ePKI EV SSL Certification Authority Certification Practice Statement of Chunghwa Telecom (ePKI EV SSL CA CPS)

Version 1.1

Chunghwa Telecom Co., Ltd.

March 14, 2018

Contents

ePKI EV SSL Certification Authority Certification Practice Statement of Chunghwa Telecom Abstract

Chunghwa Telecom Co., Ltd. has established the Certification Practice Statement (CPS) of the ePKI EV SSL Certification Authority of Chunghwa Telecom (ePKI EV SSL Certification Authority) in accordance with Article 11 of the Electronic Signatures Act and the Regulations on Required Information for Certification Practice Statements promulgated by the Ministry of Economic Affairs (MOEA). Establishment and revision of the CPS shall be published in the company website after approval by the competent authorities for issuance of certification service.

I. Competent Authority Approval No.: Chin-Shang-Tzu No. 10702216460

II. Types of Issued Certificates:

Extended Validation SSL Certificates (EV SSL certificates).

EV SSL certificates are issued to properties such as computers and communications equipment (e.g., router, firewall, database security audit software) or application software (e.g., web server, e-mail server, application server or Lync server) owned by Private Organization, Government Entity, Non-Commercial Entity, and Business Entity.

III. Certificate Assurance Levels:

The ePKI EV SSL Certification Authority operates in accordance with relevant regulations of the Certification Policy (CP) of the Chunghwa Telecom ecommerce Public Key Infrastructure (ePKI) and CA/Browser Forum Guidelines for the Issuance and Management of Extended

Validation Certificates and issues EV SSL certificates with the assurance level 3 as defined in the CP in accordance with the identity authentication procedures of the certificate applicants (See section 1.4.1).

IV. Applicable Scope:

The EV SSL certificates issued by the ePKI EV SSL Certification Authority are used for identification and data protection required by Internet and financial transactions of e-commerce and e-government and provide a strong certification and extremely high level of protection especially high monetary or high property value transaction or environments where high probability of fraud risk or malicious access (e.g. internet fraud, leaking of personal information, leaking of confidential information) exists.

Subscribers and related relying parties of the ePKI EV SSL Certification Authority must exercise due care in the use of certificates issued by the ePKI EV SSL Certification Authority and must not depart from the CPS, relevant laws and regulations and the certificate usage restrictions and prohibitions stipulated in contracts between the ePKI EV SSL Certification Authority, subscribers and relevant relying parties.

V. Important Matters Regarding Legal Responsibilities

1. Damage Indemnification Responsibility of the ePKI EV SSL Certification Authority and Registration Authority (RA)

   In the event that damages are suffered by subscribers or relying parties in relevant certification operations of the ePKI EV SSL Certification Authority and the registration authority due to intention or negligence to follow the CPS and relevant operation regulations, the ePKI EV SSL Certification Authority or the RA shall respectively be responsible for indemnity. The subscriber may make an indemnity claim in accordance with relevant provisions of the contract with the ePKI EV SSL Certification Authority or the RA; and the relying party is entitled to make an indemnity claim in accordance with relevant laws and regulations. The ePKI EV SSL Certification Authority and the RA has a NT$10,000,000 total compensation limit for each subscriber or relying party. If a contract entered into between the subscriber or relying party and the Company or RA has listed any extra stipulations regarding the scope of application of the certificate and transaction compensation limit, then it shall be dealt with accordingly.

2. Exemption of Responsibility of the ePKI EV SSL Certification Authority

   In the event that damages occur due to subscriber or related relying party failure to follow the CPS, relevant laws and regulations or the contract set down between the ePKI EV SSL Certification Authority, the subscriber and the relevant relying party or any damages occur that are not attributable to the ePKI EV SSL Certification Authority, that subscriber or the relying party shall bear sole liability.

3. Exemption of Responsibility of the Registration Authority

   In the event that a relying party suffers damages due to reasons attributable to the subscriber or any damages occur due to reasons not attributable to the RA, that subscriber or relying party shall bear sole liability.

In the event that damages occur due to subscriber or related relying party failure to follow the CPS, relevant laws and regulations or the contract entered into between the ePKI EV SSL Certification Authority, the subscriber and the relevant relying party or any damages occur that are not attributable to the RA, that subscriber or the relying party shall bear sole liability.

4. Exemption Provisions

In the event that damages are caused by a force majeure or reasons not attributable to the ePKI EV SSL Certification Authority and RA, the ePKI EV SSL Certification Authority and the RA shall not bear any legal responsibility. If the damages occurred due to exceeding the clear usage limitations set down by the ePKI EV SSL Certification Authority and RA, the ePKI EV SSL Certification Authority and the RA shall not bear any legal responsibility.

In the event that some certification services have to be suspended temporarily because of system maintenance, conversion or expansion of the ePKI EV SSL Certification Authority, the ePKI EV SSL Certification Authority may give advance notification in the repository to temporarily suspend certificate service. Subscribers or relying parties may not request compensation for damages from the ePKI EV SSL Certification Authority based on the above-mentioned actions.

5. Financial Responsibility

The ePKI EV SSL Certification Authority has financial guaranty from Chunghwa Telecom Co., Ltd. The ePKI EV SSL

Certification Authority shall perform financial audits in accordance with relevant laws and regulations. The Company has taken out a general liability insurance policy with a maximum liability amount of NT$120,000,000. The Company's finances are sound and the annual financial report signed by a CPA shows that the liquid assets exceed US$500 million and the Quick Ratio (ratio of liquid assets to current liabilities) is not less than 1.0, so the Company not only conforms to the requirements of the EV SSL Certificate Guideline but also has sufficient compensation ability when damages occur.

6. Subscriber Obligations

Subscribers shall properly safeguard and use their private keys. Suspension, revocation, renewal or re-issuance of subscriber certificates shall conform to the regulations in Chapter 4 of the CPS but the subscriber shall assume the obligations of all use of the certificate before any changes are made.

VI. Other Important Matters

1. The registration work of RAs belonging to the ePKI EV SSL Certification Authority is authorized by the ePKI EV SSL Certification Authority.

2. The subscriber must comply with the relevant regulations of the CPS and ensure that all of the submitted application information is correct.

3. The relying party must confirm the accuracy, validity and usage restrictions of the certificate being relied on in order to

reasonably rely on the certificates issued by the ePKI EV SSL Certification Authority.

4. The Company shall retain an impartial third party to conduct audits of ePKI EV SSL Certification Authority operations. The audit standards are Trust Service Principles and Criteria for Certification Authorities, WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security Version and WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL.

5. Audit results are displayed on the front page of the ePKI EV SSL Certification Authority website using WebTrust® for CA, WebTrust® for Certification Authorities – EV SSL Seal and WebTrust® for Certification Authorities – SSL Baseline Requirements Seal methods. The compliance audit report and management declaration may be viewed by clicking on the seal.

CPS Version Control

Version	Date	Revision Summary
1.0	July 26, 2016	First Release.
1.1(20170714)	July 14, 2017	1. Amendment of Section 3.2.5 about Domain Name Validation, Appendix 2. 2. Minor Change about Summary, Section 1.4.1, Section 2.1, Section 2.3, Section 3.1.2.2, Section 3.2.2.6.2, Section 3.2.2.7, Section 4.2, Section 4.9, Section 6.1 and so on.
1.1(20171023)	October 23, 2017	Minor Change such as Section 5.1、Sction 5.2、Section 6.2、Section 6.3、Chapter 7 and so on.
1.1(20180126)	January 26, 2018	Minor revisions about Section 6.1.6 & 6.2.6.
1.1(20180214)	February 14, 2018	Add Version Control.
1.1	March 14, 2018	Add Competent Authority Approval No.: Chin-Shang-Tzu No. 10702216460 in Abstract.

1. Introduction

1.1 Overview

1.1.1 Certification Practice Statement

The name of this document is ePKI EV SSL Certification Authority Certification Practice Statement (CPS) of Chunghwa Telecom. The CPS is stipulated to follow the Certification Policy (CP) for the Chunghwa Telecom ecommerce Public Key Infrastructure and complies with related international standards such as the Internet Engineering Task Force (IETF) RFC 3647, ITU-T X.509, IETF PKIX Working Group RFC 5280, CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (the Baseline Requirements), CA/Browser Forum Network and Certificate System Security Requirements, and CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates (EV SSL Certificate Guidelines).

The ePKI EV SSL Certification Authority is the Level 1 Subordinate CA of the Chunghwa Telecom e-commerce Public Key Infrastructure (ePKI) and is responsible for the issuance and management of Extended Validation (EV) SSL Certificates.

The primary purposes of an EV SSL Certificate are:

(1) to identify the legal entity that controls a Web site: Provide a reasonable assurance to the user of an Internet browser that the Web site the user is accessing is controlled by a specific legal entity identified in the EV Certificate by name, address of Place of Business, Jurisdiction of Incorporation or Registration and Registration Number or other disambiguating information; and

(2) to secure website communications with encryption: Facilitate the exchange of encryption keys in order to enable the encrypted communication of information over the Internet between the user of an Internet browser and a Web site.

The secondary purposes of an EV SSL Certificate are to help establish the legitimacy of a business claiming to operate a Web site or distribute executable code, and to provide a vehicle that can be used to assist in addressing problems related to phishing, malware, and other forms of online identity fraud. By providing more reliable third-party verified identity and address information regarding the business, EV SSL Certificates may help to:

(1) Make it more difficult to mount phishing and other online identity fraud attacks using Certificates;

(2) Assist companies that may be the target of phishing attacks or online identity fraud by providing them with a tool to better identify themselves to users; and

(3) Assist law enforcement organizations in their investigations of phishing and other online identity fraud, including where appropriate, contacting, investigating, or taking legal action against the Subject.

The Chunghwa Telecom ePKI Root Certification Authority (eCA) is the highest-level CA and trust anchor of the ePKI and Chunghwa Telecom Co., Ltd. is responsible for operation and setup. Relying parties can directly trust the certificates of the eCA itself.

1.1.2 CPS Applicability

The practice statement stipulated in this CPS applies to the ePKI EV SSL Certification Authority, Registration Authority (RA), subscribers, relying parties and the repository.

1.2 Document Name and Identification

This version is 1.1 and the issue date of this version is March 14, 2018. The latest version of this CPS can be obtained from:

http://ev.hinet.net or http://evssl.hinet.net

The EV SSL certificates issued by the ePKI SSL Certification Authority conform to the EV SSL Certificate Guidelines and the individually negotiated certificate processing methods supported by application software providers (such as browsers or application system providers) and use the CA/Browser Forum extended validation (EV) SSL certificate policy object identifier ({joint- iso- itu- t(2) international-organizations (23) ca- browser- forum(140) certificate- policies(1) ev-guidelines (1) }(2.23.140.1.1)). If there are items which are not defined in the EV SSL Certificate Guidelines, operations shall follow the ePKI CP assurance level 3.

This CPS conforms to the current version of the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates and the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org. If there are any inconsistencies between this CPS and the latest version of the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates and the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, the provisions of the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates and the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates shall take precedence.

1.3 PKI Participants

The key members of the ePKI EV SSL Certification Authority include:

(1) ePKI EV SSL Certification Authority

(2) RA

(3) Subscribers

(4) Relying Parties

1.3.1 ePKI EV SSL Certification Authority

The ePKI EV SSL Certification Authority, established and operated by Chunghwa Telecom Co., Ltd., operates and issues EV SSL certificates in accordance with the ePKI CP regulations.

1.3.2 RA

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

ePKI EV SSL CA RA is divided into two major categories: general RA and dedicated RA. Dedicated RA are set up and operated independently by customers that is recognized by the Company or have signed contracts with the Company.

The ePKI EV SSL CA does not permit any delegated third party to be the EV 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 the ePKI EV SSL CA but is delegated to assist the certificate management procedure, and is not covered by the external audit of the ePKI EV SSL CA.

1.3.3 Subscribers

Any Private Organization, Government Entity, Non-Commercial Entity, and Business Entity that has applied to the ePKI EV SSL Certification Authority to issue a certificate and has not yet completed the certificate issuing procedure are referred to as the Applicant. Subscribers refer to the subject who has applied for and obtained a certificate issued by the ePKI EV SSL Certification Authority. The relationship between the subscriber and certificate subject is listed in the table below:

Certification subject	Subscriber
Equipment	Owner of equipment
Application software	Owner of application software

Generation of subscriber key pairs shall conform to the regulations in section 6.1.1 of the CPS. The subscriber must solely possess the right and capability to control the private key that corresponds to the certificate. Subscribers may not issue certificates themselves 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

The ePKI EV SSL Certification Authority selects other authorities, which provide related trust services as the collaborative partners, the related information shall be disclosed on the website and the collaboration mechanism and mutual rights and obligations shall be set down in the CPS to ensure the efficiency and reliability of ePKI EV SSL Certification Authority quality.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

EV SSL certificates (including certificates for signature and encryption use) defined as assurance level 3 by the ePKI CP can be applied to transport layer security (TLS) and secure socket layer (SSL) communication protocol server application software. EV SSL certificates are classified as single domain name EV SSL certificates or multi-domain name EV SSL certificates.

The assurance level, authentication method, scope of usage, and risk and consequences for the EV SSL certificates issued by the ePKI EV SSL Certification Authority are as follows:

Assurance Level and Certificate Type	Authentication Method	Scope of Usage	Risk and Consequences
Level 3 EV SSL certificate	Follow CA/Browser Forum Guidelines for the Issuance	Provide communication channel encryption and must	Provide a strong certification and extremely high level of security and protection to the following

	and Management of Extended Validation Certificates to authenticate which organization is the owner of the remote domain names and webpage service and the verification of the presence of Jurisdiction of Incorporation for that organization and participate in certificate transparency to prevent mis-issuance of certificates.	authenticate which organization is the owner of the domain for application to network communication protection. Browser will show the green address bar and directly display the organization information of EV SSL certificate subject to facilitate subscriber to identify the certificate holder.	circumstances (including but not limited to): (1) Transactions with high monetary or property value; (2) Internet transactions where high probability of malicious access (e.g. internet frauds, leaking of personal information and/or confidential information) exists.

Subscribers and relying parties must carefully read the CPS and watch for CPS updates before using and trusting the certificate services provided by the ePKI EV SSL Certification Authority.

1.4.2 Restricted Certificate Uses

Subscribers shall carefully select trustworthy computer environments and application systems before private key use to prevent loss of rights due to theft or misuse of private keys by malicious hardware or software.

Relying parties shall check if the certificate type, assurance level and keyUsage conforms to use requirements before the certificate is issued by the ePKI EV SSL Certification Authority.

Relying parties shall appropriately use the individual key in accordance with the keyUsage recorded on the certificate stipulated in section 6.1.7 and correctly process the certificate attribute information listed in the certificate extension marked as critical.

1.4.3 Prohibited Certificate Uses

Use of the certificates issued by the ePKI EV SSL Certification Authority is prohibited for the following purposes:

(1) Crime

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

(3) Operation of nuclear equipment

(4) Aviation flight and control systems

(5) Scope of prohibitions announced under the law

1.5 Policy Administration

1.5.1 Organization Administering the Document

Chunghwa Telecom Co., Ltd.

1.5.2 Contact Person

If you have any questions regarding this CPS or a subscriber wishes to report a missing key, you may directly contact the ePKI EV SSL Certification Authority.

Phone: 0800080365

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

E-mail: caservice@cht.com.tw

If there is any other contact information or changes to the contact information, please check the following website: http://ev.hinet.net or http://evssl.hinet.net

1.5.3 Person Determining CPS Suitability for the Policy

The ePKI EV SSL Certification Authority shall first check whether the CPS conforms to relevant CP regulations and then submit the CPS to the ePKI Policy Management Committee for review and approval. After approval, the ePKI EV SSL Certification Authority shall officially use the CP established for this ePKI.

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

The ePKI EV SSL Certification Authority conducts regular self-audits to prove operations comply with the assurance level used with the CP. In order to ensure smooth operation of certificates by the CAs under the ePKI by operating systems, browsers, and software platforms, the ePKI has already applied to participate in the root certificate programs for operating systems, browsers and software platforms. The self-signed certificates issued by the ePKI Root Certification Authority (eCA) are widely deployed in the CA trust lists of software platforms. According to the regulations of the root certificate program, external audits of the eCA and ePKI EV SSL Certification Authority are conducted annually and the latest CPS as well as the external audit results are submitted to the root certificate programs. The ePKI EV SSL Certification Authority also continues to maintain the audit seal published in the ePKI EV SSL Certification Authority website.

1.5.4 CPS Approval Procedure

The CPS is published by the ePKI EV SSL Certification Authority following approval by the MOEA, the competent authority of the Electronic Signatures Act.

After the CPS revisions take effect, the revised CPS content shall take precedence in the event of a discrepancy between the revised and original CPS content unless stipulated otherwise. If the revisions are made by attached 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 a table of abbreviations and definitions and Appendix 2 for the glossary.

2. Publishing and Repository Responsibilities

2.1 Repository Responsibility

The ePKI EV SSL Certification Authority repository is responsible for the publication and storage of the ePKI EV SSL Certification Authority issued certificates, certificate revocation lists (CRL), CPS and CP and also provides inquiry services to subscribers and relying parties. The repository provides 24-hour round-the-clock service. The Internet address of the ePKI EV SSL Certification Authority repository is: http://evssl.hinet.net or http://evssl.hinet.nethttp://ev.hinet.net. The repository will resume normal operation within two working days if unable to operate normally for some reason.

The responsibility of the repository includes:

(1) Regularly publish issued certificates, and revoked certificates and CRL in accordance with section 2.2.

(2) Publish the latest CPS and CP information.

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

(4) Publish external audit results. (as specified in Section 8.6)

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

2.2 Publication of ePKI EV SSL Certification Authority Information

(1) This CPS and CP.

(2) CRLs.

(3) ePKI EV SSL Certification Authority 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) The latest ePKI EV SSL Certification Authority-related news.

(7) Subscriber agreement.

(8) The latest external audit results (as specified in Section 8.6).

(9) The URLs of the test websites (valid, expired, revoked) which install EV SSL certificates issued by the ePKI EV SSL CA for application software providers to test.

2.3 Time or Frequency of Publication

(1) The CPS shall be published in the ePKI EV SSL CA repository within seven calendar days upon receiving the competent authority’s approval document.

(2) The CP complied with by the ePKI EV SSL CA is published in the repository within seven calendar days upon the approval of Committee of Certificate Policy for the Chunghwa Telecom eCommerce Public Key Infrastructure.

(3) CRLs are issued by the ePKI EV SSL CA at least twice a day and

published in the repository.

(4) The ePKI EV SSL CA’s own certificates are published in the repository within seven calendar days after accepting issuance by an upper level eCA.

2.4 Access Controls on Repositories

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

The information published by the ePKI EV SSL Certification Authority under section 2.2 is primarily provided for browser inquiries by subscribers and relying parties. As a result, access control should be implemented when providing access for viewing to guarantee repository security and maintain accessibility and availability.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

The ePKI EV SSL Certification Authority uses the X.500 Distinguished Name (DN) for the certificate subject name of issued certificates.

3.1.2 Need for Names to be Meaningful

The certificate subject names of certificates issued by the ePKI EV SSL Certification Authority shall comply with our country's related subject naming rules. The names should be sufficient to represent the subject name.

The subject name and subject alternative name on the EV SSL certificate shall follow the Baseline Requirements and may not use internal names or reserved IP addresses. EV SSL certificate subject name shall include the type of business organization (OID 2.5.4.15) of the applicant verified by article 3.2.2. If the organization of the applicant is a private organization, the business type must be listed as 'Private Organization'. If it is a government organization (agency), it must be listed as 'Government Entity'. If it is another type of business entity, it must be listed as 'Business Entity'. If it is a non-commercial entity (international)), it must be listed as a 'Non-Commercial Entity'), the national code (OID 1.3.6.1.4.1.311.60.2.1.3) for the organization registration jurisdiction area of the applicant, the city or town name (localityName, OID 2.5.4.7) for the organization's registered business address of the application and organization identity information (placed in the organization name field (OID 2.5.4.11) of the application.

According to Article 9.2 of the EV SSL Certificate Guidelines, the EV SSL certificate field 'subject' content can be subdivided into required attributes, optional attributes and deprecated attributes which are organized in the table below:

Table 3-1: Required / Optional / Deprecated Attributes of the EV SSL Certificate Field Subject

Certificate Field Attribute Name	Object Identifier(OID)	Required Attribute	Optional Attribute
Organization name (organizationName)	2.5.4.10	●	
Common name (commonName)	2.5.4.3		●
Business category (businessCategory)	2.5.4.15	●	
Country code of registered jurisdiction area (jurisdictionCountryName)	1.3.6.1.4.1.311.60.2.1.3	●	
State or province name of registered jurisdiction area (jurisdictionStateOrProvinceName)	1.3.6.1.4.1.311.60.2.1.2		●
City or town name of registered jurisdiction area (jurisdictionLocalityName)	1.3.6.1.4.1.311.60.2.1.1		●
Identification code (serialNumber)	2.5.4.5	●	
Country code of the actual business premises address (countryName)	2.5.4.6	●	
State or province name of the actual business premises address (stateOrProvinceName)	2.5.4.8		●
City or town name of the actual business premises	2.5.4.7	●	

Certificate Field Attribute Name	Object Identifier(OID)	Required Attribute	Optional Attribute
address (localityName)			
Street address of the actual business premises address (streetAddress)	2.5.4.9		●
Postal code of the actual business premises address (postalCode)	2.5.4.17		●
Actual organization name of the actual business premises (organizationUnitName)	2.5.4.11		●

3.1.2.1 Required Certificate Field

(1) organizationName

According to section 9.2.1 in the EV SSL Certificate Guidelines, the EV SSL certificate field subject must include the 'organization name' attribute. Its content is the official organization name of the certificate subject and that name must be the formal name registered with the agency in the jurisdictional area or registration agency or an organization name verified by section 3.2.2 of the CPS.

ePKI EV SSL Certification Authority and RA can abbreviate the beginning or end of the organization name. For example: the organization name 'Company Name Incorporated' recorded by the official agency is changed to 'Company Name, Inc.' and the content of this abbreviation must allow the certificate subject which is established or registered in the jurisdictional area to be easily distinguished. In addition, if a pseudonym is used for the certificate subject, then the pseudonym can be placed at the beginning of the attribute content and then indicate the official organization name of the certificate subject afterwards in parenthesis.

If the organization name length exceeds 64 characters, the organization name may be abbreviated or non-essential words in the organization name may be omitted. The RA must follow the section 11.12.1 of the EV SSL

Certificate Guidelines regarding high risk certificate requests to examine the attribute content and check if the relying parties can clearly distinguish the relationship between the certificate subject and revised organization name so that the certificate subject will not be confused with another organization. In the event that the above conditions cannot be fulfilled, the ePKI EV SSL Certification Authority shall not issue the EV SSL certificate.

(2) Business Category (businessCategory)

According to section 9.2.4 in the EV SSL Certificate Guidelines, the EV SSL certificate field subject must include the 'business category' attribute to differentiate the business category of the EV SSL certificate subject. The attribute content can be 'Private Organization', 'Government Entity', 'Business Entity' and 'Non-Commercial Entity' to indicate whether it is a private organization, government agency (authority), other business group or non-profit international organization. Only one may be selected.

(3) Country Code of Registration Jurisdictional Area (jurisdictionCountryName)

According to section 9.2.5 in the EV SSL Certificate Guidelines, the EV SSL certificate field subject must record the organization level related information of the jurisdiction of the Incorporating or Registration Agency to which the certificate subject is registered including: country, state or province, or city / town information. These applicable conditions are as follows:

When the organization level of the jurisdiction of the Incorporating or Registration Agency to which the certificate subject is registered is a country, then the EV SSL certificate field subject must include the attribute 'Country code of the registration jurisdiction' which is used to record the country in which the Incorporating or Registration Agency is located but shall not include the attributes 'State or province name of the registration jurisdiction' and 'City or town name of the registration jurisdiction'.

When the organization level of the jurisdiction of the Incorporating or Registration Agency to which the certificate subject is registered is a state or province, then the EV SSL certificate field subject must include the attribute

‘Country code of the registration jurisdiction’ and ‘State or province name of the registration jurisdiction’ which is used to record the country and state or province in which the Incorporating or Registration Agency is located but shall not include the attribute ‘City or town name of the registration jurisdiction’.

When the organization level of the jurisdiction of the Incorporating or Registration Agency to which the certificate subject is registered is a city or town, then the EV SSL certificate field subject must include the attribute ‘Country code of the registration jurisdiction’, ‘State or province name of the registration jurisdiction’ and ‘City or town name of the registration jurisdiction’ which is used to record the country, state or province and city or town in which the Incorporating or Registration Agency is located.

Therefore, the EV SSL certificate field subject must include the attribute ‘Country code of the registration jurisdiction’ recording the country of the jurisdiction of the Incorporating or Registration Agency in which the certificate subject is registered and the country code indicating conformance with ISO international standard requirements.

(4) Identification Code (serialNumber)

According to section 9.2.6 of the EV SSL Certificate Guidelines, the EV SSL certificate field subject must include the ‘Identification code’ attribute. Its content may be determined based on the individual business category. For example:

> If the certificate subject is a private organization, then the identification code content must be the unique registration serial number (standard term used by the CPS is ‘registration number’) provided by RA or Registration Agency of the registration jurisdiction such as the tax ID number. If not provided, then change by indicating the establishment or registration date.

If the certificate subject is a government entity and there is no registration number or readily verifiable date of creation, then the identification code content must have suitable language to indicate that the certificate subject is a government entity.

If the certificate subject is some other business group, the identification code content must be the registration code provided by the government registration agency. If not provided, then change by indicating the establishment or registration date.

(5) Country Code (countryName) of Actual Business Premises Address

According to section 9.2.7 in the EV SSL Certificate Guidelines, the EV SSL certificate field subject must include the ‘country code of the actual business premises address’ attribute which is used to record the country of the actual business premises address of the certificate subject.

(6) State or Province Name (stateOrProvinceName) of the Actual Business Premises Address

According to section 9.2.7 in the EV SSL Certificate Guidelines, the EV SSL certificate field subject must include the ‘state or province name of the actual business premises address’ attribute which is used to record the state or province where the actual business premises address of the certificate subject is located. If there is related information in the actual address, it must be provided.

(7) City or Town Name (localityName) of the Actual Business Premises Address

According to section 9.2.7 in the EV SSL Certificate Guidelines, the EV SSL certificate field subject must include the ‘city or town name of the actual business premises address’ attribute which is used to record the city or town where the actual business premises address is located.

3.1.2.2 Optional Certificate Field

(1) State or Province Name of Registration Jurisdiction (jurisdictionStateOrProvinceName)

The attribute is defined based on the circumstance. If the organization level of the jurisdiction of the Incorporating or Registration Agency to which the certificate subject is registered is a state or province or a city or town for the statement of the ‘country code of the registration jurisdiction’ in the above required attributes, then the EV SSL certificate field subject not only must include the attribute ‘country code of the registration jurisdiction’ but also must include the attribute ‘state or province name of the registration jurisdiction’ which is used to record the state or province name of the registration jurisdiction in which the Incorporating or Registration Agency is located and the state or province name must be a complete name.

If the organization level of the jurisdiction of the Incorporating or Registration Agency to which the certificate subject is registered is a country, then the attribute ‘state or province name of the registration jurisdiction’ does not need to be included.

(2) City or Town Name of Registration Jurisdiction (jurisdictionLocalityName)

The attribute is defined based on the circumstance. If the organization level of the jurisdiction of the Incorporating or Registration Agency to which the certificate subject is registered is a city or town, then the EV SSL certificate field subject not only must include the attribute ‘country code of the registration jurisdiction’ and ‘state or province name of the registration jurisdiction’ but also must include the attribute ‘City or Town Name of the registration jurisdiction’ which is used to record the city or town name in which the Incorporating or Registration Agency is located and the city or town name must be a complete name.

If the organization level of the jurisdiction of the Incorporating or Registration Agency to which the certificate subject is registered is a country or a state or province, then the attribute ‘city or town name of the registration jurisdiction’ does not need to be included.

(3) Street Address of the Actual Business Premises Address (streetAddress)

According to section 9.2.7 in the EV SSL Certificate Guidelines, it can be determined independently whether the EV SSL certificate field subject includes the attribute ‘street name of the actual business premises address’.

If it is submitted by the applicant and verified by the RA, then the street name of the actual address of the certificate subject business premises may be recorded.

(4) Postal Code of the Actual Business Premises Address (postalCode)

According to section 9.2.7 in the EV SSL Certificate Guidelines, it can be determined independently whether the EV SSL certificate field subject includes the attribute ‘postal code of the actual business premises address’ attribute. If it is submitted by the applicant and verified by the RA, then the postal code of the actual address of the certificate subject business premises may be recorded.

3.1.2.3 Deprecated Certificate Field

(1) commonName

According to section 9.2.3 in the EV SSL Certificate Guidelines, it is not recommended to use the commonName attribute in the EV SSL certificate field ‘subject’ but there are no regulations which clearly prohibit its use. For EV SSL certificates issued by the ePKI EV SSL Certification Authority, a commonName attribute is provided in the EV SSL certificate field ‘subject’. The fully qualified domain name (FQDN) owned or controlled by the certificate subject is recorded in this attribute contents and the server corresponding to the FQDN shall be owned or operated by the certificate subject or its virtual host service provider.

Currently EV SSL certificates still do not support wildcard certificates. Therefore, wildcard domain names may not be recorded in the commonName. But if the domain is ‘.onion’ and satisfies the related issued certificates to the domain ‘.onion’ requirements in Appendix F of the EV SSL Certificate Guidelines, then this restriction does not apply.

According to section 9.2.8 in the EV SSL Certificate Guidelines, except for the required, optional and deprecated attributes, other optional attributes may be provided for the EV SSL certificate field ‘subject’. For example: If the organization unit name (organizationUnitName) is provided, then the information recorded for these attributes must all be verified and confirmed to be error-free by the RA.

Only information which is verified and confirmed to be error-free by the RA may be recorded in the EV SSL certificate field ‘subject’ optional subfields or the content may be left blank if so desired. In addition ‘.’, ‘-‘, ‘‘and / or any other type of symbol shall not be used to indicate that the field content is blank, non-existent or incomplete.

The certificate subject alternative name field of the EV SSL certificate shall record a single or multiple FQDN owned or controlled by the subscriber. The corresponding server of these FQDN shall be owned or operated by the certificate subject or its virtual host service provider.

3.1.3 Anonymity or Psuedonymity of Subscribers

The ePKI EV SSL Certification Authority does not currently issue anonymous certificates to end-entity subscribers. As a principle, the pseudonymous certificates are not issued either. For the EV SSL certificates issued by the ePKI EV SSL CA, the ownership of the domain name and the organization are manually reviewed by the RA officers. The EV SSL certificates belong to Internationalized Domain Names (IDNs), the decrypted FQDN will be deemed EV SSL certificate requests with risks, as specified in Section 4.2.1, and the additional matching will be conducted, to prevent the homographic spoofing of IDNs.

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

The ePKI EV SSL Certification Authority’s X.500 Distinguished Name for its CA certificates is:

C=TW，

O=Chunghwa Telecom Co., Ltd.，

CN=ePKI EV SSL Certification Authority – Gn

Where, n=1, 2, 3…

The ePKI EV SSL Certification Authority shall use the X.520 standard to define the various naming attributes for assembly to ensure the uniqueness of the X.500 naming space recognized by the ePKI EV SSL Certification Authority for name of the subscriber certificate subject name. The ePKI EV SSL Certification Authority subscriber certificate subject name permits (but not limited to) the use of the following naming attributes defined in the X.520 standard for assembly:

- countryName (abbreviated as C)
- stateOrProvinceName(abbreviated as S)
- localityName (abbreviated as L)
- organizationName (abbreviated as O)
- organizationalUnitName (abbreviated as OU)
- BusinessCategory
- jurisdictionOfIncorporationCountryName
- jurisdictionStateOrProvinceName
- jurisdictionLocalityName
- streetAddress
- postalCode
- commonName (abbreviated as CN)
- serialNumber

3.1.6 Recognition, Authentication and Role of Trademarks

The certificate subject name provided by subscribers must comply with relevant regulations in our country’s Trademark Act and Fair-Trade Act. The ePKI EV SSL Certification Authority shall not bear the responsibility for reviewing whether or not the certificate subject name provided by the subscriber complies with the above regulations. Related disputes and arbitration shall not be the obligation of the ePKI EV SSL Certification Authority 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 the ePKI EV SSL Certification Authority 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 the ePKI EV SSL Certification Authority may revoke that subscriber’s certificate.

3.2 Initial Identity Validation

The ePKI EV SSL Certification Authority and RA shall adopt all reasonable and necessary verification steps to satisfy the verification requirements in sections 3.2 and 3.5. The acceptable application verification (commonly included optional) which follow the CP and EV SSL Certificate Guidelines requirements are deemed to be the minimum verification standard requirements. In all cases, the ePKI EV SSL Certification Authority and RA are responsible for adopting extra verification steps to satisfy verification requirements.

3.2.1 Method to Prove Possession of Private Key

The ePKI EV SSL Certification Authority shall verify that the private key is possessed by the applicant. The subscriber self-generates the key pairs and creates the PKCS#10 Certificate Signing Request and signs it with the private key. When applying for a certification, the Certificate Signing Request is submitted to the RA. The RA shall use the 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

3.2.2.1 Verification Requirements – Overview

The purpose of organization identity authentication for application for an assurance level 3 EV SSL certificate includes:

(1) Verify Applicant's existence and identity, including;

A. Verify the Applicant's Legal Existence and identity

B. Verify the Applicant's physical existence (business presence at a physical address), and

C. Verify the Applicant's operational existence (business activity).

(2) Verify the Applicant is a registered holder, or has control, of the Domain Name(s) to be included in the EV SSL Certificate;

(3) Verify a reliable means of communication with the entity to be named as the Subject in the Certificate;

(4) Verify the Applicant's authorization for the EV SSL Certificate (As section 3.2.3 & 3.2.4), including;

A. Verify the name, title, and authority of the Contract Signer, Certificate Approver, and Certificate Requester,

B. Verify that a Contract Signer signed the Subscriber Agreement or that a duly authorized Applicant Representative acknowledged and agreed to the Terms of Use; and

C. Verify that a Certificate Approver has signed or otherwise approved the EV SSL Certificate Request.

3.2.2.2 Verification of Applicant’s Legal Existence and Identity

3.2.2.2.1 3.2.2.2.1 Verification Requirements

To verify the four kinds of Applicants’ Legal Existence and identity, the CA must do the following.

(1) Private Organization Subjects

A. Legal Existence: Verify that the Applicant is a legally recognized entity, in existence and validly formed (e.g., incorporated) with the Incorporating or Registration Agency in the Applicant’s Jurisdiction of Incorporation or Registration, and not designated on the records of the Incorporating or Registration Agency by labels such as “inactive”, “invalid”, “not current”, or the equivalent.

B. Organization Name: Verify that the Applicant’s formal legal name as recorded with the Incorporating or Registration Agency in the Applicant’s Jurisdiction of Incorporation or Registration matches the Applicant’s name in the EV SSL Certificate Request.

C. Registration Number: Obtain the specific Registration Number such as the tax ID number assigned to the Applicant by the Incorporating or Registration Agency in the Applicant’s Jurisdiction of Incorporation or Registration. Where the Incorporating or Registration Agency does not assign a Registration Number, the CA shall obtain the Applicant’s date of Incorporation or Registration.

D. Registered Agent: Obtain the identity, address and registered office of the applicant's registered agent (as applicable in the applicant's jurisdiction of incorporation or registration). The registered office is the official address of the organization recorded at the registration agency which serves as the mailing address for official and legal documents.

Private organization must provide RA Counter correct copies of related certification documents (such as the company registration card, company change registration card, legal registration certification, withholding unit establishment (change) registration application (uniform invoice number assignment notice) approved by a competent authority or legally authorized body (i.e. court). The copies of the certification documents shall be stamped with the seals of the organization and the responsible person (must be the same seals used for organization registration). The RA Counter checks the authenticity of the application information and identity or uses certificate application information digital signature of private keys corresponding to GPKI assurance level 3 or ePKI approved assurance level 3 organization certificate.

If a private organization completes the incorporation registration procedure with the competent supervisory authority in accordance with law or the identification or authentication procedure has been completed in compliance with the CPS by the ePKI EV SSL Certification Authority, RA or a notary, attorney, accountant or company personnel trusted by the ePKI EV SSL Certification Authority (the remaining registration or identification and authentication supporting information such as the seal / stamp or stamped by the notary, attorney, accountant or company personnel). The ePKI EV SSL Certification Authority or RA may permit the private organization to present supporting information in place of the above identification and authentication method when applying for a certificate.

(2) Government Entity Subjects

A. Legal Existence: Verify that the Applicant is a legally recognized Government Entity, in existence in the political subdivision in which such Government Entity operates.

B. Entity Name: Verify that the Applicant’s formal legal name matches the Applicant’s name in the EV SSL Certificate Request.

C. Registration Number: Our country’s government agencies (organizations) use the Directorate-General of Personnel Administration’s government agency code. The RA must attempt to obtain the Applicant’s date of incorporation, registration, or formation, or the identifier for the legislative act that created the Government Entity. In circumstances where this information is not available, the RA must enter appropriate language to indicate that the Subject is a Government Entity.

D. The RA must verify the existence of the government agency (organization) when a certification application is made by government agency (organization) by official document and authenticate the verification documents. The government agency (organization) can also use the certificate application information digital signature of private keys corresponding to GPKI assurance level 3 organization certificates.

(3) Non-Profit International Organization

A. Legal existence: Verify that the applicant is a legally-recognized international organization entity.

B. Entity name: Verify that the applicant’s formal legal name matches the applicant’s name in the EV SSL certificate request.

C. Registration number: The RA must attempt to obtain the applicant’s incorporation date or identify the law which established the international organization. In circumstances where this information is not available, the RA must enter appropriate language to indicate that the subject is an international organization.

(4) Business Entity

A. Legal existence: Verify that the applicant has submitted an application for a business item.

B. Organization name: Verify that the applicant's legal name is approved by the registration agency (in the applicant's jurisdiction) and matches the applicant's name recorded in the EV SSL certificate request.

C. Registration number: Attempt to obtain the applicant's unique registration number at the registration agency (applicant's jurisdiction of registration). If no registration number is assigned by the registration agency, the RA shall obtain the registration date. Business Entity registered in our country shall use the tax ID number.

D. Principal individual: Verify the identity of the principal individual. Where the principal individual is an owner, partner, management personnel, director or staff member of a private organization, government agency (organization) or other business group, the principal individual who is authorized to perform work related to EV SSL certificate request, issuance or use may be identified by their title or as an employee, contractor or entity or organization.

Business Entity must provide RA Counter correct copies of related certification documents (such as a business registration approval letter approved by competent supervisory authority, a transcript of the business registration, a copy of the certificate issued by the competent authority for the registered particulars at the place where the business is located for an application filed by business responsible person or interested party in accordance with Article 25 of the Business Registration Act, withholding unit incorporation (change) registration application certification (uniform invoice number assignment notice)). The copies of the certification documents shall be stamped with the seals of the other business group or responsible person (must be the same seals used for organization registration). The RA Counter verifies the authenticity of the application information submitted by the other business group and identity. Government agencies (organizations) also may use certificate application information digital signature of private keys corresponding to GPKI assurance level 3 or ePKI approved assurance level 3 organization certificate.

E. If another business group completes the incorporation registration procedure with the competent supervisory authority in accordance with law or the identification or authentication procedure has been completed in compliance with the CPS by the ePKI EV SSL Certification Authority, RA or a notary, attorney, accountant or company personnel trusted by the ePKI EV SSL Certification Authority (the remaining registration or identification and authentication supporting information such as the seal / stamp or stamped by the notary, attorney, accountant or company personnel). The ePKI EV SSL Certification Authority or RA may permit the other business group to present supporting information in place of the above identification and authentication method when applying for a certificate.

3.2.2.2.2 3.2.2.2.2 Acceptable Method of Verification

Acceptable method of verification:

(1). Private Organization Subjects: Legal Existence, Organization Name, Registration Number and Registered Agent must be verified directly with, or obtained directly from, the Incorporating or Registration Agency in the Applicant's Jurisdiction of Incorporation or Registration.

Such verification may be through use of a Qualified Government Information Source operated by, or on behalf of, the Incorporating or Registration Agency, or by direct contact with the Incorporating or Registration Agency in person or via mail, e-mail, Web address, or telephone, using an address or phone number obtained directly from the Qualified Government Information Source, Incorporating or Registration Agency, or from a Qualified Independent Information Source.

(2). Government Entity Subjects: Legal Existence, Organization Name, Registration Number must either be verified directly with, or obtained directly from, one of the following: A. a Qualified Government Information Source in the political subdivision in which such Government Entity operates; B. a superior governing Government Entity in the same political subdivision as the Applicant (e.g. a Secretary of State may verify the Legal Existence of a specific State Department), or C. from a judge that is an active member of the federal, state or local judiciary within that political subdivision, or D. an attorney representing the Government Entity.

Any communication from a judge shall be verified in the same manner as is used for verifying factual assertions that are asserted by an Attorney as set forth in Section 3.2.3.4.1.

Such verification may be by direct contact with the appropriate Government Entity in person or via mail, e-mail, Web address, or telephone, using an address or phone number obtained from a Qualified Independent Information Source.

(3). Business Entity, Legal Existence, Organization Name and Registration Number must be verified directly with, or obtained directly from, the Registration Agency in the Applicant's Jurisdiction of Registration.

Such verification may be performed by means of a qualified government information source such as the MOEA industry and business registration database or a qualified government tax information source (QTIS) such as information disclosed by the MOF Fiscal Information Agency or by direct contact with the registration agency in person or via mail, email, website or telephone obtained from a qualified government information source, QTIS, registration agency or qualified independent information source.

In addition, the ePKI EV SSL Certification Authority or RA must validate the principal individual associated with the other business group pursuant to the requirements in subsection (4) below.

(5) Principal Individual: A Principal Individual associated with the Business Entity must be validated in a face-to-face setting.

The CA and the RA may rely upon a face-to-face validation of the Principal Individual performed by the Registration Agency, provided that the CA and the RA has evaluated the validation procedure and concluded that it satisfies the requirements of the Guidelines for face-to-face validation procedures.

Where no face-to-face validation was conducted by the Registration Agency, or the Registration Agency's face-to-face validation procedure does not satisfy the requirements of the Guidelines, the RA shall perform face-to-face validation.

A. Face-To-Face Validation: The face-to-face validation must be conducted before either an employee of the CA, a Latin Notary, a Notary (or equivalent in the Applicant's jurisdiction), a Lawyer, or Accountant (Third-Party Validator).

The Principal Individual(s) must present the following documentation (Vetting Documents) directly to the Third-Party Validator:

(I)A Personal Statement that includes the following information:

(i) Full name or names by which a person is, or has been, known (including all other names used);

(ii) Residential Address at which he/she can be located;

(iii) Date of birth; and

(iv) An affirmation that all of the information contained in the Certificate Request is true and correct.

(II) A current signed government-issued identification document that includes a photo of the Individual and is signed by the Individual such as:

(i)A passport;

(ii)A driver's license;

(iii)A personal identification card;

(iv)A concealed weapons permit; or

(vi)A military ID.

(III) At least two secondary documentary evidences to establish his/her identity that include the name of the Individual, one of which

MUST be from a financial institution.

(i) Acceptable financial institution documents include:

(a) A major credit card, provided that it contains an expiration date and it has not expired,

(b) A debit card from a Regulated Financial Institution, provided that it contains an expiration date and it has not expired,

(c) A mortgage statement from a recognizable lender that is less than six months old,

(d) A bank statement from a Regulated Financial Institution that is less than six months old.

(ii)Acceptable non-financial documents include:

(a)Recent original utility bills or certificates from a utility company confirming the arrangement to pay for the services at a fixed address (not a mobile/cellular telephone bill),

(b)A copy of a statement for payment of a lease, provided that the statement is dated within the past six months,

(c)A certified copy of a birth certificate,

(d)A local authority tax bill for the current year,

(e) A certified copy of a court order, such as a divorce certificate, annulment papers, or adoption papers.

(IV) The Third-Party Validator performing the face-to-face validation must:

(i) Attest to the signing of the Personal Statement and the identity of the signer; and

(ii) Identify the original Vetting Documents used to perform the identification. In addition, the Third-Party Validator must attest on a copy of the current signed government-issued photo identification document that it is a full, true, and accurate reproduction of the original.

B. Verification of Third-Party Validator: The RA must independently verify that the Third-Party Validator is a legally-qualified Notary (or legal equivalent in the Applicant’s jurisdiction), lawyer, or accountant (jurisdiction of the Individual’s residency, and that the Third-Party Validator actually did perform the services and did attest to the signature of the Individual).

C. Cross-checking of Information: The RA must obtain the documents signed by the individual and copy of the identity certification documents approved by a current government authority. The RA must review the documentation to determine that the information is consistent, matches the information in the application, and identifies the principal individual. The ePKI EV SSL certification authority and RA may rely on electronic copies of this documentation, provided that:

(I) the RA verifies their authenticity (not improperly modified when compared with the underlying original) with the Third-Party Validator; and

(II) electronic copies of similar kinds of documents are recognized as legal substitutes for originals under the laws of the RA’s jurisdiction.

(5). Non-Commercial Entity Subjects (International Organization): Legal Existence, Organization Name and Registration Number must be verified either:

A. With reference to the constituent document under which the International Organization was formed; or

B. Directly with a signatory country's government in which the CA is permitted to do business. Such verification may be obtained from an appropriate Government Agency or from the laws of that country, or by verifying that the country's government has a mission to represent it at the International Organization; or

C. Directly against any current list of qualified entities that the CA/Browser Forum may maintain at www.cabforum.org.

D. In cases where the International Organization applying for the EV

SSL Certificate is an organ or agency – including a non-governmental organization of a verified International Organization, then the CA may verify the International Organization Applicant directly with the verified umbrella International Organization of which the Applicant is an organ or agency (an umbrella organization is generally an organization which cooperates, coordinates activities or shares resources with certain industries. For example, the American Federation of Labor and Congress of Industrial Organizations (AFL-CIO).

3.2.2.3 Verification of Applicant's Legal Existence and Identity – Assumed Name

3.2.2.3.1 Verification Requirements

If, in addition to the Applicant's formal legal name, as recorded with the applicable Incorporating Agency or Registration Agency in the Applicant's Jurisdiction of Incorporation or Registration, the Applicant's identity, as asserted in the EV SSL Certificate, is to contain any assumed name (also known as "doing business as", "DBA", or "d/b/a" in the US, and "trading as" in the UK) under which the Applicant conducts business, the RA must verify that:

(i) the Applicant has registered its use of the assumed name with the appropriate Government Agency for such filings in the jurisdiction of its Place of Business (as verified in accordance with these Guidelines), and (ii) that such filing continues to be valid.

3.2.2.3.1 **Acceptable Method of Verification**

To verify any assumed name under which the Applicant conducts business:

(1) The RA may verify the assumed name through use of a Qualified Government Information Source operated by, or on behalf of, an appropriate Government Agency in the jurisdiction of the Applicant's Place of Business, or by direct contact with such Government Agency in person or via mail, e-mail, Web address, or telephone; or

(2) The RA may verify the assumed name through use of a Qualified Independent Information Source provided that the QIIS has verified the assumed name with the appropriate Government Agency.

(3) The RA may rely on a Verified Legal Opinion, or a Verified Accountant Letter that indicates the assumed name under which the Applicant conducts business, the Government Agency with which the assumed name is registered, and that such filing continues to be valid.

3.2.2.4 Verification of Applicant’s Physical Existence

3.2.2.4.1 **Address of Applicant’s Place of Business**

(1) Verification Requirements: To verify the Applicant's physical existence and business presence, the CA must verify that the physical address provided by the Applicant is an address where the Applicant or a Parent/Subsidiary Company conducts business operations (not, for example, a mail drop or P.O. box, or 'care of' (C/O) address, such as an address for an agent of the Organization), and is the address of the Applicant's Place of Business.

(2) Acceptable Methods of Verification

A. Place of Business in the Country of Incorporation or Registration

(I). For Applicants whose Place of Business is in the same country as the Applicant's Jurisdiction of Incorporation or Registration and whose Place of Business is not the same as that indicated in the relevant Qualified Government Information Source used in Section 3.2.2.2 to verify Legal Existence:

(i). For Applicants listed at the same Place of Business address in the current version of either at least one QGIS (other than that used to verify Legal Existence), QIIS or QTIS, the RA must confirm that the Applicant's address, as listed in the EV SSL Certificate Request, is a valid business address for the Applicant or a Parent/Subsidiary Company by reference to such QGIS, QIIS, or QTIS, and may rely on the Applicant's representation that such address is its Place of Business;

(ii) For Applicants who are not listed at the same Place of Business address in the current version of either at least one QIIS or QTIS, the RA must confirm that the address provided by the Applicant in the EV SSL Certificate Request is the Applicant's or a Parent/Subsidiary Company's business address, by obtaining documentation of a site visit to the business address, which must be performed by a reliable Individual or firm. The documentation of the site visit must:

(a) Verify that the Applicant's business is located at the exact address stated in the EV SSL Certificate Request (e.g., via permanent signage, employee confirmation, etc.),

(b) Identify the type of facility (e.g., office in a commercial building, private residence, storefront, etc.) and whether it appears to be a permanent business location,

(c) Indicate whether there is a permanent sign (that cannot be moved) that identifies the Applicant,

(d) Indicate whether there is evidence that the Applicant is conducting ongoing business activities at the site (not that it is just, for example, a mail drop, P.O. box, etc.), and

(e) Include one or more photos of the exterior of the site (showing signage indicating the Applicant's name, if present, and showing the street address if possible), and the interior reception area or workspace.

(iii) For all Applicants, the RA may alternatively rely on a Verified Legal Opinion or a Verified Accountant Letter that indicates the address of the Applicant's or a Parent/Subsidiary Company's Place of Business and that business operations are conducted there.

(iv) For Government Entity Applicants, the RA may rely on the address contained in the records of the QGIS in the Applicant's jurisdiction.

(v) For Applicants whose Place of Business is in the same country as the Applicant's Jurisdiction of Incorporation or Registration and where the QGIS used in Section 3.2.2.2 to verify Legal Existence contains a business address for the Applicant, the RA may rely on the address in the QGIS to confirm the Applicant's or a Parent/Subsidiary Company's address as listed in the EV SSL Certificate Request, and may rely on the Applicant's representation that such address is its Place of Business.

B. Place of Business not in the Country of Incorporation or Registration: The RA must rely on a Verified Legal Opinion or Verified Accountant's Letter that indicates the address of the Applicant's Place of Business and that business operations are conducted there.

3.2.2.5 Verified Method of Communication

3.2.2.5.1 Verification Requirements

To assist in communicating with the Applicant and confirming that the Applicant is aware of and approves issuance, the RA must verify a telephone number, fax number, email address, or postal delivery address as a Verified Method of Communication with the Applicant.

3.2.2.5.2 Acceptable Methods of Verification

To verify a Verified Method of Communication with the Applicant, the RA must:

(1) Verify that the Verified Method of Communication belongs to the Applicant, or a Parent/Subsidiary or Affiliate of the Applicant, by matching it with one of the Applicant's Parent/Subsidiary or Affiliate's Places of Business in: (i) records provided by the applicable phone company; (ii) a QGIS, QTIS, or QIIS; or (iii) a Verified Legal Opinion or Verified Accountant Letter; and

(2) Confirm the Verified Method of Communication by using it to obtain an affirmative response sufficient to enable a reasonable person to conclude that the Applicant, or a Parent/Subsidiary or Affiliate of

Applicant, can be contacted reliably by using the Verified Method of Communication.

3.2.2.6 Verification of Applicant's Operational Existence

3.2.2.6.1 Verification Requirements

The RA must verify that the Applicant has the ability to engage in business by verifying the Applicant's, or Affiliate/Parent/Subsidiary Company's, operational existence.

3.2.2.6.2 Acceptable Verification Methods

To verify the Applicant's ability to engage in business, the RA must verify the operational existence of the Applicant, or its Affiliate/Parent/Subsidiary Company, by:

(1) Verifying that the Applicant, Affiliate, Parent Company, or Subsidiary Company has been in existence for at least three years, as indicated by the records of an Incorporating Agency or Registration Agency;

(2) Verifying that the Applicant, Affiliate, Parent Company, or Subsidiary Company is listed in either a current QIIS or QTIS;

(3) Verifying that the Applicant, Affiliate, Parent Company, or Subsidiary Company has an active current Demand Deposit Account with a Regulated Financial Institution by receiving authenticated documentation of the Applicant's, Affiliate's, Parent Company's, or Subsidiary Company's Demand Deposit Account directly from a Regulated Financial Institution; or

(4) Relying on a Verified Legal Opinion or a Verified Accountant Letter to the effect that the Applicant has an active current Demand Deposit Account with a Regulated Financial Institution.

3.2.2.7 Verification of Applicant's Domain Name

(1) For each Fully-Qualified Domain Name listed in a EV SSL Certificate, the RA shall confirm that, as of the date the Certificate was issued, the Applicant (or the Applicant's Parent Company, Subsidiary Company, or Affiliate, collectively referred to as "Applicant" for the purposes of this section) either is the Domain

Name Registrant or has control over the FQDN using a procedure specified in Section 3.2.5.

(2) Mixed Character Set Domain Names: EV SSL Certificates may include Domain Names containing mixed character sets only in compliance with the rules set forth by the domain registrar. The CA & RA must visually compare any Domain Names with mixed character sets with known high-risk domains. If a similarity is found, then the EV SSL Certificate Request must be flagged as High Risk. The CA & RA must perform reasonably appropriate additional authentication and verification to be certain beyond reasonable doubt that the Applicant and the target in question are the same organization.

3.2.2.8 Authorize the CA Issuing Certificate Record

Before issuing EV SSL certificates, the EV 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, and the certificates are only issued after passing the check.

The ePKI EV SSL CA or the RA checks DNS to see if the FQDN will be marked for the application of the EV SSL certificate has the DNS resource record of CAA. If the DNS resource record of CAA exists, and has not named the ePKI EV SSL CA as the CA to authorize the issuance of the EV SSL certificate, the ePKI EV SSL CA will deem that the certificate application agrees to authorize the ePKI EV SSL CA to issue the EV 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 the ePKI EV SSL CA included in the record, and the EV SSL certificate will be issued afterwards.

3.2.3 Authentication of Individual Identity

EV SSL certificates are not issued to individuals but are issued to the four types of organizations described in sections 3.1.2, 3.2.2.2 or 4.1.1. However, the personal identification of certificate requesters, contract signers, certificate approvers inside the organization must undergo verification as follows:

3.2.3.1 Verification of Name, Title, and Authority of Contract Signer and Certificate Approver

3.2.3.1.1 Verification Requirements

For both the Contract Signer and the Certificate Approver, the RA must verify the following.

(1) Name, Title and Agency: The RA must verify the name and title of the Contract Signer and the Certificate Approver, as applicable. The RA must also verify that the Contract Signer and the Certificate Approver are agents representing the Applicant.

(2) Signing Authority of Contract Signer: The RA must verify that the Contract Signer is authorized by the Applicant to enter into the Subscriber Agreement (and any other relevant contractual obligations) on behalf of the Applicant, including a contract that designates one or more Certificate Approvers on behalf of the Applicant.

EV Authority of Certificate Approver: The RA must verify, through a source other than the Certificate Approver him- or herself, that the Certificate Approver is expressly authorized by the Applicant to do the following, as of the date of the EV SSL Certificate Request:

A. Submit, and, if applicable, authorize a Certificate Requester to submit, the EV SSL Certificate Request on behalf of the Applicant; and

B. Provide, and, if applicable, authorize a Certificate Requester to provide, the information requested from the Applicant by the CA for issuance of the EV SSL Certificate; and

C. Approve EV SSL Certificate Requests submitted by a Certificate Requester.

3.2.3.1.2 Acceptable Methods of Verification – Name, Title and Agency

Acceptable methods of verification of the name, title, and agency status of the Contract Signer and the Certificate Approver include the following.

(1) Name and Title: The RA may verify the name and title of the Contract Signer and the Certificate Approver by any appropriate method designed to provide reasonable assurance that a person claiming to act in such a role is in fact the named person designated to act in such role.

(2) Agency: The RA may verify the agency of the Contract Signer and the Certificate Approver by:

A. Contacting the Applicant using a Verified Method of Communication for the Applicant, and obtaining confirmation that the Contract Signer and/or the Certificate Approver, as applicable, is an employee;

B. Obtaining an Independent Confirmation From the Applicant (as described in Section 3.2.3.4.4), or a Verified Legal Opinion (as described in Section 3.2.3.4.1), or a Verified Accountant Letter (as described in Section 3.2.3.4.2) verifying that the Contract Signer and/or the Certificate Approver, as applicable, is either an employee or has otherwise been appointed as an agent of the Applicant; or

C. Obtaining confirmation from a QIIS or QGIS that the Contract Signer and/or Certificate Approver is an employee of the Applicant.

The RA may also verify the agency of the Certificate Approver via a certification from the Contract Signer (including in a contract between the CA and the Applicant signed by the Contract Signer), provided that the employment or agency status and Signing Authority of the Contract Signer has been verified.

3.2.3.1.3 Acceptable Methods of Verification – Authority

Acceptable methods of verification of the Signing Authority of the Contract Signer, and the EV Authority of the Certificate Approver, as applicable, include:

(1) Legal Opinion: The Signing Authority of the Contract Signer, and/or the EV Authority of the Certificate Approver, may be verified by reliance on a Verified Legal Opinion (as described in Section 3.2.3.4.1);

(2) Accountant Letter: The Signing Authority of the Contract Signer, and/or the EV Authority of the Certificate Approver, may be verified by reliance on a Verified Accountant Letter (as described in Section 3.2.3.4.2);

(3) Corporate Resolution: The Signing Authority of the Contract Signer, and/or the EV Authority of the Certificate Approver, may be verified by reliance on a properly authenticated corporate resolution that confirms that the person has been granted such Signing Authority, provided that such resolution is (i) certified by the appropriate corporate officer (e.g., secretary), and (ii) the CA and RA can reliably verify that the certification was validly signed by such person, and that such person does have the requisite authority to provide such certification;

(4) Independent Confirmation from Applicant: The Signing Authority of the Contract Signer, and/or the EV Authority of the Certificate Approver, MAY be verified by obtaining an Independent Confirmation from the Applicant (as described in Section 3.2.3.4.4);

(5) Contract between CA and Applicant: The EV Authority of the Certificate Approver may be verified by reliance on a contract between the CA and the Applicant that designates the Certificate Approver with such EV Authority, provided that the contract is signed by the Contract Signer and provided that the agency and Signing Authority of the Contract Signer have been verified;

(6) Prior Equivalent Authority: The signing authority of the Contract Signer, and/or the EV authority of the Certificate Approver, may be verified by relying on a demonstration of Prior Equivalent Authority.

A. Prior Equivalent Authority of a Contract Signer may be relied upon for confirmation or verification of the signing authority of the Contract Signer when the Contract Signer has executed a binding contract between the CA or the RA and the Applicant with a legally valid and enforceable seal or handwritten signature and only when the contract was executed more than 90 days prior to the EV SSL Certificate application. The RA must record sufficient details of the previous agreement to correctly identify it and associate it with the EV SSL certificate application. Such details may include any of the following: Agreement title, Date of Contract Signer's signature, Contract reference number, and Filing location.

B. Prior Equivalent Authority of a Certificate Approver may be relied upon for confirmation or verification of the EV Authority of the Certificate Approver when the Certificate Approver has performed one or more of the following:

(I)Under contract to the CA, has served (or is serving) as an Enterprise RA for the Applicant, or

(II) Has participated in the approval of one or more certificate requests, for certificates issued by the CA and which are currently and verifiably in use by the Applicant. In this case the RA must have contacted the Certificate Approver by phone at a previously validated phone number or have accepted a signed and notarized letter approving the certificate request.

(7) QIIS or QGIS: The Signing Authority of the Contract Signer, and/or the EV Authority of the Certificate Approver, may be verified by a QIIS or QGIS that identifies the Contract Signer and/or the Certificate Approver as a corporate officer, sole proprietor, or other senior official of the Applicant.

(8) Contract Signer's Representation/Warranty: Provided that the RA verifies that the Contract Signer is an employee or agent of the Applicant, the RA may rely on the signing authority of the Contract Signer by obtaining a duly executed representation or warranty from the Contract Signer that includes the following acknowledgments：

A. That the Applicant authorizes the Contract Signer to sign the Subscriber Agreement on the Applicant's behalf,

B. That the Subscriber Agreement is a legally valid and enforceable agreement,

C. That, upon execution of the Subscriber Agreement, the Applicant will be bound by all of its terms and conditions,

D. That serious consequences attach to the misuse of an EV SSL certificate, and

E. The contract signer has the authority to obtain the digital equivalent of a corporate seal, stamp or officer's signature to establish the authenticity of the company's Web site.

3.2.3.1.4 Pre-Authorized Certificate Approver

Where the CA and Applicant contemplate the submission of multiple future EV Certificate Requests, then, after the CA:

(1) Has verified the name and title of the Contract Signer and that he/she is an employee or agent of the Applicant; and

(2) Has verified the Signing Authority of such Contract Signer in accordance with one of the procedures in Section 3.2.3.1.3.

The CA, RA and the Applicant may enter into a written agreement, signed by the Contract Signer on behalf of the Applicant, whereby, for a specified term, the Applicant expressly authorizes one or more Certificate Approver(s) designated in such agreement to exercise EV Authority with respect to each future EV SSL Certificate Request submitted on behalf of the Applicant and properly authenticated as originating with, or otherwise being approved by, such Certificate Approver(s).

Such an agreement must provide that the Applicant shall be obligated under the Subscriber Agreement for all EV Certificates issued at the request of, or approved by, such Certificate Approver(s) until such EV Authority is revoked, and must include mutually agreed-upon provisions for (i) authenticating the Certificate Approver when EV SSL Certificate Requests are approved, (ii) periodic re-confirmation of the EV Authority of the Certificate Approver, (iii) secure procedures by which the Applicant can notify the CA that the EV Authority of any such Certificate Approver is revoked, and (iv) such other appropriate precautions as are reasonably necessary.

3.2.3.2 EV SSL Verification of Signature on Subscriber Agreement and EV Certificate Requests

Both the Subscriber Agreement and each non-pre-authorized EV SSL Certificate Request must be signed. The Subscriber Agreement must be signed by an authorized Contract Signer. The EV SSL Certificate Request must be signed by the Certificate Requester submitting the document, unless the Certificate Request has been pre-authorized in line with Section 3.2.3.1.4.

If the Certificate Requester is not also an authorized Certificate Approver, then an authorized Certificate Approver must independently approve the EV SSL Certificate Request. In all cases, applicable signatures must be a legally valid and contain an enforceable seal or handwritten signature (for a paper Subscriber Agreement and/or EV SSL Certificate Request), or a legally valid and enforceable electronic signature (such as digital signatures from private keys corresponding to a GPKI assurance level 3 or ePKI EV SSL Certificate Authority assurance level 3 certificate) that binds the Applicant to the terms of each respective document.

3.2.3.2.1 Verification Requirements

(1) Signature: The RA must authenticate the signature of the Contract Signer on the Subscriber Agreement and the signature of the Certificate Requester on each EV SSL Certificate Request in a manner that makes it reasonably certain that the person named as the signer in the applicable document is, in fact, the person who signed the document on behalf of the Applicant.

(2). Approval Alternative: In cases where an EV SSL Certificate Request is signed and submitted by a Certificate Requester who does not also function as a Certificate Approver, approval and adoption of the EV SSL Certificate Request by a Certificate Approver in accordance with the requirements of Section 3.2.3.3 can substitute for authentication of the signature of the Certificate Requester on such EV Certificate Request.

3.2.3.2.2 Acceptable Methods of Signature Verification

Acceptable methods of authenticating the signature of the Certificate Requester or Contract Signer include the following:

(1) Contacting the Applicant using a Verified Method of Communication for the Applicant, for the attention of the Certificate Requester or Contract Signer, as applicable, followed by a response from someone who identifies themselves as such person confirming that he/she did sign the applicable document on behalf of the Applicant;

(2) A letter mailed to the Applicant's or Agent's address, as verified through independent means in accordance with EV SSL Certificate Guidelines, for the attention of the Certificate Requester or Contract Signer, as applicable, followed by a response through a Verified Method of Communication from someone who identifies themselves as such person confirming that he/she did sign the applicable document on behalf of the Applicant;

(3) Use of a signature process that establishes the name and title of the signer in a secure manner, such as through use of an appropriately secure login process, or through use of a digital signature made an appropriately verified certificate (such as digital signatures from private keys corresponding to a GPKI assurance level 3 or ePKI EV SSL Certificate Authority assurance level 3 certificate); or

(4) Notarization by a notary, provided that the CA or the RA independently verifies that such notary is a legally qualified notary in the jurisdiction of the Certificate Requester or Contract Signer.

3.2.3.3 Verification of Approval of EV Certificate Request

3.2.3.3.1 Verification Requirements

In cases where an EV SSL Certificate Request is submitted by a Certificate Requester, before the CA issues the requested EV SSL Certificate, the RA must verify that an authorized Certificate Approver reviewed and approved the EV Certificate Request.

3.2.3.3.2 Acceptable Methods of Verification

Acceptable methods of verifying the Certificate Approver’s approval of an EV SSL Certificate Request include:

Contacting the Certificate Approver using a Verified Method of Communication for the Applicant and obtaining oral or written confirmation that the Certificate Approver has reviewed and approved the EV SSL Certificate Request;

Notifying the Certificate Approver that one or more new EV SSL Certificate Requests are available for review and approval at a designated access-controlled and secure Web site, followed by a login by, and an indication of approval from, the Certificate Approver in the manner required by the Web site; or

Verifying the signature of the Certificate Approver on the EV SSL Certificate Request in accordance with Section 3.2.3.2 of these Guidelines.

3.2.3.4 Verification of Certain Information Sources

3.2.3.4.1 Verified Legal Opinion

(1) Verification Requirements: Before relying on a legal opinion submitted to the RA, the RA must verify that such legal opinion meets the following requirements:

A. Status of Author: The CA MUST verify that the legal opinion is authored by an independent legal practitioner retained by and representing the Applicant (or an in-house legal practitioner employed by the Applicant) (Legal Practitioner) who is either:

(I) A lawyer (or solicitor, barrister, advocate, or equivalent) licensed to practice law in the country of the Applicant’s Jurisdiction of Incorporation or Registration or any jurisdiction where the Applicant maintains an office or physical facility, or

(II) A notary that is a member of the International Union of Latin Notaries, and is licensed to practice in the country of the Applicant’s Jurisdiction of Incorporation or Registration or any jurisdiction where the Applicant maintains an office or physical facility (and that such jurisdiction recognizes the role of the Latin Notary);

B. Basis of Opinion: The RA must verify that the Legal Practitioner is acting on behalf of the Applicant and that the conclusions of the Verified Legal Opinion are based on the Legal Practitioner's stated familiarity with the relevant facts and the exercise of the Legal Practitioner's professional judgment and expertise;

C. Authenticity: The RA must confirm the authenticity of the Verified Legal Opinion.

(2) Acceptable Methods of Verification: Acceptable methods of establishing the foregoing requirements for a Verified Legal Opinion are:

(A) Status of Author: The RA must verify the professional status of the author of the legal opinion by directly contacting the authority responsible for registering or licensing such Legal Practitioner(s) in the applicable jurisdiction;

(B) For a legal practitioner who practices law in our country following the current regulations of the Lawyer's Act, has obtained a lawyer qualification certification awarded by the Ministry of Justice (MOJ), joined a local lawyer's association and has a case filed with any court in the country, the RA shall verify through use of the lawyer inquiry function with the MOJ lawyer management system (http://service.moj.gov.tw/lawer/ notice.htm) or Taiwan Bar Association (http://www.twba.org.tw/) or contact the local lawyer association.

For court or private notaries, the RA shall verify through the Judicial Yuan or local court competent supervisory authorities and the private notary register of the local court.

Basis of Opinion: The text of the legal opinion must make it clear that the Legal Practitioner is acting on behalf of the Applicant and that the conclusions of the legal opinion are based on the Legal Practitioner's stated familiarity with the relevant facts and the exercise of the practitioner's professional judgment and expertise. The legal opinion may also include disclaimers and other limitations customary in the Legal Practitioner's jurisdiction, provided that the scope of the disclaimed responsibility is not so great as to eliminate any substantial risk (financial, professional, and/or reputational) to the Legal Practitioner, should the legal opinion prove to be erroneous.

(C) Authenticity: To confirm the authenticity of the legal opinion, the RA must make a telephone call or send a copy of the legal opinion back to the Legal Practitioner at the address, phone number, facsimile, or (if available) e-mail address for the Legal Practitioner listed with the authority responsible for registering or licensing such Legal Practitioner, and obtain confirmation from the Legal Practitioner or the Legal Practitioner's assistant that the legal opinion is authentic. If a phone number is not available from the licensing authority, the RA may use the number listed for the Legal Practitioner in records provided by the applicable phone company, QGIS, or QIIS.

In circumstances where the opinion is digitally signed, in a manner that confirms the authenticity of the document and the identity of the signer, as verified by the RA in Section 3.2.3.4.1 (2) A, no further verification of authenticity is required.

3.2.3.4.2 Verified Accountant Letter

(1) Verification Requirements: Before relying on an accountant letter submitted to the RA, the RA must verify that such accountant letter meets the following requirements:

A. Status of Author: The RA must verify that the accountant letter is authored by an Accounting Practitioner retained or employed by the Applicant and licensed within the country of the Applicant's Jurisdiction of Incorporation, Jurisdiction of Registration, or country where the Applicant maintains an office or physical facility. Verification of license must be through the member organization or regulatory organization in the Accounting Practitioner's country or jurisdiction that is appropriate to contact when verifying an accountant's license to practice in that country or jurisdiction. Such country or jurisdiction must have an accounting standards body that maintains full membership status with the International Federation of Accountants.

B. Basis of Opinion: The RA must verify that the Accounting Practitioner is acting on behalf of the Applicant and that the conclusions of the Verified Accountant Letter are based on the Accounting Practitioner's stated familiarity with the relevant facts and the exercise of the Accounting Practitioner's professional judgment and expertise;

C. Authenticity: The RA must confirm the authenticity of the Verified Accountant Letter.

(2) Acceptable Methods of Verification: Acceptable methods of establishing the foregoing requirements for a Verified Accountant Letter are listed here.

A. Status of Author: The CA must verify the professional status of the author of the accountant letter by directly contacting the authority responsible for registering or licensing such Accounting Practitioners in the applicable jurisdiction. For example, for accountants practicing in our country, the Taiwan CPA Association may be contacted or the CPA practice register can be checked at the Taiwan CPA Association website (http://www.roccpa.org.tw/).

B. Basis of Opinion: The text of the Verified Accountant Letter must make clear that the Accounting Practitioner is acting on behalf of the Applicant and that the information in the letter is based on the Accounting Practitioner's stated familiarity with the relevant facts and the exercise of the practitioner's professional judgment and expertise. The Verified Accountant Letter may also include disclaimers and other limitations customary in the Accounting Practitioner's jurisdiction, provided that the scope of the disclaimed responsibility is not so great as to eliminate any substantial risk (financial, professional, and/or reputational) to the Accounting Practitioner, should the Verified Accountant Letter prove to be erroneous.

C. Authenticity: To confirm the authenticity of the accountant's opinion, the RA must make a telephone call or send a copy of the Verified Accountant Letter back to the Accounting Practitioner at the address, phone number, facsimile, or (if available) e-mail address for the Accounting Practitioner listed with the authority responsible for registering or licensing such Accounting Practitioners and obtain confirmation from the Accounting

Practitioner or the Accounting Practitioner's assistant that the accountant letter is authentic.

If a phone number is not available from the licensing authority, the RA may use the number listed for the Accountant in records provided by the applicable phone company, QGIS, or QIIS.

In circumstances where the opinion is digitally signed, in a manner that confirms the authenticity of the document and the identity of the signer, as verified by the RA in Section 3.2.3.4.2 (2) A, no further verification of authenticity is required.

3.2.3.4.3 Face-to-Face Validation

(1) Verification Requirements: Before relying on face-to-face vetting documents submitted to the RA, the RA must verify that the Third-Party Validator meets the following requirements:

A. Qualification of Third-Party Validator: The RA must independently verify that the Third-Party Validator is a legally-qualified Latin Notary or Notary (or legal equivalent in the Applicant's jurisdiction), Lawyer, or Accountant in the jurisdiction of the individual's residency;

B. Document Chain of Custody: The RA must verify that the Third-Party Validator viewed the Vetting Documents in a face-to-face meeting with the individual being validated;

C. Verification of Attestation: If the Third-Party Validator is not a Latin Notary, then the RA must confirm the authenticity of the attestation and vetting documents.

(2) Acceptable Methods of Verification: Acceptable methods of establishing the foregoing requirements for vetting documents are:

A. Qualification of Third-Party Validator: The RA must verify the professional status of the Third-Party Validator by directly contacting the authority responsible for registering or licensing such Third-Party Validators in the applicable jurisdiction;

B. Document Chain of Custody: The Third-Party Validator must submit a statement to the RA which attests that they obtained the Vetting Documents submitted to the RA for the individual during a face-to-face meeting with the individual;

C. Verification of Attestation: If the Third-Party Validator is not a Latin Notary, then the RA must confirm the authenticity of the vetting documents received from the Third-Party Validator. The RA must make a telephone call to the Third-Party Validator and obtain confirmation from them or their assistant that they performed the face-to-face validation. The RA may rely upon self-reported information obtained from the Third-Party Validator for the sole purpose of performing this verification process. In circumstances where the attestation is digitally signed, in a manner that confirms the authenticity of the documents, and the identity of the signer as verified by the RA in Section 3.2.3.4.3(1) A., no further verification of authenticity is required.

3.2.3.4.4 Independent Confirmation From Applicant

An Independent Confirmation from the Applicant is a confirmation of a particular fact (e.g., confirmation of the employee or agency status of a Contract Signer or Certificate Approver, confirmation of the EV Authority of a Certificate Approver, etc.) that is:

(1) Received by the RA from a Confirming Person (someone other than the person who is the subject of the inquiry) that has the appropriate authority to confirm such a fact, and who represents that he/she has confirmed such fact;

(2) Received by the RA in a manner that authenticates and verifies the source of the confirmation; and

(3) Binding on the Applicant.

An Independent Confirmation from the Applicant may be obtained via the following procedure:

(1) Confirmation Request: The RA must initiate a Confirmation Request via an appropriate out-of-band communication, requesting verification or confirmation of the particular fact at issue as follows:

(A) Addressee: The Confirmation Request must be directed to:

(i) A position within the Applicant's organization that qualifies as a Confirming Person (e.g., Secretary, President, CEO, CFO, COO, CIO, CISO and is identified by name and title in a current QGIS, QTIS, QIIS, or

(ii) The Applicant's Registered Agent or Registered Office in the Jurisdiction of Incorporation as listed in the official records of the Incorporating Agency, with instructions that it be forwarded to an appropriate Confirming Person; or

(iii) A named individual verified to be in the direct line of management above the Contract Signer or Certificate Approver by contacting the Applicant's Human Resources Department by phone or mail (at the phone number or address for the Applicant's Place of Business, verified in accordance with EV SSL Certificate Guidelines).

(B) Means of Communication: The Confirmation Request must be directed to the Confirming Person in a manner reasonably likely to reach such person. The following options are acceptable:

(i) By paper mail addressed to the Confirming Person at:

(1) The address of the Applicant's Place of Business as verified by the RA in accordance with these Guidelines, or

(2)The business address for such Confirming Person specified in a current QGIS, QTIS, QIIS, Verified Legal Opinion, or Verified Accountant Letter, or

(3)The address of the Applicant's Registered Agent or Registered Office listed in the official records of the Jurisdiction of Incorporation, or

(ii) By e-mail addressed to the Confirming Person at the business e-mail address for such person listed in a current QGIS, QTIS, QIIS, Verified Legal Opinion, or Verified Accountant Letter; or

(iii) By telephone call to the Confirming Person, where such person is contacted by calling the main phone number of the Applicant's Place of Business (verified in accordance with these Guidelines) and asking to speak to such person, and a person taking the call identifies him- or herself as such person; or

(iv) By facsimile to the Confirming Person at the Place of Business. The facsimile number must be listed in a current QGIS, QTIS, QIIS, Verified Legal Opinion, or Verified Accountant Letter. The cover page must be clearly addressed to the Confirming Person.

(2) Confirmation Response: The CA MUST receive a response to the Confirmation Request from a Confirming Person that confirms the particular fact at issue. Such response MAY be provided to the CA by telephone, by email, or by paper mail, so long as the CA can reliably verify that it was provided by a Confirming Person in response to the Confirmation Request.

(3) The CA MAY rely on a verified Confirming Person to confirm their own contact information: email address, telephone number, and facsimile number. The CA MAY rely on this verified contact information for future correspondence with the Confirming Person if:

(A) The domain of the e-mail address is owned by the Applicant and is the Confirming Person's own e-mail address and not a group e-mail alias;

(B) The Confirming Person's telephone/fax number is verified by the CA to be a telephone number that is part of the organization's telephone system, and is not the personal phone number for the person.

3.2.3.4.5 Qualified Independent Information Source

Qualified independent information sources are frequently updated and the databases accessible to the public are generally deemed as a trusted source of certain information; and:

(1) Industries besides certificate services rely on this database to provide accurate locations, contact information and other information; and

(2) The database provider updates the information at least once per

year.

The ePKI EV SSL Certification Authority and RA shall use documentation procedures to check the accuracy of the database and ensure acceptability of the information including review of the terms of use of the database provider.

The ePKI EV SSL Certificate Authority and RA shall not use and qualified independent information source that is (i) self-published and (ii)the information is not verified to be accurate by an independent source. If the ePKI EV SSL Certificate Authority and the Company or affiliated companies has a database holding company or if any RA or the ePKI EV SSL Certificate Authority outsources any portion of the verification process to a subcontractor (or its owner or affiliated company) maintaining ownership or substantial interest in any database, then it is not deemed to be a qualified independent information source.

3.2.3.4.6 Qualified Government Information Source

Qualified government information sources are regularly updated and are currently accessible to the public which provide accurate responses to inquiries and a design which is generally deemed to be trusted database and maintained by a government agency (organization) such as the business and industry inquiry service at the MOEA Commerce Industrial Service Portal. Information reports are based upon relevant laws and regulations. False or misleading reports are subject to criminal or civil penalties. The EV SSL Certificate Guidelines do not prohibit the use of a third-party supplier to obtain information from a government agency (organization) as long as the third-party supplier directly obtains the information from a government agency (organization).

3.2.3.4.7 Qualified Government Tax Information Source

The qualified government tax information source is a source which specifically contains individual-related tax information relating to private organizations, other business groups or individuals (such as the Fiscal Information Agency, National Taxation Bureau, Internal Revenue Service (IRS) qualified tax information sources).

3.2.4 Non-Verified Subscriber Information

Not applicable.

3.2.5 Validation of Authority

When there is a connection between a certain individual and the certificate subject name when performing a certificate lifecycle activity such as a certificate application or revocation request, the ePKI EV SSL Certification Authority or RA shall perform a validation of authority to verify that the individual can represent the certificate subject such as:

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

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

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

(4) Verification of the applicant’s EV SSL certificate authorization which is detailed in section 3.2.3 includes:

A. Verify the name, title and authority of the contract signer, certificate approver and certificate requester.

B. Verify that the contract signer has signed the subscriber agreements or the authorized representative of the applicant who has agreed to the terms of use; and

C. Verify the certificate approver has signed or approved by other means the EV SSL certificate request.

The EV SSL certificate request must choose one or several (please refer to section 3.2.5.1 to section 3.2.5.6) methods recommended in the EV SSL Certificate Guidelines to authenticate the subscriber possession of the domain name. In addition to authenticating subscriber possession of the domain name, organization or individual identity authentication must still be done in accordance with sections 3.2.2 and 3.2.3 for the EV SSL certificate request.

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 directly contacts with the Domain Name Registrar. This method may only be used if:
(1) The CA or RA authenticates the Applicant's identity under section 3.2.2.2 and the authority of the Applicant Representative under Section 3.2.3.1 OR
(2) The CA or RA is also the Domain Name Registrar, or an Affiliate of the Domain Name Registrar, of the Base Domain Name.

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.

The CA or RA MAY send the email, fax, SMS, or postal mail identified under this section to one or more than one recipient, 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.

The CA 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.

3.2.5.3 Phone Contact with Domain Contact

Confirming the Applicant's control over the requested FQDN by calling the Domain Name Registrant's phone number and obtaining a response confirming the Applicant's request for validation of the FQDN. The CA or RA MUST place the call to a phone number identified by the Domain Name Registrar as the Domain Contact.

Each phone call SHALL be made to a single number and MAY confirm control of multiple FQDNs, provided that the phone number is identified by the Domain Name Registrar as a valid contact method for every Base Domain Name being verified.

3.2.5.4 Domain Authorization Document

Confirming the Applicant's control over the requested FQDN by relying upon the attestation to the authority of the Applicant’s certificate request contained in a Domain Authorization Document. The Domain Authorization Document MUST substantiate that the communication comes from the Domain Contact. The CA or RA MUST verify that the Domain Authorization Document is either (i) dated on or after the date of the domain validation request or (ii) that the WHOIS data has not materially changed since a previously provided Domain Authorization Document for the Domain Name Space.

3.2.5.5 Agreed-Upon Change to Website

Confirming the Applicant's control over the requested FQDN by confirming one of the following under the "/.well-known/pki-validation" directory, or another path registered by IANA for the purpose of Domain Validation, on the Authorization Domain Name that is accessible by the CA via HTTP/HTTPS over an Authorized Port:

(1) The presence of Required Website Content contained in the content of a file. The entire Required Website Content MUST NOT appear in the

request used to retrieve the file or web page, or

(2) The presence of the Request Token or Request Value contained in the content of a file where the Request Token or Random Value MUST NOT appear in the request.

If a Random Value is used, the CA 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 3.5 of the CPS).

3.2.5.6 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, the CA 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 3.5 of the CPS).

3.2.6 Other Verification Requirements

3.2.6.1 High Risk Status

The requirements of Section 11.5 of the Baseline Requirements apply equally to EV SSL Certificates. Please see the CPS section 4.2.1 for the Identification and authentication of high risk certificate request.

3.2.6.2 Denied Lists and Other Legal Black Lists

(1) Verification Requirements: The CA and RAs must verify whether

the Applicant, the Contract Signer, the Certificate Approver, the Applicant’s Jurisdiction of Incorporation, Registration, or Place of Business:

A. Is identified on any government denied list, list of prohibited persons, or other list that prohibits doing business with such organization or person under the laws of the country of the CA’s jurisdiction(s) of operation; or

B. Has its Jurisdiction of Incorporation, Registration, or Place of Business in any country with which the laws of the CA’s jurisdiction prohibit doing business.

The CA must not issue any EV SSL Certificate to the Applicant if either the Applicant, the Contract Signer, or Certificate Approver or if the Applicant’s Jurisdiction of Incorporation or Registration or Place of Business is on any such list.

(2) Acceptable Methods of Verification: The CA MUST take reasonable steps to verify with the lists and regulations in EV SSL Certificate Guidelines.

3.6.2.3 Parent/Subsidiary/Affiliate Relationship

A RA verifying an Applicant using information of the Applicant's Parent, Subsidiary, or Affiliate, when allowed under section 3.2.2.4.1, 3.2.2.5, 3.2.2.6.1 or 3.2.2.7, must verify the Applicant's relationship to the Parent, Subsidiary, or Affiliate. Acceptable methods of verifying the Applicant's relationship to the Parent, Subsidiary, or Affiliate include the following:

(1) QIIS or QGIS: The relationship between the Applicant and the Parent, Subsidiary, or Affiliate is identified in a QIIS or QGIS;

(2) Independent Confirmation from the Parent, Subsidiary, or Affiliate: A RA may verify the relationship between an Applicant and a Parent, Subsidiary, or Affiliate by obtaining an Independent Confirmation from the appropriate Parent, Subsidiary, or Affiliate (as described in Section 3.2.3.4.4);

(3) Contract between CA and Parent, Subsidiary, or Affiliate: The CA or A RA may verify the relationship between an Applicant and a Parent, Subsidiary, or Affiliate by relying on a contract between the CA, A RA and the Parent, Subsidiary, or Affiliate that designates the Certificate Approver with such EV Authority, provided that the contract is signed by the Contract Signer and provided that the agency and Signing Authority of the Contract Signer have been verified;

(4) Legal Opinion: A RA may verify the relationship between an Applicant and a Parent, Subsidiary, or Affiliate by relying on a Verified Legal Opinion (as described in Section 3.2.6.2);

(5) Accountant Letter: A RA may verify the relationship between an Applicant and a Parent, Subsidiary, or Affiliate by relying on a Verified Accountant Letter (as described in Section 3.2.6.3); or

(6) Corporate Resolution: A RA may verify the relationship between an Applicant and a Subsidiary by relying on a properly authenticated corporate resolution that approves creation of the Subsidiary or the Applicant, provided that such resolution is (i) certified by the appropriate corporate officer (e.g., secretary), and (ii) the RA can reliably verify that the certification was validly signed by such person, and that such person does have the requisite authority to provide such certification.

3.2.6.4 Final Cross-Correlation and Due Diligence

Except for Enterprise EV SSL Certificates:

(1) The results of the verification processes and procedures outlined in these Guidelines are intended to be viewed both individually and as a group. Thus, after all of the verification processes and procedures are completed, ePKI EV SSL CA must have a person who is not responsible for the collection of information review all of the information and documentation assembled in support of the EV SSL certificate application and look for discrepancies or other details requiring further explanation.

(2) ePKI EV SSL CA must obtain and document further explanation or clarification from the applicant, certificate approver, certificate requester, Qualified Independent Information Sources, and/or other sources of information, as necessary, to resolve those discrepancies or details that require further explanation.

(3) ePKI EV SSL CA must refrain from issuing an EV SSL Certificate until the entire corpus of information and documentation assembled in support of the EV SSL certificate request is such that issuance of the EV SSL certificate will not communicate factual information that the ePKI EV SSL CA knows, or the exercise of due diligence should discover from the assembled information and documentation, to be inaccurate. If satisfactory explanation and/or additional documentation are not received within a reasonable time, the ePKI EV SSL CA must decline the EV SSL certificate request and should notify the applicant accordingly.

(4)In the case where some or all of the documentation used to support the application is in a language other than the ePKI EV SSL CA's normal operating language, the ePKI EV SSL CA or its Affiliate must perform the requirements of this Final Cross-Correlation and Due Diligence section using employees under its control and having appropriate training, experience, and judgment in confirming organizational identification and authorization and fulfilling all qualification requirements contained in Section 14.1 of these Guidelines. When employees under the control of ePKI EV SSL CA do not possess the language skills necessary to perform the Final Cross-Correlation and Due Diligence the CA may:

(A)Rely on language translations of the relevant portions of the documentation, provided that the translations are received from a Translator; or

(B)When ePKI EV SSLCA has utilized the services of an RA, ePKI EV SSL CA may rely on the language skills of the RA to perform the Final Cross-Correlation and Due Diligence, provided that the RA complies with subsections (1), (2) and (3) of this section. Notwithstanding the foregoing, prior to issuing the EV SSL Certificate, ePKI EV SSL CA must review the work completed by the RA and determine that all requirements have been met; or

(C)When ePKI EV SSL CA has utilized the services of an RA, ePKI EV SSL CA may rely on the RA to perform the Final Cross-Correlation and Due Diligence, provided that the RA complies with this section and is subjected to the Audit Requirements of Sections 17.5 and 17.6.

In the case of Enterprise EV SSL Certificates to be issued in compliance with the requirements of Section 14.2 of these Guidelines, the Enterprise RA may perform the requirements of this Final

Cross-Correlation and Due Diligence section.

3.2.7 Data Source Accuracy

Prior to using any data source as a Reliable Data Source, the ePKI EV SSL CA SHALL evaluate the source for its reliability, accuracy, and resistance to alteration or falsification. The ePKI EV SSL CA 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 the ePKI EV SSL CA, 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 for the purpose of fulfilling the validation requirements under Section 3.2 of CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates.

3.3 Re-key Request Identification and Authentication

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 certificates. 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

Two months prior to the expiry of a subscriber requested EV SSL certificate, the system shall send an email to remind the subscriber to submit a new certificate request. The requester generates a new keypair for use to sign the new private keypair certificate request file and passes the certificate request file and signed subscriber terms of agreement to the RA. The RA then performs identification and authentication of the subscriber who is submitting a new certificate request for an expired certificate. The RA shall use the subscriber’s public key to verify the certificate request file’s digital signature to verify the subscriber’s identity.

The ePKI EV SSL Certification Authority does not accept subscriber EV SSL certificate renewal requests.

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 the ePKI EV SSL Certification Authority. The RA shall perform subscriber identification and authentication for the certificate reapplication in accordance with the regulations in section 3.2, 3.3 and 3.4.

3.4 Identification and Authentication for Certificate Revocation Request

The ePKI EV SSL Certification Authority 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 and section 3.3.

3.5 Requirements for Re-use of Existing Documentation

For each EV SSL Certificate Request, including requests to renew existing EV SSL Certificates, the CA must perform all authentication and verification tasks required by EV SSL certificate Guidelines to ensure that the request is properly authorized by the Applicant and that the information in the EV SSL Certificate is still accurate and valid. This section sets forth the age limitations on for the use of documentation collected by the CA and RA.

3.5.1 Validation for Existing Subscribers

If an Applicant has a currently valid EV SSL Certificate issued by the CA, the CA and RA may rely on its prior authentication and verification of:

(1) The Principal Individual verified under Section 3.2.2.2.2.(4) if the individual is the same person as verified by the CA or RA in connection with the Applicant's previously issued and currently valid EV SSL Certificate;

(2) The Applicant's Place of Business under Section 3.2.2.4.1

(3) The Applicant's Verified Method of Communication required by Section 3.2.2.5 but still must perform the verification required by section 3.2.2.5.2(2);

(4) The Applicant's Operational Existence under Section 3.2.2.6;

(5) The Name, Title, Agency, and Authority of the Contract Signer, and Certificate Approver under Section 3.2.3.1; and

(6) The Applicant's right to use the specified Domain Name under Section 3.2.2.7 and Section 3.2.2.4, provided that the CA and the RA verifies that the WHOIS record still shows the same Domain

Name Registrant as when the CA and the RA verified the specified Domain Name for the initial EV SSL Certificate.

3.5.2 Re-issuance Requests

The CA may rely on a previously verified certificate request to issue a replacement certificate, so long as the certificate being referenced was not revoked due to fraud or other illegal conduct, if:

(1) The expiration date of the replacement certificate is the same as the expiration date of the EV SSL Certificate that is being replaced, and

(2) The Subject Information of the Certificate is the same as the Subject in the EV SSL Certificate that is being replaced.：

3.5.3 Age of Validated Data

(1) Except for reissuance of an EV SSL Certificate under Section 3.5.2 and except when permitted otherwise in Section 3.5.1, the age of all data used to support issuance of an EV SSL Certificate (before revalidation is required) shall not exceed the following limits:

A. Legal existence and identity – thirteen months;

B. Assumed name – thirteen months;

C. Address of Place of Business – thirteen months;

D. Verified Method of Communication – thirteen months;

E. Operational existence – thirteen months;

F. Domain Name – thirteen months;

G. Name, Title, Agency, and Authority – thirteen months, unless a contract between the CA and the Applicant specifies a different term, in which case, the term specified in such contract controls. For example, the contract may include the perpetual assignment of EV roles until revoked by the Applicant or CA, or until the contract expires or is terminated.

(2) The thirteen-month period set forth above shall begin to run on the date the information was collected by the CA.

(3) The CA may reuse a previously submitted EV SSL Certificate Request, Subscriber Agreement, or Terms of Use, including use of a single EV SSL Certificate Request in support of multiple EV SSL Certificates containing the same Subject to the extent permitted under Sections 3.2.3.2 and 3.2.3.3.

(4) The CA MUST repeat the verification process required in EV SSL Certificate Guidelines for any information obtained outside the time limits specified above except when permitted otherwise under section 3.5.1.

4. Certificate Lifecycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Computer and communications equipment (such as routers, firewalls, data**b**ase secure audit hardware) or application software (such as web server, email server, application server or Lync server) property classification, the owner of the equipment or application must submit the certificate request since property has no legal capacity to act. Organizations such as government agencies (organizations), private organizations, international non-profit organizations or business entities must serve as applicants to submit a request for EV SSL certificates.

The issuance of EV SSL certificate must have the following three types of applicant authorization roles as described in Chapter 3.

Certificate requester: The EV certificate requester must have obtained authorization for certificate requester signature and transmission.

Certificate approver: The EV certificate requester must have authorization for certificate filing review and approval.

Contract signer: The subscriber agreements used with the EV SSL certificate request must have authorization for contract signer signing.

The applicant can authorize a certain natural person to serve one or more of the above roles.

4.1.2 Enrollment Process and Responsibilities

The ePKI EV SSL Certification Authority and RA are responsible for ensuring that the certificate applicant identity is verified in compliance with CP and CPS regulations before certificate issuance. The certificate applicant is responsible for providing sufficient and accurate information (such as filling out the organization legal name or Registration Number, certificate requester's name or website fully qualified domain name based on the type of the certificate applied for) and identification documents are given to the RA. The ePKI EV SSL Certification Authority 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 the CPS and Subscriber Agreement and verify the accuracy of the information submitted for the application.

(2) The subscriber shall accept the certificate in accordance with the regulations in section 4.4 after the ePKI EV SSL Certification Authority approves the certificate application and issues the

certificate.

(3) After obtaining the certificate issued by the ePKI EV SSL Certification Authority, the subscriber shall check the accuracy of the information contained on the certificate and use the certificate 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 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 the ePKI EV SSL Certification Authority 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 procedure is as follows:

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

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

(3) The certificate requester self-generates a key, creates a PKCS#10 certificate application file and signature with the private key. When making the certificate request, the certificate request file is sent by secure channels to the RA.

4.2.1 Performing Identification and Authentication Functions

The ePKI EV SSL Certification Authority 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 the regulations in section 3.2 of the 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 the ePKI EV SSL Certification Authority and RA during the application process shall be properly kept in a secure, auditable manner in accordance with CP and CPS regulations.

The ePKI EV SSL Certificate Authority and RA shall perform pre-certificate approval verification and extra checks on high risk certificate requests. In addition to the procedures described in sections 3.1.2.1 and 3.2.2.7, those high risk FQDN used with internet phishing or other fraudulent purposes, the phishing websites announced by those organizations such as the Anti-Phishing Working Group (APWG), FQDN in previously rejected certificate request, FQDN owned by browser companies or prohibited from placement in EV SSL certificates, above black lists are collected by the ePKI EV SSV Certificate Authority and RA in the RA system to alert RA officers. RA officers can enter FQDN that will be signed in the certificate subject alternative name attribute to the Google Safe Browsing List or Miller Smiles phishing list to check if that FQDN is suspicious, to prevent the mis-issuance of EV SSL certificates.

4.2.2 Approval or Rejection of Certificate Applications

The RA shall assign another RA officer who is different from the RA officer responsible for collecting information for the identification and authentication of the applicant’s identity to review and approve the information and documentation supporting the EV SSL certificate request and see if there are still any discrepancies or other information which requires further explanation in the CPS identity identification and authentication procedure.

If the various identity authentication tasks cannot be successfully completed, the ePKI EV SSL Certificate Authority and RA may refuse the certificate request. In addition to identification and authentication of applicant’s identity, the ePKI EV SSL Certificate Authority and RA may also refuse to issue the certificate for other reasons. The ePKI EV SSL Certificate Authority and RA may refuse the certificate request due to previous refusal of the applicant’s certificate request or violations of the subscriber agreements.

As the Internet Corporation for Assigned Names and Numbers, (ICANN) opens the applications for the generic top-level domain (gTLD), the root CAs listed in its browser CA trust list are required to verify if the Subject alternative names, or the commonNames of the Subject names of the EV SSL certificates issued outwards by its PKI have ever recorded the internal names. The CAs that have issued certificates including such kind of domain names shall subscribe ICANN gTLD Notification.

The ePKI EV SSL Certificate Authority will not issue any EV SSL certificate that mark a new gTLD may be issued by ICANN. If ICANN has announced that it considers issuing a new gTLD, and the ePKI EV SSL Certificate Authority discovers some certificate applicant wishes to apply an EV SSL certificate including an Internal Name using the new gTLD to be analyzed, the ePKI EV SSL Certificate Authority shall warn the applicant. Unless the subscriber also registers its domain name, or the EV SSL certificate will be revoked once the new gTLD starts operating. The gTLD operator's contract information is available at www.icann.org; when ICANN allows the new gTLD to operate, the ePKI EV SSL Certificate Authority will check against the effective certificate to see if that gTLD is included. The issuance of EV SSL certificate for the website whose name includes that new gTLD will be suspended, unless the CA is able to prove the certificate subscriber does control that domain.

The 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

The ePKI EV SSL Certification Authority and RAs shall complete the EV SSL certificate application processing 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 for the RA to process the certificate request and the ePKI EV SSL Certificate Authority to issue the certificate depends on the certificate classification and may be disclosed in the subscriber agreements, contract or ePKI EV SSL Certificate Authority website.

The review procedure for EV SSL certificate request cases which are received and meet relevant regulations shall be completed within 5 working days by at least two RA officers and the subscriber shall be asked to accept the certificate. After the certificate is accepted, the ePKI EV SSL Certificate Authority shall complete the certificate issuance work within one working day or the desired date stipulated by the subscriber to pick up the certificate.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

After the ePKI EV SSL Certification Authority and its RAs accept the certificate application information, the relevant review procedures are followed in accordance with the regulations of Chapter 3 in the CPS to serve as a basis for determining whether approve the certificate issuance or not.

Certificate issuance steps are follows:

(1) The RA submits the certificate application information from the review process to the ePKI EV SSL Certification Authority.

(2) When the ePKI EV SSL Certification Authority receives the certificate application information submitted by the RA, the authorization status of the relevant RA is first checked, the authorized assurance level and scope is verified and then the certificate is issued based of the certificate application information submitted by the RA.

(3) If the RA authorized assurance level and scope does not comply with the certificate application, the ePKI EV SSL Certification Authority sends 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 the ePKI EV SSL Certification Authority to understand where the problem is.

(4) In order to ensure the security, integrity and non-reputability of the information transmitted by the ePKI EV SSL Certification Authority and RA, the certificate application information is encrypted with a digital signature and transmitted through the network by transport layer security (TLS) means.

(5) The ePKI EV SSL Certification Authority reserves the right to refuse certificate issuance to any entity. The ePKI EV SSL Certification Authority shall not bear any liability for damages to certificate applicants.

4.3.2 Notification to subscriber by the CA of issuance of certificate

After the ePKI EV SSL Certification Authority completes certificate issuance, the subscriber is notified to pick up the certificate or the RA is used to notify the subscriber to pick up the certificate.

If the ePKI EV SSL Certification Authority 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

The certificate acceptance procedure for EV SSL certificates issued by the ePKI EV SSL Certificate Authority is as below.

The certificate requester pre-reviews the content of the certificate to be issued. The certificate requester reviews the information that will be recorded in the certificate for accuracy and provides consistent information for the application. If the certificate requester reviews the content of the to be issued certificate and refuses to accept the information recorded in the certificate, then the certificate will not be issued. For example, while pre-reviewing, if a certificate requester discovered there were other FQDNs required for TLS encrypted channels should be record in the multi-domain EV SSL certificate's certificate subject alternative name field, the to be signed multi-domain EV SSL certificate may be refused and the certificate request may be resubmitted in accordance with sections 4.1 and 4.2.

The above certificate requester shall review the certificate field that should at least include the certificate subject name and certificate subject alternative name field before deciding to accept the certificate.

Acceptance of the certificate is deemed as the certificate applicant's consent to follow the rights and obligations in the CPS and subscriber agreements.

If there is fee collection or refund matters involved with the certificate applicant's refusal to accept the certificate, the certificate applicant shall handle matters in accordance with the contract established in compliance with the Consumer Protection Act and fair-trade principles.

4.4.1 Conduct Constituting Certificate Acceptance

The certificate requester pre-reviews the certificate content for errors. The certificate is published by the ePKI EV SSL Certification Authority in the repository or delivered to the certificate requester.

4.4.2 Publication of the Certificate by the ePKI EV SSL Certification Authority

The ePKI EV SSL Certification Authority repository service regularly publishes the issued certificates or delivers the certificate to the certificate applicant to achieve certificate publication. The RA may negotiate with the ePKI EV SSL Certification Authority about certificate delivery by the RA to the certificate applicant.

4.4.3 Notification of Certificate Issuance by the ePKI EV SSL Certification Authority to Other Entities

The ePKI EV SSL Certification Authority does not provide certificate issuance notification to other entities besides the certificate requester and the RA. Relying parties may make inquiries or download certificates through the ePKI EV SSL Certificate Authority’s repository.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers refer to the entities who request and obtain EV SSL certificates approved by the ePKI EV SSL Certification Authority. Their relationship with the certificate subject is shown in the table in section 1.3.3 of the CPS. Usage of EV SSL certificates is stipulated in section 1.4.1 of the CPS. Subscriber key pair generation shall comply with the regulations in section 6.1.1 of the CPS. Subscribers must independently possess and control the right and capability to the private key corresponding to the certificate. Subscribers themselves do not issue certificates to others. Subscribers shall protect the private key from unauthorized use or disclosure. Private keys shall only be used for correct keyUsages (keyUsage is recorded in the certificate extension) such as digital signatures and key encryption. Subscribers must correctly use certificates according to the CP listed on the certificate.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties refer to third parties who trust the binding between the certificate subject name and public key. Relying parties shall use software that is compliant with ITU-T X.509, Internet Engineering Task Force (IETF) RFC, CA/Browser Forum Baseline Requirements for the

Issuance and Management of Extended Validation Certificates related standards and specifications.

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

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

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

(3) Establish secure communication channels with the subscriber.

The above certificate status information may be obtained from CRL or OCSP services. The CRL distribution point location can be obtained from the certificate details. In addition, the relying parties shall check the CA issuer and subscriber certificate CP to verify the assurance level of the certificate.

For example, relying parties may only trust digital signatures and 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

Certificate renewal refers to the reissue of one certificate with unchanged subscriber identification information which has the same public key, the same certificate subject information and a different serial number from the original certificate but it is a certificate with a valid extension. Since random extension of public keys could result in reduced private key security and increased probability of key compromise and EV SSL certificates has the short maximum validity period (825 days) in international standards for the various SSL certificates. The reverification time of certificate request information accuracy is also the shortest period (maximum of 13 months). The ePKI EV SSL Certificate Authority does not provide certificate renewal services. Key pair generation and certificate request submission is done in the same manner as the initial registration.

4.6.1 Circumstances for Certificate Renewal

Not applicable.

4.6.2 Who May Request Renewal

Not applicable.

4.6.3 Processing Certificate Renewal Requests

Not applicable.

4.6.4 Notification of Renew Certificate Issuance to Subscriber

Not applicable.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Not applicable.

4.6.6 Publication of the Renewal Certificate by the CA

Not applicable.

4.6.7 Notification of Renewal Certificate Issuance by the ePKI EV SSL Certification Authority to Other Entities

Not applicable.

4.7 Certificate Re-Key

4.7.1 Circumstances for Certificate Re-Key

4.7.1.1 Circumstances for ePKI EV SSL Certification Authority Subordinate CA Certificate Re-Key

The ePKI EV SSL Certification Authority private key shall be routinely re-keyed in accordance with the regulations in section 6.3.2 so the new private key is used instead of the old private key to issue certificates. Notification shall be made at appropriate time to all entities that trust the ePKI EV SSL Certification Authority certificate authorities. The ePKI EV SSL Certification Authority shall issue subscriber certificates and CRLs with the new private key and the new certificates shall be published in the repository for subscriber download. The old private key shall still be used to issue CRLs and on-line certificate status protocol responses to maintain and protect all subscriber certificates issued with the old private key until their expiry.

The ePKI EV SSL Certification Authority shall re-key the key pairs used to issue certificates before the usage period of the certificate issued with the private key expires at the latest. After the key pair is re-keyed, the ePKI EV SSL Certification Authority shall apply for new certificate from the above level CA (ePKI Root Certification Authority (eCA)) in accordance with the regulations in section 4.2 of the eCA CPS. The eCA shall issue the new certificate and notify the ePKI EV SSL Certification Authority.

If the ePKI EV SSL Certification Authority's own certificate has been revoked and use of its private key has been suspended, the key pair must be re-keyed.

4.7.1.2 Circumstances for Subscriber Certificate Re-Key

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

If the subscriber's EV SSL certificate has not been revoked, the ePKI EV SSL Certification Authority or RA can start to accept the re-key and request a new certificate two months before the expiry of the subscriber's private key use period. The request procedure for the new certificate shall be handled in accordance with sections 4.1 and 4.2.

After the subscriber EV SSL certificate is revoked, use of its private key shall be suspended. After the key pair re-key, a new certificate may be requested from the ePKI EV SSL Certification Authority in accordance with sections 4.1 and 4.2.

4.7.2 Who May Request Certificate Re-Key

(1) The ePKI EV SSL Certification Authority may submit a

subordinate CA application with the eCA.

(2) A subscriber or legally authorized third party (representative authorized by the organization) may submit a subscriber certificate application with the ePKI EV SSL Certification Authority.

4.7.3 Processing certificate re-keying requests

When the ePKI EV SSL Certification Authority certificate is re-keyed, a new certificate application is submitted to the eCA. See the regulations in sections 3.1, 3.2, 3.3, 4.1 and 4.2 of the eCA CPS.

For subscriber certificate re-key, a new certificate application is submitted to the ePKI EV SSL Certification Authority. See the regulations in sections 3.1, 3.2, 3.3, 3,4, 4.1 and 4.2 of the CPS.

4.7.4 Notification of new certificate issuance to subscriber

For notification to issue subscriber certificate re-key, see the regulations in section 4.3.2.

4.7.5 Circumstances Constituting Acceptance of Certificate Re-Key

For circumstances constituting acceptance of the CA certificate re-key by the ePKI EV SSL Certification Authority, see section 4.7.5 in the eCA CPS.

The certificate applicant previews the content of the subscriber certificate to be issued. The subscriber certificate is published by the CA on the repository or delivered to the certificate applicant.

4.7.6 Publication of the Re-Keyed Certificate by the ePKI EV SSL Certification Authority

The ePKI EV SSL Certification Authority repository service regularly publishes the new certificates issued through certificate re-key or delivers the new certificate to the certificate applicant to achieve certificate re-key publication. The RA may negotiate with the ePKI EV SSL Certification Authority about certificate delivery by the RA to the certificate applicant.

4.7.7 Notification by the ePKI EV SSL Certification Authority to Other Entities

RA may receive notification of subscriber certificate re-key.

After the subordinate CA certificate is issued by the ePKI Root Certification Authority, the ePKI EV SSL Certification Authority shall publish the subordinate CA certificate on the ePKI EV SSL Certification Authority website repository to facilitate notification of other entities.

4.8 Certificate Modification

4.8.1 Circumstances for Certificate Modification

Certificate modifications are some differences between the authentication information in one new certificate and an old certificate (for example a new FQDN or other relatively unimportant attribute information) from the same certificate subject which conforms to relevant regulations in the CPS. The new certificate may have a new certificate subject public key or use the original subject public key but the certificate expiry date and the original certificate expiry date are the same. After the certificate is modified, the old certificate shall be revoked.

If there are any changes to important identity information such as the organization name, the original certificate must be revoked. The subscriber must submit a new certificate application with the modified organization name to obtain a new certificate. The certificate request shall be handled in accordance with the procedures in sections 4.1 and 4.2.

4.8.2 Who May Request Certificate Modification

Subscribers, RAs or legally authorized third parties (such as agents authorized by the organization).

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 4.1, 4.2 and 4.9 for the guidelines established by the RA. For example, if the certificate modification applicant is asked to use his private key to add a signature to the certificate application file 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 verification work, the new certificate application and the original certificate revocation request is sent to the ePKI EV SSL Certification Authority.

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

(4) If the application does not pass the above checking, the ePKI EV SSL Certification Authority 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 the ePKI EV SSL Certification Authority to understand the source of the problem.

(5) In order to ensure the security, integrity and non-reputability of the information transmitted by the ePKI EV SSL Certification Authority and RA, the certificate request information is affixed with a digital signature, encrypted and transmitted through the network by transport layer security (TLS) means.

(6) The RA shall set the time interval between the new certificate request with the certificate modification 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 the ePKI EV SSL CA 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 the CPS and related contracts.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

The certificate applicant previews the content of that will be issued in the certificate. The certificate is published by the ePKI EV SSL Certificate Authority on the repository or delivered to the certificate requester.

4.8.6 Publication of the Modified Certificate by the ePKI EV SSL Certification Authority

The ePKI EV SSL Certification Authority 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 the ePKI EV SSL Certification Authority about certificate delivery by the RA to the certificate applicant.

4.8.7 Notification of Certificate Issuance by the ePKI EV SSL Certification Authority to Other Entities

The ePKI EV SSL Certification Authority does not provide certificate issuance of modified certificates notification to entities besides subscribers and RA. Relying parties can make inquiries or download certificates from the ePKI EV SSL Certification Authority repository.

4.9 Certificate Suspension and Termination

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

4.9.1 Circumstances for Certificate Revocation

The certificate subscriber shall submit a certificate revocation request to the RA under (but not limited to) any of the following circumstances:

(1) Private key lost, stolen, modified, destroyed, disclosed without authorization or has been subject to other damage or misuse.

(2) The information recorded on the certificate is sufficient to have a significant effect on subscriber trust.

(3) Certificate is no longer needed for use.

(4) The original certificate request did not receive authorization from the subscriber and the subscriber is not willing to grant authorization retroactively.

In addition, the ePKI EV SSL Certification Authority must notify the subscriber in advance of certificate revocation under the following circumstances.

(1) Some items listed on the certificate are known to be untrue,

inaccurate, or misleading;

(2) Known misuse, counterfeiting or compromise of the certificate subscriber’s signature private key, or fail to satisfy the regulations of sections 6.1.5 and 6.1.6 of the CPS;

(3) Known ePKI EV SSL Certification Authority private key or information system misuse, counterfeiting or compromise which affects the reliability of the certificate.

(4) Known failure to issue the certificate in accordance with CP, CPS or EV SSL Certificate Guidelines regulations and procedures.

(5) Subscriber violation or inability to follow the regulations or obligations in the CP, CPS, EV SSL Certificate Guidelines, subscriber agreements, or any other contracts and relevant laws.

(6) Notification by judicial or prosecution authority or in accordance with related legal regulations.

(7) The FQDN recorded in the certificate has lost its legal right to use (for example: use of a certain domain name by the domain name registrar has been revoked by a court decision, the service agreement or authorization between the requester and domain name registrar has been terminated or the domain name registrar has not applied for an extension for a certain domain name);

(8) The authority of the ePKI EV SSL Certification Authority to issue certificates expires, is revoked or terminated, and the ePKI EV SSL CA no longer operates the repository, publishes CRLs, or provides the OCSP inquiry service;

(9) Revocation upon the regulations of the CP or the CPS;

(10) The technical contents or format of a certificate demonstrate the unacceptable risk(s) toward the application software providers or relying parties (e.g. CA/Browser Forum may determine that some cryptography, signature algorithm, or the key size incurs

unacceptable risk(s), and that certificate will be revoked or replaced by the CA within a certain period);

(11) The subscriber fails to pay the certificate fee when the fee is overdue and the subscriber has been urged to pay.

When the ePKI EV SSL Certification Authority terminates its service, if there is no CA to take over the ePKI EV SSL Certification Authority service, the competent authorities shall be notified to arrange for other CA to take over the service. If still no other CA can take over the service, the ePKI EV SSL Certification Authority shall publish the revoked certificates in the repository and notify all certificate-related persons 30 days prior to service termination.

4.9.2 Who Can Request Certificate Revocation

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

In addition, a subscriber, relying party, application software provider or other third party may submit certificate problem report to inform the ePKI EV SSL CA of reasonable reasons 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 the ePKI EV SSL Certification Authority.

(3) When the ePKI EV SSL Certification Authority receives the certificate revocation application information sent by the RA, the ePKI EV SSL Certification Authority 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, the ePKI EV SSL Certification Authority 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 the ePKI EV SSL Certification Authority to understand the source of the problem.

(5) In order to ensure the security, integrity and non-reputability of the information transmitted by the ePKI EV SSL Certification Authority and RA, the certificate application information is affixed with a digital signature, encrypted and transmitted through the network by transport layer security (TLS) means.

(6) The ePKI EV SSL Certification Authority uses the same ePKI EV SSL Certification Authority 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 inquiry service (e.g. the status of being revoked, the status of being applied, or the status is valid).

(8) The ePKI EV SSL Certification Authority receives certificate problem reports and provides the certificate problem response mechanism 24x7, 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, the ePKI EV SSL Certification Authority provides the guidelines for certificate problem reports, for the subscribers, the application software providers, the relying parties, and other third-party organizations to report the certificate problem reports when they observe the possible events of the private key 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 the ePKI EV SSL Certification Authority within one hour. When the subscriber's private key is lost or suspect or known to be compromised or the information recorded on 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. The ePKI EV SSL Certification Authority may extend the certificate revocation grace period when deemed necessary.

4.9.5 Time Within Which CA must Process the Revocation Request

After the subscriber submits a certificate revocation request, the RA shall promptly complete the review procedure within two working days. If the revocation application information is free of errors and passes the review, the ePKI EV SSL Certification Authority shall complete the certificate revocation work within one working day.

The ePKI EV SSL Certification Authority shall investigate and confirm if the request of certificate revocation is accepted by the following principles in 24 hours upon receiving the certificate problem reports. If the request of certificate revocation is accepted after the confirmation, the operation of certificate revocation will be proceeded by the regulations of Section 4.9.3.

(1)The claimed problematic content.

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

(3)The entity submits the certificate problem report.

(4)The related laws and regulations.

4.9.6 Revocation Checking Requirements for Relying Parties

Before using certificates issued by the ePKI EV SSL CA, the relying parties shall first check the CRL or OCSP responses published by the ePKI EV SSL CA 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.

The ePKI EV SSL Certification Authority publishes revoked certification information on the repository for checking purposes. There are no restrictions for the checking of CRL by relying parties. The website is as follows:

http://evssl.hinet.net

4.9.7 CRL Issuance Frequency

The CRL issuance frequency of the ePKI EV SSL Certification Authority is at least twice per day. Issued CRL are valid for no more than 36 hours. Before the CRL expires, the ePKI EV SSL Certification Authority 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 ePKI EV SSL Certification Authority repository to receive the updated certificate revocation information.

4.9.8 Maximum Latency for CRL Publishing

The ePKI EV SSL Certification Authority shall publish the CRL at the latest before the nextUpdate listed on the CRL.

4.9.9 OCSP Service

The ePKI EV SSL CA provide the inquiry to certificate revocation/status by CRL, webpage certificate inquiries and download, and OCSP responses.

The ePKI EV SSL CA uses OCSP Responder to provide the OCSP responses complying with RFC 6960 and RFC 5019 standards. The key for signatures of the ePKI EV SSL CA uses RSA 2048 w/ SHA-256 hash function algorithm to issue the certificates for OCSP Responder, for the relying parties to verify the digital signatures of the OCSP responses, for the purpose of verifying the integrity of the information sources.

4.9.10 On-Line Revocation Checking Requirements

Relying parties shall check the CRL or OCSP service in accordance with the regulations in section 4.9.6 or 4.9.9 to check if the certificates used are valid or not.

The ePKI EV SSL CA uses SHA-256 Hash Function Algorithm to issue OCSP responses.

The ePKI EV SSL CA supports the relying parties of the OCSP inquiry service to use HTTP POST and HTTP GET to execute the OCSP inquiry service.

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

In case the OCSP responders receive the status request of the un-issued certificates, the status shall not be replied as “Good,” and the ePKI EV SSL CA shall supervise if the OCSP responders reply such request complying with the above-mentioned secure responding procedures.

4.9.11 Other forms of revocation advertisements available

In order to speed up verification of high traffic website EV SSL certificates to instantly complete the EV SSL certificate status verification work, the ePKI EV SSL Certification Authority supports OCSP stapling operation based on RFC 4366 and uses subscriber agreements, supports Certificate Transparency and technical checks and provides descriptions of the relevant settings to assist subscribers who own high traffic websites to establish OCSP stapling.

4.9.12 Special Requirements Related to Key Compromise

There are no other requirements different from the regulations in sections 4.9.1, 4.9.2 and 4.9.3.

4.9.13 Circumstances for Suspension

Not applicable.

4.9.14 Who Can Request Certificate Suspension

Not applicable.

4.9.15 Procedure for Certificate Suspension

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.9.17 Procedure for Certificate Resumption

Not applicable.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The ePKI EV SSL CA submits the CRL and provides OCSP service at the CRL distribution point recorded on the subscriber certificate. The ePKI EV SSL CA also provides OCSP request services.

The revocation record of a certificate in CRL or OCSP response will only be removed once that revoked certificate expires.

4.10.2 Service Availability

The ePKI EV SSL Certification Authority shall provide 24x7 uninterrupted certificate status services.

4.10.3 Optional Features

Not stipulated.

4.11 End of Subscription

End of subscription refers to the termination of ePKI EV SSL Certification Authority services to certificate subscribers including termination of ePKI EV SSL Certification Authority services provided to subscribers upon certification expiry or service termination upon subscriber certification revocation.

The ePKI EV SSL Certification Authority shall allow the subscriber to waive renewal when the certificate is revoked or expires or terminate the purchase of certificate services due to invalidation of the subscriber agreements.

4.12 Private Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

Private keys used for signatures may not be escrowed.

4.12.2 Session Key Encapsulation and Recovery Policy and Practice

The ePKI EV SSL Certification Authority 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 ePKI EV SSL Certification Authority 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 ePKI EV SSL Certification Authority equipment.

5.1.2 Physical Access

The ePKI EV SSL Certification Authority has established suitable measures to control connections to ePKI EV SSL Certification Authority service hardware, software and hardware security module.

The ePKI EV SSL Certification Authority 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 ePKI EV SSL Certification Authority system.

Non-ePKI EV SSL Certification Authority personnel entering the facility are required to sign the entry/exit log and must be accompanied throughout by ePKI EV SSL Certification Authority personnel.

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

5.1.4 Water Exposures

The ePKI EV SSL Certification Authority 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 ePKI EV SSL Certification Authority 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 information and documents of the ePKI EV SSL Certification Authority detailed in section 9.1.3 are no longer in use, all shredded paper, magnetic tapes, hard disks, floppy disks, MO and other forms of memory shall be formatted to erase the information stored on them. 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 EPKI EV SSL Certification Authority 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, the ePKI EV SSL Certification Authority uses procedural controls to specify the trusted roles of ePKI EV SSL Certification Authority 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 ePKI EV SSL Certification Authority 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 the ePKI EV SSL Certification Authority are administrator, officer, auditor, 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 five roles are as follows:

The administrator is responsible for:

- Installation, configuration and maintenance of the ePKI EV SSL Certification Authority system.
- Creation and maintenance of system user accounts.
- Generation and backup of ePKI EV SSL Certification Authority keys.

The officer is responsible for:

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

The auditor is responsible for:

- Checking, maintenance and archiving of audit logs.
- Conducting or supervising internal audits to ensure the ePKI EV SSL Certification Authority is operating in accordance with CPS regulations.

The 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 the ePKI EV SSL CA.
- 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.

As described in section 4.2.2 and section 5.2.4, the RA system must handle certificate registration review and certificate request issuance by at least two different trusted roles using a two-factor identification login system.

5.2.2 Role Assignment

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

- The administrator, the officer, the auditor, and the cyber security coordinator cannot assume any other roles among these four trust roles at the same time, but the administrator, the officer, and the auditor can be the operator as well.
- The physical security controller shall not concurrently assume any role of the administrator, the officer, the auditor, and the operator.
- A person serving a trusted role is not allowed to perform self-audit.

5.2.3 Number of Persons Required Per Task

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

- Administrator

At least 3 qualified individuals are needed.

- Officer

At least 2 qualified individuals are needed.

- Auditor

At least 2 qualified individuals are needed.

- 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	Officer	Auditor	Operator	Physical security controller	Cyber security coordinator	Anti-virus and anti-hacking coordinator
Installation, configuration, and maintenance of the ePKI EV SSL CA system	2				1		
Establishment and maintenance of system user accounts	2				1		
Generation and backup of ePKI EV SSL CA 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		

Assignments	Administrator	Officer	Auditor	Operator	Physical security controller	Cyber security coordinator	Anti-virus and anti-hacking coordinator
Daily operation and maintenance of system equipment				1	1		
System backup and recovery				1	1		
Storage media updating				1	1		
Hardware and software updates outside the ePKI EV SSL CA 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		

5.2.4 Identification and Authentication for each Role

Use IC cards to identify and authenticate administrator, officer, auditor and 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 perform related review actions, they shall use IC cards to verify their identities and execute digital signatures.

Operating system account management by the ePKI EV SSL Certification Authority host uses login account numbers, passwords and groups to identify and authenticate administrator, officer, auditor and operator roles. The ePKI EV SSL Certification Authority uses the user's account, password, and system account administration functions, or other security mechanisms to identify the role of the cyber security coordinator.

5.3 Personnel Controls

5.3.1 Background, Qualifications, Experience and Clearance Requirements

1. Security evaluation for personnel selection

   Personnel selection includes the following items:

   (1) Personality evaluation.

   (2) Applicant experience evaluation.

   (3) Academic and professional skills and qualifications evaluation.

   (4) Personal identity check.

   (5) Trustworthiness. Check if personnel have criminal records in accordance with EV SSL Certificate Guidelines.

2. Management of Personnel Evaluation

All ePKI EV SSL Certification Authority personnel performing certificate work shall have their qualifications reviewed at the initial time of employment to verify their trustworthiness and work capabilities. After formal employment, personnel shall receive appropriate training and sign a document accepting responsibility to perform their stipulated duties. All personnel shall have their qualifications rechecked each year to reconfirm their trustworthiness 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. Management of Personnel Appointment, Dismissal and Transfer

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

4. Duty of Confidentiality Agreement

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

5.3.2 Background Check Procedures

The ePKI EV SSL Certification Authority 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. ePKI EV SSL Certification Authority security principles and mechanism. 2. Installation, configuration, and maintenance of the ePKI EV SSL Certification Authority operation procedures. 3. Establishment and maintenance of system user accounts operation procedures.

Trusted Role	Training Requirements
	4. Audit parameter configuration setting procedures. 5. ePKI EV SSL Certification Authority key generation and backup operation procedures. 6. Disaster recovery and continuous operation procedure.
Officer	1. ePKI EV SSL Certification Authority security principles and mechanism. 2. ePKI EV SSL Certification Authority 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.
Auditor	1. ePKI EV SSL Certification Authority security principles and mechanism. 2. ePKI EV SSL Certification Authority system software and hardware use and operation procedures. 3. ePKI EV SSL Certification Authority key generation and backup operation procedures. 4. Audit log check, upkeep and archiving procedures. 5. Disaster recovery and continuous operation procedure.
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.
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.

The ePKI EV SSL Certification Authority provides the required instruction and training to personnel performing certification registration review for the RA so personnel have basic knowledge of the PKI, identity authorization and information verification policies and procedures (including EV SSL certificate guidelines, the Baseline Requirements, CP and CPS), common identification and information verification procedure threat (including phishing and other social engineering attacks) knowledge and skills. Testing will be held for related training and records kept ensuring that the RA officers are able to maintain to a sufficient level of knowledge and skills to perform related tasks.

5.3.4 Retraining Frequency and Requirements

All related personnel at the ePKI EV SSL Certification Authority shall be familiar with any changes to ePKI EV SSL Certification Authority 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 trust roles. May not receive work reassignments.
2. Operators with the requisite training and clearance may be reassigned to the position of administrator, officer or auditor after two years.
3. Administrator, officer and auditor personnel who have not concurrently served in the position of operator may be reassigned to the position of administrator, officer or auditor after serving one full year as 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, officer, or 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, officer, or auditor.

5.3.6 Sanctions for Unauthorized Actions

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

5.3.7 Independent Contractor Requirement

Section 5.3 shall be followed for the security requirements of personnel employed by the ePKI EV SSL Certification Authority.

5.3.8 Documentation Supplied to Personnel

The ePKI EV SSL Certification Authority shall make available to related personnel relevant documentation pertaining to the CP, CPS, EV SSL Certificate Guidelines, the Baseline Requirements, the three types of audit standards described by Chapter 8, ePKI EV SSL Certification Authority system operation manuals, the Electronic Signatures Act and its enforcement rules.

5.4 Audit Logging Procedures

The ePKI EV SSL Certification Authority shall keep security audit logs for all events related to ePKI EV SSL Certification Authority security.

Security audit logs shall be collected by automatic system generation, logbook or paper. All security audit logs shall be retained and made available during compliance audits. Auditable security audit logs are kept in accordance with the archive retention regulations in section 5.5.2.

5.4.1 Types of Events Recorded

(1) Key generation

- ePKI EV SSL Certification Authority key generation times (not mandated for single use or single session keys).

(2) Private key loading and storage

- Loading the private key into a system component.
- All access to private keys kept by the ePKI EV SSL Certification Authority 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

The ePKI EV SSL Certification Authority 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.

The ePKI EV SSL Certification Authority shall check the audit logs once every two months.

5.4.3 Retention Period for Audit Logs

Audit logs shall be retained on-site for two months and the log retention management system shall be operated in accordance with the regulations in sections 5.4.4, 5.4.5 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) The ePKI EV SSL Certification Authority shall routinely archive event logs.

(2) The ePKI EV SSL Certification Authority 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 ePKI EV SSL Certification Authority 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

ePKI EV SSL Certification Authority certificate RAs shall conduct a vulnerability scan at least once each year and take remedy measures.

The ePKI EV SSL Certification Authority shall follow the methods and frequency stipulated in the AICPA/CPA WebTrust $^{SM/TM}$ for Certification Authorities Trust Services Principles and Criteria for Certification Authorities – SSL Baseline with Network Security –and CA/Browser Forum Network and Certificate System Security Requirement to perform vulnerability assessments at least once per quarter.

Penetration testing shall be conducted at least once per year. The ePKI EV SSL Certification Authority also must conduct penetration testing after it is determined that there is a significant upgrade or modification to the application program or infrastructure. The ePKI EV SSL Certification Authority will have reinforcement and correction actions after the penetration tests and vulnerability assessments. The ePKI EV SSL Certification Authority shall record the skills, tools and followed ethical, competitive relations and independence guidelines for those personnel or groups capable of implementing reliable vulnerability scanning, penetration testing, information security diagnosis or security surveillance.

5.5 Records Archival

A reliable mechanism shall be adopted by the ePKI EV SSL Certification Authority to accurately and completely save certificate-related records as computer data or in written form including:

(1) Important tracking records regarding the ePKI EV SSL Certification Authority'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 Recorded Events

The ePKI EV SSL Certification Authority retains the following information in its archives:

(1) ePKI EV SSL Certification Authority 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) ePKI EV SSL Certification Authority re-key records.
(11) Issued or announced CRLs.
(12) Audit logs.
(13) Used to verify and validate the content of files and other information or application programs.
(14) Audit personnel requirement documents.

5.5.2 Retention Period for Archive

The retention period for ePKI EV SSL Certification Authority file information is 10 years. The application programs used to process file data are kept 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 ePKI EV SSL Certification Authority authorization procedure.

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

5.5.4 Archive Backup Procedures

EPKI EV SSL Certification Authority 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 the ePKI EV SSL Certification Authority.

5.5.5 Requirements for Time-stamping of Records

All ePKI EV SSL Certification Authority 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 and accurate times following system calibration shall be used. 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 Information 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 on written documents must be verified.

5.6 Key Changeover

ePKI EV SSL Certification Authority private keys shall be regularly renewed in accordance with the regulations in section 6.3.2. After the key pair is renewed, an application for a new certificate shall be submitted to the eCA. The new certificate shall be published in the repository for subscriber downloading.

Certificate subscriber private keys shall be regularly renewed in accordance with the certificate subscriber private key usage period regulations in section 6.3.2.

5.7 Key Compromise and Disaster Recovery Procedures

5.7.1 Emergency and System Compromise Handling Procedures

The ePKI EV SSL Certification Authority establishes handling procedures in the event of emergencies or system compromise and conducts annual drills.

5.7.2 Computing Resources, Software and Data Corruption Recovery Procedure

The ePKI EV SSL Certification Authority establishes recovery procedures in the event of computing resource, software and data corruption and conducts annual drills.

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

5.7.3 ePKI EV SSL Certification Authority Signature Key Compromise Recovery Procedure

The ePKI EV SSL Certification Authority implements the following recovery procedure in the event of signature key compromise:

(1) Publish in the repository, notify subscribers and relying parties

(2) Revoke the ePKI EV SSL Certification Authority 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.

The ePKI EV SSL Certification Authority shall conduct at least one ePKI EV SSL Certification Authority signature key compromise drill each year.

5.7.4 ePKI EV SSL Certification Authority Security Facilities Disaster Recovery Procedure

The ePKI EV SSL Certification Authority 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 ePKI EV SSL Certification Authority repository operations and quickly reestablishing certificate issuance and management capabilities.

5.7.5 ePKI EV SSL Certification Authority Signature Key Certificate Revocation Recovery Procedure

Revoked ePKI EV SSL Certification Authority signature key certificates shall be published in the repository and relying parties shall be notified. New key pairs shall be generated in accordance with section 5.6. New certificates shall be published in the repository for subscriber and relying parties downloading.

The ePKI EV SSL Certification Authority shall conduct at least one ePKI EV SSL Certification Authority signature key certificate revocation drills each year.

5.8 ePKI EV SSL Certification Authority Service Termination

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

(1) The ePKI EV SSL Certification Authority shall notify the competent authority (MOEA) and subscribers of the service termination 30 days in advance.

(2) The ePKI EV SSL Certification Authority 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 ePKI EV SSL Certification Authority 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, the ePKI EV SSL Certification Authority shall revoke the still valid certificates, publish the revoked certificates in the repository and notify all certificate-related persons 30 days prior to service termination. The ePKI EV SSL Certification Authority shall refund the certificate issuance and renewal fees based on the certificate validity.

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

6. Technical Security Controls

This chapter describes the technical security controls implemented by the ePKI EV SSL Certification Authority.

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The ePKI EV SSL Certification Authority generate pseudo random numbers and public key pairs within the hardware security module in accordance with the regulations in section 6.2.1.

According to the regulations in section 6.2.1, the ePKI EV SSL Certification Authority generates key pairs within the hardware security module using the NIST FIPS 140-2 algorithm and procedures. The private keys are imported and exported in accordance with the regulations in sections 6.2.2 and 6.2.6.

ePKI EV SSL Certification Authority key generation is witnessed by a member of the ePKI Policy Management Committee, CHT and a Qualified Auditor.

6.1.1.1 Subscriber Key Pair Generation

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

6.1.2 Private Keys Delivery to Subscriber

Not applicable.

6.1.3 Delivery of Subscriber Public Keys to the CA

The subscriber self-generates a key pair, the subscriber shall deliver the public key by PKCS# 10 certificate request file format to the RA. The RA shall deliver the public key to the CA via secure channels after it is verified that the subscriber is in possession of the corresponding private key in accordance with the regulations in section 3.2.1.

Secure channels referred in this Chapter are the use of Transport Layer Security (TLS) or other equivalent or higher level data encryption transmission methods.

6.1.4 CA Public Keys Delivery to Relying Parties

The ePKI EV SSL Certification Authority's own public key are issued by the eCA and published in the ePKI EV SSL Certification Authority repository for direct downloading and installation by subscribers and relying parties. Relying parties shall follow the eCA CPS regulations to obtain the eCA's public key or self-signed certificate via secure channels before using the ePKI EV SSL Certification Authority's own public key. The eCA shall then check the signature on the ePKI EV SSL Certification Authority's own public key certificate to ensure the trustworthiness of the public key in the public key certificate.

6.1.5 Key Sizes

The ePKI EV SSL Certification Authority uses 2048-bit RSA keys and SHA-256 hash function algorithms to issue certificates.

Subscribers must use at least 2048-bit RSA keys or other key types of equivalent security strength on and before 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 the ePKI EV SSL CA uses Elliptic Curve Cryptography (ECC) algorithm to issue certificates, the key size will comply with NIST P-256, P-384 or P-521.

6.1.6 Public Key Parameters Generation and Quality Checking

The public key parameter of the RSA algorithm is null.

The ePKI EV SSL Certification Authority 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 software/hardware security modules but this does not guarantee that this prime number is a strong prime.

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

If the certificates are issued by Elliptic Curve Cryptosystem, the ePKI EV SSL Certificate Authority shall follow sections 5.6.2.3.2 and 5.6.2.3.3 in NIST SP 800- 56A Revision 2 to verify all the validity periods of keys which use the ECC Full Public Key Validation Routine and the ECC Partial Public Key Validation Routine.

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

The ePKI EV SSL Certification Authority’s signature private key is used to issue certificates and CRLs. The ePKI EV SSL Certification Authority’s own public key certificate is issued by the eCA. The keyUsage bits used for the keyUsage extension setting are keyCertSign and cRLSign.

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

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The ePKI EV SSL Certification Authority uses hardware security modules that have passed FIPS 140-2 Level 3 certification requirements.

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

ePKI EV SSL Certification Authority 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 ePKI EV SSL Certification Authority private key multi-person control. Therefore, it can be used as the activation method for private keys (see section 6.2.8).

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

6.2.3 Private Key Escrow

The ePKI EV SSL Certification Authority’s signature private key is not escrowed. The ePKI EV SSL Certification Authority shall not be responsible for the safekeeping of subscriber private keys.

6.2.4 Private Key Backup

Backups of ePKI EV SSL Certification Authority private keys are made according to the key splitting multi-person control methods in section 6.2.2 and IC cards verified with FIPS 140-2 Level 2 or above standards may serve as the private key splitting storage media.

6.2.5 Private Key Archival

ePKI EV SSL Certification Authority signature private keys are not archived but archiving of public key is done by certificate information methods in accordance with section 5.5.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

The ePKI EV SSL Certification Authority transfers the private key into the cryptographic modules under the following circumstances:

(1) Key generation or cryptographic module replacement.

(2) For key splitting backup recovery, the secret splitting (*n-out-of-m* control) method is used in the circumstance to recover the ePKI EV SSL Certification Authority private key. Once the private key secret splitting IC card is recovered, the complete private key is written into the hardware security module.

(3) When the cryptographic module is replaced, encryption is used for the private key importation method to ensure that key plain code is not exposed outside the cryptographic module during the importation process and the related confidential parameters generated during the importation process are completely destroyed after the private key importation is completed.

6.2.7 Private Key Storage on Cryptographic Modules

Follow the regulations in sections 6.1.1 and 6.2.1.

6.2.8 Method of Activating Private Key

ePKI EV SSL Certification Authority private key activation is controlled by multi-person controls of the different usage IC cards kept by administrator and 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 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.

(2) 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 methods in section 6.2.2 are used to deactivate ePKI EV SSL Certification Authority private keys.

The ePKI EV SSL Certification Authority does not provide subscriber private key deactivation service.

6.2.10 Method of Destroying Private Key

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

In addition to destroying the old ePKI EV SSL Certification Authority private key in the hardware security module, physical destruction of the backup secretly held IC card for the secret key is done during the ePKI EV SSL Certification Authority key renewal.

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

If services are permanent not provided by the cryptographic module, all private keys used by that secure module are erased from its security module.

No other regulations have been established for subscriber private key destruction methods.

6.3 Other Aspects of Key Pair Management

Subscribers must self-administer key pairs. The ePKI EV SSL

Certification Authority is not responsible for safeguarding subscriber private keys.

6.3.1 Public Key Archival

The ePKI EV SSL Certification Authority 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 Period

6.3.2.1 ePKI EV SSL Certification Authority Public and Private Key Usage Periods

The RSA key size for ePKI EV SSL CA public and private keys is 2048 bits. The maximum usage period for private and public keys is 14 years. The maximum usage period for EV SSL certificates issued with private keys in 10 years. However, issued CRLs, OCSP responder certificates and OCSP response usage are terminated when the issued EV SSL certificates, OCSP responder certificates, and RA certificates expire; therefore, the maximum usage period for the private keys of the ePKI EV SSL CA is 14 years. The maximum usage period for the private and public keys certificates of RAs is five years. The maximum usage period for the private and public keys certificates of OCSP responder is one and half days. The new OCSP responder certificate is disclosed daily (given to the relying parties by the OCSP response signed by the new private key digital signature which contains that certificate).

6.3.2.2 Subscriber Public and Private Key Usage Periods

The key size for ePKI EV SSL Certification Authority public and private keys is RSA 2048 or the above. The maximum usage period for private keys is 825 days. The maximum validity period for EV SSL certificates is 825 days according to the EV SSL Certificate Guidelines.

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. The activation data obtained from the IC card must be input as the IC card personal identification number (PIN).

6.4.2 Activation Data Protection

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

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

6.4.3 Other Aspects of Activation Data

The ePKI EV SSL Certification Authority private key activation data is not archived.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The ePKI EV SSL Certification Authority 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.

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

6.5.2 Computer Security Rating

ePKI EV SSL Certification Authority servers use Common Criteria EAL 4 certified computer operating systems.

6.6 Lifecycle Technical Controls

6.6.1 System Development Controls

Quality control for ePKI EV SSL Certification Authority system development complies with CMMI standards.

RA hardware and software shall be checked for malicious code during initial use and regularly scanned. Besides, it shall be checked by regularly using tools to scan, such as 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 and 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 the ePKI EV SSL CA as well as conduct program version control.

6.6.2 Security Management Controls

When software is installed for the first time, the ePKI EV SSL Certification Authority shall check if the provider has supplied the correct and unmodified version.

The ePKI EV SSL Certification Authority may only use components which have received security authorization. Unrelated hardware devices, network connections or component software may not be installed.

The ePKI EV SSL Certification Authority records and controls system configuration and any modification or function upgrades as well as detect unauthorized modifications to system software and configuration.

The ePKI EV SSL Certification Authority shall reference the methodologies and standards in ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, ISO/IEC 31000, the Baseline Requirements, EV SSL Certificate Guidelines, CA/Browser Forum Network and CertificateSystem Security Requirements, Trust Service Principles and Criteria for Certification Authorities, WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL and WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security for risk assessment, risk management and security management and control measures.

6.6.3 Life Cycle Security Controls

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

6.7 Network Security Controls

The ePKI EV SSL Certification Authority host and repository have firewalls and are connected to external networks. The repository is placed on the outside service area (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 ePKI EV SSL Certification Authority host have digital signature protection and are automatically sent from the ePKI EV SSL Certification Authority host to the repository.

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

6.8 Time Stamping

The ePKI EV SSL Certification Authority regularly conducts system synchronization with a reliable time source to maintain the correctness of system time and ensure the accuracy of the following times:

(1) Certificate issuance times.

(2) Certificate revocation times.

(3) CRL issuance times.

(4) System event occurrence times.

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

7. Certificate, CRL and OCSP Service Profiles

7.1 Certificate Profile

The certificates issued by the ePKI EV SSL Certification Authority conform to the current version of the ITU-T X.509, CA/Browser Forum Baseline Requirements for the Issuance and Management of Extended Validation Certificates, IETF PKIX Working Group RFC 5280 and other regulations.

The ePKI EV SSL Certification Authority uses Cryptographically secure pseudorandom number generator (CSPRNG) to generate the certificate serial numbers which are larger than zero, non-sequential, and containing at least 64-bit entropy.

7.1.1 Version Number(s)

The ePKI EV SSL Certification Authority Issues X.509 V3 version certificates.

7.1.2 Certificate Extensions

The certificate extensions of the certificates issued by the ePKI EV SSL Certification Authority conform to the current versions of the ITU-T X.509, CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates, PKIX Working Group RFC 5280 or other regulations.

7.1.2.1 CA Certificate of the ePKI EV SSL Certification Authority

The certificate extensions of Subordinate CA Certificate issued by the eCA to the ePKI EV SSL CA are described as the following:

a. certificatePolicies

This certificate extension is a required extension, marking the non-critical fields. The content is used to mark policyIdentifier.

b. cRLDistributionPoints

This certificate extension is a required extension, marking the non-critical fields. The content is used to mark the HTTP URL of the CRL service of the ePKI EV SSL CA.

c. authorityInfoAccess

This certificate extension is a required extension, marking the non-critical fields. The content is used to mark the HTTP URL of the OCSP responder of the eCA, as well as the HTTP URL of the self-signed certificate of the eCA.

d. basicConstraints

This certificate extension is a required extension, marking the critical fields. The content is used to mark the value of CA field as true. As the ePKI EV SSL CA does not sign the subordinate CA certificates downwards, the pathLenConstraint is set to 0.

e. keyUsage

This certificate extension is a required extension, marking the critical fields. The content is used to mark keyUsage bits as keyCertSign and cRLSign. The ePKI EV SSL CA does not sign the OCSP response with the signature private 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 certificate issued to the ePKI EV SSL CA by the eCA does not have the certificate extension.

g. extKeyUsage

The subordinate CA certificate issued to the ePKI EV SSL CA by the eCA does not have the certificate extension.

7.1.2.2 Subscriber Certificate

a. certificatePolicies

This certificate extension is a required extension, marking the non-critical fields. The content is used to mark policyIdentifier.

b. cRLDistributionPoints

This certificate extension is a required extension, marking the non-critical fields. The content is used to mark the HTTP URL of the CRL service of the ePKI EV SSL CA.

c. authorityInfoAccess

This certificate extension is a required extension, marking the non-critical fields. The content is used to mark the HTTP URL of the OCSP responder of the eCA, as well as the HTTP URL of the self-signed certificate of the eCA.

d. basicConstraints

The subscriber certificate issued by the ePKI EV SSL CA does not have the certificate extension.

e. keyUsage

This certificate extension is an optional extension, and marking the critical fields if any. The content shall not mark the used keyUsage bits as keyCertSign and cRLSign. For the keyUsages for different categories of certificates, please refer to section 6.1.7.

f. extKeyUsage

For the EV SSL certificates issued by the ePKI EV SSL CA, this certificate extension is required. It marks the non-critical fields, and the content is used to mark serverAuth and clientAuth.

Unless the reasons to include certain data in the certificates are known, the ePKI EV SSL CA does not allow certificates being issued in the following scenarios:

(1) The certificate extensions contain the configuration not applicable to the public internet, such as: in the field of extKeyUsage, only the configuration applicable to the private internet services.

(2) The contents of the certificates may mislead the relying parties believe the certificates have been validated by the ePKI EV SSL CA.

Regarding supporting the Certificate Transparency (CT), the ePKI EV SSL CA adopts the OCSP stapling mechanism recommended by RFC 6962, to conduct the signed certificate timestamp (SCT) transmission, and thus SCT is not embedded in certificates. OCSP stapling is the only SCT transmission mechanism satisfying the following conditions: when the CT log server is cracked or denied, the ePKI EV SSL CA does not need to re-issue the certificates, and the web servers at the certificate subject end is not affected. When CT log Server is running normally, the ePKI EV SSL CA does not need to alter the original process of certificate issuance, and the SCT related information is embedded in the OCSP response extension.

7.1.3 Algorithm Object Identifiers

The algorithm OIDs used for signatures on ePKI EV SSL Certification Authority issued certificates are:

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

(OID：1.2.840.113549.1.1.11)

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

(OID：1.2.840.113549.1.1.12)

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

(OID：1.2.840.113549.1.1.13)

The algorithm OID used during EPKI EV SSL Certification Authority issued certificate generation of subject keys are:

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

(OID:1.2.840.113549.1.1.1)

7.1.4 Name Forms

The subject and issuer fields of the certificate must use the X.500 distinguished name and the name attribute type shall comply with the current version of the ITU-T X.509, CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates and IETF PKIX Working Group RFC 5280 or other regulations.

The CA ceritficates of the ePKI EV SSL Certification Authority Subject information 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 the ePKI EV SSL Certification Authority 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 the ePKI EV SSL Certification Authority, trademark, or their meaningful name, for the purpose of identifying the ePKI EV SSL Certification Authority 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 the ePKI EV SSL Certification Authority.

7.1.4.1 Issuer Information

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

7.1.4.2 Subject Information–Subscriber Certificates

By issuing the subscriber certificates, the ePKI EV SSL Certification Authority and RAs have complied with the procedures specified in the CP and/or the CPS, to ensure all the values recorded in the Subject of these certificates are accurate. The commonName of the EV SSL certificate

Subject will be the FQDN validated by Section 3.2.2.5 (if it is a multi-domain EV SSL certificate, only one FQDN will be placed).

7.1.4.2.1 Subject Alternative Name Extension

The Subject Alternative Name Extensions for EV SSL certificates are as the following:

Certificate Extension	Required/Optional Extension
extension:subjectAltName	Required

This extension shall be validated the ownership or control of the domain name by the RA officers according to Section 3.2.5.

7.1.4.2.2 Subject Distinguished Name Fields

Please refer to Table 3-1 of this CPS.

7.1.4.3 Subject Information–CA Certificates

The CA certificates of the ePKI EV SSL Certification Authority is validated and issued by the eCA based on the procedures specified in the CP and/or the CPS. The Subject Distinguished Name Fields are as the following:

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 Extended-validated OID（{joint- iso- itu- t(2) international- organizations(23) ca- browser- forum(140) certificate- policies(1) ev-guidelines (1) }(2.23.140.1.1)）is used as the certificate policy object identifiers for ePKI EV SSL Certification Authority issued EV SSL certificates.

7.1.7 Usage of Policy Constraints Extension

ePKI EV SSL Certification Authority issued certificates do not contain policy constraints extension.

7.1.8 Policy Qualifiers Syntax and Semantics

The policy qualifier ID (policyQualiferId) of certificates issued by the ePKI EV SSL Certification Authority must be defined as 「id-qt 1」 in the RFC 5280 international standards and indicates that that policy qualifier ID, OID is 1.3.6.1.5.5.7.2.1.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

The certificate policy extensions contained in ePKI EV SSL Certification Authority issued certificates are not recorded as critical extensions.

7.2 CRL Profile

7.2.1 Version Number(s)

The ePKI EV SSL Certification Authority issues ITU-T X.509 v2 version CRLs.

7.2.2 CRL and CRL Entry Extensions

ePKI EV SSL CA issued CRL, CRL extensions, and CRL entry extensions conforms with the current version of the ITU-T X.509, CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates, IETF PKIX Working Group RFC 5280 or other related regulations in the latest versions. The CRL extensions are as the following：

Field	Content	Description
version	V2(1)	CRL version is V2 (note: the value of V2 is 1, not 2)
signature		The AlgorithmIdentifier of the CRL signature algorithm，the value of this field must be identical to the algorithmIdentifier of the external SIGNED certificate field
.algorithm	sha256WithRSAEncryption(1 2 840 113549 1 1 11) or ecdsaWithsha384(1 2 840 10045 4 3 3)	OID of signature algorithm
.parameter	NULL	Despite that signature algorithm does not need Parameters, but the parameters shall be filled in with NULL,

Field	Content	Description
		not with blank. The DER code of NULL is 0x0500
issuer	DN of CA	This DN must be identical to the Subject DN of CA (note: in the ePKI, the keyCertSignCertificate and cRLSignCertificate are the same on)
thisUpdate	GMT for this CRL update	By the rule of PKIX, before 23:59:59, 2049/12/31, the UTCTime data type shall be applied, the format is YYMMDDHHMMSSZ, for the second (SS), 00 must be filled in, instead of omitting; “Z” means GMT time and shall not be omitted.
nextUpdate	GMT for the next expected CRL update	By the rule of PKIX, before 23:59:59, 2049/12/31, the UTCTime data type shall be applied, the format is YYMMDDHHMMSSZ, for the second (SS), 00 must be filled in, instead of omitting; “Z” means GMT time and shall not be omitted.
revokedCertificates	RevokedCertificates ::= SEQUENCE OF RevokedCertificate	All the effective revocation even happened before thisUpdate, will be recorded in the revokedCertificates (“effective” means the certificate not yet expired)

Field	Content	Description
*.RevokedCertificate	Fill in a series of RevokedCertificate recorded, each RevokedCertificate record shall contain the following:	
.userCertificate	Fill in the Certificate Serial Number of revoked certificate	The serial number of certificate used in Epki, is a positive integer of 16 bytes. According to the 2’s Complement rule applied to the positive numbers in DER coding, “0x00” may be filled in at the beginning, and thus the positive integer with 16 bytes actually occupies the space of 17 bytes
.revocation Date	GMT when the certificate is revoked	By the rule of PKIX, before 23:59:59, 2049/12/31, the UTCTime data type shall be applied, the format is YYMMDDHHMMSSZ, for the second (SS), 00 must be filled in, instead of omitting; “Z” means GMT time and shall not be omitted.
Issuer’s Signature	The signature value of CA to CRL	

The CRL entry extensions and CRL extensions are as the following：

Field	Content	Description
.crlEntryExtensions	SEQUENCE OF CRLEntryExtension	May enter a CRLEntryExtension

	(Note: the CRLEntryExtension Information type format and Public-Key Certificate Extension information type format are completely identical)	series but the ePKI only use reasonCode this CRLEntryExtension
.reasonCode	ePKI only uses reasonCode as this CRLEntryExtension, the content is as follows:	
.extnId	Enter id-ce-reasonCode (which is 2.5.29.21) this OID	
.critical	reasonCode must be non-critical extension, so the critical value must be FALSE	Note: since FALSE is a DEFAULT VALUE, so this field in the DER code will be omitted
.extnValue	extnValue data type is OCTET STRING, for reasonCode, this type of extension must use one of the CRLReason DER code as this OCTET STRING value, CRLReason itself is 1 ENUMERATED	Some CRLReason in the ePKI may not be used in Complete CRL.
	unused(0)	Follow PKIX rules, this CRLReason may not be used in the ePKI
	keyCompromise(1)	This CRLReason is used in the event that end entities (EE) private keys are lost or suspected to be stolen or compromised and the certificate is to be revoked.
	caCompromise(2)	Use this CRLReason if it is suspected or confirmed CA keyCertSign

		or cRLSign private key is stolen or compromised, but this CRLReason may not be used to revoke EE certificates. It can only be used to revoke CA certificate (note: if a CA keyCertSign private key is suspected or confirmed to be stolen or compromised, all issued EE certificates are revoked, CA key pairs are regenerated, when the EE certificates are reissued, the EE certificate revocation CRLReason shall use superseded)
	affiliationChanged(3)	This CRLReason is used when there is identical identity information in the EE and certificate content is changed (such as changes to the company name, address) and the certificate must be revoked.
	superseded(4)	This CRLReason is used when the EE must renew certificates and revoke original certificates due to certain requirements (for example: replacement with new certificate, CA hand-over and reissue of all certificates, CA reissues all certificates due to updating of

		certificate format, a more secure key type or size must be used due to breakthroughs in code breaking methods)
	cessationOfOperation(5)	This CRLReason is used when the EE simply does not wish to continue use of the certificate or must revoke the certificate for no particular reason.
	certificateHold(6)	This CRLReason may not be used with SSL certificates.
	removeFromCRL(8)	This CRLReason may not be used with SSL certificates.
	privilegeWithdrawn(9) (note: X.509 4th Edition)	1. This CRLReason is used when EE privileges are withdrawn (for example: registration revoked or deprived of civil rights) 2 This CRLReason is generally not activated by the EE. It is generally used by the CA/RA or attribute authority (AA) 「perform revocation」 EE certificates. 3 This CRLReason is generally used to revoke Attribute certificate, but it may also be used to revoke Public-Key certificate
	aACompromise(10) (Note: X.509 4th Edition)	This CRLReason is used when it is suspected that the private keys used by

		the AA to issue Attribute Certificates is stolen or compromised, but this CRLReason may not be used to revoke Public-Key Certificate. It can only be used to revoke the AA’s own Public-KeyCertificates and EE Attribute Certificates.
crlExtensions	SEQUENCE OF CRLExtensions (note: the CRLExtension data type format and Public-Key Certificate Extension data type format is completely identical)	Content is an extension field series containing the following extension field types (the actual sequence in the certificate may not be the same as the following sequence):
.authorityKeyIdentifier	Authority Key Identifier expansion field, Key Identifier generation method follows PKIX standards, obtain Issuing CA Public Key SHA-1 Hash valve to serve as Key Identifier	The purpose of this extension field is to show which one is used by the CA to issue the keys used for this CRL to help the CA determine which CA certificate should be used to check this certificate during CA re-key and replacement of the certificate.
.extnId	Enter OID representing this expansion field OID id-ce-authorityKeyIdentifier (2.5.29.35)	
.critical	authorityKeyIdentifier must be non-critical extension in the ePKI, so the critical value is	Note: Since FALSE is the DEFAULTVALUE, this field is omitted in the DER code

	FALSE	
.extnValue	extnValue data type is OCTET STRING	For the authorityKeyIdentifier type of Extension, AuthorityKeyIdentifier DER code must be used for this OCTET STRING value
.AuthorityKeyIdentifier	AuthorityKeyIdentifier data structure contains 3 optional fields: keyIdentifier, authorityCertIssuer and authorityCertSerialNumber fields	In the ePKI, the CRL according to the PKIX only uses the keyIdentifier field and does not use authorityCertIssuer and authorityCertSerialNumber fields
.keyIdentifier	keyIdentifier field data type is KeyIdentifier and the KeyIDentifier itself is 1 OCTET STRING data type	KeyIdentifier generation method follows PKIX standards, obtain Subject Public Key SHA-1 Hash value to serve as KeyIdentifier OCTET STRING value
.cRLNumber	cRLNumber CRLExtension content is as follows:	cRLNumber extension field content is used to record this CRL serial number
.extnId	Enter id-ce-cRLNumber (2.5.29.20) as this OID	
.critical	cRLNumber must be a non-critical extension, so the critical value must be FALSE	Note: Since FALSE is a DEFAULT VALUE so this field is omitted in the DER code.
.extnValue	extnValue data type is OCTET STRING, for the cRLNumber type of Extension, it must use CRLNumber DER code to serve as this OCTET STRING value and the CRLNumber itself is1 INEGER (0..MAX)	According to the X.509 standard, the CRL Number must be one monotonically increasing sequence number. In the ePKI, the CRLNumber value in the CRL shall be one size less or equal to

	positive integer data type.	7-byte positive number.
.issuingDistributionPoint	issuingDistributionPoint CRLExtension, its content is as follows:	issuingDistributionPoint extension field is used to provide the certificate application software a way to determine if this CRL matches the CRL address on the certificate to be verified, the Issuing Distribution Point currently used by the Partitioned CRL is one URL website which is the CRL distribution point address.
.extnId	Enter id-ce-issuingDistributionPoint (2.5.29.28) as this OID	
.critical	In the Partitioned CRL, issuingDistributionPoint must be a critical extension, so the critical value must be TRUE	Note: Since TRUE is not a DEFAULT VALUE, the field may not be omitted in the DER code
.extnValue	extnValue data type is OCTET STRING	For this issuingDistributionPoint type of Extension, IssuingDistributionPoint data type DER code must be used as this OCTET STRING values
.IssuingDistributionPoint	IssuingDistributionPoint is a SEQUENCE containing distributionPoint, onlyContainsUserCerts, onlyContainsCACerts, onlySomeReasons and indirectCRL 5 fiels	In the Partitioned CRL. Issuing DistributionPoint extension field only uses the distribution Point field and does not use the other four types of fields.
.distributionPoint	distributionPoint field	In the ePKI, the

	data type is DistributionPointName, and the DistributionPointName itself us a CHOICE data type which can be selected as a fullName or nameRelativeToCRLIssuer	Partitioned CRL distributionPoint uses fullName
.fullName	fullName data type is GeneralNames and GeneralNames data type is SEQUENCE SIZE (1...MAX) OF GeneralName	In ePKI, the Partitioned CRL distribution Point field fullName only contains one GeneralName
.GeneralName	GeneralName is a CHOICE data type	ePKI has selected uniformResourceIdentifier in CHOICE and the CRL distribution point URL is recorded in this field. If this Partitioned CRL is used to verify certificate validity, then the various URL recorded in the verified cRL DistributionPoint field must have at least one URL which is completely identical to the URL recorded in this field.

7.3 OCSP Service Profile

The ePKI EV SSL Certification Authority provides OCSP services complies with IETF PKIX Working Group RFC 6960 and RFC 5019 standards and the ePKI EV SSL Certification Authority OCSP service website URL is contained in the Authority Information Access (AIA) extension in the certificate.

7.3.1 Version Number(s)

The OCSP inquiry packets accepted by the ePKI EV SSL CA shall include the following information:

- Version number
- Target certificate identifier

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

OCSP service response packets issued by the ePKI EV SSL Certification Authority 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 Responder ID	OCSP responder subject DN
Produced Time	Response packet sign time
Target certificate identifier	Includes: Hash algorithm, hash value of certificate issuer name, hash value of certificate issuer key and certificate number of 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	Response packet signature

	algorithm, can be sha256WithRSAEncryption or ecdsaWithsha384
Signature	OCSP responder signature
Certificates	OCSP responder certificate

7.3.2 OCSP Service Extensions

The OCSP response packet signed by the ePKI EV SSL Certification Authority's OCSP responder includes the following extensions:

- OCSP responder authority key identifier
- In addition, when the OCSP inquiry packet contains a nonce field, OCSP response packet also must contain the same nonce field.
- Signed certificate timestamp.
- OID is 1.3.6.1.4.1.11129.2.4.5 for use with certificate transparency.

7.3.3 Regulations for Operation of OCSP

The operation of OCSP in the ePKI EV SSL CA including:

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

The certificate for OCSP responding server used by the end of OCSP server is issued by the ePKI EV SSL CA, and it must be valid short-term certificate, and will be issue and updated regularly by the ePKI EV SSL CA.

8. Compliance Audit and Other Assessments

8.1 Frequency or Circumstances of Assessment

The ePKI EV SSL Certification Authority received one annual external audit and one non-routine internal audit with an audit period of no more than 12 months to ensure that ePKI EV SSL Certification Authority operations are in compliance with the security regulations and procedures in the CP and CPS. The standards used for the audit are Trust Service Principles and Criteria for Certification Authorities, WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL and Trust Services Principles and Criteria for Certification Authorities – SSL Baseline with Network Security.

8.2 Identity / Qualifications of Assessor

The Company shall retain an qualified auditor to perform the ePKI EV SSL Certification Authority compliance audit work who is familiar with ePKI EV SSL Certification Authority operations and has been authorized by AICPA/CPA as a licensed WebTrust practitioner to perform Trust Service Principles and Criteria for Certification Authorities, WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL, WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security to provide fair and impartial audit services. Audit personnel shall be a qualified and authorized Certified Information Systems Auditor (CISA) or have equivalent qualifications 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. The qualified auditor must maintain Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage. The ePKI EV SSL Certification Authority shall conduct identity identification of audit personnel during audits.

8.3 Assessor's Relationship to Assessed Entity

The Company shall retain an impartial third party to conduct audits of ePKI EV SSL Certification Authority operations.

8.4 Topics covered by assessment

The scope of audit is stipulated as follows:

(1) Whether or not the ePKI EV SSL Certification Authority operations comply with the CPS including management and technical audit of the physical environment, personnel procedural controls, key control, certificate lifecycle control, hardware security module.

(2) Whether or not the RA operations comply with the CPS and related procedures.

The RA responsible for verification of assurance level 3 EV SSL certificate requests or revocation shall undergo one external audit every year noting any CP / CPS non-compliance or exceptions and the actions taken to correct the deficiencies.

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

The Company reserves the rights to conduct a compliance audit on whether or not a dedicated RA is in compliance with the CP and CPS to reduce any risk derived from any non-conformity with the CP or CPS. The Company has the right the conduct the following (but not limited to) review and examination items to ensure the trustworthiness of the ePKI EV SSL Certification Authority:

(1) If there is an event that causes the Company to reasonably suspect the dedicated RA is unable to comply with CP and CPS in the event of a computer emergency event or key compromise.

(2) If the compliance audit has not been completed or there are special developments, the Company 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, the Company must conduct the related review or examination.

The Company 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 the Company and the personnel conducting the audit and examination.

Audit personnel shall conduct at least one continuous internal audit of the EV SSL certificate RA and on at least a quarterly basis against a randomly selected sample of at least three percent of the quantity of EV SSL certificates issued (less than one counted as one) after the previous sample was taken for the ePKI EV SSL Certification Authority in accordance with the EV SSL Certificate Guidelines. If the section 3.2.6.4 final cross-correlation and due diligence survey of issued EV SSL certificates is performed by the RA, a continuous random sample of at least 6% of the quantity of EV SSL certificate issued (less than one counted as one) must be performed during a period after the previous sample for self-audit in order to control service quality.

8.5 Action Taken as a Result of Deficiency

If audit personnel find that the establishment and operation ePKI EV SSL Certification Authority or an RA does not conform with CPS regulations, the following actions shall be taken:

(1) Record non-conformities.

(2) Notify the ePKI EV SSL Certification Authority about the non-conformities.

(3) With regard to the non-conformities, the ePKI EV SSL Certification Authority shall submit an improvement plan within 30 days, promptly implement the plan and record the tracking items for subsequent audits. RAs are notified to make improvements to RA-related deficiencies.

8.6 Communications of Results

Except for those scopes could result in system attacks or information defined in section 9.3, the ePKI EV SSL Certification Authority shall publish public disclosure information provided by the qualified auditors. The audit results shall be presented on the front page of the ePKI EV SSL

Certification Authority website using WebTrust® for CA, WebTrust® for Certification Authorities – EV SSL Seal and WebTrust® for Certification Authorities – SSL Baseline Requirements Seal methods. The external audit results and management's assertions may be viewed by clicking on the seal. The latest conformance audits and management's assertions are posted on the repository within three months after the end of the audit period. If there is a delay in posting the most recent audit results, the ePKI EV SSL Certification Authority shall provide a signed letter of explanation provided 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, renewal between the ePKI EV SSL Certification Authority and subscribers shall be established 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 established in related contract terms and conditions and subscribers may directly connect to the repository to check related terms and conditions.

9.1.3 Certificate Revocation or Status Information Access Fees

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

9.1.4 Refund Policy

With regard to the certificate issuance and renewal fees collected by the ePKI EV SSL Certification Authority, if a subscriber is unable to use a certificate due to oversight by the ePKI EV SSL Certification Authority, the ePKI EV SSL Certification Authority shall issue a new certificate after conducting an investigation. If the subscriber does not accept the newly issued certificate, the ePKI EV SSL Certification Authority 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

If the damages incurred are not within the scope of general liability insurance compensation coverage disclosed in section 9.2.1, then liability for damage compensation for other assets shall conform to EV SSL Certificate Guidelines requirements disclosed in section 9.2.2.

9.2.1 Insurance Coverage

The ePKI EV SSL Certification Authority is operated by Chunghwa Telecom Co., Ltd. Its financial responsibilities are the responsibilities of Chunghwa Telecom Co., Ltd. The company has taken out a General Liability Insurance Policy with a maximum compensation amount of NT$120,000,000. If the competent authority has related regulations for the certification authority in the future, the ePKI EV SSL Certification Authority will cooperate accordingly.

9.2.2 Other Assets

EPKI EV SSL Certification Authority finances are a part of the overall finances of the Chunghwa Telecom Co., Ltd. Chunghwa Telecom Co., Ltd. is a publicly listed company and a Republic of China company listed on the New York Stock Exchange. In accordance with Article 36 of the Securities and Exchange Act, annual financial reports duly audited and attested by a certified public accountant, approved by the board of directors and recognized by the supervisors are publicly announced and registered with the competent authority within three months after the close of each fiscal year. Financial reports duly reviewed by a certified public accountant and reported to the board of directors are publicly announced and registered within 45 days after the end of the first, second and third quarters of each fiscal year. The operating status for the preceding month is publicly announced and registered within the first 10 days of each month. The ePKI EV SSL Certification Authority can provide self-insured asset prices based on the Company’s financial reports. The Company’s finances are sound. The ratio of liquid assets to current liabilities meets the lower than 1.0 requirement in the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates.

9.2.3 Insurance or Warranty Coverage for End-Entities

No insurance and warranty obligations have been stipulated for EE (subscribers and relying parties).

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The generation, receipt and safekeeping of information by the ePKI EV SSL Certification Authority or RAs shall be deemed to be 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 the ePKI EV SSL Certification Authority.

(5) Audit logs and reports made by audit personnel during the audit process.

(6) Operation-related documents listed as confidential-level operations.

Current and departed ePKI EV SSL Certification Authority and RA personnel and various audit personnel shall keep confidential information in strict confidence.

9.3.2 Information Not Within the Scope of Confidential Information

(1) Identification information and information listed on the certificate, unless stipulated otherwise, is not deemed to be confidential information.

(2) Issued certificates, revoked certificates, suspension information and the CRLs published in the ePKI EV SSL

Certification Authority are not deemed to be confidential information.

9.3.3 Responsibility to Protect Confidential Information

The ePKI EV SSL Certification Authority shall handle subscriber application information in accordance with the Electronic Signatures Act, Trust Service Principles and Criteria for Certification Authorities, EV SSL Certificate Guidelines, Baseline Requirements, WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL , Trust Services Principles and Criteria for Certification Authorities – SSL Baseline with Network Security and Personal Information Protection Act.

9.4 Privacy of Personal Information

9.4.1 Privacy Protection Plan

The ePKI EV SSL Certification Authority has posted its personal information statement and privacy declaration on its website. The ePKI EV SSL Certification Authority conducts privacy impact analysis and personal information risk assessments and also has established a privacy protection plan.

9.4.2 Information treated as private

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

9.4.3 Information Not Deemed Private

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

Issued certificates, revoked certificates, suspension information and CRLs published in the repository is deemed to be confidential and private information.

9.4.4 Responsibility to Protect Private Information

The personal information required for the operation of the ePKI EV SSL Certification Authority, 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 comply with related regulations in the Electronic Signatures Act, Trust Service Principles and Criteria for Certification Authorities standards, CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, Trust Services Principles and Criteria for Certification Authorities – SSL Baseline with Network Security and Personal Information Protection Act related regulations. The ePKI EV SSL Certification Authority shall negotiate protection of private information with RAs.

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 CPS. The subscriber may check the subscriber’s own application information specified in section 9.3.1 paragraph (3). However, the ePKI EV SSL Certification Authority shall reserve the right to collect reasonable fees from subscribers applying for access to this information.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

If there is investigative or evidence collection requirements by judicial, administrative or law enforcement authorities, the information privacy regulations in section 9.4.2 must be checked in accordance with legal procedures. However, the ePKI EV SSL Certification Authority shall reserve the right to collect reasonable fees from authorities applying for access to this information.

9.4.7 Other Information Disclosure Circumstances

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

9.5 Intellectual Property Rights

The following is the intellectual property of the ePKI EV SSL

Certification Authority:

(1) ePKI EV SSL Certification Authority and RA key pair and key splitting.

(2) Related documents or system development for certificate management work performed by the ePKI EV SSL Certification Authority.

(3) Certificates and CRLs issued by the ePKI EV SSL Certification Authority.

(4) This CPS.

The Company agrees that the CPS may be freely downloaded from the ePKI EV SSL Certification Authority repository. Copying and distribution may be done in accordance with relevant copyright regulations but it must be copied in full and copyright noted as being owned by Chunghwa Telecom Co., Ltd. Fees may not be collected from others for the copying and distribution of CPS. The Company shall prosecute improper use or distribution which violates the CPS in accordance with the law.

9.6 Representations and Warranties

9.6.1 ePKI EV SSL Certification Authority Representations and Warranties

ePKI EV SSL Certification Authority shall follow the procedures in the CPS to perform related certificate management work. ePKI EV SSL Certification Authority obligations include:

(1) Comply with CP and CPS and EV SSL Certificate Guidelines in operations.

(2) Perform certificate application identification and

authentication.

(3) Provide certificate issuance and publication services.

(4) Revoke, suspend or resume use of certificates.

(5) Issue and publish CRLs.

(6) Issue OCSP response.

(7) Securely generate ePKI EV SSL Certification Authority 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.

(11) Identification and authentication of CA and RA personnel.

9.6.2 Registration Authority Representations and Warranties

RAs shall follow the procedures in CPS and EV SSL Certificate Guidelines regulations and are responsible for registration work including the collection and verification of certificate subscriber identity and certificate 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 the ePKI EV SSL Certification Authority. Its checking level is the review results of the RAO at that time but no guarantee is provided for the credit status, financial capability, technical capability or reliability of the subscriber.

RA obligations include:

(1) Provide certificate application services.

(2) Follow the procedures in the CPS and EV SSL Certificate Guidelines for identification and authentication of certificate requests.

(3) Notify subscribers and relying parties of the obligations and responsibility with regard to the ePKI EV SSL Certification Authority and RA.

(4) Notify subscribers and relying parties to follow CPS related regulations when obtaining and using the certificates issued by the ePKI EV SSL Certification Authority.

(5) Implement identification and authentication procedures for RAO.

(6) Manage RA private keys.

9.6.3 Subscriber Representations and Warranties

Subscribers shall commit to and bear the following obligations: If there is a violation, subscribers shall bear liability for damages in accordance with the Civil Code and related laws and regulations:

(1) Subscribers shall comply with related application regulations in the 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 the ePKI EV SSL Certification Authority approved the certificate application and issued the certificate.

(3) Subscribers shall check the information contained on the certificate after obtaining the certificate issued from the ePKI

EV SSL Certification Authority 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 securely generate the key pair and 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 the ePKI EV SSL Certification Authority is unable to operate normally for some reason, the subscribers shall speedily seek other ways for completion of legal acts and the inability for the ePKI EV SSL Certification Authority to operate normally shall not be used as a defense to others.

9.6.4 Relying Parties Representations and Warranties

Relying parties using certificates issued by the ePKI EV SSL Certification Authority shall bear the following obligations. If there is a violation, relying parties shall bear liability for damages in accordance with the Civil Code and related laws and regulations:

(1) Relying parties shall follow relevant CPS regulations when using the certificates issued by the ePKI EV SSL Certification Authority or checking the ePKI EV SSL Certification Authority repository.

(2) Relying parties shall first check if the certificate assurance level protects their rights during use of certificates issued by the ePKI EV SSL Certification Authority.

(3)Relying parties shall check the certificate and keyUsage listed on the certificate during use of the certificate issued by the ePKI EV SSL Certification Authority.

(4) Relying parties shall first check the CRL or OCSP to determine if the certificate is valid during use of certificates issued by the ePKI EV SSL Certification Authority.

(5) Relying parties shall first valid the digital signature to determine if the certificate or CRL, OCSP is correct when using certificates or CRL, OCSP issued by the ePKI EV SSL Certification Authority.

(6) Relying parties 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 relying parties shall bear sole responsibility.

(7) If the ePKI EV SSL Certification Authority is unable to operate normally for some reason, the relying parties shall speedily seek other ways for completion of legal acts and the inability for the ePKI EV SSL Certification Authority to operate normally shall not be used as a defense to others.

(8) Relying party acceptance of a certificate issued by the ePKI EV SSL Certification Authority indicates understanding and

agreement of the ePKI EV SSL Certification Authority legal liability clauses in accordance with the scope of certificate use outlined in section 1.4.1.

9.6.5 Representations and Warranties of Other Participant

Not stipulated

9.7 Disclaimer of warranties

In the event that damages are suffered by subscribers and relying parties due to failure to use the certificates according to the scope of use stipulated in section 1.4.1 or failure to follow the CPS, related laws and regulations and subscriber and related relying party contract provisions or any damages occur which are not attributable to the ePKI EV SSL Certification Authority, subscribers or relying parties shall be held liable.

In the event that relying parties suffer damages due to reasons attributable to the subscriber or damages occur which are not attributable to the RA, subscribers or relying parties shall be held liable.

In the event that damages are suffered by subscribers and relying parties due to failure to follow the CPS, related laws and regulations or related relying party contract provisions or damages occur which are not attributable to the RA, subscribers or relying parties shall be held liable.

9.8 Limitations of Liability

When it comes to outage due to ePKI EV SSL Certification Authority maintenance, conversion or expansion requirements, notification shall be posted in the repository three days in advance.

Subscribers and relying parties may not use temporary suspension of some certificate services as a reason to claim compensation from the ePKI EV SSL Certification Authority.

If the subscriber submits a certificate revocation request is submitted due the reasons for certification revocation stipulated in section 4.9.1, the ePKI EV SSL Certification Authority shall complete the certificate revocation work within one working day, and issue and post the CRL on the repository after the certification revocation request is approved. Before the certificate revocation status is published, subscribers shall take appropriate action to reduce the effect on relying parties and bear responsibility arising from use of the certificates.

9.9 Indemnities

9.9.1 ePKI EV SSL Certification Authority Compensation Liability

If the subscriber or relying parties suffer damages suffered due to the intentional or unintentional failure of the ePKI EV SSL Certification Authority to follow the CP, CPS, EV SSL Certificate Guidelines, relevant laws and regulations and the provisions of contracts signed between the ePKI EV SSL Certification Authority, subscribers and related relying parties when processing subscriber certificate-related work, the Company shall be held liable. The subscriber may claim compensation for damages based on the related provisions of the contract set down between the ePKI EV SSL Certification Authority and the subscriber. Relying parties shall request compensation in accordance with relevant laws and regulations. The financial liability of the Company is detailed in sections 9.2.1 and 9.2.2. If there are damages resulting from certificate mis-issue or CA private key compromise, the compensation ability shall comply with EV SSL Certificate Guidelines requirements. The total compensation limit of the ePKI EV SSL Certification Authority for each subscriber or relying party is shown in the Table below. If the subscriber or relying party has signed a contract with the Company, the certificate scope of use and transaction compensation limit shall be determined separately.

Certificate Assurance Level	Compensation Limit (NTD)
Level 3 EV SSL certificate	10,000,000

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

9.9.2 RA Compensation Liability

If subscribers or relying parties suffer damages due to the RA intentional or unintentional failure to follow the CPS, related laws and regulations or subscriber and related relying party contract provisions when processing subscriber certification registrations, the RA shall be held liable. The Company shall be held liable if the damage were caused by the general RA for which the Company is responsible for establishment, maintenance and operation. The customer who signed the contract with the Company shall be held liable for damages that were caused by dedicated RA maintained and operated by the customer. Compensation limits for RAs are detailed in section 9.9.1. If a contract has been entered into by the subscriber or relying party, the certificate scope of use and transaction compensation amounts shall be determined separately. Compensation claims by subscribers shall be made in accordance with related provisions in the contract set down with the RA. Compensation claims by related parties shall be made in accordance with relevant laws and regulations.

9.10 Term and Termination

9.10.1 Term

The CPS and any attachments take effect when approved by the Electronic Signatures Act competent authority and published on the ePKI EV SSL Certification Authority website and repository and remain effective until replaced with a newer version.

9.10.2 Termination

The CPS and any attachments remain effective until a newer version is approved by the Electronic Signatures Act competent authority and published. The old version is then terminated.

9.10.3 Effect of Termination and Survival

The conditions and effect of the CPS termination shall be communicated via the ePKI EV SSL Certification Authority website and repository. This communication shall emphasize which provisions survive CPS termination. At the minimum, the responsibilities related to protecting confidential information shall survive even CPS terminated.

9.11 Individual Notices and Communication with Participants

The ePKI EV SSL Certification Authority, RAs, subscribers, relying parties shall take respective actions to establish notification and communication channels including but not limited to: official document, letters, telephone, fax, e-mail or secure e-mail.

9.12 Amendments

9.12.1 Procedure for Amendment

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

Every year, the ePKI EV SSL CA regularly review the terms and conditions in the official version of Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates issued by CA/Browser Forum: http://www.cabforum.org, to assess if the CPS shall be modified. Shall the CPS be contradictory to the regulation of the forum in the description of EV SSL certificate issuance management, the terms and conditions issued by CA/Browser Forum shall prevail, and the CPS is modified accordingly.

9.12.2 Notification Mechanism and Period

9.12.2.1 Notification Mechanism

All changed items are posted in the ePKI EV SSL Certification Authority repository. No additional notification is made for non-material changes to the CPS.

9.12.2.2 Modification Items

Assess the level on impact of change items on subscribers and relying parties:

(1) Significant impact: Post 30 calendar days in the ePKI EV SSL Certification Authority repository before making the revision.

(2) Less significant impact: Post 15 calendar days in the ePKI EV SSL Certification Authority repository before making the revision.

9.12.2.3 Comment Reply Period

The reply period for comments on change items is:

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

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

9.12.2.4 Comment Handling Mechanism

For comments on changed items, the reply method posted in the ePKI EV SSL Certification Authority repository is transmitted to the ePKI EV SSL Certification Authority prior to the end of the comment reply period. The ePKI EV SSL Certification Authority shall consider related comments when evaluating the change items.

9.12.2.5 Final Notification Period

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

9.12.3 Circumstances Under Which the OID Must Be Changed

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

9.13 Dispute Resolution Provisions

In the event of a dispute between subscribers or RA and the ePKI EV SSL Certification Authority, 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 ePKI EV SSL Certification Authority issued certificates, the applicable related ROC laws and regulations shall govern.

9.15 Compliance with Applicable Law

Interpretations of any agreement signed accordance to this CPS, shall accordance with the provisions of ROC's relevant laws and regulations.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

An entire agreement clause, which typically identifies the document or documents comprising the entire agreement between the key participants (ePKI EV SSL Certification Authority, RA, Subscribers and relying parties) and states that such agreements supersede all prior and contemporaneous written or oral understandings relating to the same subject matter and the CPS entire agreement shall be the final agreement mutually agreed upon for the CPS.

9.16.2 Assignment

The rights and obligations of key participants described in the CPS may not be assigned in any form to other parties without notifying the ePKI EV SSL Certification Authority.

9.16.3 Severability

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

Regarding the issuance of EV SSL certificates, the CPS complies with the requirements in the official version of Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates and Guidelines for the Issuance and Management of Extended Validation Certificates issued by CA/Browser Forum (http://www.cabforum.org); however, if the related requirements of the Baseline Requirements and EV SSL Certificate Guidelines conflict with the related domestic laws and regulations complied by the CPS, the CPS may be adjusted to satisfy the requirements of the laws and regulations and notify CA/Browser Forum about the changed contents of the CPS. If the domestic laws and regulations are not applicable anymore, or the Baseline Requirements and EV SSL Certificate Guidelines are revised their contents to be compatible with the domestic laws and regulations, the CPS will delete and amend the adjusted contents. The aforesaid actions shall be completed in 90 calendar days.

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

In the event that the ePKI EV SSL Certification Authority suffers damages attributable to an intentional or unintentional violation of related CPS regulations by a subscriber or relying party, the ePKI EV SSL Certification Authority may seek compensation for damages from the responsible party related to the dispute or litigation.

The ePKI EV SSL Certification Authority's failure to assert rights with regard to the violation of the CPS regulations does not waive the ePKI EV SSL Certification Authority's right to pursue the violation of the CPS subsequently or in the future.

9.16.5 Force Majeure

In the event that a subscriber or a relying party suffers damages due to a force majeure or other circumstances not attributable to the ePKI EV SSL Certification Authority including but not limited to natural disasters, war or terrorist attack, the ePKI EV SSL Certification Authority shall not bear any legal liability. The ePKI EV SSL

Certification Authority shall set clear limitations for certificate usage and shall not bear any legal responsibility for damages caused by exceeding these usage limitations.

9.17 Other Provisions

Not stipulated

Appendix 1: Acronyms and Definitions

Acronyms	Full Name	Definition
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.
CEO	Chief Executive Officer	
CFO	Chief Financial Officer	
CIO	Chief Information Officer	
CISO	Chief Information Security Officer	
COO	Chief Operating Officer	
CMM	Capability Maturity Model	See Appendix 2.
CP	Certificate Policy	See Appendix 2.
CPA	Chartered Professional Accountants Canada	See Appendix 2.
CP OID	CP Object Identifier	
CPS	Certification Practice Statement	See Appendix 2.
CRL	Certificate Revocation	See Appendix 2.

Acronyms	Full Name	Definition
	List	
CT	Certificate Transparency	See Appendix 2.
DN	Distinguished Name	
DNS	Domain Name System	See Appendix 2.
eCA	ePKI Root Certification Authority	See Appendix 2.
EE	End Entities	See Appendix 2.
ePKI	Chunghwa Telecom ecommerce Public Key Infrastructure	See Appendix 2.
EV	Extended Validation	See Appendix 2.
FIPS	(US Government) Federal Information Processing Standard	See Appendix 2.
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.
NIST	(US Government) National Institute of Standards and Technology	See Appendix 2.
OCSP	Online Certificate Status Protocol	See Appendix 2.
OID	Object Identifier	See Appendix 2.
PIN	Personal Identification	

Acronyms	Full Name	Definition
	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.
QIIS	Qualified Independent Information Source	See Appendix 2.
RA	Registration Authority	See Appendix 2.
RFC	Request for Comments	See Appendix 2.
SSL	Security Socket Layer	See Appendix 2.
TLS	Transport Layer Security	See Appendix 2.
UPS	Uninterrupted Power System	See Appendix 2.

Appendix 2: Glossary

Access	Use the information processing capabilities of system resources
Access Control	Authorization procedure for access to information system resources given to subscribers, programs, procedures and other systems.
Activation Data	The private data required besides keys to access the cryptographic module (such as data used to activate the private key for signatures or encryption).
American Institute of Certified Public Accountants (AICPA)	Institution which jointly drafted The Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy system standards with the Chartered Professional Accountants Canada and the management organization for WebTrust for CA and SSL Baseline Requirement & Network Security mark.
Applicant	Subscribers who request certificates from a CA and have not yet completed the certificate procedure.
Application Software Supplier	A supplier of Internet browser software or other relying- party application software that displays or uses Certificates and incorporates Root Certificates.
Archive	A physically separate storage site for long-term information (storage site for important information) which can be used to support audit, usage and integrity services.
Assurance	A reliable basis to determine that an entity conforms to certain security requirements (see Article 2-1, Chapter 1 for the rules which should be stated in CPS)
Assurance Level	A level possessing a relative assurance level (see Article 2-1, Chapter 1 for the rules which should be stated in CPS)

Audit	Assessment of whether system controls are adequate and ensure conformance with existing policy and operation procedures, and independent checking and review of recommended required improvements to existing controls, policies and procedures.
Audit Data	Activity logs of a system organized in the order of time of occurrence that can be used to reconstruct or investigate the time sequence or changes that occurred during a certain event.
Authenticate	(1) Authentication is the process by which a claimed identity is verified. (A Guide to Understanding Identification and Authentication in Trusted Systems, National Computer Security Center) (2) Determination of identity authenticity when an identity of a certain entity is shown.
Authentication	(1) The process of establishing confidence in the identity of users or information systems. (2) Security measures used for information transmission, messages and ways to authorize individuals to receive certain types of information. (3) "authentication" is proof of identification. Mutual authentication refers to authentication mutually conducted between two parties during communication activities.
Authority Information Access (AIA)	Records extensions related to certificate authority information access. The content may include: OCSP service sites and certificate issuance authority certificate verification path downloading site.
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 as published by the CA/Browser Forum and any amendments to such document.
Binding	The process for binding (connecting) two related information elements.
Biometric	The physical or behavioral attributes of a person.
Business Entity	Any entity that is not a Private Organization, Government Entity, or Non-Commercial Entity as defined herein. Examples include, but are not limited to, general partnerships, unincorporated associations, sole proprietorships, etc.
CA Certificate	Certificates issued to CAs.
Capability Maturity Model (CMM)	Software Process Assessment (SPA) and Software Capability Evaluation (SCE) from the Software Engineering Institute (SEI) at Carnegie Mellon

	University (CMU) serves as the basic framework to assist software developers find places for improvement in software development processes.
Certificate	(1) Refers to verification information carrying a digital signature used to verify the identity and qualifications of the signer in electronic form (Article 2.6 of the Electronic Signatures Act) (2) Digital presentation of information. The contents include: A. Issuing certificate authority B. Subscriber name or identity C. Subscriber public key D. Certificate validity period E. Certification authority digital signature The term ‘certificate’ referred to in the certificate policy specifically refers to ITU-T X.509 v.3 format certificates which states the certificate policy object identifier in the ‘certificate policy’ field.
Certificate Approver	A natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant to (i) act as a Certificate Requester and to authorize other employees or third parties to act as a Certificate Requester, and (ii) to approve EV Certificate Requests submitted by other Certificate Requesters.
Certificate Requester	A natural person who is either the Applicant, employed by the Applicant, an authorized agent who has express authority to represent the Applicant, or a third party (such as an ISP or hosting company) that completes and submits an EV Certificate Request on behalf of the Applicant.
Certification Authority (CA)	(1) The agency or natural person that issues certificate (Article 2.5 of the Electronic Signatures Act) (2) The competent body trusted by the subscriber.

	Its functions are the issuance and administration of ITU-T X.509 format public key certificates, CARLs and CRLs.
Certification Authority Authorization (CAA)	From RFC 6844 (http:tools.ietf.org/html/rfc6844): “The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify the Certification Authorities (CAs) authorized to issue certificates for that domain. Publication of CAA Resource Records allows a public Certification Authority to implement additional controls to reduce the risk of unintended certificate mis-issue.”
Certificate Policy (CP)	(1) Refers to a named set of rules that indicates the applicability to a certain community or class of application with common security requirements (Article 2.3 Chapter 1, in the Regulations on the Required Information for Certification Practice Statements) (2) Certificate policy refers to the dedicated profile administration policy established for the electronic transactions performed through certificate administration. Certificate policy covers a variety of issues including the formation, generation, delivery, auditing, administration and restoration after compromise. Certificate policy indirectly controls the use and operation of certificate security systems to protect the transactions performed by the communication systems. The security services required for certain application are provided through control of the

	certificate extension methods, certificate policy and related technology.
Certification Practice Statement (CPS)	(1) External notification by the certificate authority used to describe the practice statement of the certificate authority governing certificate issuance and processing of other certification work. (Article 2.7 Electronic Signatures Act) (2) Announcement of a statement that certain procedures of the certificate authority for certificate work (including issuance, suspension, revocation, renewal and access) comply with certain requirements (listed in the certificate policy or other service contracts).
Certificate Problem Reports	The complaints regarding suspected cracking of keys, certificate misused, or other types of fraud, cracks, abuse, or inappropriate behaviors related to certificates.
Certificate Transparency, CT	The certificate transparency system is an open architecture for the public monitoring and auditing of all certificates on the Internet (priority target at the current stage is EV SSL certificates), through open certificate issuance and existing information to given to the domain owner, CA and domain user to determine whether the certificate has been mis-issued or maliciously issued. In other words, the purpose is to provide a usable TLS/SSL certificate system and public monitoring and information disclosure environment for the review and approval of specific TLS/SSL certificates to curb certificate-related threats. The certificate transparency system is mainly comprised of a

	certificate log, certificate monitored and certificate auditor.
Certificate Revocation List (CRL)	(1) The certificate revocation list digitally signed by the certification authority provided for relying party use. (Article 2.8, Chapter 1 in the Regulations on Required Information for Certification Practice Statements) (2) List maintained by the certificate authority. The expiry dates of the above revoked certificates issued by the certification authority are recorded on the list.
Chartered Professional Accountants 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.
Component Private Key	Private keys associated with certificate issuance equipment functions as opposed to private keys associated with operators or administrators.
Compromise	Information disclosed to unauthorized persons or unauthorized intentional or unintentional disclosure, modification, destruction or loss of objects which constitutes a violation of information security policy.
Confidentiality	Information which will not be known or be accessed by unauthorized entities or programs.
Confirming Person	A position within an Applicant's organization that confirms the particular fact at issue.
Contract Signer	A natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant, and who has authority on behalf of the Applicant to sign Subscriber Agreements.

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.
Crypto period	The validity period set for each key.
Data Integrity	Information that has been subjected to unauthorized access or accidental modification, damage or loss.
Demand Deposit Account	A deposit account held at a bank or other financial institution, the funds deposited in which are payable on demand. The primary purpose of demand accounts is to facilitate cashless payments by means of check, bank draft, direct debit, electronic funds transfer, etc. Usage varies among countries, but a demand deposit account is commonly known as a share draft account, a current account, or a checking account.
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	The label assigned to a node in the Domain Name System.
Domain Name Registrant	Sometimes referred to as the “owner” of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the “Registrant” by WHOIS or the Domain Name Registrar.

Domain Name Registrar	A person or entity that registers Domain Names under the auspices of or by agreement with: (1) the Internet Corporation for Assigned Names and Numbers (ICANN), (2) a national Domain Name authority/registry, or (3) a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns).
Domain Name System (DNS)	Distributed database used to automatically transfer IP addresses and domain names.
Duration	A certificate field made up of two subfields “start time of the validity period” (notBefore) and “end time of the validity period” (notBefore).
E-commerce	Provision of goods for sale and other services through the use of network technology (specifically the Internet).
Encryption Certificate	A certificate including a public key used for encryption of electronic messages, files, documents or other information. This key can also be used to establish or exchange a variety of short-term secret keys for encryption.
End Entity	The PKI includes the following two types of entities: (1) Those responsible for the safeguarding and use of certificate public keys. (2) Third parties who trust the certificates issued by the PKI (not holders of private keys and not a certificate authority). The end entities are subscribers and relying parties including personnel, organizations, accounts, devices and sites.
End-Entity Certificate	Certificates issued to end-entities.
Enterprise EV Certificate	An EV Certificate that an Enterprise RA authorizes the CA to issue at third and higher domain levels.
Enterprise RA	An RA that is authorized by the CA to authorize the CA to issue EV Certificates at third and higher

	domain levels.
Chunghwa Telecom ecommerce Public Key Infrastructure (ePKI)	In order to promote Electronic Policy and create a sound e-commerce infrastructure, the Chunghwa Telecom Co., Ltd. shall follow the ITU-T X.509 standards to establish the public key infrastructure for use with various applications in e-commerce and e-government.
Chunghwa Telecom ecommerce Public Key Infrastructure Policy Management Committee (ePKI Policy Management Committee)	An organization which was established for the purpose of: Discuss and review the ePKI CP and electronic certificate system framework, accept subordinate CA and subject CA interoperation applications and other matters such as review and study of CPS and electronic certificate management matters.
ePKI Root CA (eCA)	The Chunghwa Telecom Public Key Infrastructure Root Certification Authority (Root CA) is the top-level certificate authority in this hierarchical public key infrastructure. Their public keys are the trust anchor.
Extended Validation, EV	The Validation Procedures defined in CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates.
EV Certificate	A certificate that contains subject information specified in CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates and that has been validated in accordance with CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates.
Federal Information	Except for military organizations in the US Federal Government System, information

Processing Standard (FIPS)	processing standard for all government organizations and government subcontractors. The security requirement standard for the cryptographic module is FIPS no. 140 standard (FIPS 140). FIPS 140-2 divides the cryptographic module into 11 types of security requirements. Each security requirement type is then divided into 4 security levels.
Firewall	An access restriction gateway between networks which complies with near-end (local area) security policy.
Fully Qualified Domain Name (FQDN)	A specific domain name which is used to designate to the computer its precise location in the domain hierarchy. The fully qualified domain name consists of the host name (service name) and domain name. For example, for ourserver.ourdomain.com.tw. ourserver is the host name, ourdomain.com.tw is the domain name. Of this ourdomain is the secondary domain name, . com is the generic top-level domain (gTLD), .twis the country code top-level domain (ccTLD). The beginning of the FQDN must be the host name.
Government Agency	In the context of a Private Organization, the government agency in the Jurisdiction of Incorporation under whose authority the legal existence of Private Organizations is established (e.g., the government agency that issued the Certificate of Incorporation). In the context of Business Entities, the government agency in the jurisdiction of operation that registers business entities. In the case of a Government Entity, the entity that enacts law, regulations, or decrees establishing the legal existence of Government Entities.
High Risk Certificate Request	A Request that the CA flags for additional scrutiny by reference to internal criteria and databases maintained by the CA, which may include names at higher risk for phishing or other fraudulent usage, names contained in previously rejected certificate requests or revoked Certificates, names listed on the Miller Smiles phishing list or the

	Google Safe Browsing list, or names that the CA identifies using its own risk- mitigation criteria.
Identification	A statement of whom the user is (globally known). (A Guide to Understanding Identification and Authentication in Trusted Systems). "Identification" is a statement of whom the user is (globally known).
Incorporating Agency	In the context of a Private Organization, the government agency in the Jurisdiction of Incorporation under whose authority the legal existence of the entity is registered (e.g., the government agency that issues certificates of formation or incorporation). In the context of a Government Entity, the entity that enacts law, regulations, or decrees establishing the legal existence of Government Entities.
Independent Confirmation from Applicant	Confirmation of a particular fact received by the CA pursuant to the provisions of the Guidelines or binding upon the Applicant.
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.
International Organization	An organization founded by a constituent document, e.g., a charter, treaty, convention or similar document, signed by, or on behalf of, a minimum of two Sovereign State governments.
Internationalized Domain Name	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)	Internet address assignment authority responsible for administering IP addresses, domains, names and many other parameters used with the Internet.
Internet	Responsible for the development and promotion of

Engineering Task Force (IETF)	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	In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.
Jurisdiction of Incorporation	In the context of a Private Organization, the country and (where applicable) the state or province or locality where the organization's legal existence was established by a filing with (or an act of) an appropriate government agency or entity (e.g., where it was incorporated). In the context of a Government Entity, the country and (where applicable) the state or province where the Entity's legal existence was created by law.
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 require that one or more than one agencies have possession of the subscriber key provided it is beneficial to the subscriber, employer or another party in accordance with the provisions of the agreement.
Key Exchange	Mutual exchange of keys to establish a secure communication processing procedure.
Key Pair	Two mathematically linked keys possessing the following attributes: (1) One of the keys is used for encryption. This encrypted data may only be decrypted by the other key. (2) It is impossible to determine one key from another (from a mathematical calculation standpoint).

Latin Notary	A person with legal training whose commission under applicable law not only includes authority to authenticate the execution of a signature on a document but also responsibility for the correctness and content of the document. A Latin Notary is sometimes referred to as a Civil Law Notary.
Legal Existence	A Private Organization, Government Entity, or Business Entity has Legal Existence if it has been validly formed and not otherwise terminated, dissolved, or abandoned.
Legal Practitioner	A person who is either a lawyer or a Latin Notary as described in the EV SSL Certificate Guidelines and competent to render an opinion on factual claims of the Applicant.
Non-Repudiation	Provide proof of delivery to the information sender and proof of sender identity to the receiver so neither party may repudiate the processing of this information after the fact. Technically speaking, non-repudiation refers to the guarantee that this signature must be signed by the corresponding private key if a certain public key can be used to verify a certain digital signature for a trusting party. Legally speaking, non-repudiation refers to the establishment of a possession and control system for private signature keys.
Object Identifier (OID)	(1) One type of unique alphanumeric / numeric identified registered under the International Standard Organization registration standard which could be used to identify the uniquely corresponding certificate policy; where the certificate policy is modified, the OID is not changed accordingly. (Article 2.4 Chapter 1 in the Regulations on Required Information for Certification Practice Statements) (2) When a special form of code, object or object type is registered with the International Standard Organization (ISO), the unique code may be used as an identified. For example, this code can be used in the public key

	infrastructure to indicate what certificate policy and cryptographic algorithms are used.
Online Certificate Status Protocol (OCSP)	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	An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests.
OCSP Stapling	This is a form of TLS Certificate Status Request extension, which may replace the OCSP to check X.509 certificate status. 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 SSL certificate status from the CA when connecting to a high traffic TLS website, and thus to decrease the burden of the CA. This mechanism also prevents the privacy concern that the OCSP Responder knows which subscribers attempting to browsing that SSL website by having the TLS website referring the 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.
Place of Business	The location of any facility (such as a factory, retail store, warehouse, etc.) where the Applicant’s business is conducted.
Principal Individual	An individual of a Private Organization, Government Entity, or Business Entity that is either an owner, partner, managing member,

	director, or officer, as identified by their title of employment, or an employee, contractor or agent authorized by such entity or organization to conduct business related to the request, issuance, and use of EV SSL Certificates.
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.
Private Organization	Private Organization: A non-governmental legal entity (whether ownership interests are privately held or publicly traded) whose existence was created by a filing with (or an act of) the Incorporating Agency or equivalent in its Jurisdiction of Incorporation.
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 17.6 of the EV SSL Certificate

	Guidelines and 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, 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.
Qualified Independent Information Source (QIIS)	A regularly-updated and publicly available database that is generally recognized as a dependable source for certain information. A database qualifies as a QIIS if the CA determines that: (1) Industries other than the certificate industry relies on the database for accurate location, contact, or other information; and (2) The database provider updates its data on at least an annual basis. The CA SHALL use a documented process to check the accuracy of the database and ensure its data is acceptable, including reviewing the database provider’s terms of use.
Random Value	A value specified by a CA to the Applicant that exhibits at least 112 bits of entropy.
Registration	A Governmental Agency that registers business information in connection with an entity’s business

Agency	formation or authorization to conduct business under a license, charter or other certification. A Registration Agency MAY include, but is not limited to (i) company registration agency (ii) competent authority of the relevant industry (such as: Ministry of Transportation and Communication); or (iii) a chartering agency, such as the Financial Supervisory Commission and National Communications Commission.
Registered Agent	An individual or entity that is:(1) authorized by the Applicant to receive service of process and business communications on behalf of the Applicant; and (2) listed in the official records of the Applicant's Jurisdiction of Incorporation as acting in the role specified in (1) above.
Registered Office	The official address of a company, as recorded with the Incorporating Agency, to which official documents are sent and at which legal notices are received.
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.
Registration Number	(1) The unique number assigned to a Private Organization by the Incorporating Agency in such entity's Jurisdiction of Incorporation. (EV SSL Certificate Guidelines)。 (2) For companies registered in our country, the government assigns a tax ID number. For government agencies established by our country's government, the Directorate-General of Personnel Administration assigns a government agency code. The ePKI EV SSL Certification Authority considers these to be registration numbers.

Regulated Financial Institution	A financial institution that is regulated, supervised, and examined by governmental, national, state or provincial, or local authorities.
Re-key (a certificate)	Changing the key values used in the cryptographic system application program. It is commonly achieved by issuing a new certificate for the new public key.
Relying Party	(1) Recipient of a certificate who acts in reliance of that certificate or a digital signature to verify the public key listed in the certificate, or the counterpart to identify (or its attributes) of the subject named in a trusted certificate and public key listed in the certificate. (Article 2.6, Chapter 1 in the Regulations on Required Information for Certification Practice Statements) (2) The individual or agency which receives information including a certificate and digital signature (the public key listed on the certificate may be used to verify the digital signature) and may rely on this information.
Renew (a certificate)	The procedure for issuing a new certificate to renew the validity of information bound together with the public key.
Repository	(1) A trustworthy system used to store and retrieve certificates and other information relevant to certification. (Article 2.7, Chapter 1 in the Regulations on Required Information for Certificate Practice Statements) (2) The database containing the certificate policy and certificate-related information.
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 Socket 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.
Secret Key	Shared secret in the symmetric cryptosystem, identity authentication of the subscriber is performed by sharing other secrets through passwords, PIN or remote host (or service). The single key is jointly held by two parties. The sender uses it to encrypt the transmitted information and the receiver uses it to decrypt the information. This jointly held key is generated with previously agreed upon algorithms.
Subordinate CA	In the public key infrastructure hierarchy, certificates that are issued by another certificate authority and the activities of the certificate authority are restricted to this other certificate authority.
Subscriber	(1) Refers to a subject named or identified in the certificate that holds the private key that corresponds with the public key listed in the certificate. (Article 2.5, Chapter 1 Regulations on Required Information for Certification Practice Statements) (2) An entity having the following attributes including (but not limited to) individuals, organizations, server software or network devices: (a) Subject listed on an issued certificate.

	(b) A private key that corresponds to the public key listed on the certificate. (c) Other partiers that do not issue certificates.
Technical Non-Repudiation	Technical evidence provided by the public key system to support non-repudiation security service.
Threat	Any status or event which may cause damage (including destruction, disclosure, malicious tampering or denial of service) to information systems. Can be divided into internal threats and outside threats. Internal threats are use of authorization to employ information destruction, disclosure, tampering or denial of service methods to damage the information system. Outside threats are an outside unauthorized entity which has the potential to damage the information system (including information destruction, tampering, disclosure and interruption of service).
Time Stamp	Trusted authority proves that a certain digital object exists at a certain time through digital signature.
Transport Layer Security (TLS)	SSL protocol established in RFC 2246 by the IETF. Called Transport Layer Security (TLS). Latest version is RFC 5246 which is the TLS 1.2 protocol.
Trust List	List of trusted certificates used by relying parties to authenticate certificates.
Trusted Certificate	Certificate trusted by relying party obtained through a secure and reliable transmission method. The public key contained in this type of certificate comes from a trusted path. Also called a trust anchor.
Trustworthy 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 establishing the identity of certificate applicants.
Verified Method of Communication	The use of a telephone number, a fax number, an email address, or postal delivery address, confirmed by the CA in accordance with Section 11.5 of the EV SSL Certificate Guidelines as a reliable way of communicating with the Applicant.
Zeroize	Method to delete electronically stored information. Storage of changed information to prevent information recovery.