obtain a new certificate in accordance with the procedures in Sections 4.1 and 4.2.

4.8.2 Who May Request Certificate Modification

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

4.8.3 Processing Certificate Modification Requests

(1) The certificate modification applicant shall submit the certificate modification request in accordance with the guidelines established by the RA. After the RA receives the certificate modification request the review procedure is followed and all the changes in the new certificate application request and the original certificate revocation request are kept for recordkeeping including the applicant name, contact information reason for the new certificate application, reason for the original certificate revocation and the time and date of the original certificate revocation to serve a basis for subsequent accountability. See Sections 4.2 and 4.9 for the guidelines established by the RA. For example, if the certificate modification applicant is asked to add a signature to the certificate application file corresponding to its

private key and submit the certificate application file to the RA, the RA shall verify the digital signature on that certificate application file with the subscriber's public key to authenticate the subscriber's identity.

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

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

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

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

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

4.8.4 Notification of New Certificate Issuance to Subscriber

The regulations from PublicCA for notification to issue certificate modification shall comply with Section 4.3.2.

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

4.8.5 Conduct Constituting Acceptance of Modified Certificate

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

4.8.6 Publication of the Modified Certificate by the CA

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

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.9 Certificate Revocation and Suspension

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

Requirements, SSL certificates shall not suspend and resume the use (Sections 4.9.13 to 4.9.17 are not applicable).

4.9.1 Circumstances for Revocation

PublicCA shall revoke a certificate within 24 hours if one or more of the following occurs:

(1) The subscriber requests in writing to PublicCA that they wish to revoke the certificate;
(2) The subscriber notifies PublicCA that the original certificate request was not authorized and does not retroactively grant authorization;
(3) PublicCA obtains evidence that the subscriber's private key corresponding to the public key in the certificate suffered a key compromise;
(4) PublicCA is made aware of a demonstrated or proven method that can easily compute the subscriber's private key based on the public key in the certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys); or
(5) PublicCA obtains evidence that the validation of domain authorization or control for any FQDN or IP address in the certificate should not be relied upon.

PublicCA should revoke a certificate within 24 hours and must revoke a certificate within 5 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) PublicCA obtains evidence that the certificate was misused;
(3) PublicCA is made aware that a subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;

(4) PublicCA is made aware of any circumstance indicating that use of a FQDN or IP address in the certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);

(5) PublicCA is made aware that a wildcard certificate has been used to authenticate a fraudulently misleading Subordinate FQDN;

(6) PublicCA is made aware of a material change in the information contained in the certificate;

(7) PublicCA is made aware that the certificate was not issued in accordance with these requirements or the ePKI CP or this CPS;

(8) PublicCA determines or is made aware that any of the information appearing in the certificate is inaccurate;

(9) PublicCA's right to issue certificates under these requirements expires or is revoked or terminated, unless PublicCA has made arrangements to continue maintaining the CRL/OCSP Repository;

(10) Revocation is required by the ePKI CP and/or this CPS;

(11) PublicCA is made aware of a demonstrated or proven method that exposes the subscriber's private key to compromise or if there is clear evidence that the specific method used to generate the private key was flawed; or

(12) Under the circumstance that the payment deadline has expired and the subscriber has been notified, the subscriber has still not paid the fee.

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

4.9.2 Who Can Request Revocation

Subscribers, PublicCA, 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 suppliers or other third party may submit certificate problem report to advise PublicCA 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 work, the certificate revocation application information is sent to PublicCA;

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

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

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

the data transmitted between PublicCA and its RA, the data of the certificate application is encrypted with a digital signature and transmitted through the network by TLS protocol;

(6) PublicCA 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) PublicCA 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, PublicCA 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 PublicCA 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.

PublicCA 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, PublicCA 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, PublicCA 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 PublicCA 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 certificates issued by PublicCA, the relying parties shall first check the CRLs or OCSP responses published by PublicCA to verify

the validity of certificates. The relying parties shall verify the revoking time of certificates, the validity of signatures of the CRL or OCSP responses, and certificate chains with their validity.

PublicCA publishes the information of suspended and revoked certificates to the repository for checking purposes. There are no restrictions for the checking of CRL by relying parties. The website is at: http://publicca.hinet.net

4.9.7 CRL Issuance Frequency

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

4.9.8 Maximum Latency for CRLs

After a CRL is produced by PublicCA, it will be released immediately. The system has no pre-signed behavior.

4.9.9 On-line Revocation/Status Checking Availability

PublicCA provides the inquiry to certificate revocation/status by CRL, webpage certificate inquiries and download, and OCSP responses.

PublicCA uses OCSP Responder to provide the OCSP responses complying with RFC 6960 and RFC 5019 standards. PublicCA 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.

Thr OCSP responder uses 2048-bit RSA keys and SHA-256 hash function algorithm to issue OCSP responses.

PublicCA provides the OCSP service, and the OCSP responder operated by PublicCA supports the HTTP-based POST and GET methods, as described in RFC 6960 and RFC 5019.

The OCSP of PublicCA is updated at least once per hour, and the validity period of the OCSP responses is greater than or equal to 8 hours and less than 16 hours.

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

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

4.9.11 Other Forms of Revocation Advertisements Available

In order to speed up and instantly complete the verification of the SSL

certificates status of high-traffic websites, PublicCA supports OCSP stapling operation based on RFC 4366 and through the Subscriber Agreements, support of Certificate Transparency and technical review, or provision of relevant setting instructions to assist subscribers who own high-traffic websites to implement OCSP stapling.

4.9.12 Special Requirements Related to Key Compromise

In case of a compromise of the subscriber's private key, the subscriber must immediately notify PublicCA of the event. PublicCA will revoke the concerned certificate (choose the reason for the revocation as 'key compromised') according to the procedures set forth in Sections 4.9.1, 4.9.2 and 4.9.3 of this CPS, and publish a CRL to inform relying parties that the certificate can no longer be trusted.

In case of a compromise of PublicCA's private key, eCA will publish a certification authority revocation list (CARL) to inform software suppliers, subscribers, and relying parties about the private key compromise event.

The acceptable methods used by third parties as proof of key compromise are as follows:

(1) Confirming the third party's possession of the private key by signing a challenge provided by PublicCA using the compromised private key; or

(2) Submitting the private key itself.

4.9.13 Circumstances for Suspension

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

(1) Suspected theft of certificate key pair.

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

In addition, PublicCA may suspend the certificate under the following

circumstances without advance permission from the subscriber:

(1) The subscriber is ordered to suspend operations.

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

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

4.9.14 Who Can Request Suspension

The following two groups may apply for certificate suspension:

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

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

4.9.15 Procedure for Suspension Request

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

4.9.16 Limits on Suspension Period

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

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

If the subscriber cancels the certificate suspension during the

certificate suspension period, certificate use is resumed and the certificate recovers its validity.

4.9.17 Procedure for Certificate Resumption

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

4.10 Certificate Status Services

4.10.1 Operational Characteristics

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

PublicCA maintains 24x7 availability of certificate status service.

PublicCA 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 PublicCA’s

services. PublicCA 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

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

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

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

5.1.2 Physical Access

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

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

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

software or hardware security module.

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

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

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

(1) Check if system equipment is operating normally.

(2) Check if the computer racks are locked.

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

5.1.3 Power and Air Conditioning

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

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

5.1.4 Water Exposures

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

5.1.5 Fire Prevention and Protection

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

5.1.6 Media Storage

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

5.1.7 Waste Disposal

When the documents of PublicCA 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 PublicCA facility. The backup content shall include information and system programs.

5.2 Procedural Controls

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

5.2.1 Trusted Roles

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

The seven PKI personnel roles assigned by PublicCA are administrator, CA officer, internal auditor, system operator, physical security controller, cyber security coordinator and anti-virus and anti-hacking coordinator 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 seven roles are as follows:

The administrator is responsible for:

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

The 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 PublicCA 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 PublicCA
- The 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

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 PublicCA system	2				1		
Establishment and maintenance of system user accounts	2				1		
Generation and backup of PublicCA keys	2		1		1		
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				1	1		

Assignments	Administrator	CA Officer	Internal Auditor	System Operator	Physical security controller	Cyber security coordinator	Anti-virus and anti-hacking coordinator
equipment							
System backup and recovery				1	1		
Storage media updating				1	1		
Hardware and software updates outside the PublicCA 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 PublicCA host uses login account numbers, passwords and groups to identify and authenticate

administrator, CA officer, internal auditor and system operator. PublicCA 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

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

- Administrator, CA officer, internal auditor, and cyber security coordinator cannot assume any other roles among these four trust 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 PublicCA personnel performing certificate work shall have their qualifications reviewed at the initial time of employment to verify their reliability and work capabilities. After formal employment, personnel shall receive appropriate training and sign a document accepting responsibility to perform certain duties. All personnel shall have their qualifications rechecked each year to reconfirm their reliability and work ability. If personnel do not pass the qualification check, that person shall be reassigned to another position and a qualified person shall be assigned to serve in that position.

(3) Appointment, Dismissal and Transfer

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

(4) Duty of Confidentiality Agreement

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

5.3.2 Background Check Procedures

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

5.3.3 Training Requirements

Trusted Role	Training Requirements
Administrator	(1) PublicCA security principles and mechanism. (2) Installation, configuration, and maintenance of the PublicCA operation procedures. (3) Establishment and maintenance of system user accounts operation procedures. (4) Audit parameter configuration setting procedures. (5) PublicCA key generation and backup operation procedures. (6) Disaster recovery and continuous operation procedure.
CA Officer	(1) PublicCA security principles and mechanism. (2) PublicCA 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) PublicCA security principles and mechanism. (2) PublicCA system software and hardware use and operation procedures. (3) PublicCA key generation and backup operation procedures. (4) Audit log check, upkeep and archiving procedures. (5) Disaster recovery and continuous operation procedure.
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.
Cyber security coordinator	(1) Maintenance of the network and network facilities. (2) Security mechanism for the network.

Trusted Role	Training Requirements
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.

5.3.4 Retraining Frequency and Requirements

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

5.3.5 Job Rotation Frequency and Sequence

(1) May not concurrently serve 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

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

5.3.7 Independent Contractor Requirements

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

5.3.8 Documentation Supplied to Personnel

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

5.4 Audit Logging Procedures

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

5.4.1 Types of Events Recorded

(1) Key generation

- Key generation of PublicCA (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 PublicCA for key recovery work.

(3) Certificate registration

- Certificate registration request procedure.

(4) Certificate revocation

- Certificate revocation request procedure.

(5) Account administration

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

(6) Certificate profile management

- Certificate profile changes.

(7) CRL profile management

- CRL profile changes.

(8) Physical access / site security

- Known or suspect violation of physical security regulations.

(9) Anomalies

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

5.4.2 Frequency of Processing Log

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

PublicCA shall check the audit logs once every two months.

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) PublicCA shall routinely archive event logs.

(2) PublicCA 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 PublicCA security-related events. Security audit logs shall be collected by automatic system generation, logbook or paper. All security audit logs shall be retained and made available during compliance audits.

5.4.7 Notification to Event-causing Subject

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

5.4.8 Vulnerability Assessments

Starting from January 2015, the RAs conduct a vulnerability scan at

least once each year and take remedy measures.

Starting from July 2014, PublicCA follow the methods and frequency stipulated in the AICPA/CPA WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security Version 2.0 and Network and Certificate System Security Requirements Version 1.0 to conduct the vulnerability assessments at least once per quarter and the penetration testing at least once per year. PublicCA will implement the enhancement and correction measures after the penetration testing and the vulnerability assessment. PublicCA also must conduct penetration testing after it is determined that there is a significant upgrade or modification to the application program or infrastructure. PublicCA shall record the skills, tools, followed ethics, competitive relations and independence guidelines for those personnel or groups capable of implementing reliable vulnerability scans, penetration testing, or information security diagnosis or security surveillance.

5.5 Records Archival

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

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

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

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

5.5.1 Types of Records Archived

PublicCA retains the following information in its archives:

(1) PublicCA accreditation information from competent authorities.

(2) CPS.

(3) Major contracts.

(4) System and equipment configuration settings.

(5) System and configuration setting modifications and updates.

(6) Certificate application information.

(7) Revocation request information.

(8) Subscriber identity identification information stipulated in Section 3.2.

(9) Issued and published certificates.

(10) PublicCA re-key records.

(11) Issued or announced CRLs.

(12) Audit logs.

(13) 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

PublicCA retains archived data for at least 2 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 PublicCA authorization procedure.

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

5.5.4 Archive Backup Procedures

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

5.5.5 Requirements for Time-stamping of Records

All PublicCA computer systems are regularly calibrated to ensure the accuracy and trustworthiness of the date and time information on electronic records. For archived electronic records (such as certificates, CRLs and audit logs), the timestamping information on each record shall include the date and time information 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

PublicCA 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.

PublicCA 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 PublicCA's certificate has been revoked, PublicCA 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

PublicCA establishes incident and compromise reporting and handling procedures and conducts drills annually.

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

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

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

5.7.3 Entity Private Key Compromise Procedures

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

(1) Publish in the repository and notify subscribers and relying parties about the event of key compromise.

(2) Revoke the PublicCA signature key certificate and issued subscriber certificates.

(3) Generate new key pairs in accordance with the procedures in Section 5.6. New certificates are published in the repository for subscriber and relying party downloading.

PublicCA shall conduct the drills at least once a year.

5.7.4 Business Continuity Capabilities after a Disaster

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

5.8 CA or RA Termination

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

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

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

- For certificates which are valid at the time of termination, arrangements shall be made for other CA to take over the service. Matters regarding service termination and service acceptance by other CAs shall be published in the repository and subscribers with valid certificates stall be notified. This shall not apply if notification cannot be made.
- All records and files during the operation period shall be

handed over to the other CA that is taking over this service.

- If there is no CA willing to take over the PublicCA service, a report shall be submitted to the competent authority to arrange for other CA to take over this service.
- If the competent authority arranges for other CA to take over the service but no other CA takes over the service, PublicCA shall revoke the still valid certificates, publish the revoked certificates in the repository and notify all certificate-related persons 30 days prior to the scheduled termination of service. PublicCA will refund the certificate issuance and renewal 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, PublucCA shall stop its rights of review actions.

6. Technical Security Controls

This chapter describes the technical security controls implemented by PublicCA.

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

PublicCA and 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, PublicCA generates key pairs within the hardware security module by using the algorithm and the procedures 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.

PublicCA 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

If the token used by the subscriber is an IC chip, the key pair is generated by the card management center on behalf of the subscriber; for other types of certificates, subscribers must generate their key pairs.

6.1.2 Private Keys Delivery to Subscriber

PublicCA should not generate key pair on behalf of the subscriber. If the card management center generates a key pair for subscriber, the RA shall deliver the token (such as IC card) containing the subscriber key to the subscriber after certificate issuance by PublicCA.

6.1.3 Public Key Delivery to Certificate Issuer

If the card management center generates a key pair for a subscriber, the RA shall deliver the subscriber public key to PublicCA via secure channels.

If a subscriber self-generates a key pair, the subscriber shall deliver the public key to the RA via a certificate signing request file with PKCS# 10 format. The RA shall delivery the public key to PublicCA 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 TLS or other equivalent or higher level data encryption transmission protocols.

6.1.4 CA Public Key Delivery to Relying Parties

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

6.1.5 Key Sizes

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

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

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

The subscriber key may generate the prime numbers needed for the RSA algorithm inside the IC card or other software/hardware security modules but this does not guarantee that this prime number is a strong prime.

According to Section 5.3.3 of NIST SP 800-89, PublicCA 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 should also have the following characteristics: an odd number, not the power of a prime, and have no factors smaller than 752.

If the certificates are issued with Elliptic Curve Cryptosystem (ECC) algorithm, PublicCA shall follow 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)

PublicCA’s private signing key is used to issue certificates and CRLs. PublicCA’s own public key certificate is issued by eCA. The keyUsage bits

used for the keyUsage extension setting are keyCertSign and cRLSign.

When the token used by the subscriber is IC card, or USB token consolidating IC card and card reader, the token contains keyEncipherment and digitalSignature, which are two certificates with different keyUsages.

When the token used by the subscriber is non-IC card or non-USB token, keyUsage may contain keyEncipherment and digitalSignature at the same time.

The keyUsage extension of SSL certificate includes keyEncipherment and digitalSignature. The extKeyUsage extension includes serverAuth and clientAuth.

For the dedicated server application software certificate, it can be further categorized into the following three types:

(1) E-mail type: the rule of critical keyUsage extension shall be (digitalSignature | keyEncipherment | dataEncipherment), and the extKeyUsage extension shall only contain emailProtection. Besides, the Subject Alternative Name Extension is rfc822Name.

(2) Dvcs type: the rule of critical keyUsage extension shall be (digitalSignature | nonRepudiation), and the critical extKeyUsage extension shall only contain dvcs. In addition, it does not have Subject Alternative Name Extension.

(3) Other type: the rule of critical keyUsage extension shall be (digitalSignature | keyEncipherment | dataEncipherment | nonRepudiation), and the extKeyUsage extension shall only contain clientAuth and one chtDedicated value which is id-cht-ePKI-kp-dedicated (1.3.6.1.4.1.23459.100.1.1). In addition, it does not have Subject Alternative Name Extension.

For the PDF Signing certificate issued by PublicCA, the combination of keyUsage and extKeyUsage complies with the AATL technical requirements.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

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

Storage media for subscriber key pairs may be chip validated by FIPS 140-2 Level 2, ISO 15408, or Common Criteria EAL (EAL) 4+ or higher level, hardware security module complying with FIPS 140-2 Level 3 or other tokens.

Storage media for the private key of the Adobe PDF Signing certificate shall be chip validated by FIPS 140-2 Level 2, ISO 15408, or EAL 4+ or higher level, or hardware security module complying with FIPS 140-2 Level 2.

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

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

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

6.2.4 Private Key Backup

Backups of PublicCA private keys are made according to the key splitting multi-person control 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

PublicCA 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

PublicCA transfers private keys into cryptographic modules under the following circumstances:

(1) Key generation or cryptographic module replacement;

(2) For the recovery of a backed up key, the secret splitting (*n-out-of-m* control) is used to recover the PublicCA 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

PublicCA 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 methods to activate the private keys of subscribers are categorized by the private key storage media as the following:

(1) If it is an IC card, the private keys shall be activated by the subscribers' (whose identity is validated) configuration and the PINs only known to the subscribers.
(2) If it is a hardware security module, the private keys are activated by the IC cards controlled by multiple people. The controlling IC cards for different purposes are maintained by different people.
(3) For other private key tokens, subscribers shall use strong passwords or other identification with the same level to activate the private keys, in order to prevent the unauthorized access or use of the private keys.

6.2.9 Method of Deactivating Private Key

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

PublicCA does not provide subscriber private key deactivation service.

6.2.10 Method of Destroying Private Key

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

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

If services are permanently not provided by a cryptographic module but it is still accessible, all private keys (already used or possibly used) stored in that cryptographic module must be destroyed. After destroying the keys, the key management tools provided by this cryptographic module must be used to verify that the above keys no longer exist.

If services are permanent not provided by a cryptographic module, all used private keys stored in that cryptographic module must be erased from the cryptographic module.

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

6.3.1 Public Key Archival

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

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

6.3.2.1 PublicCA Certificate Operational Periods and Key Pair Usage Periods

PublicCA certificate operational periods and key pair usage periods are:

Type of Cert.	Private Key Usage Period	Certificate Term
CA Certificate of PublicCA	■ Issuing subscriber 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 (provide the relying parties with the OCSP response signed by the new private key along with that certificate).

6.3.2.2 Subscriber Certificate Operational Periods and Key Pair Usage Periods

The key size of public and private keys for the subscriber in PublicCA is RSA 2048 bit or the above, or ECC-256 or the above when ECC algorithm is applied. The subscriber certificate operational periods and key pair usage periods are:

Type of Cert.	Private Key Usage Period	Certificate Term
Non-TLS/SSL Certificate	■ See Section 6.1.7: 10 years	10 years
TLS/SSL Certificate	■ See Section 6.1.7: no stipulation	398 days

6.3.2.3 SHA-1 Hash Function Algorithm Validity Period

PublicCA has eliminated SHA-1 SSL certificates by the schedule specified in the Baseline Requirements version 1.2.1.

PublicCA use RSA-2048 or the above key w/SHA-256 to issue OCSP response.

From the end of 2014, PublicCA issues all kinds of subscriber

certificates by RSA-2048 or the above key w/SHA-256. At the end of November 2018, all SHA-1 subscriber certificates are shifted to SHA-256 subscriber certificates.

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 shall 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 PublicCA private key activation data is not archived.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

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

(1) Trusted role or identity authentication login,

(2) Provide discretionary access control,

(3) Provide security audit capability, and

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

6.5.2 Computer Security Rating

PublicCA servers use EAL 3 certified computer operating systems.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

Quality control for PublicCA 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 PublicCA as well as conduct program version control.

6.6.2 Security Management Controls

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

PublicCA shall only use components with security authorization. Unrelated hardware devices, network connections or component software shall not be installed.

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

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

6.6.3 Life Cycle Security Controls

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

6.7 Network Security Controls

PublicCA implements network security control measures in compliance with the Network and Certificate System Security Requirements.

The PublicCA 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 PublicCA host have digital signature protection and are automatically delivered from the PublicCA

host to the repository.

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

PublicCA monitors the configuration of access control permissions, continuously monitors for system health and security events, and performs penetration test.

6.8 Time-stamping

PublicCA regularly conducts system synchronization with a reliable time source to maintain the correctness of system time and ensure the accuracy of the following times:

(1) 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 PublicCA conform to the official versions of the ITU-T X.509, Baseline Requirements and RFC 5280.

PublicCA 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)

PublicCA issues X.509 version 3 certificates.

7.1.2 Certificate Extensions

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

7.1.2.1 Subordinate CA Certificate of PublicCA

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

a. certificatePolicies

This extension is required and marked as non-critical. It asserts the policy identifier. The policy qualifier field of this extension may be used to mark the published URL of the eCA CPS as needed.

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 PublicCA 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 keyCertSign and cRLSign. PublicCA does not sign the OCSP response with the private signing key, but issues the OCSP responder certificate, and the OCSP responder issues OCSP responses, and thus the configuration does not use digitalSignature.

f. nameConstraints

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

g. extKeyUsage

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

h. authorityKeyIdentifier

This extension is required and marked as non-critical. It MUST contain a keyIdentifier field and it MUST NOT contain a authorityCertIssuer or authorityCertSerialNumber field.

7.1.2.2 Subscriber Certificate

a. certificatePolicies

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

the policy identifier. The policy qualifier field of this extension may be used to mark the published URL of this CPS as needed.

b. cRLDistributionPoints

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

c. authorityInfoAccess

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

d. basicConstraints

The subscriber certificates issued by PublicCA do not have this extension.

e. keyUsage

This extension is optional and marked as critical if any. The bits of both keyCertSign and cRLSign must not be set. For the key usage extension of various certificates, please refer to Section 6.1.7.

f. extKeyUsage

For the certificates issued by PublicCA, this extension is required and marked as non-critical. The extension contains both serverAuth and clientAuth bits, where the value anyExtendedKeyUsage MUST NOT be present.

g. authorityKeyIdentifier

This extension is required and marked as non-critical. It MUST contain a keyIdentifier field and it MUST NOT contain a authorityCertIssuer or authorityCertSerialNumber field.

For the extKeyUsage of PDF signing certificate, please refer to Section 6.1.7. Unless the reasons to include certain data in the certificates

are known, PublicCA does not allow certificates being issued in the following scenarios:

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

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

Regarding supporting the CT, PublicCA adopts the X.509 version 3 Extension mechanism, which is currently the most commonly used, to transmit SCTs for OV SSL certificates. Therefore, the SCT will be individually obtained from the multiple CT logs through submitting the pre-signed precertificate's certificate chain, and the SCT chain will be embedded into the target certificate before it is issued to the subscriber. According to the latest Google and Apple CT policies, adopting X.509 v3 Extension mechanism has the following benefits: SSL certificate subscribers can obtain SSL certificates compliant with the CT specifications by past certificate application; no additional restrictions exist as OCSP Stapling SCT transmission method listed in the RFC 6962 (it requires subscriber web server OCSP Stapling configuration settings to be enabled, and there are still a few web servers unsupportable for OCSP Stapling); PublicCA just needs to ensure that the connected CT logs are currently qualified during issuing the target certificate; therefore, it won't be affected by the status changes of CT logs in the future.

7.1.3 Algorithm Object Identifiers

The algorithm OIDs used for signatures on PublicCA 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 PublicCA 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, Baseline Requirements and RFC 5280.

The Subject information in the CA certificates of PublicCA 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 PublicCA 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 PublicCA, trademark, or their meaningful name, for the purpose of identifying PublicCA more precisely; it is not allowed to contain the commonName only. For example: CA1. Please refer to Section 3.1.5 for the X.500 distinguished name of the CA certificate of PublicCA.

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 issuing CA. Therefore, for the subscriber certificate issued by PublicCA, the Issuer DN must be identical to the content of the Subject DN of PublicCA.

7.1.4.2 Subject Information–Subscriber Certificates

By issuing the subscriber certificates, PublicCA and RAs have complied with the procedures specified in the ePKI CP and/or this CPS, to ensure all the Subject information recorded in these certificates are accurate. If the commonName field in the certificate Subject appears, it

must be one of the subjectAltNames (SANs) which contains the FQDNs validated by one of the methods stated in Section 3.2.5. In addition, subject attributes MUST NOT contain only metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.

7.1.4.2.1 Subject Alternative Name Extension

The Subject Alternative Name Extensions for OV, DV, and IV SSL certificates are as follows:

Certificate Extension	Required/Optional Extension
extension:subjectAltName	Required

The Subject Alternative Name Extensions for none SSL certificates are as follows:

Certificate Extension	Required/Optional Extension
extension:subjectAltName	Optional

Underscore characters ("_") must not be present in dNSName entries.

The Subject Alternative Name Extension will mark the e-mail account, or FQDN's certificate application. The RA officers shall validate the ownership or control of the email account or domain name.

7.1.4.2.2 Subject Distinguished Name Fields

The Subject Distinguished Name Fields of various subscriber certificates issued by PublicCA are described as follows:

Certificate field	Organization certificate /PDF Signing certificate	OV SSL certificate	Personal certificate /PDF Signing certificate	IV SSL certificate	DV SSL certificate	Dedicated server application software certificate
subject:commonName (OID 2.5.4.3)	Δ	Δ	Δ	Δ	Δ	○

Certificate field	Organization certificate /PDF Signing certificate	OV SSL certificate	Personal certificate /PDF Signing certificate	IV SSL certificate	DV SSL certificate	Dedicated server application software certificate
subject:organizationName (OID 2.5.4.10)	○	○	Δ	Δ	×	○
subject:givenName (OID 2.5.4.42) and subject:surname (OID 2.5.4.4)	×	×	Δ	○	×	×
subject:streetAddress (OID 2.5.4.9)	Δ	Δ	Δ	Δ	×	×
subject:localityName (OID 2.5.4.7)	Δ	Δ	Δ	Δ	×	Δ
subject:stateOrProvinceName (OID 2.5.4.8)	Δ	Δ	Δ	Δ	×	Δ
subject:postalCode(OID 2.5.4.17)	Δ	Δ	Δ	Δ	×	×
subject:countryName(OID 2.5.4.6)	○	○	○	○	×	○
subject:organizationUnitName(OID 2.5.4.11)	Δ	Δ	Δ	Δ	Δ	Δ

Symbols' meaning:

Optional: Δ Required: ○ Prohibited: ×

7.1.4.3 Subject Information–CA Certificates

The CA certificates of PublicCA 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:

7.1.4.3.1 Subject Distinguished Name Field

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

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

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

The PDF Signing certificate issued by PublicCA uses 1.3.6.1.4.1.23459.100.0.9 for the OID.

7.1.7 Usage of Policy Constraints Extension

Certificates issued by PublicCA do not contain policy constraints extension.

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates issued by PublicCA 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 PublicCA are not marked as critical.

7.2 CRL Profile

7.2.1 Version Number(s)

PublicCA 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 PublicCA conform to the official versions of the ITU-T X.509, Baseline Requirements and RFC 5280.

7.3 OCSP Profile

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

7.3.1 Version Number(s)

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

- Version number, and
- Target certificate identifier

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

The OCSP response issued by 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
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;
- Signed certificate timestamp; and
- OID 1.3.6.1.4.1.11129.2.4.5 which is for CT.

7.3.3 Regulations for Operation of OCSP

The operation of OCSP in PublicCA 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 PublicCA with short-term validity, and it shall be issued and updated regularly by PublicCA.

8. Compliance Audit and Other Assessments

8.1 Frequency or Circumstances of Assessment

PublicCA 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.

8.2 Identity/Qualifications of Assessor

CHT retains a qualified auditor, who is familiar with the operations of PublicCA and is authorized by WebTrust for CA program as a licensed WebTrust practitioner to perform WebTrust Principles and Criteria for Certification Authorities and WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security audit schemes 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. PublicCA 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 PublicCA operations.

8.4 Topics Covered by Assessment

PublicCA undergoes an audit in accordance with the following schemes: “WebTrust for CAs v2.1 or newer” and “WebTrust for CAs SSL Baseline with Network Security v2.3 or newer”.

The assessment shall include the following topics:

(1) Whether PublicCA 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 PublicCA 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 PublicCA.

The RA responsible for the verification of certificate requests or revocation shall undergo the external audit annually; record every non-compliance or exceptions with respect to the ePKI CP and this CPS; and take actions to correct the deficiencies.

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

If an organization or business under a dedicated RA is unable to undergo the above external audit due to regulations or other factors, the RA may state their exclusion from the scope of audit for that year in an audit report or management's assertions but CHT reserves the rights to conduct

a compliance audit on whether or not the above RA is in compliance with the ePKI CP and this CPS to reduce any risk derived from any non-conformity. CHT has the right the conduct the following (but not limited to) review and examination items to ensure the trustworthiness of PublicCA:

(1) If there is an event of computer emergency or key compromise that causes CHT to reasonably suspect the dedicated RA is unable to comply with the ePKI CP and this CPS.
(2) If the compliance audit has not been completed or there are special developments, CHT has the right to conduct a risk management review.
(3) If action or inaction by the RA causes actual or potential security and integrity threat to the ePKI, CHT must conduct the related review or examination.

CHT has the right to retain a third-party auditor to perform audit and examination functions. The audited Dedicated RA shall provide full and reasonable cooperation to CHT and the personnel conducting the audit and examination.

During the period in which it issues SSL certificates, PublicCA must strictly control its service quality by performing ongoing self audits against a randomly selected sample of at least three percent of the SSL certificates (less than one counted as one) it has issued in the period beginning immediately after the last sample was taken in accordance with the Baseline Requirements and WebTrust for Certification Authorities - SSL Baseline with Network Security.

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 PublicCA or its RA, the following actions shall be taken:

(1) Note the discrepancy,

(2) Notify PublicCA about the discrepancy, and

(3) PublicCA 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, PublicCA shall make its audit report publicly available. Audit results are displayed with appropriate seals, including WebTrust for Certification Authorities and WebTrust for Certification Authorities – SSL Baseline Requirements seals, on PublicCA's homepage. The audit report and management's assertions may be viewed by clicking on the seals. PublicCA 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, PublicCA 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, issuance, and renewal between PublicCA 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

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

9.1.3 Revocation or Status Information Access Fees

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

9.1.4 Fees for Other Services

No charge at the moment.

9.1.5 Refund Policy

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

9.2 Financial Responsibility

9.2.1 Insurance Coverage

PublicCA is owned and operated by CHT. Its financial responsibilities are the responsibilities of CHT. PublicCA has taken out a Commercial General Liability insurance of USD 5 million in coverage and a Professional Liability/Errors & Omissions insurance of USD 10 million in coverage.

9.2.2 Other Assets

PublicCA finances are a part of the overall finances of CHT. CHT is a publicly listed company. In accordance with Article 36 of the Securities and Exchange Act, annual financial reports duly audited and attested by a certified public accountant, approved by the board of directors and recognized by the supervisors are publically announced and registered with the competent authority within three months after the close of each fiscal year. Financial reports duly reviewed by a certified public accountant and reported to the board of directors are publicly announced and registered within 45 days after the end of the first, second and third quarters of each fiscal year. The operating status for the preceding month is publicly announced and registered within the first 10 days of each month. PublicCA 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 PublicCA 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 PublicCA,
(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 PublicCA 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 PublicCA repository are not deemed confidential information.

9.3.3 Responsibility to Protect Confidential Information

PublicCA shall handle subscriber application information in accordance with the Electronic Signatures Act, WebTrust Principles and

Criteria for Certification Authorities audit criteria, Baseline Requirements, WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security audit criteria and Personal Information Protection Act.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

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

9.4.2 Information Treated as Private

The personal information listed on certificate applications should not be disclosed without the subscriber's consent or in accordance with related laws. Subscriber information that cannot be obtained through certificates, CRLs or certificate catalog service, identifiable information of personnel in PublicCA such as names together with palmprint or fingerprint biometrics, and personal information on confidentiality agreements or contracts are deemed private information which requires protection. PublicCA and its RAs 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 or suspension information and CRLs published in the PublicCA repository are not private information.

9.4.4 Responsibility to Protect Private Information

The personal information required for the operation of PublicCA, in either paper or digital form, must be security stored and protected in accordance with the personal information protection and privacy rights declaration posted on the website and must comply with the Electronic Signatures Act, WebTrust Principles and Criteria for Certification Authorities audit criteria, Baseline Requirements, WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security audit criteria and Personal Information Protection Act. PublicCA 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, PublicCA 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, PublicCA 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 PublicCA operations is handled in accordance with related laws 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 PublicCA:

(1) Key pairs and split keys of PublicCA and RA;
(2) Related documents or system development for certificate management of PublicCA;
(3) Certificates and CRLs issued by PublicCA; and
(4) This CPS.

This CPS may be freely downloaded from the PublicCA 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

PublicCA shall follow the procedures in Chapter 4 of this CPS to perform related certificate management work. PublicCA 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, suspend or resume certificates;
(5) Issue and publish CRLs;
(6) Issue and provide OCSP response messages;
(7) Securely generate PublicCA and RA private keys;

(8) Secure management of private keys;

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

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

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

9.6.2 RA Representations and Warranties

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

Certificate subject identity check is done for certificates issued by PublicCA. 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) Provide certificate application services,

(2) Perform certificate application identification and authentication,

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

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

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

(6) RA private keys are securely managed.

9.6.3 Subscriber Representations and Warranties

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

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

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

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

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

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

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

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

9.6.4 Relying Party Representations and Warranties

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

(1) Comply with the provisions of this CPS when using the certificates or checking the PublicCA repository;

(2) Check the certificate assurance level during use of certificates;

(3) Check the certificate and keyUsage field listed in the certificate prior to the use of the certificate;

(4) Check the CRL or OCSP response to determine if a certificate is valid prior to the use of certificates;

(5) Check the digital signature to determine if the certificate, CRL or OCSP response is correct when using certificates, CRL or OCSP response issued by PublicCA;

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

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

(8) Have understood and agreed to the legal liability clauses of PublicCA and will use the certificate in accordance with Section 1.4.1 when accepting the certificate.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

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

9.8 Limitations of Liability

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

9.9 Indemnities

9.9.1 Indemnification by PublicCA

If subscribers or relying parties suffer damages due to the intentional or unintentional failure of PublicCA to follow the ePKI CP, this CPS, relevant laws and the provisions of contracts signed between PublicCA, subscribers and related relying parties when processing subscriber certificate-related work, the subscriber shall request compensation in accordance with the relevant provisions of the contract signed between PublicCA and RA. Relying parties shall request compensation in accordance with relevant laws. The total compensation limit of PublicCA for each subscriber or relying party is shown in the Table below. If the subscriber 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 1	3,000
Level 2	100,000
Level 3	3,000,000

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

9.9.2 Indemnification by RA

If subscribers or relying parties suffer damages due to the RA intentional or unintentional failure to follow this CPS, related laws or the provisions of contracts signed between the RA and subscribers/relying parties when processing subscriber certification registrations, the RA shall be held liable. Compensation claims by subscribers shall be made in accordance with related provisions in the contract set down with the RA. Compensation claims by relying parties shall be made in accordance with relevant laws and regulations.

9.10 Term and Termination

9.10.1 Term

This CPS is effective when approved by the Electronic Signatures Act competent authority and published to PublicCA's repository.

9.10.2 Termination

The new version of this CPS is announced after being approved by the Electronic Signatures Act competent authority, and the current version is terminated.

9.10.3 Effect of Termination and Survival

The effect of this CPS remains valid until the expiration or revocation of the last certificate issued according to this CPS.

9.11 Individual Notices and Communications with Participants

PublicCA, 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

PublicCA 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 PublicCA 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 PublicCA, 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 PublicCA issued certificates, the applicable ROC laws shall govern.

9.15 Compliance with Applicable Law

Related ROC laws must be followed regarding the interpretation 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 (PublicCA, RAs, subscribers and relying parties).

9.16.2 Assignment

The participants, including PublicCA, 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 PublicCA.

9.16.3 Severability

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

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

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

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

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

9.16.5 Force Majeure

PublicCA 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 PublicCA, including natural disasters, wars, or terrorism which may cause the interruption of telecommunications network. PublicCA 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
AATL	Adobe Approved Trust Lis	
AIA	Authority Information Access	See Appendix 2.
AICPA	American Institute of Certified Public Accountants	See Appendix 2.
CA	Certification Authority	See Appendix 2.
CAA	Certification Authority Authorization	See Appendix 2.
CARL	Certification Authority Revocation List	See Appendix 2.
CMMI	Capability Maturity Model Integration	See Appendix 2.
CP	Certificate Policy	See Appendix 2.
CPA	Chartered Professional Accountants Canada	See Appendix 2.
CP OID	CP Object Identifier	
CPS	Certification Practice Statement	See Appendix 2.
CDN	Content Delivery Network	See Appendix 2.
CRL	Certificate Revocation List	See Appendix 2.
DN	Distinguished Name	
DNS	Domain Name System	See Appendix 2.
DV	Domain Validation	See Appendix 2.
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	See Appendix 2.

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

Appendix 2: Glossary

Access	Use the information processing capabilities of system resources
Access Control	Authorization procedure for access to information system resources given to subscribers, programs, procedures and other systems.
Activation Data	Private data, other than keys, that are required to access cryptographic modules and that need to be protected (i.e., unlock private keys for signing or decryption events).
American Institute of Certified Public Accountants (AICPA)	Institution which jointly drafted The Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy system standards with the Chartered Professional Accountants Canada and the management organization for WebTrust for CA and SSL Baseline Requirement and Network Security mark.
Applicant	Subscribers who request certificates from a CA and have not yet completed the certificate procedure.
Archive	A physically separate storage site for long-term information (storage site for important information) which can be used to support audit, usage and integrity services.
Assurance	A 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) 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.
Authentication	(1) The process of establishing confidence in user identities electronically presented to an information system. [NIST.SP.800-63-2 Electronic Authentication Guideline] (2) Safety measures used to secure data transmission or ways to authorize the privilege of individuals upon receiving certain types of information. (3) Authentication is the process by which a claimed identity is verified. [A Guide to Understanding Identification and Authentication in Trusted Systems] Mutual authentication means that the authentication is performed between two parties during communication.
Authority Information Access (AIA)	Records extensions related to certificate authority information access. The content may include: OCSP service sites and certificate issuance authority certificate verification path downloading

	site.
Authorization Domain Name	The Domain Name used to obtain authorization for certificate issuance for a given FQDN. The CA may use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. If the FQDN contains a wildcard character, then the CA MUST remove all wildcard labels from the left most portion of requested FQDN. The CA may prune zero or more labels from left to right until encountering a Base Domain Name and may use any one of the intermediate values for the purpose of domain validation.
Backup	Information or program copying that can be used for recovery purposes when needed.
Base Domain Name	The portion of an applied-for FQDN that is the first domain name node left of a registry controlled or public suffix plus the registry-controlled or public suffix (e.g. "example.co.uk" or "example.com"). For FQDNs where the right-most domain name node is a gTLD having ICANN Specification 13 in its registry agreement, the gTLD itself may be used as the Base Domain Name.
Baseline Requirements	“The Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates” issued by CA/Browser Forum, and all the amendments.
Binding	The process for binding (connecting) two related information elements.
Biometric	The physical or behavioral attributes of a person.
CA Certificate	Certificates issued by CAs.
CA Key Pair	A Key Pair where the Public Key appears as the Subject Public Key Info in one or more Root CA Certificate(s) and/or Subordinate CA Certificate(s).
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 this CPS specifically refers to ITU-T X.509 v.3 format certificates which states the certificate policy object identifier in the 'certificate policy' field.
Certification Authority (CA)	(1) The agency or natural person that issues certificate [Article 2-5, Electronic Signatures Act] (2) The competent body trusted by the subscriber. Its functions are the issuance and administration of ITU-T X.509 format public key certificates, CARLs and CRLs.
Certification Authority Authorization (CAA)	The certification authority authorization (CAA) DNS resource record allows a DNS domain name holder to specify one or more certification authorities (CAs) authorized to issue certificates for that domain. CAA resource records allow a public CA to implement additional controls to reduce the risk of unintended certificate mis-issue. [RFC 8659]
Certification Authority Revocation List (CARL)	A signed and time stamped list. The list contains the serial numbers of revoked CA The list contains the serial numbers of revoked CA public key certificates (including subordinate CA certificates and cross-certificates).
Certificate Policy	(1) Refers to a named set of rules that indicates the

(CP)	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 (CPS)	(1) External notification by the certificate authority used to describe the practice statement of the certificate authority governing certificate issuance and processing of other certification work. [Article 2-7, Electronic Signatures Act] (2) Announcement of a statement that certain procedures of the certificate authority for certificate work (including issuance, suspension, revocation, renewal and access) comply with certain requirements (listed in the certificate policy or other service contracts).
Certificate Profile	A set of documents or files that defines requirements for Certificate content and Certificate extensions in accordance with Section 7 of the Baseline Requirements. e.g. a Section in a CA's CPS or a certificate template file used by CA software.
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.
Chartered Professional Accountants Canada (CPA)	Institution which jointly drafted The Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy system standards with the American Institute of Certified Public Accountants (AICPA) and the management organization for WebTrust for CA and SSL Baseline Requirement & Network Security mark. Canadian Institute of Chartered Accountants is abbreviated as CICA.
Compromise	Information disclosed to unauthorized persons or unauthorized intentional or unintentional disclosure, modification, destruction or loss of objects which constitutes a violation of information security policy.
Confidentiality	Information which will not be known or be accessed by unauthorized entities or programs.
Content Delivery Network (CDN)	Use Internet interconnection with computer network systems to provide a highly efficient, expandable, low cost network for transmit content to users.
Cross-Certificate	A certificate used to establish a trust relationship between two root CA. This certificate is a type of CA certificate and not a subscriber certificate.
Cryptographic Module	A set of hardware, software, firmware or combination of the above used to run cryptologic or programs (including crypto algorithms) and included within the cryptographic boundaries of the module.
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 Contact	The Domain Name Registrant, technical contact, or administrative contract (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record.
Domain Name	A node label assigned by the domain name system. Converts the IP address into a text name that is easily remembered by humans.
Domain Name Registrant	Sometimes referred to as the domain name owner, but it is more appropriate to say a certain individual or entity who have registered with the Domain Name Registrar to have the right to use a domain name and the Domain Name Registrant or WHOIS has listed the 'registrant' as a natural person or legal person.
Domain Name Registrar	A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns).
Domain Name System (DNS)	A distributed database used to automatically convert the IP address to domain name.
DNS CAA Email Contact	The email address defined in BR Section A.1.1.
DNS TXT Record Email Contact	The email address defined in BR Section A.2.1.
Domain Validation (DV)	Before SSL certificate approval and issuance, authentication of subscriber domain name control rights but no authentication of subscriber

	organization or individual identity, therefore, connection to a domain validation SSL certificate installed websites is able to provide SSL encryption channels but is unable to know who the owner of the website is.
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.
End-Entity Certificate	Certificates issued to end-entities.
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.
Chunghwa Telecom Certificate Policy Management Authority (PMA)	An organization which was established for electronic certificate management matters, such as (i) discussion and review of the CP and the electronic certificate framework of the PKI owned by CHT and (ii) review of interoperation requests submitted by subordinate 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	Except for military organizations in the US Federal Government System, information processing

Processing Standard (FIPS)	standard for all government organizations and government subcontractors. The security requirement standard for the cryptographic module is FIPS no. 140 standard (FIPS 140). FIPS 140-2 divides the cryptographic module into 11 types of security requirements. Each security requirement type is then divided into 4 security levels.
Firewall	An access restriction gateway between networks which complies with near-end (local area) security policy.
Fully Qualified Domain Name (FQDN)	An unambiguous domain name that specifies the exact location of a computer within the domain's hierarchy. The fully qualified domain name consists of two parts: the host name (service name) and domain name. For example, ourserver.ourdomain.com.tw, ourserver is the host name and ourdomain.com.tw is the domain name. In this name, ourdomain is the third-level domain, com is the second-level domain name and tw is the country code top-level domain (ccTLD). A fully qualified domain name always starts with a host name. For example, www.ourdomain.com，www is the host name. Ourdomain is the the second-level domain name. com is Generic Top-Level Domain, gTLD.
High Risk Certificate Request	The CA marks the request to be referred to the internal standards maintained by the CA and other database for reviewing. They may include the high-risk names used for phishing or other wrongful purposes, Miller Smiles phishing list, Google Safe Browsing list, or the names identified by the CA with the risk-reducing standards.
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.

Individual Validation (IV)	Except for identification and authentication of natural person subscriber's domain control rights, identification and authentication of subscriber personal identity according to the certificate's assurance level during the SSL certificate approval process. Therefore, linking to the install IV SSL certificate website can provide a TLS encryption channel. It is known which individual is the owner of that website to ensure the integrity of data transmission.
Integrity	Protecting information so that it is not subject to unauthorized modification or damage. Preserve information in an untampered state during transmission and storage following generation at its source until receipt by the final recipient.
Internationalized Domain Name (IDN)	A kind of internet domain name, including at least one script or alphabetic character of one specific language, and then encoded with Punycode, and used for the domain name service only accepting ASCII codes.
Internet Assigned Numbers Authority (IANA)	An organization that oversees the allocation of global IP address, domain names and many other parameters used for Internet.
Internet Engineering Task Force (IETF)	Responsible for the development and promotion of Internet standards. Official website is at: https://www.ietf.org/. Its vision is the generation of high quality technical documents affects how man designs, uses and manages the Internet and allows the Internet to operate smoothly.
Issuing CA	For a particular certificate, the CA that issues the certificate is the issuing CA.
Key Escrow	Storage of related information using the subscriber's private key and according to the terms of the mandatory subscriber escrow agreement (or similar contract). The terms of this escrow agreement requires that one or more than one agencies have possession of the subscriber key provided it is beneficial to the subscriber, employer or another party in accordance with the provisions of the agreement.

Key Exchange	Mutual exchange of keys to establish a secure communication processing procedure.
Key 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.
OCSP Stapling	This is a form of TLS/SSL Certificate Status Request extension, which may replace the OCSP to check X.509 certificate status. In practice, a website may obtain a "time limited (e.g. two hours)" OCSP response from the OCSP Responder and cache it. Next, this cached OCSP response will be sent to the subscriber (typically a browser) whenever initiating the TLS Handshake. The subscriber only needs to verify the validity of that OCSP response without sending the request of OCSP to the CA. In that way, the subscriber will not need to request the TLS/SSL certificate status from the CA when connecting to a high traffic TLS website, and thus to decrease the burden of the CA. This mechanism also prevents the privacy concern that the OCSP Responder knows which subscribers attempting to browsing that TLS website by having the TLS website referring the TLS/SSL certificate validity message issued regularly by the OCSP Responder to the CA.
Out-of-Band	Delivery method other than ordinary information delivery channels. If the delivery method is by electric cable, a special secure channel may be the use of physical registered mail.
Organization Validation, (OV)	In the SSL certificate approval process, except for identification and authentication of subscriber domain name control rights, following the certificate assurance level to identify and authenticate the identity of subscriber organizations and individuals. Therefore, connection to a website installed by an Organization Validation SSL certificate is able to provide SSL encryption channels, in order to know who is the owner of the website and ensure the integrity of the transmitted information.
Private Key	(1) The key in the signature key pair used to

	generate digital signatures. (2) The key in the encryption key pair used to decrypt secret information. This key must be kept secret under these two circumstances.
Public Key	(1) The key in the signature key pair used to verify the validity of the digital signature. (2) The key in the encryption key pair used for encrypting secret information. These keys must be made public (usually in a digital certificate form) under these two circumstances.
Public-Key Cryptography Standard (PKCS)	In order to promote the use of public key technology, the RSA laboratory under the RSA Information Security Company has developed a series of public key cryptography standards that are widely used by the industry.
Public Key Infrastructure (PKI)	A set of law, policy, standards, personnel, equipment, facilities, technology, processes, audits and services developed on a broad scale and management of asymmetric cryptography and public key certificates.
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.
Random Value	A value specified by a CA to the Applicant that exhibits at least 112 bits of entropy.
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.
Request Token	A value derived in a method specified by the CA which binds this demonstration of control to the certificate request. The Request Token SHALL incorporate the key used in the certificate request. A Request Token MAY include a timestamp to indicate when it was created. A Request Token MAY include other information to ensure its uniqueness. A Request Token that includes a timestamp SHALL remain valid for no more than 30 days from the time of creation. A Request Token that includes a timestamp SHALL be treated as invalid if its timestamp is in the future. A Request Token that does not include a timestamp is valid for a single use and the CA SHALL NOT re-use it for a subsequent validation. The binding SHALL use a digital signature algorithm or a cryptographic hash algorithm at least as strong as that to be used in signing the certificate request.
Required Website Content	Either a Random Value or a Request Token, together with additional information that uniquely identifies the Subscriber, as specified by the CA.
Reserved IP Addresses	IPv4 and IPv6 addresses reserved in the IANA setting. See: http://www.iana.org/assignments/ipv4-address-

	space/ipv4-address-space.xml and http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml
Revoke a Certificate	Termination of a certificate prior to its expiry date.
Request for Comments (RFC)	A series of memos issued by the Internet Engineer Task Force that include Internet, UNIX and Internet community standards, protocols and procedures for number assignment.
Secure 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.
Transport Layer Security (TLS)	TLS 1.0 was first defined in RFC 2246 by the IETF 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]
WHOIS	Information retrieved directly from the Domain Name Registrar or registry operator via the protocol defined in RFC 3912, the Registry Data Access Protocol defined in RFC 7482, or an HTTPS website.
Zeroize	Method to delete electronically stored information. Storage of changed information to prevent information recovery.