HiPKI EV TLS Certification Authority Certification Practice Statement (HiPKI EV TLS CA CPS)

Version 1.1

Chunghwa Telecom Co., Ltd.

July 2, 2020

Contents

Document History

Version	Release Date	Revision Summary
1.0	February 22, 2019	First Release.
1.05	March. 2, 2020	(1) Information update of CAA issuer domain names in Section 2.2; (2) Add Sections 3.2.5.6 and 3.2.5.7 about domain validation methods to comply with CABF Ballot SC13; (3) Remove domain validation method "Phone Contact with Domain Contact" to comply with CABF Ballot SC14; (4) Amendments are made on Section 4.9.10 to comply with CABF Ballot SC23; (5) Amendments are made on Sections 1.5.2.1, 3.2.5, 4.2.1, 4.9, 7.1.2 and 9.6 according to BR v1.6.7; and (6) Amendments are made on Sections 1.3.3, 3.3.2, 4.2.2, 4.2.3, 4.3, 4.4, 4.5.2, 4.7.1, 4.12.1, 5.1.2, 5.1.7, 5.2.1, 5.2.4, 5.3.1, 5.3.7, 5.4, 5.5, 5.6, 5.7.1, 5.8, 6.1, 6.2, 6.3.2, 6.4, 7.1, 7.1.3, 7.2.2, 7.3, 9.1, 9.2.2, 9.4 and 9.16.1.
1.1	July 2, 2020	Amendments are made on Sections 1.3.4, 1.4.1, 1.4.2, 1.5.4, 1.6.1, 2.2, 3.1.5, 4.2.2, 4.9.10 and 9.9.1.

1. Introduction

1.1. Overview

1.1.1. Certification Practice Statement

The HiPKI EV TLS Certification Authority (HiPKI EV TLS CA) Certification Practice Statement (CPS) describes the practices used to comply with the HiPKI Certificate Policy (CP), current versions of the

(1) Electronic Signatures Act and

(2) its sub-law "Regulations on Required Information for Certification Practice Statements"

of R.O.C. and current versions of related international standards or regulations, including

(1) The Internet Engineering Task Force (IETF) request for comments (RFC) 3647 and RFC 5280;

(2) ITU-T X.509; and

(3) Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (Baseline Requirements), Guidelines for the Issuance and Management of Extended Validation Certificates (EV SSL Certificate Guidelines), and Network and Certificate System Security Requirements published by CA/Browser Forum (http://www.cabforum.org),

to provide guidance and requirements for what HiPKI EV TLS CA should include in its CPS.

According to the HiPKI CP, HiPKI Root Certification Authority (HiPKI RCA) is a top-level CA and a trust anchor of HiPKI. HiPKI RCA must maintain a high level of credibility that relying parties can directly trust its certificates. HiPKI EV TLS CA is a level-one Subordinate CA of HiPKI RCA that obtains certificates from HiPKI RCA and is responsible for the issuance and management of Extended Validation (EV) TLS/SSL certificates. The SSL (Secure Sockets Layer) protocol has been replaced by the TLS (Transport Layer Security) protocol, because SSL certificates and TLS certificates refer

to certificates that can also operate the TLS protocol. The current trend is called TLS certificates but not widely used SSL certificates, to avoid confuse, we use “TLS/SSL certificates” in this CPS.

The primary purposes of an EV TLS/SSL Certificate are:

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

(2) Securing website communications with encryption: Facilitate the exchange of encryption keys in order to enable the encryption of transmitted information over the Internet between the user of a browser and a website.

The secondary purposes of an EV TLS/SSL Certificate are to help establish the legitimacy of an organization claiming to operate a website, and to provide a solution 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 organization, EV TLS/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.

1.1.2. CPS Applicability

The practice statement stipulated in this CPS applies to HiPKI EV TLS CA, Registration Authority (RA), subscribers and relying parties.

1.2. Document Name and Identification

This document is HiPKI EV TLS CA Certification Practice Statement and was approved for publication on July 2, 2020. The current version of this CPS can be obtained at the website: https://eca.hinet.net.

The EV TLS/SSL certificates issued by HiPKI EV TLS CA conform to the EV SSL Certificate Guidelines and the individually negotiated certificate processing methods supported by application software suppliers (such as browsers or operating system providers) may use the CP object identifier (OID, which is {joint-iso-itu-t(2) international-organizations (23) ca-browser-forum(140) certificate- policies(1) ev-guidelines (1) }(2.23.140.1.1)) defined by the CA/Browser Forum for EV TLS/SSL certificates. If any part is not regulated under the documents of CA/Browser Forum, the rule of assurance level 3 in the HiPKI CP is applicable.

With regard to EV TLS/SSL certificates, if there is any inconsistency between this CPS and the EV SSL Certificate Guidelines and Baseline Requirements, then the EV SSL Certificate Guidelines and Baseline Requirements take precedence.

1.3. PKI Participants

The participants of HiPKI EV TLS CA include:

(1) HiPKI EV TLS CA

(2) RA

(3) Subscribers

(4) Relying Parties

1.3.1. Certification Authorities

HiPKI EV TLS CA, established and operated by Chunghwa Telecom Co., Ltd (CHT), operates and issues EV TLS/SSL certificates under the HiPKI CP.

1.3.2. Registration Authorities

The RA is responsible for collection and authentication of subscriber identity and certificate-related information. The RA is comprised of many RA

counters under the organization authorized and approved by HiPKI EV TLS CA. Each RA counter has several RA officers (RAOs) who are responsible for performing certification application, revocation, re-key and renewal.

HiPKI EV TLS CA does not permit any delegated third party to be the RA counter to verify the ownership or control of domain names or IP addresses. The delegated third party means any natural person or legal entity that is not HiPKI EV TLS CA but is delegated to assist the certificate management procedures, and is not covered by the external audit of HiPKI EV TLS CA.

1.3.3. Subscribers

Any Private Organization, Government Entity, Non-Commercial Entity, or Business Entity that has applied to a certificate from HiPKI EV TLS CA and has not yet completed the certificate issuing procedures is referred to the Applicant. A Subscriber refers to the subject who has applied for and obtained a certificate issued by HiPKI EV TLS CA. The relationship between the subscriber and certificate subject is listed in the table below:

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

Generation of subscriber key pairs shall comply with Section 6.1.1 of this CPS. The subscriber must have the right and capability to control the private key that corresponds to its subscriber certificate. The subscriber is not capable of issuing certificates to other parties.

1.3.4. Relying Parties

A relying party refers to an entity who believes in the connection between the certificate subject name and a public key. The relying party must check the validity of the received certificate by checking the CA certificate and the appropriate certificate status information. The certificate may be used for the following work after checking the validity of the certificate:

(1) Identify subscriber name and its extended validation information,

(2) Identify the fully qualified domain name (FQDN) owned or controlled by the subscriber, or

(3) Establish secure communication channel with the certificate subject.

1.3.5. Other Participants

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

1.4. Certificate Usage

1.4.1. Appropriate Certificate Uses

HiPKI EV TLS CA issues EV TLS/SSL certificates (for signature and encryption use) defined in the HiPKI CP. The certificates can be applied to server application software with transport layer security (TLS) communication protocol. HiPKI EV TLS CA issues two types of EV TLS/SSL certificates, which are single-domain and multi-domain.

The applicable scope for EV TLS/SSL certificates and organization certificates in this CPS is described as follows:

Cert. Type	Scope of Applications
EV TLS/SSL	• Provide communication channel encryption and protection. • Require verifying the identity of the organization that owns the domain name. • The green branded address bar is the most highly recognizable sign of an EV-secured webpage. It shows visitors the organization information of the certificate subject. • Scope of application includes: 1. e-commerce transactions, and 2. e-government.

Subscribers and relying parties must carefully read, comply with this CPS and shall pay attention to the update of this CPS before using and trusting the certificate services provided by HiPKI EV TLS CA.

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

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

1.4.2. Prohibited Certificate Uses

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

(1) Crime,

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

(3) Operation of nuclear equipment, and

(4) Aviation flight and control systems.

1.5. Policy Administration

1.5.1. Organization Administering the Document

Chunghwa Telecom Co., Ltd.

1.5.2. Contact Person

1.5.2.1. CPS Related Issues

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

Tel: +886 2-2344-4820

Address: 10048 HiPKI EV TLS Certification Authority (4F), Data

Communication Building, No. 21, Sec.1, Hsinyi Rd.,
Taipei City, Taiwan (R.O.C.)
E-mail: caservice@cht.com.tw

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

1.5.2.2. Certificate Problem Report

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

HiPKI EV TLS CA may or may not revoke in response to this request. See Section 4.9.3 and 4.9.5 for detail of actions performed by HiPKI EV TLS CA for making this decision.

1.5.3. Person Determining CPS Suitability for the Policy

HiPKI EV TLS CA shall submit this CPS to the Chunghwa Telecom Certificate Policy Management Authority (PMA) for review and approval after checking whether this CPS conforms to the HiPKI CP.

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

HiPKI EV TLS CA conducts regular self-audits to demonstrate that it has operated with the assurance level under the HiPKI CP. HiPKI has applied to the root certificate programs of most operating systems, web browsers, and software platforms to include our root certificate, the self-signed certificate of HiPKI RCA, into their CA trust list. This makes each root certificate program can use our root certificate to anchor a chain of trust for certificates used by TLS/SSL servers and other applications without having to ask users for further permission or information.

According to the criteria of each program, full-surveillance period-of-

time audits must be conducted and updated audit information provided no less frequently than annually. That is, successive audits must be contiguous (no gaps). In addition, external audits for HiPKI EV TLS CA and HiPKI RCA must conduct and HiPKI EV TLS CA must submit the current CPS and audit report to each root certificate program annually. HiPKI EV TLS CA shall also continue to maintain the audit seals published on the HiPKI EV TLS CA website.

1.5.4. CPS Approval Procedures

This CPS is published by HiPKI EV TLS CA following approval by the PMA or MOEA, the competent authority of the Electronic Signatures Act. This CPS must be revised in response to any revision of the HiPKI CP, and the revised CPS must be submitted to the PMA and MOEA for approval.

After the revisions of this CPS take effect, if there is any inconsistency between the original CPS and the revised CPS, then the revised CPS takes precedence unless stipulated otherwise.

1.6. Definitions and Acronyms

1.6.1. Definitions

Term	Definition
Access	Ability to make use of any information system (IS) resource.
Access Control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems.
Activation Data	Private data, other than keys, that are required to access cryptographic modules and that need to be protected (i.e., unlock private keys for signing or decryption events).
Applicant	The subscriber who request a certificate from a CA and has not yet completed the certificate issuance procedure.
Application Software Supplier	A supplier of Internet browser software or other relying-party application software that displays or

	uses certificates and root certificates.
Archive	A long-term, physically separate storage which can be used to support audit, availability and integrity services.
Assurance	A basis that the trusted entity has complied with certain security requirements. [Article 2-1, Regulations on Required Information for Certification Practice Statements]
Assurance Level	A certain level in a relative assurance tier. [Article 2-2, Regulations on Required Information for Certification Practice Statements]
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.
Authenticate	To confirm the identity of an entity when that identity is presented.
Authentication	(1) The process of establishing confidence in user identities electronically presented to an information system. [NIST.SP.800-63-2 Electronic Authentication Guideline] (2) Safety measures used to secure data transmission or ways to authorize the privilege of individuals upon receiving certain types of information. (3) Authentication is the process by which a claimed identity is verified. [A Guide to Understanding Identification and Authentication in Trusted Systems] Mutual authentication means that the authentication is performed between two parties during communication.
Authority Information Access (AIA)	An extension that indicates how to access information and services with regard to the issuer of a certificate, including the address of the OCSP responder and the URL pointing to the location

	where issuer of this certificate is located.
Authorization Domain Name	The Domain Name used to obtain authorization for certificate issuance for a given FQDN. A CA may use the FQDN returned from a domain name system (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	Copy of files and programs made to facilitate recovery if necessary.
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.
Binding	Process of associating two related information elements.
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 and sole proprietorships.
CA Certificate	Certificates that is issued to certification authorities.
Capability Maturity Model Integration (CMMI)	Capability Maturity Model Integration (CMMI) is the successor of the Capability Maturity Model (CMM) and was developed by the Software Engineering Institute at Carnegie Mellon University. CMMI models provide guidance for developing or improving processes that meet the business goals of an organization. Its purpose is to

	help improve organizational performance.
Certificate	(1) An electronic certification on certification material with signature for use in confirming identity and qualification of the signature party. [Article 2-6, Electronic Signatures Act] (2) Digital presentation of information, the content includes at least: a. information of issuing CA, b. names or identities its subscriber, c. the subscriber's public key, d. operational period, and e. digital signature of issuing CA The term "certificate" referred to this CP shall be a certificate with the format of ITU-T X.509 version 3 and has asserted the OIDs of this CP in the certificate policy extension.
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 TLS/SSL 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) Institution, finance corporation signing and issuing certificate [Article 2-5, Electronic Signatures Act] (2) An authority trusted by one or more users that issues and manages X.509 public key certificates and CRLs (or CARLs).
Certification Authority Authorization (CAA)	The certification authority authorization (CAA) DNS resource record allows a DNS domain name

	holder to specify one or more certification authorities (CAs) authorized to issue certificates for that domain. CAA resource records allow a public certification authority to implement additional controls to reduce the risk of unintended certificate mis-issue. [RFC 6844]
Certificate Policy (CP)	(1) A named set of rules that indicates the applicability of a certificate to a particular community or class of application with common security requirements. [Article 2-3, Regulations on Required Information for Certification Practice Statements] (2) A certificate policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A certificate policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates. A certificate policy can also indirectly govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.
Certification Practice Statement (CPS)	(1) A practice statement published by a certification service provider to specify the practices that the certification service provider employs in issuing certificates and managing other certification-related services. [Article 2-7, Electronic Signatures Act] (2) A statement of the practices that a certification authority employs in issuing, suspending, revoking, and renewing or re-keying certificates and that complies with certain particular requirements specified in its CP or other service contracts.
Certificate Problem	The complaints regarding suspected cracking of

Report	keys, certificate misused, or other types of fraud, cracks, abuse, or inappropriate behaviors related to certificates.
Certificate Re-key	Changing the key pair used in a cryptographic system application. It is commonly achieved by issuing a new certificate that contains the new public key.
Certificate Renewal	The procedure of extending the validity of the data stated in the original certificate by issuing a new certificate.
Certificate Revocation	To prematurely terminate the operational period of a certificate prior to its expiry date.
Certificate Revocation List (CRL)	A regularly updated list of revoked certificates that is created and digitally signed by the CA that issued the certificates. The list contains the certificates that the issuing CA has issued that are revoked prior to their stated expiration date.
Certificate Transparency (CT)	CT is an open platform for the public monitoring and auditing of all certificates on the Internet (TLS/SSL certificate is the priority objective at the current stage). It provides related information of issued certificates to domain owners, CA, and domain subscribers to determine whether any certificate has been issued improperly. In other words, CT provides a public monitoring and information disclosure environment which can be used to monitor all issuance mechanisms of CAs that issue TLS/SSL certificates and to review any specific TLS/SSL certificate to lessen any risk that caused by mis-issued certificates. CT comprises certificate journals, certificate monitors and certificate auditors.
Chunghwa Telecom Certificate Policy Management Authority (PMA)	An organization which was established for electronic certificate management matters, such as (i) discussion and review of the CP and the electronic certificate framework of the PKI owned by CHT and (ii) review of interoperation requests submitted by subordinate CAs and cross-certified CAs and that of CPS.

Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes.
Confirming Person	A position within an Applicant's organization that confirms the particular fact at issue.
Contract Signer	Applicant, personnel employed by the applicant, an authorized representative who can make a declaration on behalf of the applicant or a natural person who can sign the purchase agreement on behalf of the applicant.
Cryptographic Module	A set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module.
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 the 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 contact (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record, or

	as obtained through direct contact with the Domain Name Registrar.
Domain Name	The label assigned to a node in the DNS, i.e., translates an IP address into a text name that is easily remembered.
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)	An Internet service that translates domain names into IP addresses.
Duration	A certificate field that contains two subfields, a start time "notBefore" and an end time "notAfter."
E-commerce	Provision of goods for sale and other services through the use of network technology (specifically the Internet).
End-Entity Certificate	A certificate in which the subject is not a CA.
Enterprise EV TLS/SSL Certificate	An EV TLS/SSL 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 TLS/SSL certificates at third and higher domain levels.
EV TLS/SSL Certificate	A certificate that contains subject information specified in the EV SSL Certificate Guidelines and that has been validated in accordance with the

	EV SSL Certificate Guidelines.
Extended Validation (EV)	Validation processes defined in the EV SSL Certificate Guidelines.
EV Authority	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 submit the EV TLS/SSL Certificate Request:
Federal Information Processing Standards (FIPS)	The standards developed by the U.S. federal government for use in computer systems by non-military government agencies and government contractors. The 140 series of FIPS are U.S. government computer security standards that specify requirements for cryptographic modules. As of December 2016, the current version of the standard is FIPS 140-2. FIPS 140 imposes requirements in eleven different areas and FIPS 140-2 defines four levels of security.
Firewall	Gateway that limits access between networks which complies with local security policy.
Fully Qualified Domain Name (FQDN)	An absolute domain name that specifies its exact location in the DNS hierarchy. A FQDN consists of two parts, a host name (service name) and a domain name. For example, a website with the hostname *ourserver* in the parent domain *ourdomain.com.tw* has the FQDN *ourserver.ourdomain.com.tw*, where *ourdomain* is the third-level domain, *.com* is the second-level domain and *.tw* is the country code top-level domain (ccTLD). In addition, a website with the hostname *www* in the parent domain *ourdomain.com* has the FQDN *www.ourdomain.com*, where *ourdomain* is the second-level domain and *.com* is the generic top-level domain (gTLD). A FQDN always starts with a host name.
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 a 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.
HiPKI	A hierarchical PKI established by CHT in compliance with ITU-T X.509 to promote electronic services.
HiPKI Root Certification Authority (HiPKI RCA)	The Root CA and top-level CA in HiPKI, and its public key is the trust anchor of HiPKI.
Identification	A statement of who the user is. [A Guide to Understanding Identification and Authentication in Trusted Systems] A way that can be used to describe or claim the identity of an individual or entity, e.g., user account, name or e-mail.
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	Confirmation of a particular fact received by the CA pursuant to the provisions of the Guidelines or

Applicant	binding upon the Applicant.
Integrity	Protection against unauthorized modification or destruction of information. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.
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)	An organization that oversees the allocation of global IP address, domain names and many other parameters used for Internet.
Internet Engineering Task Force (IETF)	An organization that develops and promotes Internet standards concerned with the evolution of the Internet architecture and the smooth operation of the Internet to make the Internet work better. Official website is at: https://www.ietf.org/.
Issuing CA	For a particular certificate, the issuing CA is 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 Compromise	A private key is said to be compromised if its value has been disclosed to an unauthorized person or an unauthorized person has had access

	to it.
Key Escrow	A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer, or other party, upon provisions set forth in the agreement.
Key Pair	Two mathematically related keys having the following properties: (1) One (public) key can be used to encrypt a message that can only be decrypted by using the other (private) key, and (2) It is computationally infeasible to determine one key from another.
Legal Entity	A Private Organization, Government Entity, Business Entity, or Non-Commercial Entity. [EV SSL Certificate Guidelines]
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.
National Institute of Standards and Technology (NIST)	Official website is at http://www.nist.gov/. Its mission is to promote U.S. innovation and industry competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. The hardware cryptographic module standards and certification, key security assessment and U.S. federal government civil servant and contractor identity card standards defined by NIST are widely referenced and employed.
Non-Repudiation	Technical evidence provided by the public key cryptosystem to support non-repudiation security

	service. Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. Technical non-repudiation refers to the guarantee that if a public key is used to validate a digital signature, that signature must be signed by the corresponding private key for a relying party.
Object Identifier (OID)	(1) A unique alphanumeric/numeric identifier registered under the International Standard Organization (ISO) registration standard, and which could be used to identify the uniquely corresponding CP; where the CP is modified, the OID is not changed accordingly. [Article 2-4, Regulations on Required Information for Certification Practice Statements] (2) A specialized formatted and unique identifier that is registered with an ISO and refers to a specific object or object class. For example, OIDs can be used to uniquely identify the CP and cryptographic algorithms of PKIs.
Online Certificate Status Protocol (OCSP)	An online certificate-checking protocol that enables relying party application software to determine the status of an identified certificate, e.g., revoked or valid.
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/SSL certificate status request extension, which may replace the OCSP to check X.509 certificate status. In practice, a website may obtain a "time limited (e.g. two hours)" OCSP response from the OCSP Responder and cache it. Next, this cached OCSP response will be sent to the subscriber (typically a browser) whenever initiating the TLS Handshake. The subscriber only needs to verify the validity of that OCSP response without sending the request of OCSP to the CA. In that way, the subscriber

	will not need to request the TLS/SSL certificate status from the CA when connecting to a high traffic TLS website, and thus to decrease the burden of the CA. This mechanism also prevents the privacy concern that the OCSP Responder knows which subscribers attempting to browsing that TLS website by having the TLS website referring the TLS/SSL certificate validity message issued regularly by the OCSP Responder to the CA.
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 TLS/SSL Certificates.
Private Key	(1) The key of a signature key pair that is used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.
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 of a signature key pair that is used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is publicly available and is normally made in the form of a digital certificate.
Public Key	A set of law, policy, rules, people, equipment, facilities, technology, processes, audits, and

Infrastructure (PKI)	services used for the purpose of administering certificates and public/private key pairs.
Public-Key Cryptography Standards (PKCS)	These are a group of public-key cryptography standards devised and published by RSA Security LLC. The company published the standards to promote the use of the cryptography techniques.
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, such as Ministry of Economic Affairs Bussiness & Factory Registration Database, the reporting of data is required by law, and false or misleading reporting is punishable with criminal or civil penalties. Nothing in the EV SSL Certificate Guidelines shall prohibit the use of third-party vendors to obtain the information from the Government Entity provided that the third party obtains the information directly from the Government Entity.
Qualified Government Tax Information Source (QTIS)	A qualified governmental information source that specifically contains tax information relating to private organizations, business entities, or individuals, such as Ministry of Finance in Taiwan (R.O.C.) or 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 Agency	A Governmental Agency that registers business information in connection with an entity's business 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; or (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)	An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates. An RA is not a CA but can be part of CAs.
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. HiPKI EV TLS 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.
Relying Party	A recipient of a certificate who acts in reliance on that certificate. [Article 2-6, Regulations on Required Information for Certification Practice Statements]
Repository	(1) A system for storing and retrieving certificates or other information relevant to certificates. [Article 2-7, Regulations on Required Information for Certification Practice Statements] (2) A database that contains information and data relating to certificates as specified in the CP/CPS.
Request Token	A value derived in a method specified by the CA which binds this demonstration of control to the certificate request. The Request Token shall incorporate the key used in the certificate request. A Request Token may include a time-stamp to indicate when it was created. A Request Token may include other information to ensure its uniqueness. A Request Token that includes a time-stamp shall remain valid for no more than 30 days from the time of creation. A Request Token that includes a time-stamp shall be treated as invalid if its time-stamp is in the future. A Request Token that does not include a time-

	stamp 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.
Request for Comments (RFC)	A series of memos issued by IETF that include standards, protocols and procedures with reference to Internet, UNIX, and Internet community and are scheduled by numbers.
Reserved IP Addresses	An IPv4 or IPv6 address that the IANA has marked as reserved: http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml
Secure Sockets Layer (SSL)	Protocol issued by Netscape through promotion of their web browser which can encrypt network communication in the transport layer, ensure the integrity of transmitted information, and perform identity authentication on the server and client. The SSL protocol is independent of the application layer protocol, such that high level application layer protocols, e.g., HTTP, FTP and Telnet, may be established based on SSL. The SSL protocol completes encryption by algorithm, secret key agreement for a communication and server certification prior to the communication with the application layer protocol. This protocol is a predecessor of the Transport Layer Security (TLS) protocol.
Signing Authority	One or more certificate approvers who has been assigned as representative by the Applicant.
Subordinate CA	In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA.
Subscriber	An entity that (1) is the subject named or identified in a certificate issued to that entity,

	(2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual, an organization, an application or network device.
Threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. The threat may be internal or external. An internal threat refers to the aforementioned circumstance or event was caused by an entity with authorized access; an external threat refers to the aforementioned circumstance or event was caused by an unauthorized entity from outside the domain perimeter.
Time-stamp	A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.
Transport Layer Security (TLS)	TLS 1.0 was first defined in RFC 2246 by the IETF based on the SSL 3.0 and updated in RFC 5246 and RFC 6176 as TLS 1.2. The current version is TLS 1.3 defined in RFC 8446 by the IETF in 2018.
Trust List	List of trusted certificates used by relying parties to authenticate other certificates.
Trusted Certificate	A certificate that is trusted by the relying party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a “trust anchor.”
Uninterrupted Power System (UPS)	Provide emergency power to a load in the event of abnormal power conditions (such as power outage, noise or sustained overvoltage) to allow continual operation of critical equipment or precision instruments (e.g., servers or switches) and to prevent loss of calculation data, interruption of communication network 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. [RFC 3647]
Verified Accountant Letter	A document that complies with Section 11.11.2 of the EV SSL Certificate Guidelines.
Verified Legal Opinion	A document that complies with Section 11.11.1 of the EV SSL Certificate Guidelines.
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.
WebTrust	The current version of CPA Canada's WebTrust Program(s) for Certification Authorities.
WHOIS	Information retrieved directly from the domain name registrar or registry operator via the protocol defined in RFC 3912, the registry data access protocol defined in RFC 7482, or an HTTPS website.
Zeroize	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. [FIPS 140-2]

1.6.2. Acronyms

Acronyms	Full Name	Definition
AIA	Authority Information Access	See Section 1.6.1
CA	Certification Authority	See Section 1.6.1
CAA	Certification Authority Authorization	See Section 1.6.1
CEO	Chief Executive Officer	
CFO	Chief Executive Officer	
CIO	Chief Information Officer	

CISO	Chief Information Security Officer	
CMMI	Capability Maturity Model Integration	See Section 1.6.1
COO	Chief Operating Officer	
CP	Certificate Policy	See Section 1.6.1
CPS	Certification Practice Statement	See Section 1.6.1
CRL	Certificate Revocation List	See Section 1.6.1
CT	Certificate Transparency	See Section 1.6.1
DN	Distinguished Name	
DNS	Domain Name System,	See Section 1.6.1
EE	End Entities	
EV	Extended Validation	See Section 1.6.1
FIPS	(U.S. Government) Federal Information Processing Standard	See Section 1.6.1
FQDN	Fully Qualified Domain Name	See Section 1.6.1
HiPKI RCA	HiPKI Root Certification Authority	See Section 1.6.1
IANA	Internet Assigned Numbers Authority	See Section 1.6.1
IETF	Internet Engineering Task Force	See Section 1.6.1
NIST	(U.S. Government) National Institute of Standards and Technology	See Section 1.6.1
OCSP	Online Certificate Status Protocol	
OID	Object Identifier	See Section 1.6.1
PIN	Personal Identification Number	
PKCS	Public Key Cryptography Standards	See Section 1.6.1
PKI	Public Key Infrastructure	See Section 1.6.1
QGIS	Qualified Government Information Source	See Section 1.6.1
QIIS	Qualified Independent Information Source	See Section 1.6.1
QTIS	Qualified Government Tax Information Source	See Section 1.6.1

RA	Registration Authority	See Section 1.6.1
RFC	Request for Comments	See Section 1.6.1
SSL	Secure Sockets Layer	See Section 1.6.1
TLS	Transport Layer Security	See Section 1.6.1
UPS	Uninterrupted Power System	See Section 1.6.1
UTC	Coordinated Universal Time	

2. Publication and Repository Responsibilities

2.1. Repositories

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

2.2. Publication of Certification Information

HiPKI EV TLS CA shall take responsibility for making the following information publicly accessible in its repository:

(1) The HiPKI CP and this CPS,

(2) Certificate revocation information,

(3) HiPKI EV TLS CA certificates (until the expiry of all certificates issued with private key corresponding to that certificate's public key),

(4) Issued certificates,

(5) Privacy protection policy,

(6) Related latest news regarding HiPKI EV TLS CA,

(7) Subscriber agreement,

(8) The last result of the external audit (as specified in Section 8.6),

(9) The URLs of the test websites which install EV TLS/SSL certificates (including valid, expired, and revoked ones) issued by HiPKI EV TLS CA for application software suppliers, and

(10) CAA (Certification Authority Authorization) Issuer Domain Names (as specified in Section 4.2.1), including pki.hinet.net and tls.hinet.net.

2.3. Time or Frequency of Publication

(1) This CPS is reviewed and updated annually. New or modified version

of this CPS is published in the repository within seven calendar days upon receiving the approval letter from the competent authority;

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

(3) HiPKI EV TLS CA issues CRLs at least twice a day and publishes CRLs in the repository; and

(4) HiPKI EV TLS CA certificates issued by HiPKI RCA are published in the repository within seven calendar days upon issuance and receipt of the certificates.

2.4. Access Controls on Repositories

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

The information published by HiPKI EV TLS CA 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

HiPKI EV TLS CA 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 HiPKI EV TLS CA 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 TLS/SSL certificate shall follow the Baseline Requirements and may not use internal names or reserved IP addresses. EV TLS/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 TLS/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 TLS/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 address (localityName)	2.5.4.7	●	
Street address of the actual business premises address (streetAddress)	2.5.4.9		●

Certificate Field Attribute Name	Object Identifier (OID)	Required Attribute	Optional Attribute
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 of the EV SSL Certificate Guidelines, the EV TLS/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 the method in Section 3.2.2 of this CPS.

HiPKI EV TLS CA and its 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 regulations in 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, HiPKI EV TLS CA shall not issue any EV TLS/SSL certificate.

(2) Business Category (businessCategory)

According to Section 9.2.4 of the EV SSL Certificate Guidelines, the EV TLS/SSL certificate field subject must include the 'business category' attribute to differentiate the business category of the EV TLS/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 of the EV SSL Certificate Guidelines, the EV TLS/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 TLS/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 TLS/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 TLS/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 TLS/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 TLS/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 of the EV SSL Certificate Guidelines, the EV TLS/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) City or Town Name (localityName) of the Actual Business Premises Address

According to Section 9.2.7 of the EV SSL Certificate Guidelines, the EV TLS/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 TLS/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 TLS/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) State or Province Name (stateOrProvinceName) of the Actual Business Premises Address

According to Section 9.2.7 of the EV SSL Certificate Guidelines, the EV TLS/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.

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

According to Section 9.2.7 of the EV SSL Certificate Guidelines, it can be determined independently whether the EV TLS/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.

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

According to Section 9.2.7 of the EV SSL Certificate Guidelines, it

can be determined independently whether the EV TLS/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 of the EV SSL Certificate Guidelines, it is not recommended to use the commonName attribute in the EV TLS/SSL certificate field 'subject' but there are no regulations which clearly prohibit its use. For EV TLS/SSL certificates issued by HiPKI EV TLS CA, a commonName attribute is provided in the EV TLS/SSL certificate field 'subject'. The FQDNs 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 TLS/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 of the EV SSL Certificate Guidelines, except for the required, optional and deprecated attributes, other optional attributes may be provided for the EV TLS/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 TLS/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 TLS/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.

The certificate subject alternative name field of the multi-domain EV TLS/SSL certificate shall record multiple FQDN owned or controlled by the subscriber.

3.1.3. Anonymity or Psuedonymity of Subscribers

HiPKI EV TLS CA does not currently issue anonymous certificates to end-entity subscribers. As a principle, the pseudonymous certificates are not issued either. For the EV TLS/SSL certificates issued by HiPKI EV TLS CA, the ownership of the domain name and the organization are manually reviewed by the RAOs. The EV TLS/SSL certificates belong to Internationalized Domain Names (IDNs), the decrypted FQDN will be deemed EV TLS/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

HiPKI EV TLS CA's X.500 distinguished name for its CA certificates is:

C = TW,

O = Chunghwa Telecom Co., Ltd.,

CN = HiPKI EV TLS CA – Gn, where, n=1, 2, 3…

HiPKI EV TLS CA 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 HiPKI EV TLS CA for name of the subscriber certificate subject name. The HiPKI EV TLS CA 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
- jurisdictionCountryName
- jurisdictionStateOrProvinceName
- jurisdictionLocalityName
- streetAddress
- postalCode
- commonName (abbreviated as CN)
- serialNumber

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 HiPKI EV TLS CA 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 HiPKI EV TLS CA may revoke that subscriber's certificate (see Section 4.9.1).

3.1.6. Recognition, Authentication, and Role of Trademarks

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

3.2. Initial Identity Validation

HiPKI EV TLS CA and its 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 HiPKI CP and EV SSL Certificate Guidelines are deemed to be the minimum verification standard requirements. In all cases, HiPKI EV TLS CA and its RA are responsible for adopting extra verification steps to satisfy verification requirements.

3.2.1. Method to Prove Possession of Private Key

HiPKI EV TLS CA 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 EV TLS/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 TLS/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 TLS/SSL Certificate (As Sections 3.2.3 and 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 TLS/SSL Certificate Request.

3.2.2.2. Verification of Applicant's Legal Existence and Identity

3.2.2.2.1. **Verification Requirements**

The RA validates four kinds of organizations regarding Applicants' Legal Existence and identity as follows:

(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 TLS/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

RA 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 then checks the authenticity of the application information and identity. As an alternative, the certificate application information can also be provided to the RA Counter by signing and sending a digital signature signed with the private key corresponding to a GPKI issued assurance level 3 organization certificate. In that case, providing the copies of the aforementioned certified documents is not necessary.

If a private organization completes the incorporation registration procedure from the competent supervisory authority according to the related law or throuth the identification or authentication procedure conducted by HiPKI EV TLS CA, RA or a notary, attorney, accountant or company personnel trusted by HiPKI EV TLS CA; and remains registration or identification and authentication supporting information such as a seal/stamp or a certified stamp stamped by the notary, attorney, accountant or company personnel. HiPKI EV TLS CA or its 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 Agencies

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 TLS/SSL Certificate Request.

C. Registration Number:

Our country's government agencies (organizations) may 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 submitted by a government agency (organization) by official document and authenticate the verification documents. The government agency may also use a digital signature signed with the private key corresponding to a GPKI issued assurance level 3 organization certificate to apply to the RA for the certificate. In that case, providing the copies of the aforementioned certified documents is not necessary.

(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 TLS/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 TLS/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 TLS/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. Business Enitity may also use a digital signature signed with the private key corresponding to a

GPKI issued assurance level 3 organization certificate to apply to the RA for the certificate. In that case, providing the copies of the aforementioned certified documents is not necessary.

If another business group completes the incorporation registration procedure from the competent supervisory authority according to the related law or throuth the identification or authentication procedure conducted by HiPKI EV TLS CA, RA or a notary, attorney, accountant or company personnel trusted by HiPKI EV TLS CA; and remains registration or identification and authentication supporting information such as a seal/stamp or a certified stamp stamped by the notary, attorney, accountant or company personnel. HiPKI EV TLS CA or its 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. **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 (QGIS) 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 QGIS, Incorporating or Registration Agency, or from a Qualified Independent Information Source (QIIS).

(2) Government Entity Subject:

Legal Existence, Organization Name, Registration Number must either be verified directly with, or obtained directly from, one of the following: (i) a QGIS in the political subdivision in which such Government Entity operates; (ii) 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), (iii) a judge that is an active member of the federal, state or local judiciary within that political subdivision, or (iv) 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 QIIS.

(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 QGIS 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 QGIS, QTIS, registration agency or QIIS.

In addition, HiPKI EV TLS CA or its RA must validate the principal individual associated with the other business group pursuant to the requirements in subsection (4) below.

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

HiPKI EV TLS CA and its RA may rely upon a face-to-face validation of the Principal Individual performed by the Registration Agency, provided that HiPKI EV TLS CA and its RA has evaluated the validation procedure and concluded that it satisfies the requirements of the EV SSL Certificate 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 EV SSL Certificate 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 HiPKI EV TLS 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

(v) 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. HiPKI EV TLS CA and its 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 HiPKI EV TLS 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 TLS/SSL Certificate is an organ or agency – including a non-governmental organization of a verified International Organization, then the RA 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 TLS/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:

(1) 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

(2) that such filing continues to be valid.

3.2.2.3.2. 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 QGIS 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 QIIS 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 RA 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 QGIS 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 TLS/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 TLS/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 TLS/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 TLS/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 TLS/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 TLS/SSL Certificates may include Domain Names containing mixed character sets only in compliance with the rules set forth by the domain registrar. HiPKI EV TLS CA and its RA must visually compare any Domain Names with mixed character sets with known high-risk domains. If a similarity is found, then the EV TLS/SSL Certificate Request must be flagged as High Risk. HiPKI EV TLS CA and its 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.

3.2.3. Authentication of Individual Identity

EV TLS/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.

(3) 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 TLS/SSL Certificate Request:

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

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

C. Approve EV TLS/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 HiPKI EV TLS 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) HiPKI EV TLS CA and its 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 HiPKI EV TLS CA and Applicant: The EV Authority of the Certificate Approver may be verified by reliance on a contract between HiPKI EV TLS 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 HiPKI EV TLS CA or its 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 TLS/SSL Certificate application. The RA must record sufficient details of the previous agreement to correctly identify it and associate it with the EV TLS/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 HiPKI EV TLS 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 HiPKI EV TLS 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. The Applicant authorizes the Contract Signer to sign the Subscriber Agreement on the applicant's behalf,

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

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

D. Serious consequences attach to the misuse of an EV TLS/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 website.

3.2.3.1.4. Pre-Authorized Certificate Approver

Where HiPKI EV TLS CA and the Applicant contemplate the submission of multiple future EV Certificate Requests, then, after HiPKI EV TLS CA (or RA):

(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.

HiPKI EV TLS CA (or 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 TLS/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 TLS/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 HiPKI EV TLS 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 TLS/SSL Verification of Signature on Subscriber Agreement and EV Certificate Requests

Both the Subscriber Agreement and each non-pre-authorized EV TLS/SSL Certificate Request must be signed. The Subscriber Agreement must be signed by an authorized Contract Signer. The EV TLS/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 TLS/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 TLS/SSL Certificate Request), or a legally valid and enforceable electronic signature (such as digital signatures signed with the private key corresponding to a GPKI issued 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 TLS/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 TLS/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 TLS/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 the 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 signed with the private key corresponding to a GPKI issued assurance level 3 certificate); or

(4) Notarization by a notary, provided that HiPKI EV TLS 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 TLS/SSL Certificate Request is submitted by a Certificate Requester, before HiPKI EV TLS CA issues the requested EV TLS/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 TLS/SSL Certificate Request include:

(1) 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 TLS/SSL Certificate Request;

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

(3) Verifying the signature of the Certificate Approver on the EV TLS/SSL Certificate Request in accordance with Section 3.2.3.2.

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: HiPKI EV TLS 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.

C. 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.

D. 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: HiPKI EV TLS 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:

- 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;
- Received by the RA in a manner that authenticates and verifies the source of the confirmation; and
- 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 the 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:

(i) The address of the Applicant's Place of Business as verified by the RA in accordance with the EV SSL Certificate Guidelines, or

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

(iii) 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 the EV SSL Certificate 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: HiPKI EV TLS 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 HiPKI EV TLS CA by telephone, by email, or by paper mail, so long as HiPKI EV TLS CA can reliably verify that it was provided by a Confirming Person in response to the Confirmation Request.

(3) HiPKI EV TLS CA MAY rely on a verified Confirming Person to confirm their own contact information: email address, telephone number, and facsimile number. HiPKI EV TLS 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 HiPKI EV TLS 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

QIISs are frequently updated and the databases accessible to the public are generally deemed 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.

HiPKI EV TLS CA and its 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.

HiPKI EV TLS CA and its RA shall not use QIIS that is (i) self-

published and (ii) the information is not verified to be accurate by an independent source. If HiPKI EV TLS CA and CHT or CHT's affiliates has a database holding company or if any RA or HiPKI EV TLS CA has outsourced any portion of the verification process to a subcontractor (or its owner or affiliated company) to maintain the ownership or substantial interest of any database, then it is not deemed to be a QIIS.

3.2.3.4.6. Qualified Government Information Source

QGISs 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 Bussiness & Factory Registration Database. 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 QTIS 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, and Internal Revenue Service (IRS) qualified tax information sources).

3.2.4. Non-verified Subscriber Information

Not applicable.

3.2.5. Validation of Authority

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

(1) Confirming the organization legal existence through third-party identity verification service or database, documents issued by government or authorized organizations, an attestation letter written by a government official, lawyer, or accountant, or a site visit by the HiPKI EV TLS CA or a third party who is acting as an agent for the HiPKI EV TLS CA;

(2) Using telephone, postal letter, e-mail not provided by the representative or any equivalent way to confirm that the individual affiliated with the certificate subject (organization or company) and is authorized to represent the certificate subject;

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

(4) Verification of the applicant's EV TLS/SSL certificate authorization which is detailed in Section 3.2.3, including:

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 TLS/certificate request.

The EV TLS/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 validate the subscriber's right to use or control the domain name. In addition, organization or individual's identity authentication must still be done in accordance with Sections 3.2.2 or 3.2.3 for assurance level 3 of this CPS.

3.2.5.1. Validating the Applicant as a Domain Contact

Confirming the Applicant's control over the FQDN by validating the Applicant is the Domain Contact. This method may only be used if HiPKI EV TLS CA or RA is also the Domain Name Registrar, or an Affiliate of the

Registrar, of the Base Domain Name. For example, Data Communications Business Group, Chunghwa Telecom Co., Ltd. is the Domain Name Registrar of .tw, and is responsible for the operation of HiPKI EV TLS CA.

Once the FQDN has been validated using this method, HiPKI EV TLS CA MAY also issue SSL Certificates for other FQDNs that end with all the labels of the validated FQDN. This method of validation confirms to Section 3.2.2.4.12 of the Baseline Requirements.

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

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

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

HiPKI EV TLS 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.

HiPKI EV TLS 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.

Once the FQDN has been validated using this method, HiPKI EV TLS CA MAY also issue EV TLS/SSL Certificates for other FQDNs that end with all the labels of the validated FQDN. This method of validation confirms to Section 3.2.2.4.2 of the Baseline Requirements.

3.2.5.3. Constructed Email to Domain Contact

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

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

The Random Value SHALL be unique in each email.

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

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

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

3.2.5.4. Agreed-Upon Change to Website

Confirming the applicant's control over the 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 HiPKI EV TLS 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, HiPKI EV TLS 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 Section 3.5 of this CPS).

Once the FQDN has been validated using this method, HiPKI EV TLS CA MAY also issue EV TLS/SSL Certificates for other FQDNs that end with all the labels of the validated FQDN. This method of validation confirms to Section 3.2.2.4.6 of the Baseline Requirements.

3.2.5.5. DNS Change

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

If a Random Value is used, HiPKI EV TLS 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 Section 3.5 of this CPS).

Once the FQDN has been validated using this method, HiPKI EV TLS CA MAY also issue EV TLS/SSL Certificates for other FQDNs that end with all the labels of the validated FQDN. This method of validation confirms to Section 3.2.2.4.7 of the Baseline Requirements.

3.2.5.6. Email to DNS CAA Contact

Confirming the Applicant's control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to a DNS CAA Email Contact. The relevant CAA Resource Record Set MUST be found using the search algorithm defined in RFC 6844 Section 4, as amended by Errata 5065 (Appendix A).

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

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

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

3.2.5.7. Email to DNS TXT Contact

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

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

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

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

3.2.6. Criteria for Interoperation

HiPKI EV TLS CA is not a Root CA. Not appliable.

3.2.7. Data Source Accuracy

Prior to using any data source as a Reliable Data Source, HiPKI EV TLS CA shall evaluate the source for its reliability, accuracy, and resistance to alteration or falsification. HiPKI EV TLS 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 HiPKI EV TLS 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 the Baseline Requirements.

3.2.8. Other Verification Requirements

3.2.8.1. High Risk Status

The requirements of Section 4.2.1 of the Baseline Requirements apply equally to EV TLS/SSL Certificates. Please refer to Section 4.2.1 of this CPS for the Identification and authentication of high risk certificate request.

3.2.8.2. Denied Lists and Other Legal Black Lists

(1) Verification Requirements: HiPKI EV TLS CA and its RA 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 HiPKI EV TLS 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 HiPKI EV TLS CA's jurisdiction prohibit doing business. HiPKI EV TLS CA must not issue any EV TLS/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: HiPKI EV TLS CA MUST take reasonable steps to verify with the lists and regulations in the EV SSL Certificate Guidelines.

3.2.8.3. 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: HiPKI EV TLS CA or a RA may verify the relationship between an Applicant and a Parent, Subsidiary, or Affiliate by relying on a contract between

HiPKI EV TLS CA, the 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;

(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; 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.

3.2.8.4. Final Cross-Correlation and Due Diligence

Except for Enterprise EV TLS/SSL Certificates:

(1) The results of the verification processes and procedures outlined in the EV SSL Certificate Guidelines are intended to be viewed both individually and as a group. Thus, after all of the verification processes and procedures are completed, HiPKI EV TLS 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 TLS/SSL certificate application and look for discrepancies or other details requiring further explanation.

(2) HiPKI EV TLS CA must obtain and document further explanation or clarification from the Applicant, certificate approver, certificate requester, QIISs, and/or other sources of information, as necessary, to resolve those discrepancies or details that require further

explanation.

(3) HiPKI EV TLS CA must refrain from issuing an EV TLS/SSL certificate until the entire corpus of information and documentation assembled in support of the EV TLS/SSL certificate request is such that issuance of the EV TLS/SSL certificate will not communicate factual information that HiPKI EV TLS 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, HiPKI EV TLS CA must decline the EV TLS/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 HiPKI EV TLS CA's normal operating language, HiPKI EV TLS 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 the EV SSL Certificate Guidelines. When employees under the control of HiPKI EV TLS CA do not possess the language skills necessary to perform the Final Cross-Correlation and Due Diligence, HiPKI EV TLS 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 HiPKI EV TLS CA has utilized the services of an RA, HiPKI EV TLS 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 TLS/SSL Certificate, HiPKI EV TLS CA must review the work completed by the RA and determine that all requirements have been met; or

(C)When HiPKI EV TLS CA has utilized the services of an RA, HiPKI EV TLS 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 TLS/SSL Certificates to be issued in compliance with the requirements of Section 14.2 of the EV SSL Certificate Guidelines, the Enterprise RA may perform the requirements of this Final Cross-Correlation and Due Diligence section.

3.3. Identification and Authentication for Re-key Requests

If the subscriber's private key needs to be renewed upon expiry of the certificate usage period, certificate rekey work may be performed and the subscriber may re-apply for 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 TLS/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.

HiPKI EV TLS CA does not accept subscriber EV TLS/SSL certificate renewal requests.

3.3.2. Identification and Authentication for Re-key after Revocation

If the subscriber's private key needs to be re-keyed due to certificate revocation, the Subscriber shall re-apply for the certificate with HiPKI EV

TLS CA. The RA will identify and authenticate the Subscriber who re-apply for the certificate in accordance with the regulations in Sections 3.2, 3.3 and 3.4.

3.4. Identification and Authentication for Revocation Request

HiPKI EV TLS CA or its RA must perform authentication of the certificate revocation application to verify that the Applicant has the right to submit the certificate revocation. The authentication procedure for certificate revocation applications is the same as the regulations in Sections 3.2 and 3.3.

3.5. Requirements for Re-use of Existing Documentation

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

3.5.1. Validation for Existing Subscribers

If an Applicant has a currently valid EV TLS/SSL Certificate issued by HiPKI EV TLS CA, HiPKI EV TLS 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 HiPKI EV TLS CA or RA in connection with the Applicant's previously issued and currently valid EV TLS/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 HiPKI EV TLS CA and the RA verifies that the WHOIS record still shows the same Domain Name Registrant as when HiPKI EV TLS CA and the RA verified the specified Domain Name for the initial EV TLS/SSL Certificate.

3.5.2. Re-issuance Requests

HiPKI EV TLS 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 TLS/SSL Certificate that is being replaced, and

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

3.5.3. Age of Validated Data

(1) Except for reissuance of an EV TLS/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 TLS/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 HiPKI EV TLS 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 HiPKI EV TLS CA.

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

(4) HiPKI EV TLS CA MUST repeat the verification process required in this CPS and the 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 Life-cycle Operational Requirements

4.1. Certificate Application

4.1.1. Who Can Submit a Certificate Application

Computer and communications equipment (such as routers, firewalls, database 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 TLS/SSL certificates.

The issuance of EV TLS/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 TLS/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

HiPKI EV TLS CA and its RA are responsible for ensuring that the identity of the Applicant is verified in compliance with the HiPKI CP and this CPS before certificate issuance. The Applicant is responsible for providing enough and accurate information (such as filling out the organization legal name or Registration Number, certificate requester's name or website FQDN based on the type of the certificate applied for) and identification documents

are given to the RA. HiPKI EV TLS CA 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 HiPKI EV TLS CA approves the certificate application and issues the certificate.

(3) After obtaining the certificate issued by HiPKI EV TLS CA, 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 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 HiPKI EV TLS CA is unable to operate normally for some reason, the subscriber shall speedily seek other ways for completion of legal acts and may not be used as a defense to others.

4.2. Certificate Application Processing

The certificate application procedures are as follows:

(1) The certificate Applicant fills out the certificate request information

and agrees to the Subscriber Agreements.

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

(3) The certificate Applicant 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

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

HiPKI EV TLS CA and its RA shall perform pre-certificate approval verification and extra checks on high risk certificate requests. That is, in addition to the procedures described in Sections 3.1.2.1 and 3.2.2.7, the RA system SHALL maintain an internal database of all previously revoked certificates and previously rejected certificate requests due to suspected phishing or other fraudulent usage or concerns and use this information to identify subsequent suspicious certificate requests prior to issuing a certificate. For 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 TLS/SSL certificates, above black lists are collected by HiPKI EV TLS CA and its RA in the RA system to alert RAOs. RAOs 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 TLS/SSL certificates.

4.2.1.1. Authorize the CA Issuing Certificate Record

Before issuing EV TLS/SSL certificates, the EV TLS/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 RAOs will access to DNS to check the Certification Authority Authorization (CAA) DNS Resource Record based on RFC 6844 as amended by Errata 5065, and the certificates are only issued after passing the check. That is, if a FQDN's "issue" tag contains "pki.hinet.net" or "tls.hinet.net", HiPKI EV TLS CA will issue the EV TLS/SSL certificate of that FQDN. In case of the property tag "iodef" is present in the CAA records, RAOs will determine whether to issue EV TLS/SSL certificate after communicating with the Applicant.

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

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

4.2.2. Approval or Rejection of Certificate Applications

The RA shall assign another RAO who is different from the RAO 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 TLS/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. When the procedure of Final Cross-Correlation and Due Diligence described in Section 3.2.8.4 is performed under the related regulations, HiPKI EV TLS CA and its RA may approve the certificate application. The system used for processing and approving EV TLS/SSL certificate request shall be handled by at least two personnel in trusted roles.

If the various identity authentication tasks cannot be successfully completed, HiPKI EV TLS CA and its RA may refuse the certificate request. Except for identity identification and authentication reason, HiPKI EV TLS CA and its RA may also refuse to issue the certificate for other reasons. HiPKI EV TLS CA and its RA may refuse the certificate application from Applicants who have previously been rejected or have previously violated 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 TLS/SSL certificates issued outwards by its PKI have ever recorded the internal names. CAs that have issued certificates including such kind of domain names shall subscribe ICANN gTLD Notification.

HiPKI EV TLS CA will not issue EV TLS/SSL certificates to domain names that have been marked as new gTLDs which may be issued by ICANN. If ICANN has announced that it considers issuing a new gTLD, and HiPKI EV TLS CA discovers some Applicants wishes to apply an EV TLS/SSL certificate including an Internal Name using the new gTLD to be analyzed, HiPKI EV TLS CA shall warn the Applicants. Unless the subscriber also registers its domain name, or the EV TLS/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, HiPKI EV TLS CA will check against the effective certificate to see if that

gTLD is included. The issuance of EV TLS/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

HiPKI EV TLS CA and its RA shall complete the EV TLS/SSL certificate application within a reasonable period of time. Provided that the information submitted by the Applicant is complete and complies with the HiPKI CP, this 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 that for HiPKI EV TLS CA to issue the certificates depends on the certificate classification and may be disclosed in the Subscriber Agreements, contract or HiPKI EV TLS CA website.

The review procedure for the applications of EV TLS/SSL certificates which are received and meet relevant regulations shall be completed within 5 working days by at least two RAOs and the subscriber shall be asked to accept the certificate. After the certificate is accepted, HiPKI EV TLS CA shall complete the certificate issuance within one working day or the date specified by the Subscriber on which the certificate is to be obtained by the Subscriber.

4.3. Certificate Issuance

4.3.1. CA Actions during Certificate Issuance

Upon HiPKI EV TLS CA and its RA receive the certificate application, the relevant review procedures are enforced in accordance with Chapter 3 of this CPS to serve as a basis for determining whether approve the certificate issuance.

Certificate issuance steps are as follows:

(1) The RA submits the certificate application passed the review procedures to HiPKI EV TLS CA,

(2) When HiPKI EV TLS CA receives the certificate application submitted by the RA, the authorization status of the RA is first checked, the authorized assurance level and scope is verified and then the certificate is issued according to the information of the certificate application submitted by the RA,

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

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

(5) HiPKI EV TLS CA reserves the right to refuse certificate issuance to any entity. HiPKI EV TLS CA shall not bear any liability for damages to the Applicants who is refused to issue the certificate.

4.3.2. Notification to Subscriber by the CA of Issuance of Certificate

After HiPKI EV TLS CA completes certificate issuance, the subscriber is notified to draw the certificate or notify the Subscriber to draw the certificate through the RA.

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

If the information in the certificate is found to be incorrect or is inconsistent with the information provided at the time of application when the Subscriber accepts the certificate, the RA should be notified immediately. Otherwise, it shall be deemed that the subscriber consents to abide by the rights and obligations in the CPS and related contracts.

4.4. Certificate Acceptance

The certificate acceptance procedure for EV TLS/SSL certificates issued by HiPKI EV TLS CA 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 certificate to be issued and refuses to accept 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 TLS/SSL certificate's certificate subject alternative name field, the to be signed multi-domain EV TLS/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 the Applicant's consent to comply with the rights and obligations in this CPS, Subscriber Agreements or related contracts.

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

4.4.1. Conduct Constituting Certificate Acceptance

The certificate applicant prereviews the content of a subscriber certificate to be issued. The certificate is published by HiPKI EV TLS CA in the repository or is delivered to the certificate applicant.

4.4.2. Publication of the Certificate by the CA

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

4.4.3. Notification of Certificate Issuance by the CA to Other Entities

HiPKI EV TLS CA 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 HiPKI EV TLS CA repository.

4.5. Key Pair and Certificate Usage

4.5.1. Subscriber Private Key and Certificate Usage

Subscribers refer to the entities that request and obtain EV TLS/SSL certificates approved by HiPKI EV TLS CA. Their relationship with the certificate subject is shown in the table in Section 1.3.3 of this CPS. Usage of EV TLS/SSL certificates is stipulated in Section 1.4.1 of this CPS. Key pairs of subscribers shall be generated in compliance with Section 6.1.1 of this CPS. Subscribers must be able to control the private keys and do not issue certificates to others. Subscribers shall protect the private key from unauthorized use or disclosure by third parties and shall use their private keys only for the correct key usage (i.e., the policy for key usage specified in the extension of the certificates), such as digitalSignature or keyEncipherment. Subscribers shall correctly use their certificates adhering to the certificate policies listed in the certificates.

4.5.2. Relying Party Public Key and Certificate Usage

Relying parties refer to third parties who trust the binding between the certificate subject name and public key. Relying parties shall use software that is compliant with ITU-T X.509, IETF RFCs or EV SSL Certificate Guidelines to verify the validity of the certificate used. 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, and

(3) Establish secure communication channels with the subscriber.

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

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 the reverification time of EV TLS/SSL certificate request information accuracy is also the shortest (as specified in Section 3.5.1) between various SSL certificates as the requirements of CA/Browser Forum. HiPKI EV TLS CA does not provide certificate renewal service. Key pair generation and certificate request submission is done in the same manner as the initial registration.

4.6.1. Circumstance for Certificate Renewal

Not applicable.

4.6.2. Who May Request Renewal

Not applicable.

4.6.3. Processing Certificate Renewal Requests

Not applicable.

4.6.4. Notification of New Certificate Issuance to Subscriber

Not applicable.

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

Not applicable.

4.6.6. Publication of the Renewal Certificate by the CA

Not applicable.

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

Not applicable.

4.7. Certificate Re-key

4.7.1. Circumstance for Certificate Re-key

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

If the subscriber's EV TLS/SSL certificate has not been revoked, HiPKI EV TLS CA or its RA can start to process the re-key and new certificate application 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's EV TLS/SSL certificate is revoked, use of its private key shall be suspended. After the key pair is re-keyed, a new certificate

may be requested from HiPKI EV TLS CA in accordance with Sections 4.1 and 4.2.

4.7.2. Who May Request Certification of a New Public Key

A subscriber or legally authorized third party (e.g., a representative authorized by the organization).

4.7.3. Processing Certificate Re-keying Requests

For subscriber certificate re-keying, subscribers shall submit a new certificate application to HiPKI EV TLS CA. The related procedures must be implemented in accordance with Sections 3.1, 3.2, 3.3, 4.1 and 4.2.

4.7.4. Notification of New Certificate Issuance to Subscriber

As stated in Section 4.3.2.

4.7.5. Conduct Constituting Acceptance of a Re-keyed Certificate

As stated in Section 4.4.1.

4.7.6. Publication of the Re-keyed Certificate by the CA

As stated in Section 4.4.2.

4.7.7. Notification of Certificate Issuance by the CA to Other Entities

RA may receive notification of re-keyed certificate issuance.

4.8. Certificate Modification

4.8.1. Circumstance for Certificate Modification

Certificate modification means creating a new certificate for the same subject, where authenticated information that slightly differs from the old certificate (e.g., changes to DN or FQDNs). The new certificate has a new certificate serial number but with the same subject public key and ‘NotAfter’

date. If there is any change to the organization name or FQDN, the subscriber must submit a new certificate application with the modified organization name or FQDN to obtain a new certificate in accordance with the procedures in Sections 4.1 and 4.2. The old certificate shall be revoked after modification is complete.

4.8.2. Who May Request Certificate Modification

Certificate applicants include Subscribers or legally authorized third parties (such as agents authorized by the organization).

4.8.3. Processing Certificate Modification Requests

(1) The Applicant shall submit the certificate modification request in accordance with the operation procedures 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's name and 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. The RA can establish the operation procedures referring to Sections 4.1, 4.2 and 4.9. For example, if the 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 HiPKI EV TLS CA.

(3) When HiPKI EV TLS CA receives the new certificate application and the original certificate revocation request information, HiPKI EV TLS CA 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, HiPKI EV TLS CA 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 HiPKI EV TLS CA to understand the source of the problem.

(5) In order to ensure the security, integrity and non-reputability of the information transmitted by HiPKI EV TLS CA and its 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

As stated in Section 4.3.2.

4.8.5. Conduct Constituting Acceptance of Modified Certificate

As stated in Section 4.4.1.

4.8.6. Publication of the Modified Certificate by the CA

As stated in Section 4.4.2.

4.8.7. Notification of Certificate Issuance by the CA to Other Entities

HiPKI EV TLS CA 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 HiPKI EV TLS CA repository.

4.9. Certificate Revocation and Suspension

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

4.9.1. Circumstances for Revocation

HiPKI EV TLS CA shall revoke an EV TLS/SSL certificate within 24 hours if one or more of the following occurs:

(1) The subscriber requests in writing to HiPKI EV TLS CA that they wish to revoke the certificate;

(2) The subscriber notifies HiPKI EV TLS CA that the original certificate request was not authorized and does not retroactively grant authorization;

(3) HiPKI EV TLS CA obtains evidence that the subscriber's private key corresponding to the public key in the certificate suffered a key compromise; or

(4) HiPKI EV TLS CA obtains evidence that the validation of domain authorization or control for any FQDN or IP address in the certificate should not be relied upon.

HiPKI EV TLS CA should revoke an EV TLS/SSL certificate within 24 hours and must revoke a certificate within 5 days if one or more of the following occurs:

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

(2) HiPKI EV TLS CA obtains evidence that the certificate was misused;

(3) HiPKI EV TLS CA is made aware that a subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;

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

Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);

(5) HiPKI EV TLS CA is made aware of a material change in the information contained in the certificate;

(6) HiPKI EV TLS CA is made aware that the certificate was not issued in accordance with these requirements or the HiPKI CP or this CPS;

(7) HiPKI EV TLS CA determines or is made aware that any of the information appearing in the certificate is inaccurate;

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

(9) Revocation is required by the HiPKI CP and/or this CPS; or

(10) HiPKI EV TLS CA is made aware of a demonstrated or proven method that exposes the subscriber's private key to compromise, methods have been developed that can easily calculate it based on the public key (such as a Debian weak key, see https://wiki.debian.org/SSLkeys), or if there is clear evidence that the specific method used to generate the private key was flawed.

HiPKI EV TLS CA may at its own discretion revoke subscriber certificaters under the aforementioned circumstances.

4.9.2. Who Can Request 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) can request certificate revocation.

4.9.3. Procedure for Revocation Request

(1) The Applicant shall submit the certificate revocation request in accordance with the operation procedures 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 the Applicant's name and

contact information, reason for revocation, and 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 HiPKI EV TLS CA;

(3) Upon receiving the certificate revocation application sent by the RA, HiPKI EV TLS CA 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. The serial number of the revoked certificate and the reason of revocation must be added to the appropriate CRL until the revoked certificate has expired;

(4) If the application does not pass the above checking, HiPKI EV TLS CA 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 HiPKI EV TLS CA to understand the source of the problem;

(5) In order to ensure the security, integrity and non-reputability of the data transmitted between HiPKI EV TLS CA and its RA, the data of the certificate application is encrypted with a digital signature and transmitted through the network by transport layer security (TLS) protocol;

(6) HiPKI EV TLS CA uses the same CA private key issuing the certificate to publish the revoked certificate serial number and the reason for revocation to the CRL by the digital signature.

(7) Provide a timelier OCSP service; and

(8) HiPKI EV TLS CA receives certificate problem reports and provides 24x7 availability of certificate problem response mechanism, as specified in Section 4.9.3.1.

4.9.3.1. Mechanism for Responding the Certificate Problems

Under “the Announcement of CPS” at the repository, HiPKI EV TLS CA provides the guidelines for certificate problem reports. Subscribers, relying parties, application software suppliers, and other third parties may

submit certificate problem reports through the information specified in Section 1.5.2.2 to notify HiPKI EV TLS CA of a suspected reasonable cause to revoke the certificate.

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 HiPKI EV TLS CA within one hour. When the subscriber's private key is lost or suspect or known to be compromised or the information appearing in the certificate has expired or is inaccurate, the subscriber shall promptly submit a certificate revocation application to the RA. The certificate revocation request grace period is two working days. HiPKI EV TLS CA may extend the certificate revocation grace period when deemed necessary.

4.9.5. Time within Which CA Must Process the Revocation Request

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

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

(1) The nature of the alleged problem (scope, context, severity, magnitude, risk of harm);

(2) The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties);

(3) The number of certificate problem reports received about a particular certificate or subscriber;

(4) The entity making the complaint; and

(5) Relevant legislation.

4.9.6. Revocation Checking Requirement for Relying Parties

Before using certificates issued by HiPKI EV TLS CA, the relying parties shall first check the CRLs or OCSP responses published by HiPKI EV TLS CA to verify the validity of certificates. The relying parties shall verify the revoking time of certificates, the validity of signatures of the CRLs or OCSP responses, and certificate chains with their validity.

HiPKI EV TLS CA publishes the information of revoked certificates to the repository for checking purposes. There are no restrictions for the checking of CRLs by relying parties. The website is at: http://tls.hinet.net.

4.9.7. CRL Issuance Frequency

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

4.9.8. Maximum Latency for CRLs

HiPKI EV TLS CA shall publish the CRL no later than the time specified in the nextUpdate field of the previously issued CRL.

4.9.9. On-line Revocation/Status Checking Availability

HiPKI EV TLS CA provides the inquiry to certificate revocation/status by CRL, webpage certificate inquiries and download, and OCSP responses.

HiPKI EV TLS CA uses OCSP Responder to provide the OCSP responses complying with RFC 6960 and RFC 5019 standards. HiPKI EV TLS CA uses the private signing key to issue the OCSP responder certificates

with the security strength at least RSA 4096 w/SHA-256 with which the relying parties can verify the digital signatures of the OCSP responses and confirm the integrity of the information sources.

4.9.10. On-line Revocation Checking Requirements

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

HiPKI EV TLS CA uses SHA-256 Hash Function Algorithm to issue OCSP responses.

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

The OCSP of HiPKI EV TLS CA is updated at least once every 1 hour, and the validity period of the OCSP responses is greater than or equal to 8 hours and less than 16 hours. Relying parties SHOULD check the information of nextUpdate before checking the certificate through the OCSP responses provided by HiPKI EV TLS CA; and measure whether to trust the information.

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

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

4.9.11. Other Forms of Revocation Advertisements Available

In order to speed up and instantly complete the verification of the EV TLS/SSL certificates status of high-traffic websites, HiPKI EV TLS CA supports OCSP stapling operation based on RFC 4366 and through the Subscriber Agreements, support of Certificate Transparency (CT) and technical review, or provision of relevant setting instructions to assist subscribers who own high-traffic websites to implement OCSP stapling.

4.9.12. Special Requirements Related to Key Compromise

As stated in Sections 4.9.1, 4.9.2 and 4.9.3.

4.9.13. Circumstances for Suspension

HiPKI EV TLS CA does not provide the service of certificate suspension.

4.9.14. Who Can Request Suspension

Not applicable.

4.9.15. Procedure for Suspension Request

Not applicable.

4.9.16. Limits on Suspension Period

Not applicable.

4.10. Certificate Status Services

4.10.1. Operational Characteristics

HiPKI EV TLS CA provides CRL service and the HTTP URL of the CRL service is presented in the cRLDistributionPoints extension of its subscriber certificates. HiPKI EV TLS CA also provides OCSP service.

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

4.10.2. Service Availability

HiPKI EV TLS CA maintains 24x7 availability of certificate status service that application software can use to automatically check the status of all unexpired certificates issued by HiPKI EV TLS CA.

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

4.10.3. Optional Features

No stipulation.

4.11. End of Subscription

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

4.12. Key Escrow and Recovery

4.12.1. Key Escrow and Recovery Policy and Practices

HiPKI EV TLS CA and subscriber's private signing keys shall not be escrowed.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

HiPKI EV TLS CA does not currently support session key encapsulation and recovery.

5. Facility, Management, and Operational Controls

5.1. Physical Controls

5.1.1. Site Location and Construction

The HiPKI EV TLS CA 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 HiPKI EV TLS CA equipment.

5.1.2. Physical Access

HiPKI EV TLS CA has established suitable measures to control connections to the hardware, software and hardware security module that serves to HiPKI EV TLS CA.

The HiPKI EV TLS CA 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 HiPKI EV TLS CA system.

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

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

5.1.4. Water Exposures

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

5.1.6. Media Storage

Audit records, archives and backups are kept in storage media at the

facility described in Section 5.1.1. In addition, one copy shall be kept at a secure location.

5.1.7. Waste Disposal

When the documents of HiPKI EV TLS CA detailed in Section 9.1.3 are no longer in use, it shall be shredded by the paper shredder. Any magnetic tape, hard disk, floppy disk, MO and other forms of memory shall be formatted to erase the information stored on them before scrapping. Optical disks shall be physically destroyed.

5.1.8. Off-site Backup

The off-site backup location shall be over 30 km away from the HiPKI EV TLS CA 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, HiPKI EV TLS CA uses procedural controls to specify the trusted roles of HiPKI EV TLS CA 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 HiPKI EV TLS CA functions are properly distinguished to prevent undetected malicious use of the system, the trusted role authorized to perform each system access task is clearly defined.

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

The administrator is responsible for:

- Installation, configuration and maintenance of the HiPKI EV TLS CA system
- Creation and maintenance of system user accounts
- Generation and backup of HiPKI EV TLS CA keys

The CA officer is responsible for:

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

The internal auditor is responsible for:

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

The system operator is responsible for:

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

The physical security controller is responsible for:

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

The cyber security coordinator is responsible for:

- Maintenance of the network and network facilities
- Patches management for the vulnerabilities of the network facilities
- The cyber security of HiPKI EV TLS CA
- Detection and report of the cyber security events

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

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

The RAO is responsible for:

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

As described in Sections 4.2.2 and 5.2.4, the RA system requiring two-factor authentication must handle certificate vetting process and certificate issuance by at least two different personnel in trusted roles.

5.2.2. Number of Persons Required per Task

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

- Administrator

  At least 3 qualified individuals are needed.

- CA Officer

  At least 2 qualified individuals are needed.

- Internal Auditor

  At least 2 qualified individuals are needed.

- System Operator

  At least 2 qualified individuals are needed.

- Physical security controller

  At least 2 qualified individuals are needed.

- Cyber security coordinator

  At least 1 qualified individual.

- Anti-virus and anti-hacking coordinator

  At least 1 qualified individual.

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

Assignments	Administrator	CA Officer	Internal Auditor	System Operator	Physical security controller	Cyber security coordinator	Anti-virus and anti-hacking coordinator
Installation, configuration, and maintenance of the HiPKI EV TLS CA system	2				1		
Establishment and maintenance of system user accounts	2				1		
Generation and backup of HiPKI EV TLS 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		
Daily operation and maintenance of system equipment				1	1		
System backup and recovery				1	1		
Storage media updating				1	1		
Hardware and software updates				1	1		

Assignments	Administrator	CA Officer	Internal Auditor	System Operator	Physical security controller	Cyber security coordinator	Anti-virus and anti-hacking coordinator
outside the HiPKI EV TLS CA certificate management system							
Website maintenance				1	1		
Daily operation and maintenance of the network and network facilities				1	1	1	
Patching the vulnerabilities of the network facilities	1				1	1	
Reporting the threats and vulnerabilities of computer virus							1
Keep the antivirus system's signatures update and patches for the vulnerabilities				1	1		

5.2.3. Identification and Authentication for Each Role

Use IC cards to identify and authenticate administrator, CA officer, internal auditor and system operator roles as well as central access system to determine the authority to identify and authenticate physical security controller role. When the RAOs who log in the RA system and conduct related review actions, they shall use IC cards to verify their identities and execute digital signatures.

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

5.2.4. Roles Requiring Separation of Duties

Trusted roles of HiPKI EV TLS CA requiring separation of duties are described as follows:

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

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

5.3. Personnel Controls

5.3.1. Qualifications, Experience, and Clearance Requirements

(1) Security evaluation for personnel selection

Personnel selection includes the following items:

(A) Personality evaluation,

(B) Applicant experience evaluation,

(C) Academic and professional skills and qualifications evaluation,

(D) Personal identity check, and

(E) Evaluation of personnel conduct. Check if personnel have criminal records in accordance with the EV SSL Certificate Guidelines.

(2) Management of Personnel Evaluation

All 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 HiPKI EV TLS CA stating that personnel may not disclose business secrets verbally or by photocopy, loan, delivery, publishing or other methods.

5.3.2. Background Check Procedures

HiPKI EV TLS CA 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) HiPKI EV TLS CA security principles and mechanism. (2) Installation, configuration, and maintenance of the HiPKI EV TLS CA operation procedures. (3) Establishment and maintenance of system user accounts operation procedures. (4) Audit parameter configuration setting procedures. (5) HiPKI EV TLS CA key generation and backup operation procedures. (6) Disaster recovery and continuous operation procedure.
CA Officer	(1) HiPKI EV TLS CA security principles and mechanism. (2) HiPKI EV TLS CA system software and hardware use and operation procedures. (3) Activation/deactivation of certification issuance operation procedure. (4) Activation/ deactivation of certification revocation

Trusted Role	Training Requirements
	operation procedure. (5) Activation/ deactivation of certificate CRL issuance service operation. (6) Disaster recovery and continuous operation procedure.
Internal Auditor	(1) HiPKI EV TLS CA security principles and mechanism. (2) HiPKI EV TLS CA system software and hardware use and operation procedures. (3) HiPKI EV TLS CA key generation and backup operation procedures. (4) Audit log check, upkeep and archiving procedures. (5) Disaster recovery and continuous operation procedure.
System Operator	(1) Daily operation and maintenance procedures for system equipment. (2) System backup and recovery procedure. (3) Upgrading of storage media procedure. (4) Disaster recovery and continuous operation procedure. (5) Network and website maintenance procedure.
Physical Security Controller	(1) Physical access authorization setting procedure. (2) Disaster recovery and continuous operation procedure.
Cyber Security Coordinator	(1) Maintenance of the network and network facilities. (2) Security mechanism for the network.
Anti-virus and Anti-hacking Coordinator	(1) Prevention and control to the threats and vulnerabilities of computer virus. (2) Security mechanism for the operating system and the network.
RAO	(1) Basic knowledge of the PKI (2) Identity authorization and information verification policies and procedures (including the EV SSL certificate guidelines, Baseline Requirements, HiPKI CP and this CPS) (3) Common identification and information verification procedure threat (including phishing and other social engineering attacks) knowledge and skills.

Trusted Role	Training Requirements
	(4) The procedure of disaster recovery and continuous operation.

Testing will be held for related training and records kept ensuring that the RAOs 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 HiPKI EV TLS CA shall be familiar with any changes to HiPKI EV TLS CA and related work procedures, laws and regulations. When there is any significant change, an appropriate amount of training time shall be scheduled within one month to conduct retraining and the training status shall be recorded to ensure that work procedures and regulatory changes are understood.

5.3.5. Job Rotation Frequency and Sequence

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

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

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

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

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

5.3.6. Sanctions for Unauthorized Actions

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

5.3.7. Independent Contractor Requirements

The duties, sanctions for unauthorized actions and required training documents of independent contractor serving a trusted role shall meet the requirements of Section 5.3 and the event logging and document retention shall meet the requirements of Section 5.4.1.

5.3.8. Documentation Supplied to Personnel

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

5.4. Audit Logging Procedures

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

5.4.1. Types of Events Recorded

(1) Key generation

- Key generation of HiPKI EV TLS CA (not mandated for the generation of keys that are used once or only once).

(2) Private key loading and storage

- Loading the private key into a system component.
- All access to private keys kept by HiPKI EV TLS CA 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

HiPKI EV TLS CA 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.

HiPKI EV TLS CA shall check the audit logs monthly.

5.4.3. Retention Period for Audit Log

Audit logs of HiKPKI EV TLS CA shall be retained in compliance with the retention period specified in Section 5.5.2. Prior to save audit logs to a secure off-site location, the audit logs shall be retained at the site of HiKPKI EV TLS CA for at least two months.

HiKPKI EV TLS CA shall make these audit logs available to its qualified

auditor upon request. After the end of the audit log retention period, the removal task shall be performed only by the internal auditor.

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) HiPKI EV TLS CA shall routinely archive event logs.

(2) HiPKI EV TLS CA 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 HiPKI EV TLS CA 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

HiPKI EV TLS CA shall follow the methods and frequency stipulated in WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security (WebTrust for CA – SSL BR) and Network and Certificate System Security Requirements to conduct the vulnerability assessments at least once per quarter and the penetration testing at least once per year. HiPKI EV TLS CA also must conduct penetration testing after it is determined that there is a significant upgrade or modification to the application program or infrastructure. HiPKI EV TLS CA will have reinforcement and correction actions after the penetration tests and vulnerability assessments. HiPKI EV TLS CA shall record the skills, tools and

followed ethical, competitive relations and independence 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 HiPKI EV TLS CA to accurately and completely save certificate-related records as computer data or in written form, including:

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

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

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

5.5.1. Types of Records Archived

HiPKI EV TLS CA retains the following information in its archives:

(1) HiPKI EV TLS CA 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) HiPKI EV TLS CA re-key records.

(11) Issued or announced CRLs.

(12) Audit logs.

(13) Other data or application programs used to verify and corroborate the archived content.

(14) Documents required by the auditor.

5.5.2. Retention Period for Archive

HiPKI EV TLS CA retains archived data for at least 10 years. The application programs used to process archived data are retained for 10 years.

5.5.3. Protection of Archive

(1) Amendments, modifications and deletion of archived information not allowed by any user.

(2) Transfer of archived information to another storage media which has passed through the HiPKI EV TLS CA authorization procedure.

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

5.5.4. Archive Backup Procedures

HiPKI EV TLS CA 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 HiPKI EV TLS CA.

5.5.5. Requirements for Time-stamping of Records

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

5.5.6. Archive Collection System (Internal or External)

There is currently no archive information collection system.

5.5.7. Procedures to Obtain and Verify Archive Information

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

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

5.6. Key Changeover

HiPKI EV TLS CA shall periodically change its private keys in accordance with Section 6.3.2.1 and shall change its key pair before the usage period of its private key has expired. After key changeover, an application for a new certificate shall be submitted to HiPKI RCA. The new certificate shall be published in the repository for subscribers and relying parties downloading.

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

If HiPKI EV TLS CA's certificate has been revoked, HiPKI EV TLS CA shall stop using its private keys and shall change its private keys.

5.7. Compromise and Disaster Recovery

5.7.1. Incident and Compromise Handling Procedures

HiPKI EV TLS CA establishes incident and compromise reporting and handling procedures. The procedures shall be reviewed, drilled, and updated at least annually.

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

HiPKI EV TLS CA establishes recovery procedures in the event of computing resource, software or data corruption and conducts annual drills.

If the HiPKI EV TLS CA computer equipment is damaged or unable to operate, but the HiPKI EV TLS CA signature key has not been destroyed, priority shall be given to restoring operation of the HiPKI EV TLS CA

repository and quickly reestablishing the generation of certificate status information.

5.7.3. Entity Private Key Compromise Procedures

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

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

(2) Revoke the HiPKI EV TLS CA 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.

HiPKI EV TLS CA shall conduct the drills at least once a year.

5.7.4. Business Continuity Capabilities after a Disaster

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

5.8. CA or RA Termination

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

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

(2) HiPKI EV TLS CA shall take the following measures when terminating their service:

- For certificates which are valid at the time of termination,

arrangements shall be made for other CA to take over the service. Matters regarding service termination and service acceptance by other CAs shall be notified to subscribers with valid certificates. This shall not apply if notification cannot be made.

- All records and files during the operation period shall be handed over to the other CA that is taking over this service.
- If there is no CA willing to take over the HiPKI EV TLS CA 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, HiPKI EV TLS CA 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. HiPKI EV TLS CA shall refund the certificate issuance fees based on the propotion of the certificate validity.
- The competent authorities, if necessary, may publish the certificates which are still valid at the time of revocation.

In case that the RA terminates the service, HiPKI EV TLS CA shall stop its rights of review actions.

6. Technical Security Controls

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

HiPKI EV TLS CA generates pseudo random numbers and public key pairs within the hardware security module in accordance with Section 6.2.1.

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

HiPKI EV TLS CA key generation is witnessed and videotaped by the PMA members and the qualified auditors.

6.1.1.1. Subscriber Key Pair Generation

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

6.1.2. Private Key Delivery to Subscriber

HiPKI EV TLS CA shall not generate the key pairs on behalf of subscribers. The private keys shall be generated and stored by subscribers in their cryptographic modules.

6.1.3. Public Key Delivery to Certificate Issuer

If the subscriber self-generates a key pair and delivers the public key to the RA via a certificate request file with PKCS# 10 format. The RA shall deliver the public key to HiPKI EV TLS 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 Key Delivery to Relying Parties

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

6.1.5. Key Sizes

HiPKI EV TLS CA uses 4096-bit or the above RSA keys and SHA-256 hash function algorithm to issue certificates.

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

For ECDSA keys, HiPKI EV TLS CA shall use one of the following curve-hash pairs: P-256 with SHA-256, P-384 with SHA-384.

6.1.6. Public Key Parameters Generation and Quality Checking

The public key parameter of the RSA algorithm is null.

The HiPKI EV TLS CA 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.

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

If the certificates are issued with ECC algorithm, HiPKI EV TLS CA shall comply with the requirements of Sections 5.6.2.3.2 and 5.6.2.3.3 in NIST SP 800-56A Revision 2 to confirm the validity of all keys using either the ECC Full Public Key Validation Routine or the ECC Partial Public Key Validation Routine.

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

HiPKI EV TLS CA's private signing key is used to issue certificates and CRLs. HiPKI EV TLS CA's own public key certificate is issued by HiPKI RCA. The keyUsage bits used for the keyUsage extension are keyCertSign and cRLSign. If HiPKI EV TLS CA's private signing key is used for signing OCSP responses, then the digitalSignature bit will be set.

The keyUsage extension of EV TLS/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

HiPKI EV TLS CA uses FIPS 140-2 Level 3 certified hardware security modules.

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

HiPKI EV TLS CA key splitting multi-person control uses n-out-of-m LaGrange Polynomial Interpolation. It is a perfect secret sharing method used

for private key splitting and recovery, where n and m must be values greater than or equal to 2 and n must be less than or equal to m. Use of this method can provide the highest security level for HiPKI EV TLS CA private key multi-person control. Therefore, it can be used as the activation method for private keys as well (see Section 6.2.8).

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

6.2.3. Private Key Escrow

HiPKI EV TLS CA's private signing key is not escrowed. HiPKI EV TLS CA shall not be responsible for the safekeeping of subscriber private keys.

6.2.4. Private Key Backup

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

6.2.5. Private Key Archival

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

6.2.6. Private Key Transfer into or from a Cryptographic Module

HiPKI EV TLS CA transfers the private key into the cryptographic modules under the following circumstances:

(1) Key generation,

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

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

6.2.7. Private Key Storage on Cryptographic Module

As stated in Sections 6.1.1 and 6.2.1.

6.2.8. Method of Activating Private Key

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

Subscribers shall choose a secure computer environment and a trustworthy application system carefully and keep and use the private keys properly. The methods to activate the private keys of subscribers are categorized by the private key storage media as the following:

(1) If it is a hardware cryptographic 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 controls in Section 6.2.2 are used to deactivate HiPKI EV TLS CA private keys.

HiPKI EV TLS CA does not provide subscriber private key deactivation service.

6.2.10. Method of Destroying Private Key

In order to prevent the theft of HiPKI EV TLS CA private keys which

could endanger the authenticity of the entire certificate, the private key must be destroyed at the end of the HiPKI EV TLS CA key lifecycle. Therefore, when HiPKI EV TLS CA completes the key renewal and HiPKI RCA issues a new HiPKI EV TLS CA certificate, after no additional certificates or CRL are issued (see Section 4.7), zeroization is done on the old HiPKI EV TLS CA private key stored in the hardware cryptographic module to ensure that the old HiPKI EV TLS CA private key is destroyed.

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

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

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

The destruction method for subscriber private keys is not stipulated.

6.2.11. Cryptographic Module Rating

See Section 6.2.1.

6.3. Other Aspects of Key Pair Management

Subscribers must manage their own key pairs. HiPKI EV TLS CA is not responsible for safeguarding subscriber private keys.

6.3.1. Public Key Archival

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

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

6.3.2.1. HiPKI EV TLS CA Certificate Operational Periods and Key Pair Usage Periods

HiPKI EV TLS CA certificate operational periods and key pair usage periods are:

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

The new OCSP responder certificate is disclosed daily (provide the relying parties with the OCSP response signed by the new private key along with that certificate).

6.3.2.2. Subscriber Certificate Operational Periods and Key Pair Usage Periods

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

Type of Cert.	Private Key Usage	Certificate Term
EV TLS/SSL Certificate	■ See Section 6.1.7: 825 days	825 days

6.4. Activation Data

6.4.1. Activation Data Generation and Installation

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

6.4.2. Activation Data Protection

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

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

6.4.3. Other Aspects of Activation Data

The HiPKI EV TLS CA private key activation data is not archived.

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

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

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

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

(3) Provide security audit capability, and

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

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

6.5.2. Computer Security Rating

HiPKI EV TLS CA servers use Common Criteria EAL 3 certified computer operating systems.

6.6. Life Cycle Technical Controls

6.6.1. System Development Controls

Quality control for HiPKI EV TLS CA system development complies with CMMI standards.

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

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

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

6.6.2. Security Management Controls

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

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

HiPKI EV TLS CA documents and controls system configurations and any modification and upgrade of functions as well as detect unauthorized modifications to system software or configurations.

HiPKI EV TLS CA references the methodologies and standards in the ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, ISO/IEC 31000, Baseline Requirements, EV SSL Certificate Guidelines, Network and Certificate System Security Requirements, WebTrust Principles and Criteria for

Certification Authorities (WebTrust for CA), WebTrust for CA – Extended Validation SSL (WebTrust for CA – EV SSL) and WebTrust for CA – SSL BR 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 HiPKI EV TLS CA host and repository have firewalls and are connected to external networks. The repository is placed on the outside service area (de-militarized zone, DMZ) in the firewall and connected to the Internet. Except during required maintenance or backup, the repository provides uninterrupted certificate and CRL inquiry services.

The certificates and CRLs issued by the HiPKI EV TLS CA host have digital signature protection and are automatically delivered from the HiPKI EV TLS CA host to the repository.

The HiPKI EV TLS CA 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

HiPKI EV TLS CA regularly conducts system clock synchronization with a reliable time source to maintain the correctness of system time and ensure the accuracy of the following times:

(1) Time of subscriber certificate issuance,

(2) Time of subscriber certificate revocation,

(3) Time of CRL issuance, and

(4) Time of system event occurrence.

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

7. Certificate, CRL, and OCSP Profiles

7.1. Certificate Profile

The certificates issued by HiPKI EV TLS CA conform to the official versions of the ITU-T X.509, EV SSL Certificate Guidelines and RFC 5280.

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

7.1.1. Version Number(s)

HiPKI EV TLS CA issues X.509 version 3 certificates.

7.1.2. Certificate Extensions

The extensions of the certificates issued by HiPKI EV TLS CA are set in compliance with the official versions of the ITU-T X.509, EV SSL Certificate Guidelines and RFC 5280.

7.1.2.1. CA Certificate of HiPKI EV TLS CA

The extensions of Subordinate CA certificates that HiPKI RCA issued to HiPKI EV TLS CA are described as follows:

a. certificatePolicies

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

b. cRLDistributionPoints

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

c. authorityInfoAccess

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

d. basicConstraints

This extension is required and marked as critical. The cA field is set to true. As a result of HiPKI EV TLS CA does not sign the subordinate CA certificates downwards, the pathLenConstraint field is set to zero (0).

e. keyUsage

This extension is required and marked as critical. This extension is used to mark keyUsage bits as keyCertSign and cRLSign. HiPKI EV TLS CA does not sign the OCSP response with the private signing key, but issues the OCSP responder certificate, and the OCSP responder issues OCSP responses, and thus the configuration does not use digitalSignature.

f. nameConstraints

The subordinate CA certificates issued to HiPKI EV TLS CA by HiPKI RCA do not have this extension.

g. extKeyUsage

For the subordinate CA certificate that HiPKI RCA issues to HiPKI EV TLS CA, this extension is required and marked as non-critical. This extension contains serverAuth and clientAuth bits; however, both the id-kp-serverAuth and id-kp-emailProtection KeyPurposeIds must not be contained in this extrnsion at the same time.

7.1.2.2. Subscriber Certificate

a. certificatePolicies

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

b. cRLDistributionPoints

This extension is required and marked as non-critical. It contains the HTTP URL of HiPKI EV TLS CA’s CRL service.

c. authorityInfoAccess

This extension is required and marked as non-critical. It contains the HTTP URL of HiPKI EV TLS CA’s OCSP responder and the HTTP URL

to download the certificate of HiPKI EV TLS CA.

d. basicConstraints

This extension is optional and marked as non-critical if any. The cA field is set to false. As a result of the subscriber certificate cannot be used to sign the subordinate CA certificates downwards, the pathLenConstraint field is set to zero (0).

e. keyUsage

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

f. extKeyUsage

For the EV TLS/SSL certificates issued by HiPKI EV TLS CA, this extension is required and marked as non-critical. The extension contains both serverAuth and clientAuth bits.

Unless the reasons to include certain data in the certificates are known, HiPKI EV TLS CA is not allowed to issue certificates in the following conditions:

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

(2) Semantics that will mislead a Relying Party about the certificate information verified by HiPKI EV TLS CA.

Regarding supporting the CT, HiPKI EV TLS CA adopts the X.509 version 3 Extension mechanism, which is currently the most commonly used, to transmit SCTs for EV TLS/SSL certificates. Therefore, the SCT will be individually obtained from the multiple CT logs through submitting the pre-signed precertificate's certificate chain, and the SCT chain will be embedded into the target certificate before it is issued to the subscriber. According to the latest Google and Apple CT policies, adopting X.509 v3 Extension mechanism has the following benefits: SSL certificate subscribers can obtain SSL certificates compliant with the CT specifications by past certificate

application; no additional restrictions exist as OCSP Stapling SCT transmission method listed in the RFC 6962 (it requires subscriber web server OCSP Stapling configuration settings to be enabled, and there are still a few web servers unsupportable for OCSP Stapling); HiPKI EV TLS CA just needs to ensure that the connected CT logs are currently qualified during issuing the target certificate; therefore, it won't be affected by the status changes of CT logs in the future.

7.1.3. Algorithm Object Identifiers

The algorithm OIDs used for signatures on HiPKI EV TLS CA issued certificates are:

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

(OID: 1.2.840.113549.1.1.11)

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

(OID: 1.2.840.113549.1.1.12)

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

(OID: 1.2.840.113549.1.1.13)

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

(OID: 1.2.840.10045.4.3.2)

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

(OID: 1.2.840.10045.4.3.3)

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

(OID: 1.2.840.10045.4.3.4)

The algorithm OID used during HiPKI EV TLS CA issued certificate generation of subject keys are:

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

(OID: 1.2.840.113549.1.1.1)

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

(OID: 1.2.840.10045.2.1)

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

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

(OID: 1.2.840.10045.3.1.7)

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

(OID: 1.3.132.0.34)

7.1.4. Name Forms

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

The Subject information in the CA ceritficate of HiPKI EV TLS CA 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 HiPKI EV TLS CA 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 HiPKI EV TLS CA, trademark, or their meaningful name, for the purpose of identifying HiPKI EV TLS CA more precisely; it is not allowed to contain the commonName only, e.g., CA1. Please refer to Section 3.1.5 for the X.500 distinguished name of the CA certificate of HiPKI EV TLS CA.

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 HiPKI EV TLS CA, the Issuer DN has to be identical to the content of the Subject DN of HiPKI EV TLS CA.

7.1.4.2. Subject Information–Subscriber Certificates

By issuing the subscriber certificates, HiPKI EV TLS CA and its RA have complied with the procedures specified in the HiPKI CP and/or this CPS, to ensure all the Subject information recorded in these EV TLS/SSL certificates are accurate. If the commonName field in the certificate Subject appears, it will be the FQDN validated by Section 3.2.2.5 (if it is a multi-domain EV TLS/SSL certificate, only one FQDN will be placed). In addition, subject attributes MUST NOT contain only metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.

7.1.4.2.1. Subject Alternative Name Extension

The Subject Alternative Name Extensions for EV TLS/SSL certificates are as follows:

Certificate Extension	Required/Optional Extension
extension:subjectAltName	Required

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

This extension shall be validated the ownership or control of the domain name by the RAOs 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 certificate of HiPKI EV TLS CA is validated and issued by

HiPKI RCA based on the procedures specified in the HiPKI CP and/or HiPKI RCA CPS. The Subject Distinguished Name Fields are as follows:

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

7.1.5. Name Constraints

No name constraints are used.

7.1.6. Certificate Policy Object Identifier

The certificate policies extension contains the EV SSL CP OID ({joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) ev-guidelines (1)} (2.23.140.1.1)) defined by CA/Browser Forum.

7.1.7. Usage of Policy Constraints Extension

Certificates issued by HiPKI EV TLS CA do not contain policy constraints extension.

7.1.8. Policy Qualifiers Syntax and Semantics

The policy qualifier ID (policyQualiferId) of certificates issued by HiPKI EV TLS CA must be defined as 「id-qt 1」 in the RFC 5280 international standards and indicates 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 the certificates issued by HiPKI EV TLS CA are not marked as critical.

7.2. CRL Profile

7.2.1. Version Number(s)

HiPKI EV TLS CA issues ITU-T X.509 version 2 CRLs.

7.2.2. CRL and CRL Entry Extensions

The extensions of crlExtensions and crlEntryExtensions in the CRLs issued by HiPKI EV TLS CA conform to the official versions of the ITU-T X.509, EV SSL Certificate Guidelines and RFC 5280. CRLs have the following extensions:

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, 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 HiPKI EV TLS CA, the keyCertSign cert and cRLSign cert are the

Field	Content	Description
		same cert)
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 Fill in a series of RevokedCertificate records	All the effective revocation even happened before thisUpdate, will be recorded in the revokedCertificates (“effective” means the certificate not yet expired)
*.RevokedCertificate	Each RevokedCertificate record shall contain the following:	The asterisk (*) means there are multiple RevokedCertificate records
.userCertificate	Fill in the Certificate Serial Number of revoked certificate	The serial number of certificate used in HiPKI EV TLS CA 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

Field	Content	Description
		beginning, and thus the positive integer with 16 bytes actually occupies the space of 17 bytes
.revocationDate	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 (Note: the CRLEntryExtension Information type format and Public-Key Certificate Extension information type format are completely identical)	May fill in a series of CRLEntryExtensions, but HiPKI EV TLS CA only use reasonCode as the CRLEntryExtension
.reasonCode	HiPKI only uses reasonCode as this CRLEntryExtension, the content is as follows:	
.extnId	Fill in the OID id-ce-cRLReasons (2.5.29.21)	
.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	Some CRLReason in HiPKI

Field	Content	Description
	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	EV TLS CA may not be used in Complete CRL
	unused(0)	According to the PKIX, this CRLReason extension may not be used in HiPKI EV TLS CA
	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

Field	Content	Description
		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

Field	Content	Description
		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	An Authority Key Identifier extension, where Key Identifier generation method follows PKIX standards and its value is the output of SHA-1 Hash using Issuing CA's Public Key as input	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	Fill in the OID id-ce-authorityKeyIdentifier (2.5.29.35)	

Field	Content	Description
.critical	authorityKeyIdentifier must be non-critical extension in HiPKI, so the critical value is FALSE	Note: Since FALSE is the DEFAULTVALUE, this field is omitted in the DER code
.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	The data structure of authorityKeyIdentifier contains 3 optional fields: keyIdentifier, authorityCertIssuer and authorityCertSerialNumber fields	In HiPKI EV TLS CA, the CRL only uses the keyIdentifier field rather than the authorityCertIssuer and authorityCertSerialNumber fields in compliance with PKIX.
.keyIdentifier	keyIdentifier field data type is KeyIdentifier and the KeyIDentifier itself is 1 OCTET STRING data type	KeyIdentifier generation method follows PKIX standard, it obtains the SHA-1 Hash value of Subject Public Key to serve as KeyIdentifier's OCTET STRING value.
.cRLNumber	cRLNumber CRLExtension content is as follows:	cRLNumber extension field content is used to record this CRL serial number.
.extnId	Fill in the OID id-ce-cRLNumber (2.5.29.20) that represents this extension	
.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	According to the X.509 standard, the CRL Number must be one monotonically increasing sequence number. In HiPKI, the

Field	Content	Description
	value and the CRLNumber itself is1 INEGER (0..MAX) positive integer data type.	CRLNumber value in the CRL shall be one size less or equal to 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	Fill in the OID id-ce-issuingDistributionPoint (2.5.29.28) that represents this extension	
.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 data	In HiPKI EV TLS CA, the

Field	Content	Description
	type is DistributionPointName, and the DistributionPointName itself is a CHOICE data type which can be selected as a fullName or nameRelativeToCRLIssuer	distributionPoint extension of the partitioned CRL uses fullName.
.fullName	fullName data type is GeneralNames and GeneralNames data type is SEQUENCE SIZE (1...MAX) OF GeneralName	In HiPKI EV TLS CA, the fullName in distributionpoint extension of the partitioned CRL only contains one GeneralName.
.GeneralName	GeneralName is a CHOICE data type	HiPKI EV TLS CA 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 Profile

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

7.3.1. Version Number(s)

An OCSP request accepted by HiPKI EV TLS CA shall contain the following information:

- Version number, and
- Target certificate identifier

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

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

Field	Description
Status	Response status, includes success, request format error, internal error, try again later, request no signature or request no certificate authorization, the following items must be included when status is successful
Version	v.1 (0x0)
OCSP Responder ID	The subject DN of OCSP responder
Produced Time	OCSP Response sign time
Target certificate identifier	The contents of this field include the hash algorithm, the hash of the issuer's DN, the hash of the issuer's public key and the serial number of the target certificate.
Certificate Status	Certificate status code (0: valid /1: revoked /2: unknown)
ThisUpdate/NextUpdate	Recommended validity region for this response packet includes: ThisUpdate and NextUpdate
Signature Algorithm	OCSP Response signature algorithm, which can be either sha256WithRSAEncryption or ecdsaWithsha384
Signature	OCSP responder signature
Certificates	OCSP responder certificate

7.3.2. OCSP Extensions

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

- Authority key identifier of the OCSP responder;
- If an OCSP request contains a nonce field, the OCSP response must also contain the same nonce field;
- Signed certificate timestamp; and
- OID 1.3.6.1.4.1.11129.2.4.5 which is for CT.

7.3.3. Regulations for Operation of OCSP

The operation of OCSP in HiPKI EV TLS CA includes:

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

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

8. Compliance Audit and Other Assessments

8.1. Frequency or Circumstances of Assessment

HiPKI EV TLS CA shall undergo routine external audits at least once per year (the audited period may not exceed 12 months) and non-routine internal audits to confirm that the security regulations and procedures of the HiPKI CP and this CPS are being implemented and enforced. The standards used for the audit are WebTrust for CA, WebTrust for CA – SSL BR and WebTrust for CA – EV SSL.

8.2. Identity/Qualifications of Assessor

CHT retains a qualified auditor, who is familiar with the operations of HiPKI EV TLS CA and is authorized by WebTrust for CA program as a licensed WebTrust practitioner to perform WebTrust for CA, WebTrust for CA – EV SSL and WebTrust for CA – SSL BR audit standards in R.O.C., to provide impartial and objective audit services. Audit personnel shall be a certified information system auditor or a person who has equivalent qualification; and shall at least possess the experience of conducting a WebTrust for CA seal audit twice at 4 man-days or the experience of conducting a CA information security management audit twice at 8 man-days. Audit practitioners who conduct WebTrust for CA – EV SSL audits shall take out a professional liability/errors and omissions insurance policy with a maximum claim amount of at least one million US dollars. HiPKI EV TLS CA shall conduct identity identification of auditors during auditing.

8.3. Assessor’s Relationship to Assessed Entity

CHT shall retain an impartial third party to conduct audits of HiPKI EV TLS CA operations.

8.4. Topics Covered by Assessment

The assessment shall include the following topics:

(1) Whether HiPKI EV TLS CA is operating in accordance with this CPS, including management and technical audit of the physical

environment, personnel procedural controls, key control, certificate lifecycle control, and hardware cryptographic module control;

(2) Whether the RA of HiPKI EV TLS CA complies with this CPS and related procedures; and

(3) Whether the requirements of this CPS are being implemented and enforced subject to the HiPKI CP, and whether the requirements are suitable for the practical operations of HiPKI EV TLS CA.

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

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

(1) If there is an event of computer emergency or key compromise that causes CHT to reasonably suspect the dedicated RA is unable to comply with the HiPKI CP and this CPS,

(2) If the compliance audit has not been completed or there are special developments, CHT has the right to conduct a risk management review, and

(3) If action or inaction taken by the RA causes actual or potential security and integrity threat to HiPKI, CHT must conduct the related review or examination.

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

During the period in which it issues EV TLS/SSL certificates, HiPKI EV TLS CA must strictly control its service quality by performing ongoing self audits against a randomly selected sample of at least three percent of the EV TLS/SSL certificates (less than one counted as one) it has issued in the period

beginning immediately after the last sample was taken in accordance with the EV SSL Certificate Guidelines. For all EV TLS/SSL certificates where the final cross-correlation and due diligence requirements of Section 3.2.8.4 is performed by the RA, HiPKI EV TLS CA must strictly control its service quality by performing ongoing self audits against a randomly selected sample of at least six percent of the EV TLS/SSL certificates (less than one counted as one) it has issued in the period beginning immediately after the last sample was taken.

8.5. Actions Taken as a Result of Deficiency

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

(1) Note the discrepancy,

(2) Notify HiPKI EV TLS CA about the discrepancy, and if the discrepancy is a critical fault, the PMA shall be notified as well, and

(3) HiPKI EV TLS CA shall submit an improvement plan regarding the discrepancy items within 30 days and promptly implement it. The discrepancy items shall also be listed as follow-up audit tracking items. The RA is notified to make improvements to RA-related deficiencies.

8.6. Communications of Results

Except for any audit findings that could result in system attacks and the stipulations in Section 9.3, HiPKI EV TLS CA shall make its audit report publicly available. Audit results are displayed with appropriate seals, including WebTrust for CA, WebTrust for CA – SSL BR or WebTrust for CA – EV SSL seals, on HiPKI EV TLS CA's homepage. The audit report and management's assertions may be viewed by clicking on the seals. HiPKI EV TLS CA should make its audit report and management's assertions publicly available no later than three months after the end of the audit period. In the event of a delay greater than three months, HiPKI EV TLS CA shall provide an explanatory letter signed by the qualified auditor.

9. Other Business and Legal Matters

9.1. Fees

9.1.1. Certificate Issuance or Renewal Fees

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

9.1.2. Certificate Access Fees

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

9.1.3. Revocation or Status Information Access Fees

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

9.1.4. Fees for Other Services

No stipulation.

9.1.5. Refund Policy

With regard to the certificate issuance fee charged by HiPKI EV TLS CA, if a subscriber is unable to use a certificate due to oversight by HiPKI EV TLS CA, HiPKI EV TLS CA shall issue a new certificate after conducting an investigation. If the subscriber does not accept the newly issued certificate, HiPKI EV TLS CA 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 incurred damages are not within the scope of Commercial General Liability insurance compensation coverage disclosed in Section 9.2.1, then liability for damage compensation with other assets shall conform to the EV SSL Certificate Guidelines disclosed in Section 9.2.2.

9.2.1. Insurance Coverage

HiPKI EV TLS CA is owned and operated by CHT, its financial responsibilities are the responsibilities of CHT. CHT has taken out a Commercial General Liability insurance with policy limits of a maximum compensation amount of NT$120,000,000. If the competent authority has related regulations for the certification business in the future, HiPKI EV TLS CA will cooperate accordingly.

9.2.2. Other Assets

HiPKI EV TLS CA finances are a part of the overall finances of CHT. CHT is a publicly listed company and a Republic of China company listed on the New York Stock Exchange. In accordance with Article 36 of the Securities and Exchange Act, annual financial reports duly audited and attested by a certified 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 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. HiPKI EV TLS CA can provide self-insured asset prices based on CHT's financial reports. CHT's finances are sound and its ratio of current assets to current liabilities is no lower than 1.0 which meets the requirement of the EV SSL Certificate Guidelines.

9.2.3. Insurance or Warranty Coverage for End-Entities

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

9.3. Confidentiality of Business Information

9.3.1. Scope of Confidential Information

The following information generated, received and kept by HiPKI EV TLS CA or its RA is deemed confidential information:

(1) Private keys and passphrases used for operations,

(2) Key splitting safekeeping information,

(3) Subscriber application information,

(4) Audit and tracking logs generated and kept by HiPKI EV TLS CA,

(5) Audit logs and reports made by audit personnel during the audit process which must not be fully disclosed, and

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

Current and departed personnel in HiPKI EV TLS CA and RA and audit personnel shall keep secrets for the aforementioned confidential information.

9.3.2. Information Not Within the Scope of Confidential Information

(1) Identification information and information listed in certificates are not deemed confidential information unless stipulated otherwise, and

(2) Issued certificates, revoked certificates or suspended information and CRLs published in the HiPKI EV TLS CA repository are not deemed confidential information.

9.3.3. Responsibility to Protect Confidential Information

HiPKI EV TLS CA shall handle subscriber application information in accordance with the Electronic Signatures Act, Baseline Requirements, EV SSL Certificate Guidelines, WebTrust for CA audit criterion, WebTrust for CA – EV SSL audit criterion, WebTrust for CA – SSL BR audit criterion and Personal Information Protection Act.

9.4. Privacy of Personal Information

9.4.1. Privacy Plan

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

9.4.2. Information Treated as Private

Private information includes:

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

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

(3) Identifiable information of personnel in HiPKI EV TLS CA, such as names together with palmprint or fingerprint biometrics, and

(4) Personal information on confidentiality agreements or contracts.

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

9.4.3. Information Not Deemed Private

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

Issued certificates, revoked certificates or suspension information and CRLs published in the HiPKI EV TLS CA repository are not deemed private information.

9.4.4. Responsibility to Protect Private Information

The personal information required for the operation of HiPKI EV TLS

CA, in either paper or digital form, must be security stored and protected in accordance with the personal information protection and privacy rights declaration posted on the website and must comply with the Electronic Signatures Act, Baseline Requirements, EV SSL Certificate Guidelines, WebTrust for CA audit criteria, WebTrust for CA – EV SSL audit criteria, WebTrust for CA – SSL BR audit criteria and Personal Information Protection Act. HiPKI EV TLS CA shall negotiate the liability of protecting private information with its RA.

9.4.5. Notice and Consent to Use Private Information

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

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

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

9.4.7. Other Information Disclosure Circumstances

Subscriber personal information obtained during HiPKI EV TLS CA 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 HiPKI EV TLS CA:

(1) Key pairs and split keys of HiPKI EV TLS CA and RA;

(2) Related documents or system development for certificate management of HiPKI EV TLS CA;

(3) Certificates and CRLs issued by HiPKI EV TLS CA; and

(4) This CPS.

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

9.6. Representations and Warranties

9.6.1. CA Representations and Warranties

HiPKI EV TLS CA represents and warrants to the Certificate Beneficiaries including Subscribers, Relying Parties, and Application Software Suppliers that, during the period when the Certificate is valid, HiPKI EV TLS CA has complied with the HiPKI CP and this CPS in issuing and managing the Certificate.

The Certificate Warranties specifically include, but not limited to, the following:

(1) **Right to Use Domain Name**: That, at the time of issuance, HiPKI EV TLS CA (i) implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the Domain Name(s) listed in the Certificate's subject field and subjectAltName extension (or, only in the case of Domain Names, was delegated such right or control by someone who had such right to use or control); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CPS (see Section 3.2);

(2) **Authorization for Certificate**: That, at the time of issuance, HiPKI EV TLS CA (i) implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CPS (see Section 3.2.5);

(3) **Accuracy of Information**: That, at the time of issuance, HiPKI EV TLS CA (i) implemented a procedure for verifying the accuracy of all of the information contained in the Certificate (with the exception of the subject:organizationalUnitName attribute); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CPS (see Sections 3.2.2, 3.2.3 and 3.2.7);

(4) **No Misleading Information**: That, at the time of issuance, HiPKI EV TLS CA (i) implemented a procedure for reducing the likelihood that the information contained in the Certificate's subject:organizationalUnitName attribute would be misleading; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CPS (see Sections 3.2.2, 3.2.3 and 3.2.7);

(5) **Identity of Applicant**: That, if the Certificate contains Subject Identity Information, HiPKI EV TLS CA (i) implemented a procedure to verify the identity of the Applicant in accordance with Sections 3.2.2 and 3.2.3; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CPS;

(6) **Subscriber Agreement**: That, if HiPKI EV TLS CA and Subscriber are not Affiliated, the Subscriber and HiPKI EV TLS CA are parties to a legally valid and enforceable Subscriber Agreement that satisfies the Baseline Requirements, or, if HiPKI EV TLS CA and Subscriber are the same entity or are Affiliated, the Applicant Representative acknowledged the Terms of Use;

(7) **Status**: That HiPKI EV TLS CA maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates (see Section 4.10.2); and

(8) **Revocation**: That HiPKI EV TLS CA will revoke the Certificate for any of the reasons specified in the Baseline Requirements and/or EV SSL Certificate Guidelines (see Section 4.9.1).

For EV TLS/SSL Certificates, HiPKI EV TLS CA represents to Subscribers, Relying Parties, and Application Software Suppliers that HiPKI EV TLS CA followed the EV SSL Certificate Guidelines when verifying information and issuing EV TLS/SSL Certificates.

9.6.2. RA Representations and Warranties

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

RAs shall represent and warrant that:

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

(2) All information provided to the issuing CA does not contain any false or misleading information,

(3) Translations performed by the RA are an accurate translation of the original information,

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

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

(6) RA private keys are securely managed.

9.6.3. Subscriber Representations and Warranties

For the express benefit of HiPKI EV TLS CA and the Certificate

Beneficiaries, the Applicant shall warrant that, prior to the issuance of a certificate, HiPKI EV TLS CA will obtain, either:

(1) The Applicant's agreement to the Subscriber Agreement with HiPKI EV TLS CA, or

(2) The Applicant's acknowledgement of the Terms of Use.

Applicant (or human sponsor for device certificates or agent under a subcontractor or hosting service relationship) shall represent and warrant to HiPKI EV TLS CA that it will:

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

(2) Provide accurate and complete information to HiPKI EV TLS CA and RA,

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

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

(5) Promptly notify HiPKI EV TLS CA, cease using a certificate, and request revocation of the certificate, if

(i) any information in the certificate is or becomes incorrect or inaccurate, or

(ii) there is any actual or suspected misuse or compromise of the Subscriber's private key associated with the public key included in the certificate (and cease using the private key),

(6) Use the certificate only for legal and authorized purposes, consistent with the HiPKI CP, this CPS and Subscriber Agreement, including only installing TLS/SSL certificates on servers accessible at the domain listed in the certificate and not using private keys in code signing certificates to sign malicious code that is downloaded without a user's consent, and

(7) Promptly cease using the certificate and related private key after the certificate's expiration.

9.6.4. Relying Party Representations and Warranties

Each relying party represents and warrants to:

(1) Comply with the provisions of this CPS when using a certificate or inquiring the HiPKI EV TLS CA repository;

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

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

(4) Validate a certificate (issued by HiPKI EV TLS CA) by using a CRL or OCSP published by HiPKI EV TLS CA in accordance with the proper certificate path validation procedure;

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

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

(7) Have understood and agreed to the legal liability clauses of HiPKI EV TLS CA and will use the certificate in accordance with Section 1.4.1 when accepting the certificate.

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

9.6.5. Representations and Warranties of Other Participants

No stipulation.

9.7. Disclaimers of Warranties

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

9.8. Limitations of Liability

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

9.9. Indemnities

9.9.1. Indemnification by HiPKI EV TLS CA

If subscribers or relying parties suffer damages due to intentional or unintentional failure of HiPKI EV TLS CA work personnel to follow the HiPKI CP, this CPS, EV SSL Certificate Guidelines, relevant laws and regulations or the provisions of contracts signed between HiPKI EV TLS CA and subscribers/relying parties when processing subscriber certificate-related work, CHT shall be held liable. Subscribers may claim compensation for damages based on the related provisions of the contract set down between HiPKI EV TLS CA (or its RA) and subscribers. Relying parties shall request compensation in accordance with relevant laws and regulations. The financial liability of CHT 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 of CHT complies with the EV SSL Certificate Guidelines.

9.9.2. Indemnification by RA

The RA is set up by CHT. If subscribers or relying parties suffer damages due to the RA intentional or unintentional failure to follow this CPS, related laws and regulations or the provisions of contracts signed between the RA and subscribers/relying parties when processing subscriber certificates registrations, CHT shall be held liable. Compensation limits for the RA are detailed in Section 9.9.1. If the RA and subscribers or relying parties have a contract determing the usage of certificates and transaction compensation amounts, then the contract takes precedence. Compensation

claims by subscribers shall be made in accordance with related provisions in the contract set down with the RA. Compensation claims by relying parties shall be made in accordance with relevant laws and regulations.

9.10. Term and Termination

9.10.1. Term

This CPS and any amendments are effective when approved by the Electronic Signatures Act competent authority and published to the HiPKI EV TLS CA website and repository. This CPS remains effective until replaced with a newer version.

9.10.2. Termination

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

9.10.3. Effect of Termination and Survival

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

9.11. Individual Notices and Communications with Participants

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

9.12. Amendments

9.12.1. Procedure for Amendment

This CPS is reviewed annually, and an assessment is made to

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

9.12.2. Notification Mechanism and Period

HiPKI EV TLS CA will post appropriate notice on its websites of any major or significant changes to this CPS as well as any appropriate period by when the revised CPS becomes effective. If subscribers or relying parties have any comment on the change items, they can submit the comment within the comment period. Reassess to the changes and response may or may not be made by HiPKI EV TLS CA according to these comments.

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

9.12.3. Circumstances under which OID Must Be Changed

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

9.13. Dispute Resolution Provisions

In the event of a dispute between subscribers or RAs and HiPKI EV TLS CA, 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 HiPKI EV TLS CA issued certificates, the applicable ROC laws and regulations shall govern.

9.15. Compliance with Applicable Law

Related ROC laws and regulations must be followed regarding the interpretation and legality of any agreement signed based on this CPS.

9.16. Miscellaneous Provisions

9.16.1. Entire Agreement

The commitments set forth in this CPS constitute the entire agreement between the participants (HiPKI EV TLS CA, RAs, subscribers and relying parties) and supersedes all prior verbal or written representations between the parties on the same matters.

9.16.2. Assignment

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

9.16.3. Severability

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

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

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

In the event that HiPKI EV TLS CA suffers damages attributable to

an intentional or unintentional violation of this CPS by a subscriber or relying party, HiPKI EV TLS CA may seek compensation for damages and indemnification and attorneys' fees related to the dispute or litigation from the responsible party.

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

9.16.5. Force Majeure

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

9.17. Other Provisions

No stipulation.