HiPKI Root Certification Authority

Certification Practice Statement

Version 1.17

Chunghwa Telecom Co., Ltd.

June 16, 2022

Contents

Document History

Version	Release Date	Revision Summary
1.0	February 22, 2019	First Release.
1.05	March 2, 2020	(1) Amendments are made on Sections 1.5.2.1, 3.2.5, 4.9.9, 4.9.10 and 9.6 and Section 3.2.7 is added according to BR v1.6.7 and actual condition; (2) Amendments are made on Sections 7.1.2, 7.15 and 7.1.8 regarding the description of EKU field and certificatePolicies extension fields to reflect the revision of Mozilla Root Store Policy v2.7; and (3) Amendments are made on Sections 1.6.1, 4.9.11, 5.3.3, 5.5.2, 5.7.1, 6.1.1, 6.1.6, 6.1.7, 6.3.2, 6.6.2, 7.1.3, 7.1.4, 7.1.6, 7.3.1 and 9.2.2.
1.1	July 2, 2020	Amendments are made on Sections 1.3.3, 1.3.4, 1.4.2, 1.5.4, 1.6.1, 4.1.2.1, 4.2.1.1, 4.4.2 and 7.1.4.
1.15	April 13, 2021	Amendments are made on Sections 1.4.1, 2.3, 2.4, 3.2.2, 3.2.3, 3.2.5, 4.5.1, 4.5.2, 4.9.6, 4.10.1, 4.10.2, 6.1.5, 6.1.6, 6.2.6, 6.3.2, 6.6.1, 6.6.2, 6.6.3, 6.8, 7.1.2, 7.1.3, 7.1.4, 7.1.6, 7.1.7, 7.1.9, 7.2.2, 7.3.1, 8.1, 8.4, 9.4.2, 9.10, 9.16.1 and 9.16.5 in compliance with the Baseline Requirements and our current practice.
1.16	June 17, 2021	(1) Delete the descriptions/regulations related to individuals, time stamp, Code Signing and EV Code Signing certificates in compliance with the Google Chrome Root Program Transition. (become a pure TLS Root CA/PKI). (2) Amendments are made on Sections 1.1.1, 1.2, 1.3.5, 1.6.1, 1.6.2, 3.1.2, 3.2.2, 3.2.3, 3.2.4, 4.5.2, 4.6, 4.9.10, 4.9.12, 6.3.2, 6.3.2.2, 6.3.2.3, 6.6.1, 6.6.2, 6.7, 7.1.2, 7.1.4, 7.2.2, 9.5, 9.6.1 and 9.12.1.
1.17	June 16, 2022	Amendments are made on Sections 4.5.2, 5.1.1, 5.2.2, 6.6.2 and 7.3.2.

1. Introduction

1.1. Overview

1.1.1. Certification Practice Statement

The HiPKI Root Certification Authority (HiPKI RCA) 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 a Subordinate CA of HiPKI RCA should include in its CPS.

This CPS mainly describes how HiPKI RCA performs the issuance and management of self-signed certificates, self-issued certificates, subordinate CA certificates, and cross-certificates in accordance with the assurance level 4 defined in the HiPKI CP.

According to the HiPKI CP, 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.

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.

According to ITU-T X.509, the assurance levels defined in the HiPKI CP must be expressed with CP object identifiers (OIDs, see Section 1.2), which will be listed in the certificatePolicies extension of certificates.

Assurance levels imply the degree of trust regarding the following terms for a relying party:

(1) There are two types of certificates issued by CAs, one is end entity (EE) certificates, and the other is CA certificates. For an EE certificate, it has only one CP OID which indicates the assurance level that the certificate is followed for identity authentication and issuance when applying; for a CA certificate, there may be one or more CP OIDs which means the CA is able to issue certificates met the assurance levels of these CP OIDs to EEs. Certificates issued to CAs may contain a subset of these OIDs;

(2) The CA-related operating procedures, including certificate issuance and administration and private key delivery; and

(3) The ability of the subscriber or subject described in the certificate to effectively control the private key corresponding to the public key listed in the certificate, e.g., storing the private key with software or hardware by the subscriber. In other words, whether the binding relationship between the subject and the public key can be trusted by the relying party.

CAs in HiPKI shall include appropriate CP OIDs when issuing certificates, where policy mapping can be confirmed if the issuing CA and subject CA have included the same CP OID.

1.1.2. CPS Applicability

The practice statement stipulated in this CPS applies to HiPKI RCA related entities, including HiPKI RCA, subordinate CAs, cross-certified CAs, and relying parties.

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

1.2. Document Name and Identification

This document is HiPKI RCA Certification Practice Statement, the current version of this CPS can be obtained at the website: https://eca.hinet.net. CAs in HiPKI is authorized to issue the following certificates:

(1) Domain validation (DV) TLS/SSL certificates

(2) Organization validation (OV) TLS/SSL certificates

(3) Extended validation (EV) TLS/SSL certificates

HiPKI classifies the certificates issued by CAs into four assurance levels according to the authentication method and appropriate scope implemented by the CAs. The high the assurance level, the higher the security, reliability, and the more strict the authentication method.

The certificate policy that the issued certificates followed must be listed in the certificatePolicies extension of those certificates except self-signed certificates. The following OIDs are reserved for use by CAs as an optional means of asserting compliance with various certificates and documents described in the HiPKI CP and this CPS.

Object Name	OIDs
HiPKI CP document	1 3 6 1 4 1 23459 200 0
Assurance levels	
Level 1	1 3 6 1 4 1 23459 200 0 1
Level 2	1 3 6 1 4 1 23459 200 0 2
Level 3	1 3 6 1 4 1 23459 200 0 3
Level 4	1 3 6 1 4 1 23459 200 0 4
Baseline Requirements	
DV TLS/SSL certificates	2.23.140.1.2.1
OV TLS/SSL certificates	2.23.140.1.2.2
EV SSL Certificate Guidelines	
EV TLS/SSL certificates	2.23.140.1.1 (EV SSL Certificate Guidelines)

OIDs with a prefix of {2.23.140} are required by CA/Browser Forum; where OID {2.23.140.1.2} indicates the Baseline Requirements and OID {2.23.140.1} indicates the EV SSL Certificate Guidelines. The arc id-pen-cht ::= {1 3 6 1 4 1 23459} is a private enterprise number (PEN) registered in IANA by Chunghwa Telecom Co., Ltd (CHT). The OID for HiPKI is {1 3 6 1 4 1 23459 200}, which has been quoted to the OIDs of various assurance levels.

If the EV TLS/SSL certificates issued by subordinate CAs conform to the EV SSL Certificate Guidelines and the individually negotiated certificate processing methods supported by application software suppliers (such as browsers or application system providers), the certificates of both subordinate CA and its subscribers are allowed to use the 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)) for EV TLS/SSL certificates defined by the CA/Browser Forum.

Regarding TLS/SSL certificates, if there is any inconsistency between this CPS and the Baseline Requirements, then the Baseline Requirements takes precedence. Regarding EV TLS/SSL certificates, if there is any inconsistency between this CPS and the EV SSL Certificate Guidelines, then the EV SSL Certificate Guidelines takes precedence.

1.3. PKI Participants

The participants of HiPKI RCA include:

(1) HiPKI RCA,

(2) Subordinate CAs,

(3) Cross-certified CAs, and

(4) Relying Parties.

1.3.1. Certification Authorities

1.3.1.1. HiPKI RCA

HiPKI RCA is a Root CA as well as being a principal CA in HiPKI. HiPKI RCA is established and operated by CHT and is responsible for:

(1) Issuing and administrating certificates issued by HiPKI RCA, including self-signed, self-issued and Subordinate CA certificates.

(2) Establishing the cross-certification procedures between HiPKI RCA and any Root CA outside HiPKI, including issuance and administration of the cross-certificates.

(3) Publishing the newly issued certification authority revocation lists (CARLs) to the repository and ensure that the repository operates regularly.

1.3.1.2. Subordinate CA

A Subordinate CA is another form of CA in HiPKI responsible for the issuance and administration of EE certificates. When necessary, the

hierarchy of the Subordinate CA can be extended to multiple levels, i.e., a level 1 Subordinate CA can issue certificates to a level 2 Subordinate CA, or a level 2 Subordinate CA can issue certificates to a level 3 Subordinate CA and so on. However, any Subordinate CA is not allowed to cross-certify with any CA outside HiPKI directly.

Subordinate CAs shall be established in accordance with the HiPKI CP, and a contact window is required responsible for the interoperation with HiPKI RCA and other Subordinate CAs.

Currently, HiPKI has only one Subordinate CA, namely HiPKI EV TLS CA, which is operated by CHT.

1.3.1.3. Cross-Certified CA

A cross-certified CA refers to a CA which is a root CA outside HiPKI that performs cross-certification with HiPKI RCA. Any root CA, which wishes to apply for cross-certification with HiPKI RCA, must conform to the certificate policy assurance level asserted in its certificate, possess the establishment and management capabilities of the PKI, digital signature, and certificate issuance technology, determine related responsibilities and obligations for CA, registration authority (RA), and relying parties, and pass external audits equivalent in strength to HiPKI.

1.3.2. Registration Authorities

HiPKI RCA directly accepts certificate registration and revocation requests and is responsible for collecting and verifying the identity and certificate-related information of Subordinate CAs and cross-certified CAs. There is no need to set up a RA.

1.3.3. Subscribers

A subscriber is the certificate subject not capable of issuing

certificates and is the entity possessing the private key that corresponds with the certificate's public key. A Root CA, subordinate CA or cross-certified CA is not called "subscriber" in the HiPKI CP and this CPS because they are capable of issuing certificates.

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) Verify the integrity of a digitally signed electronic document,

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

(3) Establish confidential communications with the certificate subject.

1.3.5. Other Participants

If HiPKI RCA selects other related authorities, such as a bridge CA or data archiving service authority, 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 RCA.

1.4. Certificate Usage

1.4.1. Appropriate Certificate Uses

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

A self-signed certificate is used to establish the trust anchor of HiPKI.

A self-issued certificate is used for HiPKI RCA certificate re-keying or certificate policy mapping between trust paths. A subordinate CA certificate is used to establish mutual trust relationships between CAs under the same PKI to construct the certificate trust path needed for the interoperability. A cross-certificate is used to establish a mutual trust relationship between root CAs under different PKIs to construct the certificate trust path needed for the interoperability.

The issuance subject of the self-signed certificate is HiPKI RCA itself. The self-signed certificate contains HiPKI RCA public key which can be used to verify the digital signatures on subordinate CA certificates, cross-certificates, self-issued certificates and CARLs issued by HiPKI RCA.

The issuance subject of the subordinate CA certificate is subordinate CAs established under HiPKI. The subordinate CA certificate contains the subordinate CA public key which can be used to verify the digital signatures on certificates and certification revocation lists (CRLs) issued by the subordinate CA.

The issuance subject of the cross-certificates is a root CA which is established under another PKI and cross-certifies with HiPKI RCA. The cross-certificate contains the cross-certified CA public key which can be used to verify the digital signatures on certificates and CARLs issued by the root CA.

Relying parties shall obtain the trusted HiPKI RCA public keys or self-signed certificates via one of the secure distribution channels described in Section 6.1.4. The self-signed certificate contains HiPKI RCA public key which can be used to verify the digital signatures of self-issued certificates, subordinate CA certificates, cross-certificates and CARLs issued by HiPKI RCA.

Relying parties shall carefully select a secure computer environment

and trusted application systems to prevent the HiPKI RCA public keys or self-issued certificates from being damaged or replaced. This can ensure use of the correct HiPKI RCA public key or self-signed certificate as to verify the digital signatures of self-issued certificates, subordinate CA certificates, cross-certificates and CARLs issued by HiPKI RCA.

The type of assurance level that a subordinate CA can issue is listed in the subordinate CA certificate issued by HiPKI RCA. Relying parties can decide whether to trust the subordinate CA and its certificate.

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

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

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

1.4.2. Prohibited Certificate Uses

Certificates issued under this CPS are prohibited from being used in the scope of:

(1) Crime,

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

(3) Operation of nuclear equipment, 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 Root 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://eca.hinet.net.

1.5.2.2. Certificate Problem Report

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

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

1.5.3. Person Determining CPS suitability for the Policy

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

1.5.4. CPS Approval Procedures

This CPS is published by HiPKI RCA 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.
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.
Audit Data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event.
Authenticate	To confirm the identity of an entity when that

Term	Definition
	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.
Backup	Copy of files and programs made to facilitate recovery if necessary.
Binding	Process of associating two related information elements.
Biometrics	A physical or behavioral characteristic of a human being.
CA Certificate	Certificates that is issued to certification authorities.
Capability Maturity Model Integration (CMMI)	CMMI is the successor of the Capability Maturity Model (CMM) and was developed by the Software Engineering Institute at Carnegie Mellon University. CMMI models provide guidance for developing or improving processes that meet the business goals of an organization. Its purpose is to help improve organizational performance.

Term	Definition
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.
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 Revocation List (CARL)	A regularly updated list that contains the information of revoked CA certificates, which can be the self-issued certificates, subordinate CA certificates or cross-certificates, together with the revoked time and reason. The list is available to relying parties and is digitally signed by the root CA that issued the CA certificates within the validity of the CA certificates to provide integrity and non-repudiation.
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]

Term	Definition
	(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 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.

Term	Definition
Certificate Problem Report	A report on suspected private key compromise, certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to certificates.
Certificate Revocation List (CRL)	A regularly updated list of revoked certificates that is created and digitally signed by the CA that issued the certificates. The list contains the certificates that the issuing CA has issued that are revoked prior to their stated expiration date.
Certificate Transparency (CT)	CT is an open platform for the public monitoring and auditing of all certificates on the Internet (TLS/SSL certificate is the priority objective at the current stage). It provides related information of issued certificates to domain owners, CA, and domain subscribers to determine whether any certificate has been issued improperly. In other words, CT provides a public monitoring and information disclosure environment which can be used to monitor all issuance mechanisms of CAs that issue TLS/SSL certificates and to review 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,

Term	Definition
	destruction, or loss of an object may have occurred.
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes.
Cross-certificate	A certificate that is used to establish a trust relationship between two root CAs. The certificate is a type of CA certificates and not a subscriber certificate.
Cross-Certification Agreement (CCA)	An agreement between a root CA and cross-certified CAs that includes the items and individual liability and obligation which must be followed during the period of joining the PKI where the root CA is established.
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.
Data Integrity	Assurance that the data are unchanged from creation to reception.
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 Name	The label assigned to a node in the domain name system, i.e., translates an IP address into a text name that is easily remembered.
Domain Name System (DNS)	An Internet service that translates domain names into IP addresses.
Domain Validation (DV)	Prior to issuance of a DV TLS/SSL certificate, only a subscriber's ownership or control of the domain is validated, but identification or authentication of the subscriber's affiliate or identity is exclude from the validation. Therefore, anyone links to a website installed

Term	Definition
	a DV TLS/SSL certificate can get a TLS encryption channel but knows nothing about who owns the website.
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.
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.
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

Term	Definition
	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.
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.
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.
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.
Key Compromise	A private key is said to be compromised if its value has been disclosed to an unauthorized

Term	Definition
	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.
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

Term	Definition
	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.

Term	Definition
	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.
Organization Validation (OV)	Prior to issuance of an OV TLS/SSL certificate, not only a subscriber's ownership or control of the domain is validated, but also identification or authentication of the subscriber's affiliate or identity is made according to the assurance level of the certificate. Therefore, anyone links to a website installed an OV TLS/SSL certificate can get a TLS encryption channel and know who owns the website that provides integrity of data transmission.
Out-of-Band	A communication method (between parties) that differs from the current on-line methods and can be regarded as a special secure channel, e.g., one party uses physical registered mail to communicate with another party.
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.
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 Infrastructure (PKI)	A set of law, policy, rules, people, equipment, facilities, technology, processes, audits, and

Term	Definition
	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.
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.
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 this CP.
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

Term	Definition
Root Certification Authority (Root CA)	The top-level certification authority in a hierarchical PKI that issues subordinate CA certificates and self-signed certificates.
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.
Self-issued Certificate	Self-issued certificates may be generated to implement a key change-over or to support changes in policy. The certificates, including the old-with-new certificate, new-with-old certificate and new-with-new certificate, are signed by the root CA with new/old private keys to establish a trusted path between the old and new keys or the certificate policies.
Self-signed Certificate	(1) Self-issued certificates are CA certificates in which the issuer and subject are the same entity. In other words, it is a certificate containing the corresponding public key or other information signed with the private key. (2) A self-signed certificate in a PKI may serve as a trust anchor for a certification path. The subject of certificate is the root CA itself. (3) Self-issued certificates can be used by

Term	Definition
	relying parties to validate the self-issued certificates, subordinate CA certificates, cross-certificates and CARLs issued by a root CA.
Signature Certificate	A public key certificate contains a public key used for verifying a digital signature (not used for data encryption or other cryptographic uses).
Subject CA	In the context of a particular CA certificate, the subject CA is the CA whose subject is certified in the certificate.
Subordinate CA	In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA.
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

Term	Definition
	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]
WebTrust	The current version of CPA Canada's WebTrust Program(s) for Certification Authorities.
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
CARL	Certification Authority Revocation List	See Section 1.6.1
CCA	Cross Certification Agreement	See Section 1.6.1
CMMI	Capability Maturity Model Integration	See Section 1.6.1
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	See Section 1.6.1
DNS	Domain Name System,	See Section 1.6.1
DV	Domain Validation	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	See Section 1.6.1
OID	Object Identifier	See Section 1.6.1
OV	Organization Validation	See Section 1.6.1

Acronyms	Full Name	Definition
PIN	Personal Identification Number	
PKCS	Public Key Cryptography Standards	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

2. Publication and Repository Responsibilities

2.1. Repositories

The repository, under the management of HiPKI RCA, publishes HiPKI RCA issued certificates, CARLs and other certificate-related information and provides 24-hour round-the-clock service. The website of the HiPKI RCA repository is at http://eca.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 RCA 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) Self-signed certificates of HiPKI RCA,
(4) Self-issued certificates cross-signed with HiPKI RCA's old and new keys,
(5) Subordinate CA certificates,
(6) Cross-certificates,
(7) Privacy protection policy,
(8) The last result of the external audit (as specified in Section 8.6), and
(9) Related latest news.

Furthermore, if the subordinate CAs under HiPKI RCA or the subordinate CAs chain up to cross-certified CAs that cross certify with HiPKI RCA provide the TLS/SSL certificates issuance service, HiPKI RCA will require the issuing CA to publish three TLS/SSL certificate website URLs to the application software suppliers which are used for valid,

revoked, and expired TLS/SSL certificates, respectively. The application software suppliers can therefore test whether their software is able to use that TLS/SSL certificates to chain up to the self-signed certificate of HiPKI RCA.

2.3. Timing or Frequency of Publication

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

(2) New or modified version of the HiPKI CP complied with by HiPKI RCA is published in the repository as soon as possible upon the approval of the PMA;

(3) HiPKI RCA issues CARLs at least twice a day and publishes CARLs in the repository; and

(4) Self-signed certificates, self-issued certificates, cross-certificates and subordinate CA certificates are published in the repository within seven calendar days upon issuance and receipt of the certificates.

2.4. Access Controls on Repositories

There is no network connection between the HiPKI RCA host and repository server. Therefore, the certificates and CARLs issued by the HiPKI RCA host cannot be transmitted directly to the repository server via network. When HiPKI RCA wants to publish the issued certificates and CARLs, HiPKI RCA personnel store the certificates and CARLs that need to be published on portable media and then copy the files to the repository server offline manually for publication.

The information published by HiPKI RCA as described in Section 2.2 is primarily provided for inquiring by subordinate CAs, cross-certified CAs and relying parties. HiPKI RCA implements access control where it provides only viewing access to prevent anyone from unauthorized writing operation which would put repository security in risk.

3. Identification and Authentication

3.1. Naming

3.1.1. Types of Names

The subject distinguished name of the certificate issued by HiPKI RCA conforms to the distinguished name (DN) of ITU-T X.500. Self-signed certificates, self-issued certificates, subordinate CA certificates issued to subordinate CAs, and cross-certificates issued to cross-certified CAs use the distinguished name format.

3.1.2. Need for Names to be Meaningful

The naming of subject names of organizations applying to become subordinate CAs or cross-certified CAs shall comply with the Baseline Requirements and conform to the regulations under the Jurisdiction country's law of the applicant organization.

3.1.3. Anonymity or Pseudonymity of Subscribers

Not applicable for CA certificates issued by HiPKI RCA.

3.1.4. Rules for Interpreting Various Name Forms

Rules for interpreting various name forms should comply with the name attribute definition of ITU-T X.520.

3.1.5. Uniqueness of Names

HiPKI RCA examines the uniqueness of the CA names applying to become a subordinate CA and cross-certified CA. If a duplicate name is found, the applying CA is required to change the name. CHT shall handle disputes regarding naming rights.

The self-signed certificate of HiPKI RCA uses the following name form:

C = TW,

O = Chunghwa Telecom Co., Ltd.,

CN = HiPKI Root CA - Gn, where n = 1, 2, 3….

Moreover, for the self-signed certificate issued by HiPKI RCA, its issuer content is identical to the subject content.

3.1.6. Recognition, Authentication, and Role of Trademarks

The certificate subject name provided by subordinate CAs and cross-certified CAs includes the trademark or any legally protected name, trade name, business name or symbol, HiPKI RCA is not responsible for their examination but their names must conform to the Trademark Act, Fair Trade Act and other relevant regulations in Taiwan. HiPKI RCA does not guarantee the approval, verification, legality or uniqueness of the trademark including in the certificate subject name. Relevant disputes or arbitrations related to the trademark shall not be the obligation of HiPKI RCA. Instead, the subordinate CA and cross-certified CA shall submit applications to relevant competent authorities or courts.

3.2. Initial Identity Validation

3.2.1. Method to Prove Possession of Private Key

When a CA applies for a certificate, HiPKI RCA checks if the CA’s private key and public key listed in the certificate form a pair. One PKCS#10 Certificate Signing Request file is generated by the CA and HiPKI RCA uses the CA’s public key to check the signature to prove the CA possesses the corresponding private key.

3.2.2. Authentication of Organization Identity

When a CA self-established by CHT becomes a subordinate CA (e.g., HiPKI EV TLS CA), the identity authentication is reviewed by a PMA meeting convened by CHT.

For cross-certificate application submitted by CA not self-established by CHT, the application shall include the organization name, locality, representative and other information which is sufficient to identify the organization. HiPKI RCA shall confirm the existence of the organization as well as the authenticity of the application, representative identity and the representative's authority to represent the organization. The representative is required to apply for the certificate in person.

If the usage of the certificate issued by a subordinate CA is for encrypted transmission of TLS server, the subordinate CA shall validate the domain authorization or control of each fully qualified domain name (FQDN) listed in the TLS/SSL certificate the applicant requested prior to issuance. If the subject identity information is to include the name or address of an organization, the subordinate CA shall authenticate the identity and address of the organization and that the address is the applicant’s address of existence or operation. If the TLS/SSL certificate is for organization validation (OV), the documentation provided by, or through communication with, the reliable sources described in Section 3.2.2.1 of the Baseline Requirements may be used for verification; if the TLS/SSL certificate is for extended validation (EV), the subordinate CA shall authenticate the subject identity information in accordance with the EV SSL Certificate Guidelines.

3.2.3. Authentication of Individual Identity

Not applicable for CA established by CHT. For CA not established by

CHT, CA certificates must be applied by representatives (individuals authorized to submit cross-certificate applications) appointed by official document. When applying for a CA certificate, the representative shall present the relevant identity documents (e.g., a ROC ID or passport) by which HiPKI RCA can authenticate the identity and the authorization of the representative.

Subordinate CAs under HiPKI RCA do not issue certificate to individuals.

3.2.4. Non-validated Subscriber Information

All information to be listed in the certificates must be verified.

3.2.5. Validation of Authority

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

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

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

3.2.6. Criteria for Interoperation

HiPKI RCA does not sign a Cross Certification Agreement with any root CA of other PKIs currently.

3.2.7. Data Source Accuracy

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

3.3. Identification and Authentication for Re-key Requests

Certificate rekey is the issue of a new certificate of equivalent characteristics and assurance level as the old certificate and the new certificate not only has a new and different public key (corresponding to the new and different private key) and different serial numbers but also may be assigned a different validity period.

The subordinate CA or cross-certified CA should reapply for a certificate from HiPKI RCA when making a rekey request, HiPKI RCA shall follow the rules in Section 3.2.2 to identify and authenticate the CA reapplying for the certificate.

3.3.1. Identification and Authentication for Routine Re-Key

HiPKI RCA is not allowed to renew self-signed certificates, self-

issued certificates, subordinate CAs certificates, or cross-certificates. CAs shall re-establish their identity using the initial registration processes of Section 3.2.

3.3.2. Identification and Authentication for Re-key after Revocation

CAs whose certificate has been revoked shall re-establish its identity using the initial registration processes of Section 3.2.

3.4. Identification and Authentication for Revocation Request

The authentication procedure for HiPKI RCA self-signed certificates, subordinate CA certificates and cross-certificates revocation requests is the same as the rules in Section 3.2.2.

4. Certificate Life-cycle Operational Requirements

4.1. Certificate Application

4.1.1. Who Can Submit a Certificate Application

Certificate applicants include HiPKI RCA, any subordinate CA and any root CA outside HiPKI.

4.1.2. Enrollment Process and Responsibilities

4.1.2.1. HiPKI RCA Obligations

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

subordinate CAs, and

(13) Accept cross-certificate registration and revocation applications of cross-certified CAs.

4.1.2.2. Subordinate CA Obligations

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

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

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

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

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

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

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

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

(9) Revoke a subordinate CA certificate if a certificate revocation event of subordinate CA occurred as described in Section 4.9.1 (such as the disclosure or loss of private key information), and HiPKI RCA shall be notified immediately. However, the subordinate CA shall bear legal responsibility for use of that certificate prior to the notification or before the change has been made, and

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

4.1.2.3. Cross-Certified CA Obligations

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

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

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

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

(5) Acceptance of a cross-certificate issued by HiPKI RCA indicates that the cross-certified CA has checked the accuracy of the information contained in the certificate and may use the certificate

in accordance with Section 4.5,

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

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

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

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

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

4.2. Certificate Application Processing

Subordinate CAs at each level in HiPKI shall not accept other CA applications to become Subordinate CA unless permission is given by a superior CA.

A negotiation between the PMA and HiPKI RCA shall be conducted prior to the issuance of a cross-certificate issued by HiPKI RCA to a Root CA outside HiPKI.

4.2.1. Performing Identification and Authentication Functions

4.2.1.1. Initiation

(1) Initiation application

For CA established by CHT, CHT convenes a PMA meeting to review the PKCS#10 certificate application file and the validity period, the certificate subject name and other related information for the certificate to be issued. For CA not established by CHT, the cross-certificate application, CPS and PKCS#10 certificate application file must be submitted. If the CA follows a certificate policy other than the HiPKI CP, the certificate policy followed should be attached. For external subordinate CA or root CA under another PKI and is not established by CHT, an up-to-date point-in-time audit report and/or period-of-time audit report should be attached, and for CAs that issue TLS/SSL certificates should also attach the Baseline Requirement Assessment form.

(2) Identity identification and authentication

Follow the regulations in section 3.2.2 to perform the mutual authentication procedures for the applications between HiPKI RCA, subordinate CA or Cross-Certified CA.

(3) Perform the following checking procedure

Check the application to make sure there are no technical compatibility issues between the subordinate CA, cross-certified CA and HiPKI RCA for cross-certification.

If the CA applying for the cross-certificate follows a certificate policy other than the Certificate Policy for the Chunghwa Telecom ecommerce Public Key Infrastructure, check the corresponding relations between its certificate policy and the HiPKI CP.

Check if the CPS of the CA follows the certificate policy used by the CA.

Check the PKCS#10 application file submitted for the initialization application to make sure actual cross-certification work can be completed.

4.2.2. Approval or Rejection of Certificate Applications

4.2.2.1. Examination

A PMA meeting is convened to review the application when HiPKI RCA submits a self-signed certificate application.

A PMA meeting is convened to review the application when a CA submits a subordinate CA certificate application.

A PMA meeting is convened to review the related document information submitted by the CA and HiPKI RCA checking results when the CA submits a cross-certification application to determine the appropriateness of the CA and HiPKI RCA cross-certification. The PMA ultimately decides whether the application enters the next stage, supplemental information is required, or the application is rejected.

4.2.2.2. Arrangement

CAs established by CHT does not need to sign a Cross-Certification Agreement (CCA).

When a CA not established by CHT submits the cross-certificate application, a meeting is convened and the CA applying for cross-certification is notified to attend. The following steps are followed:

(1) Identity identification and authentication

Follow the regulations in Section 3.2.3 before the meeting starts to perform the identity identification and authentication procedure for

the representative of the CA applying for cross-certification.

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

(3) Determine if cross-certification is approved for CA applying for cross-certification. If approved, the CA applying for cross-certification signs the CCA.

(4) Enter the certificate issuance procedure.

4.2.3. Time to Process Certificate Applications

After the information submitted by the CA for the certificate application is determined to be complete, conforming to the certificate policy and HiPKI RCA CPS, technically compatible, HiPKI RCA compatible and passes the PMA meeting review, HiPKI RCA shall complete the certificate issuance within seven calendar days.

4.3. Certificate Issuance

4.3.1. CA Actions during Certificate Issuance

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

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

HiPKI RCA follows the PMA meeting approval results (meeting minutes) when deciding whether to issue subordinate CA certificates or cross-certified CA certificates.

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

If the certificate application is approved, the subordinate CA or the cross-certified CA is notified and HiPKI RCA performs the work related

to certificate issuance. After the certificate is issued, CHT shall notify the CA by letter and attach the issued certificate.

If certificate application is not approved, the subordinate CA or cross-certified CA which submitted the application is notified by letter and the reasons why the application was not approved are stated within.

4.4. Certificate Acceptance

4.4.1. Conduct Constituting Certificate Acceptance

After HiPKI RCA confirms the information on the self-signed certificate and self-issued certificate is free of errors, the internal issuance procedures are followed to publish the self-signed certificate and self-issued certificate in the repository.

After receiving notification of approval of their certificate application, the subordinate CA or the cross-certified CA must check the attached certificate to make sure the certificate contents are accurate. If there are no errors in the certificate, HiPKI RCA shall be notified. CA not established by CHT must sign a certificate acceptance confirmation document and reply by letter to CHT to complete the certificate acceptance procedure.

If the CA does not return the certificate acceptance confirmation document within 30 calendar days, it shall be deemed refusal of certificate acceptance. HiPKI RCA revokes that certificate and no publication is made.

4.4.2. Publication of the Certificate by the CA

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

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

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

If there are newly issued self-signed, self-issued, subordinate CA or cross certificates, HiPKI RCA will upload the related certificates to the Common CA Database (CCADB) in accordance with the root certificate program of operating systems, browsers and software platforms.

4.5. Key Pair and Certificate Usage

4.5.1. Subscriber Private Key and Certificate Usage

Key pairs of subscribers shall be generated in compliance with Section 6.1.1 of the HiPKI CP. Subscribers must be able to control the private keys corresponding to the public key of their certificates and do not issue certificates to others. Subscribers shall protect their private keys from unauthorized use or disclosure 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). Subscribers shall correctly use their certificates adhering to the certificate policies listed in the certificates.

4.5.2. Relying Party Public Key and Certificate Usage

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

Relying parties must verify the integrity of digital signature, the correctness of the content of specific fields, and certificate status information for each certificates in the certificate path to confirm the validity of the aforementioned certificate. After that, the TLS/SSL certificate in the certificate path can be used to authenticate the domain name of the server and the identity of the server owner and create an encrypted channel between the client and the server.

The above certificate status information can be obtained from the CARLs, CRLs, or OCSP services. The CARL and CRL download URLs can be obtained in the CRL distribution points (CDP) extension of certificates; the URL of the OCSP service can be obtained from the authority information access (AIA) extension of certificates. In addition, the relying parties shall check the certificate policies of the issuing CA certificate and TLS/SSL certificates that the CA issued to confirm the assurance level of the certificates.

4.6. Certificate Renewal

HiPKI does not allow renewal of CA certificates.

4.6.1. Circumstance for Certificate Renewal

Not applicable.

4.6.2. Who May Request Renewal

Not applicable.

4.6.3. Processing Certificate Renewal Requests

Not applicable.

4.6.4. Notification of New Certificate Issuance to Subscriber

Not applicable.

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

Not applicable.

4.6.6. Publication of the Renewal Certificate by the CA

Not applicable.

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

Not applicable.

4.7. Certificate Re-key

4.7.1. Circumstance for CA Certificate Re-key

Under the following three circumstances, the subordinate CA will renew the key and issue a new subordinate CA certificate:

(1) The lifecycle of currently used keys has ended.

(2) Security issues exist for currently used keys (such as suspected or confirmed key compromise).

(3) Security issues regarding the cryptographic algorithm or international protective measures eliminated in advance (such as the CA/Browser Forum's decision to phase out the use of the SHA-1 hash function algorithm in October 2014).

Under the following two circumstances, the Cross-Certified CA will renew the key and a new cross-certificate shall be issued by HiPKI RCA:

(1) The lifecycle of currently used keys has ended.

(2) Security issues exist for currently used keys (such as suspected or confirmed key compromise).

Private keys of Subordinate CAs shall be regularly renewed in accordance with Section 6.3.2. After certificate re-keyed, subordinate CAs shall request new certificates from HiPKI RCA in accordance with Sections 4.1 and 4.2.

Private keys of cross-certified CAs shall be regularly renewed in accordance with Section 6.3.2. After certificate re-keyed, cross-certified CAs shall request new certificates from HiPKI RCA in accordance with Sections 4.1 and 4.2.

For the CA which issue assurance level 2, 3 and 4 certificates, if its certificate has not been revoked, HiPKI RCA can start to accept its rekey and apply for a new certificate one month before the CA private key usage period expires. Follow the regulations in Section 4.2 for the new certificate application procedure.

CAs can submit new certificate applications to HiPKI RCA prior to the expiry of the operational period of their CA private keys used for issuing subscriber certificates, where there are international protective security measures or other matters approved by the PMA.

4.7.2. Who May Request Certification of a New Public Key

Applications may be submitted by subordinate CAs or any root CA outside HiPKI.

4.7.3. Processing Certificate Re-keying Requests

For CA certificate re-keying, the CA shall submit a new certificate application to HiPKI RCA. 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 CAs

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

As stated in Section 4.4.3.

4.8. Certificate Modification

4.8.1. Circumstance for Certificate Modification

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

4.8.2. Who May Request Certificate Modification

Certificate applicants include HiPKI RCA, subordinate CA or root CA outside HiPKI.

4.8.3. Processing Certificate Modification Requests

As stated in Section 4.2.

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

No stipulation.

4.9. Certificate Revocation and Suspension

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

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

4.9.1. Circumstances for Revocation

HiPKI RCA must submit a certificate revocation request under (but not limited to) the following circumstances:

(1) Suspected or confirmed private key compromise including disclosure or loss of private key information.
(2) Certificate is no longer needed for use including termination of HiPKI RCA services.

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

(1) The Subordinate CA or cross-certified CA requests revocation in writing;
(2) The Subordinate CA or cross-certified CA notifies the issuing CA that the original certificate request was not authorized and does not retroactively grant authorization;
(3) HiPKI RCA obtains evidence that the Subordinate CA or cross-

certified CA's private key corresponding to the public key in the certificate suffered a key compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6;

(4) HiPKI RCA obtains evidence that the certificate was misused;

(5) HiPKI RCA is made aware that the certificate was not issued in accordance with or that Subordinate CA or cross-certified CA has not complied with the HiPKI CP or this CPS;

(6) HiPKI RCA determines that any of the information appearing in the certificate is inaccurate or misleading;

(7) The Subordinate CA or cross-certified CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the certificate;

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

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

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

4.9.2. Who Can Request Revocation

Subordinate CAs or cross-certified CAs may request revocation of their certificates to HiPKI RCA.

Additionally, relying parties, application software suppliers, and other third parties may submit certificate problem reports informing HiPKI RCA

of reasonable cause to revoke the certificate. After receiving the certificate problem reports, HiPKI RCA will decide whether the revocation request is accepted in accordance with the principles described in Section 4.9.5.

4.9.3. Procedure for Revocation Request

4.9.3.1. Initiation

(1) Initiation request

Request shall be made by letter with the certificate revocation request form attached.

(2) Identity identification and authentication

Identity identification and authentication of HiPKI RCA, subordinate CA or Cross-Certified CA shall be carried out in accordance with Section 3.2.2.

(3) Request review

The related information on submitted document is reviewed to determine the appropriateness of the certificate revocation request.

(4) Determination

Determine whether to enter the next stage, ask for supporting documents or notify the subordinate CA or Cross-Certified CA by official letter of the denial of the revocation request. The reasons for the denial shall be stated.

4.9.3.2. Certificate Revocation

HiPKI RCA adds the revoked certificate to the CARL and posts the CARL in the repository before the next CARL posting at the latest. The subordinate CA or Cross-Certified CA is notified by letter after the certificate revocation. The certificate status information posted in the repository includes revoked certificates until the certificates expire.

4.9.3.3. Responding Mechanism to Certificate Problems

HiPKI RCA provides the instruction and guidelines for certificate problem report. CAs, application software suppliers, relying parties, and other third parties may visit the HiPKI RCA website to obtain the instructions/guidelines for certificate problem report; and report the certificate problems to HiPKI RCA accordingly.

4.9.4. Revocation Request Grace Period

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

If any of the circumstances described in Section 4.9.1, HiPKI RCA can revoke the certificates on its discretion without the prior consents from the subordinate CAs or cross-certified CAs. HiPKI RCA may request the revocation of the certificate once the reason of revocation is confirmed, and then inform the subordinate CAs or cross-certified CAs.

4.9.5. Time within Which CA Must Process the Revocation Request

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

After reviewing the facts and circumstances, HiPKI RCA shall work with CAs and any entity reporting the Certificate Problem Report or other revocation-related notice to establish whether or not the certificate will be revoked, and if so, the period from receipt of the Certificate Problem

Report or revocation-related notice to published revocation must not exceed the time frame set forth in Section 4.9.1. The date selected by HiPKI RCA shall consider the following criteria:

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

4.9.6. Revocation Checking Requirements for Relying Parties

Before using the subordinate CA certificates, cross-certificates, or self-issued certificates issued by HiPKI RCA, relying parties shall verify the validity of these certificates using CARLs or OCSP responses published by HiPKI RCA. The relying parties shall also check the authenticity, integrity, and validity of the signatures of the CARLs or OCSP responses before using them. The following is illustrated by the example of the use of CARLs:

- Relying parties shall check if the content of issuer distinguished name field of CARLs matches the subject distinguished name of the self-signed certificate of HiPKI RCA.
- The relying parties shall use the public key listed in the self-signed certificate of HiPKI RCA to verify the signature of the CARLs.
- The relying parties shall check if the CARL is the latest version. The update time of the CARL is listed in the “thisUpdate” field on the CARL and the “nextUpdate” field specifies the expected time for the next update by HiPKI RCA. When the relying parties

verify the CARL, if they find the system time (which shall be calibrated regularly) is later than the next update time of the CARL, it means the CARL is not the most updated one. The relying parties shall download the latest CARL in the repository.

- In case of verifying the old data (e.g. the archived data), the relying parties shall check if the CARL used at the time the data were generated was valid at that time.

4.9.7. CARL Issuance Frequency

CARLs are issued at least twice per day, and the CARL shall expire within 36 hours. The updated CARLs are published in the repository. Because HiPKI RCA may issue the new CARL before the old one expires, the effective period of new CARL may overlap with the old one. During the overlapped period, the new CARL is available at the HiPKI RCA repository before the old one expires, for the relying parties to obtain the most updated CA revocation information.

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

4.9.8. Maximum Latency for CRLs

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

4.9.9. On-line Revocation/Status Checking Availability

HiPKI RCA provides CARLs and OCSP services for certificate status checking.

HiPKI RCA provides the OCSP responses, complying with RFC 6960 and RFC 5019, by OCSP responders. HiPKI RCA uses the private signing

key to issue the OCSP responder certificates with the security strength at least RSA 2048 w/SHA-256 with which the relying parties can verify the digital signature of the OCSP responses and confirm the integrity and reliability of the information sources. The certificates of the OCSP responders shall include the extension “id-pkix-ocsp-nocheck” meeting the specification of RFC 6960.

4.9.10. On-line Revocation Checking Requirements

If the relying party is unable to use the CARL in accordance with Section 4.9.6 to check if the certificate used is valid or not, OCSP services as described in Section 4.9.9 shall be used.

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

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

RCA may provide responses for OCSP requests with “assigned” or “unused” certificate serial numbers.

If the OCSP responder receives a request for the status of a certificate serial number that is “assigned”, the responder shall respond with the status at that time of the certificate assigned with that serial number. If the OCSP responder receives a request for the status of a certificate serial number that is “unused”, the responder shall not respond with a "good" status. HiPKI RCA 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 TLS/SSL certificates status of high-traffic websites, HiPKI RCA supports the operation of OCSP stapling.

4.9.12. Special Requirements Related to Key Compromise

In case of a compromise of the subordinate CA or cross-certified CA’s private key, the subordinate CA or cross-certified CA must immediately notify HiPKI RCA of the event. HiPKI RCA will revoke the concerned certificate (choose the reason for the revocation as ‘key compromised’) according to the procedures set forth in Sections 4.9.1, 4.9.2 and 4.9.3 of this CPS, and publish a certification authority revocation list (CARL) to inform relying parties that the certificate can no longer be trusted.

In case of a compromise of HiPKI RCA’s private key, HiPKI RCA will inform software suppliers, subscribers, and relying parties about the private key compromise event.

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

(1) Confirming the third party's possession of the private key by signing a challenge provided by HiPKI RCA using the compromised private key.

(2) Submitting the private key itself.

4.9.13. Circumstances for Suspension

Certificate suspension services are not provided.

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 RCA provides CARLs and OCSP services. The CARL download URL is noted in the CRL distribution points extension of self-issued certificates, subordinate CA certificates, and cross-certificates.

Revocation entries on the CARLs or OCSP responses must not be removed before the validity period of the revoked certificates.

4.10.2. Service Availability

HiPKI RCA operates and maintains its CARL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

HiPKI RCA maintains an online 24x7 uninterrupted repository that

application software can use to automatically check the current status of all unexpired certificates issued by HiPKI RCA.

HiPKI RCA maintains a continuous 24x7 ability to respond to a high-priority certificate problem report. HiPKI RCA may report such a complaint to the law enforcement and revoke the problematic certificate upon its discretion.

4.10.3. Optional Features

No stipulation.

4.11. End of Subscription

End of subscription signifies that subordinate CAs or cross-certified CAs cease to use the services of HiPKI RCA.

HiPKI RCA allows subordinate CAs or cross-certified CAs to end their subscription to certificate services by having their certificate revoked or by allowing the certificate or applicable Cross Certification Agreement to expire without renewal.

4.12. Key Escrow and Recovery

4.12.1. Key Escrow and Recovery Policy and Practices

HiPKI RCA's private signing keys shall not be escrowed. HiPKI RCA does not support the escrowing and recovery of the private keys of subordinate CAs, cross-certified CAs, or subscribers.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

HiPKI RCA 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 RCA facility is located in the building of the Information Technology Group of CHT. The construction of the facility housing is consistent with facilities used to house high value, sensitive information. Combined with other physical security mechanisms including access control, guards, intrusion detectors and video monitoring, it provides robust protection against unauthorized access to related HiPKI RCA equipment.

5.1.2. Physical Access

Physical control regulations and operation of HiPKI RCA meets level 4 assurance level standards. There are four guarding levels in HiPKI RCA facility housing. On the first and second levels, there are year-round entrance and building security controls in place. On the third level, access is controlled to this floor using a card access control system. On the fourth level, a fingerprint recognition control system is used to control access for facility personnel. The fingerprint scanner uses 3D sampling technology which is capable of detecting whether the fingerprint is from a live object by fingerprint depth and color.

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

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 RCA system.

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

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

5.1.4. Water Exposures

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

5.1.5. Fire Prevention and Protection

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

5.1.6. Media Storage

Audit records, archives and backups are kept in storage media for one year at the HiPKI RCA facility. After one year, the data shall be moved offsite for storage at a separate location.

5.1.7. Waste Disposal

When confidential information and documents of HiPKI RCA detailed in Section 9.3.1 are no longer in use, all shredded paper, magnetic tapes, hard disks, floppy disks, MO and other forms of memory shall be formatted to erase the information stored on them and physically destroyed.

5.1.8. Off-site Backup

The off-site backup location is over 30 km away from the HiPKI RCA facility. One backup of the all information including data and system programs shall be made at least once per week. Backups of modified data shall be done on the same day of the modification. The non-technical security control of backup site has an equivalent security level as HiPKI RCA.

5.2. Procedural Controls

In order to protect the security of system procedures, HiPKI RCA uses procedural controls to specify the trusted roles of related system tasks, the number of people required for each task and how each role is identified and authenticated.

5.2.1. Trusted Roles

In order to properly distinguish the duties of each system task and to prevent undetected malicious use of the system, the trusted role authorized to perform each system access task is clearly defined.

The seven trusted roles at HiPKI RCA are: administrator, CA officer, internal auditor, system operator, physical security controller, cyber security coordinator and anti-virus and anti-hacking coordinator. Each trusted role is administrated according to section 5.3 to prevent damage caused internal operations. Each trusted role may be performed by multiple persons, but one person shall be assigned the chief role. The tasks performed by each role are as follows:

(1) The administrator is responsible for:

- Installation, configuration and maintenance of the HiPKI RCA system,
- Creation and maintenance of HiPKI RCA system user accounts,
- Setting of audit parameters,
- Generation and backup of HiPKI RCA keys, and
- Publishing of CARLs in the repository.

(2) The CA officer is responsible for:

- Activate/deactivate the issuance services of certificate,
- Activate/deactivate the revocation services of certificate, and
- Activate/deactivate the issuance services of CARL.

(3) The internal auditor is responsible for:

- Checking, maintenance and archiving of audit logs, and
- Perform or supervise internal audits to ensure HiPKI RCA is operating in accordance with this CPS.

(4) The system operator is responsible for:

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

- Storage media updating,
- Hardware and software updates outside the HiPKI RCA system,
- Maintenance of the website(s), and
- Protecting mechanism such as system security or defending the threats of virus or malicious software.

(5) The physical security controller is responsible for:

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

(6) The cyber security coordinator is responsible for:

- Maintenance of the network and network facilities,
- Patches management for the vulnerability of the network facilities,
- The cyber security of HiPKI RCA, and
- The detection and report of the cyber security events.

(7) The anti-virus and anti-hacking coordinator is responsible for:

- Researching, applying, or providing the anti-virus, anti-hacking, and anti-malicious software technologies or measures to ensure the security of the system and the internet and
- Reporting the collected threats of computer virus or vulnerability to the administrator or the cyber security coordinator for enhancement.

5.2.2. Number of Persons Required per Task

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

(1) Administrator: at least 3 qualified individuals,

(2) CA Officer: at least 3 qualified individuals,

(3) Internal auditor: at least 2 qualified individuals,

(4) System operator: at least 2 qualified individuals,

(5) Physical security controller: at least 2 qualified individuals,

(6) Cyber security coordinator: at least 1 qualified individual, and

(7) Anti-virus and anti-hacking coordinator: at least 1 qualified individual.

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

Assignments	Administrator	CA officer	Internal auditor	System operator	Physical security controller	Cyber security coordinator	Anti-virus and anti-hacking coordinator
Installation, configuration, and maintenance of the HiPKI RCA system	2				1		
Establishment and maintenance of HiPKI RCA certificate management system user accounts	2				1		
Generation and backup of HiPKI RCA keys	2	2	1		1		
Activation / deactivation of certificate issuance, certificate revocation and CRL issuance	2	2			1		
Checking, maintenance and archiving of audit logs			1	1	1		
Daily operation and maintenance of system equipment				1	1		
System backup and recovery	1				1		
Storage media updating				1	1		
Software and hardware updates outside of HiPKI RCA system	1				1		
Website maintenance	1				1		
Daily operation and maintenance of the network and network facilities				1	1	1	
Patching the vulnerabilities of the network facilities	1				1	1	
Reporting the threats of computer virus or							1

Assignments	Administrator	CA officer	Internal auditor	System operator	Physical security controller	Cyber security coordinator	Anti-virus and anti-hacking coordinator
vulnerability							
Patching the anti-virus and vulnerabilities (audit system)	1		1	1	1		
Patching the anti-virus and vulnerabilities (systems other than the audit system)	1			1	1		

5.2.3. Identification and Authentication for Each Role

HiPKI RCA utilized system account, password and group management functions and IC cards to identify and authenticate administrator, CA officer, internal auditor, system operator and physical security controller roles as well as central access control system authorization setting function to identify and authenticate physical security controllers. HiPKI RCA uses the user's account, password, and system account administration functions, or other security mechanism to identify the role of the cyber security coordinators.

5.2.4. Roles Requiring Separation of Duties

The seven trusted roles are defined in Section 5.2.1. The HiPKI RCA trusted roles must conform to the following regulations:

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

5.3. Personnel Controls

5.3.1. Qualifications, Experience, and Clearance Requirements

(1) Personnel selection and security clearance items

- Personality
- Experiences
- Academic and professional skills and qualifications
- Personal identity check
- Trustworthiness

(2) Management of personnel evaluation

All HiPKI RCA personnel shall have their qualifications checked before employment to verify their qualifications and work abilities. After formal employment, personnel shall receive appropriate training and sign a document accepting responsibility to perform certain duties. All personnel shall have their qualifications rechecked each year. If personnel do not pass the qualification check, a qualified individual shall be assigned to serve in this position.

(3) Appointment, dismissal and transfer

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

(4) Duty of confidentiality agreement

All HiPKI RCA related personnel shall sign an agreement to fulfill the duty of confidentiality and sign a non-disclosure agreement stating that business confidential information may not be disclosed verbally or by photocopy, loan, delivery, article or other methods.

5.3.2. Background Check Procedures

HiPKI RCA shall check the related documents that verify the identity and certify the qualifications of the personnel performing the trusted roles defined in Section 5.2.1.

5.3.3. Training Requirements

Trusted Roles	Training Requirements
Administrator	(1) HiPKI RCA security clearance system. (2) Installation, configuration, and maintenance of the HiPKI RCA operation procedures. (3) Establishment and maintenance Cross-Certified CA account operation procedures. (4) Set up audit parameter configuration operation procedures. (5) HiPKI RCA key generation and backup operation procedures. (6) Operative procedure to publish CARLs in the repository (7) Disaster recovery and continuous operation procedure.
CA Officer	(1) HiPKI RCA security clearance system. (2) HiPKI RCA software and hardware use and operation procedures (3) Activate/deactivate the issuance services of certificate. (4) Activate/deactivate the revocation services of certificate. (5) Activate/deactivate the issuance services of CARL. (6) Disaster recovery and continuous operation procedure.
Internal Auditor	(1) HiPKI RCA security clearance system. (2) HiPKI RCA software and hardware use and operation procedures (3) HiPKI RCA key generation and backup operation procedures.

Trusted Roles	Training Requirements
	(4) Audit log check, upkeep and archiving procedures. (5) Disaster recovery and continuous operation procedure.
System Operator	(1) HiPKI RCA security clearance system. (2) Daily operation and maintenance procedures for system equipment. (3) Upgrading of storage media procedure. (4) Disaster recovery and continuous operation procedure. (5) Network and website maintenance procedure.
Physical Security Controller	(1) Physical access authorization setting procedure. (2) Disaster recovery and continuous operation procedure.
Cyber Security Coordinator	(1) Maintenance of the network and network facilities. (2) Security mechanism for the network.
Anti-virus and Anti-hacking Coordinator	(1) Prevention and control to the threats of computer virus and vulnerability (2) Security mechanism for the operating system and the network.

5.3.4. Retraining Frequency and Requirements

For hardware/software upgrades, work procedure changes, equipment replacement and amendments to related regulations, HiPKI RCA will schedule retraining for related personnel and record the training status to ensure that work procedures and regulatory changes are understood.

5.3.5. Job Rotation Frequency and Sequence

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

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

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

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

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

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

5.3.6. Sanctions for Unauthorized Actions

HiPKI RCA shall take appropriate administrative and disciplinary actions against personnel who violated the CP, CPS or other procedures announced by other HiPKI RCA. 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 RCA shall make available to related personnel relevant documentation pertaining to the HiPKI CP, technical specifications, this CPS, system operation manuals and the Electronic Signatures Act.

5.4. Audit Logging Procedures

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

5.4.1. Types of Events Recorded

(1) Security audits

- Any change to major audit parameters such as audit frequency, audit event type and new / old parameter content.
- Any attempt to delete or modify audit log files.

(2) Identification and authentication

- Attempt to set up a new role no matter whether successful or not
- Change in the maximum allowable time for identity authentication attempts
- Maximum of identity authentication attempt failure times when the user logs in the system
- Locked account number unlocked by administrator and the account number is locked due to the number of failed identity authentication attempts
- Administrator changes system identity authentication system such as change from password to biometrics.

(3) Key generation

- HiPKI RCA key generation times

(4) Private key load and storage

- Loading the private key into a system component
- All access to certificate subject private keys kept by the CA

(5) Trusted public key addition, deletion and saving

- Trusted public key modification including addition, deletion

and saving

(6) Private key export

- Export of private keys (does not include single session keys or keys limited to one use)

(7) Certificate registration

- Certificate registration request process

(8) Certificate revocation

- Certificate revocation request process

(9) Certificate status change approval

- Approve or deny certificate status change requests

(10) HiPKI RCA configuration

- HiPKI RCA security related configuration setting changes

(11) Account administration

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

(12) Certificate profile management

- Certificate profile changes

(13) CARL profile management

- CARL profile changes

(14) Miscellaneous

- Installation of operating systems.
- Installation of HiPKI RCA systems.
- Installation of hardware cryptographic modules.
- Removal of hardware cryptographic modules.
- Destruction of hardware cryptographic modules.
- System startup.
- Logon attempts to the HiPKI RCA certificate management system.
- Hardware and software receipt.
- Attempts to set passwords.

- Attempts to modify passwords.
- HiPKI RCA internal data backups.
- HiPKI RCA internal data recovery.
- File manipulation (such as creation, renaming, moving)
- Posting of any information to the repository
- Access to the HiPKI RCA internal database.
- Any certificate compromise complaints.
- Certificate loading into token.
- Token transmission process.
- Token zeroization.
- HiPKI RCA or Cross-Certified CA rekey

(15)HiPKI RCA service configuration changes

- Hardware
- Software
- Operating system
- Patches
- Security profile

(16)Physical access / site security

- Personnel access to the HiPKI RCA facility.
- Access to the HiPKI RCA servers.
- Known or suspect violation of physical security regulations

(17)Anomalies

- Software defect
- Software integrity check failure
- Acceptance of unsuitable information
- Irregular routing information
- Network attack (suspect or confirmed)
- Equipment failure
- Power anomalies
- UPS failure
- Clear and significant network service or access failure
- Certificate policy violation

- CPS violation
- Reset system clock

5.4.2. Frequency of Processing Log

HiPKI RCA shall review audit logs once every month and track and investigate major events. Review work includes verifying that the audit logs have not been tampered with, examining all log entries and checking any warnings or anomalies. HiPKI RCA reinforces the review on audit logs regarding security event after the previous audit review. HiPKI RCA makes an investigation for any evidence of malicious activity and documents any actions taken as a result of a review.

5.4.3. Retention Period for Audit Log

Audit logs of HiPKI RCA 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 HiPKI RCA for at least two months.

HiPKI RCA 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

Signature and encryption technology shall be used to protect the current and archived audit logs. CD-R or other unmodifiable media shall be used to save the audit logs.

The private keys used to sign event logs may not be used for other purposes. It is prohibited to use audit system private keys for other purposes. The private keys used for the audit system may not be disclosed.

Manual audit logs shall be stored is a secure location.

5.4.5. Audit Log Backup Procedures

Electronic audit logs are backed up and saved to a secure off-site location once a month.

HiPKI RCA shall routinely make backups of the event logs. The audit system shall automatically archive audit trail information regularly on a daily, weekly and monthly basis.

HiPKI RCA shall keep the event log files in a secure location.

5.4.6. Audit Collection System (Internal vs. External)

The audit log collection system is an internal component of the certificate administration system. Audit processes shall be initiated at system startup and end only at system shutdown.

If the automated audit system cannot operate normally, HiPKI RCA shall suspend certificate issuance services until the issue is resolved before resuming service again to protect system information integrity and confidentiality when the security system is in a high-risk state.

5.4.7. Notification to Event-causing Subject

No stipulation.

5.4.8. Vulnerability Assessments

HiPKI RCA follows the approaches and frequency required by the 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 assess the vulnerability at least once per season, and conducts the penetration test once per year. After acknowledging the material change or update for the applications or infrastructures, HiPKI RCA must conduct the penetration test as well. The remedy and correction measures are taken after the

penetration test and the vulnerability assessment by HiPKI RCA. HiPKI RCA shall record the skills, tools, ethic codes to be complied with, competing relationship and independence of the personnel and organization that are trustworthy to execute the vulnerability scanning, the penetration test, the health check of information security, or security monitor.

5.5. Records Archival

5.5.1. Types of Records Archived

- HiPKI RCA accreditation information from competent authorities (hypothetical use)
- CPS
- CCA (hypothetical use)
- System and equipment configuration setting
- System and configuration setting modifications and updates
- Certificate request information
- Revocation request information
- Certificate acceptance confirmation documents
- Issued or announced certificates
- HiPKI RCA rekey records
- Issued or announced CARLs
- Audit logs
- Used to verify and validate the content of files and other explanatory information or application programs.
- Audit personnel requirement documents
- Organization and personal identity authentication information

5.5.2. Retention Period for Archive

HiPKI RCA retains archived data for 20 years. The application

programs used to process archived data are retained for 20 years.

After the retention period of archived data has expired, the data shall be destroyed in a safe manner if it is retained in writing; and the data which is retained in electronic shall be backed up separately to other storage media given adequate protection or be destroyed in a safe manner.

5.5.3. Protection of Archive

Additions, modifications or deletion of archive information is not allowed.

HiPKI RCA may transfer the archive information to another storage media which is given adequate protection. The protection level may not be lower than the original protection level.

Archive information is stored in a safe location.

5.5.4. Archive Backup Procedures

Archive information is backed up at an offsite backup center. See section 5.1.8 for the offsite backup location.

5.5.5. Requirements for Time-stamping of Records

Archived electronic records (such as certificates, CARLs and audit logs) include data and time information and some of these records have appropriate digital signature protection which can be used to check the date and time information on the records for alteration. However, the date and time information on these electronic records are not electronic time-stamp information provided by an accredited third party. The date and time are from a computer operating system. All HiPKI RCA computer systems are regularly calibrated to ensure the accuracy and trustworthiness of the date and time information on electronic records.

Date information is recorded on written archive records. If necessary, time information is also recorded on written archive records. The date and time records on written records may not be arbitrarily changed. If it is necessary to make changes, the changes must be signed by audit personnel.

5.5.6. Archive Collection System (Internal or External)

HiPKI RCA does not have an archive information collection system.

5.5.7. Procedures to Obtain and Verify Archive Information

Archive information may be obtained after a written request for formal authorization is approved.

Audit personnel are responsible for verification of archive information. The authenticity of document signatures and dates on written documents must be verified. The digital signatures on archive information must be verified for electronic files.

5.6. Key Changeover

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

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

HiPKI RCA 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, HiPKI RCA shall sign a new self-signed certificate (by using the new private key) and mutually sign a new self-issued certificate (by using the new and old private keys, separately). The issuance procedures for these three new certificates need to comply with Section 4.3. The new self-signed certificate shall be

delivered to relying parties in accordance with Section 6.1.4 while the new self-issued certificates shall be published in HiPKI RCA repository for download.

5.7. Compromise and Disaster Recovery

5.7.1. Incident and Compromise Handling Procedures

HiPKI RCA establishes incident and compromise reporting and handling procedures, and conducts the test annually.

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

HiPKI RCA establishes recovery procedures in the event of computer resources, software or data corruption and conducts the drills annually.

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

5.7.3. Entity Private Key Compromise Procedures

HiPKI RCA establishes recovery procedures in the event that a CA private key is compromised in order to restore the operation of certificate issuance and administration as soon as possible and conducts the drills annually.

5.7.4. Business Continuity Capabilities after a Disaster

HiPKI RCA holds a drill of its disaster recovery plan annually.

5.8. CA or RA Termination

HiPKI RCA shall follow the regulations of the Electronic Signatures Act in the event of service termination.

HiPKI RCA shall follow the items below to ensure that service termination has a minimal effect on subordinate CAs, Cross-Certified CAs and relying parties:

(1) HiPKI RCA shall notify subordinate CAs and Cross-Certified CAs (does not apply if unable to notify), and the application software suppliers (e.g. browsers or operating system supplier) in the trust list of the self-issued certificate root CA of HiPKI RCA, of the service termination three months in advance and post the notification in the repository.

(2) HiPKI RCA shall revoke all unrevoked and unexpired certificates when terminating their service as well as safeguard and transfer the related files and records in accordance with the Electronic Signatures Act.

6. Technical Security Controls

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

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

HiPKI RCA key generation is witnessed and videotaped by those related personnel who have signed key initiation witness document (the public key of the generated key pair is listed on it). This public key of the key pairs of HiPKI RCA is distributed via trusted channels. The related personnel shall include the members of the PMA and the qualified auditors.

Subordinate CA and cross-certified CA must generate key pairs in accordance with CP regulations.

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

HiPKI RCA uses a hardware cryptographic module to generate random numbers, public keys and corresponding keys.

Subordinate CAs must follow CP regulations and select suitable software and hardware for key generation. Before subordinate CA certificates are issued, HiPKI RCA shall review the suitability of the software or hardware selected by the subordinate CA.

Cross-certified CA must follow CP regulations and select suitable software and hardware for key generation. Before cross-certificates are issued, HiPKI RCA shall review the suitability of the software or hardware selected by the CA.

HiPKI RCA only provides the self-signed certificate, self-issued certificate, the certificates of the subordinate CAs and the cross- certificate, but not the certificate of subscriber. For the related requirements for generating keys of the certificate of subscriber please refer to the CPS of the subordinate CAs under HiPKI or the CPS of the cross-certified CAs.

6.1.2. Private Key Delivery to Subscriber

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

Any cross-certified CA cross certified with HiPKI RCA must self-generate the private key. Therefore, HiPKI RCA does not need to deliver the private key to the cross-certified CA.

6.1.3. Public Key Delivery to Certificate Issuer

The PKCS#10 certificate request file is submitted when the CA requests the certificate.

6.1.4. CA Public Key Delivery to Relying Parties

The HiPKI RCA public key is distributed in a HiPKI RCA self-signed certificate. There are the following secure distribution channels:

(1) Upon the key pair is generated, HiPKi RCA publishes its public key on the spot and specifies the public key in a certificate validation file witnessed and later be signed by the PMA members and qualified auditor. HiPKi RCA then issues a self-signed certificate and publishes the certificate in its repository.

(2) After a CA certificate is issued, HiPKi RCA delivers the CA certificate along with a HiPKI RCA self-signed certificate or public key to the subordinate CA. The subordinate CA stores the HiPKI RCA self-signed certificate or public key into a token (such

as IC card) and the token is distributed to its subscribers or relying parties in a secure way.

(3) After a cross-certificate is issued, HiPKI RCA delivers the cross-certificate along with a HiPKI RCA self-signed certificate or public key to the cross-certified CA. The cross-certified CA stores the HiPKI RCA self-signed certificate or public key into a token (such as IC card) and the token is distributed to its subscribers or relying parties in a secure way.

(4) The HiPKI RCA self-signed certificate is built in the software issued by a trusted third party. Subscribers can obtain this software via secure channel (for example purchase software installation CD-ROM from trusted distributor or install from major operating system or browser) from which the HiPKI RCA self-signed certificate can be obtained after installed the software.

(5) The HiPKI RCA self-signed certificate is stored in mass circulation CD-ROMs, subscribers can obtain these CD-ROMs via secure channels from which the HiPKI RCA self-signed certificate can be obtained.

6.1.5. Key Sizes

Key size and algorithms applied to certificates, CARLs, and CRLs issued by HiPKI RCA, subordinate CAs, and cross-certified CAs must meet the following requirements:

(1) HiPKI RCA

- HiPKI RCA uses 4096-bit RSA keys and SHA-256, SHA-384, or SHA-512 hash function algorithm to issue certificates.
- If HiPKI RCA uses Elliptic Curve Cryptography (ECC) algorithms to issue certificates, the key size will comply with NIST P-384.

(2) Subordinate CAs and Cross-Certified CAs

- According to the HiPKI CP, subordinate CAs and cross-certified CAs uses 4096-bit RSA keys and SHA-256, SHA-384, or SHA-512 hash function algorithm to issue certificates.
- If subordinate CAs or cross-certified CAs uses ECC algorithms to issue certificates, the key size will comply with NIST P256 or P-384.

HiPKI RCA shall examine whether the CA has chosen an appropriate key size before the subordinate CA certificate or cross-certificate is issued by HiPKI RCA.

6.1.6. Public Key Parameters Generation and Quality Checking

The public key parameter of the RSA algorithm is null.

HiPKI RCA and subordinate CAs use an ANSI X9.31 algorithm or NIST FIPS 186-4 standard to generate the prime number needed for the RSA algorithm and ensure that the prime number is a strong prime.

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

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

In the future, if certificates are issued with ECC algorithms, HiPKI RCA will comply with the requirements of Sections 5.6.2.3.2 and 5.6.2.3.3 in NIST SP 800-56A Revision 2 to confirm the validity of all keys using 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)

The private key corresponding to the HiPKI RCA self-signed certificate can only be used for issuing self-signed certificates, self-issued certificates, subordinate CA certificates, cross-certificates, CARLs, OCSP responder certificates, or OCSP responses.

The key usage extension is present in the HiPKI RCA's self-signed certificates and is marked critical. Bit positions for keyCertSign and cRLSign are set. If the HiPKI RCA private signing key is used for signing OCSP responses, then the digitalSignature bit will be set.

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

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

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic Module Standards and Controls

HiPKI RCA uses hardware cryptographic modules complying with FIPS 140-2 Level 3 in accordance with the HiPKI CP.

The subordinate CA must follow the HiPKI CP regulations when choosing an appropriate cryptographic module. HiPKI RCA shall examine whether the CA has chosen an appropriate cryptographic module security level before the subordinate CA certificate is issued by HiPKI RCA.

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

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

The multi-person control for HiPKI RCA key splitting uses n-out-of-m LaGrange Polynomial Interpolation. It is a perfect secret sharing method used for private key splitting backup/recovery, where n and m must be values greater than or equal to 2 and n must be less than or equal to m. Use of this method can provide the highest security level for the HiPKI RCA private key multi-person control. Therefore, it can be used as the activation method for private keys (see Section 6.2.8).

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

6.2.3. Private Key Escrow

HiPKI RCA’s private signing keys cannot be escrowed. HiPKI RCA is not responsible for safekeeping the private signing keys from subordinate CAs and cross-certified CAs.

6.2.4. Private Key Backup

Backups of private keys are performed according to the key splitting multi-person control methods in Section 6.2.2 and highly secure IC cards are used as the secret sharing storage media.

The subordinate CA and cross-certified CA must follow the HiPKI

CP regulations when choosing an appropriate private key backup method. HiPKI RCA shall examine whether the CA has chosen an appropriate private key backup method before the subordinate CA certificate or cross-certificate is issued by HiPKI RCA.

HiPKI RCA is not responsible for the safekeeping of the private key backups made by the subordinate CA and cross-certified CA.

6.2.5. Private Key Archival

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

6.2.6. Private Key Transfer into or from a Cryptographic Module

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

The subordinate CA and cross-certified CA must follow the HiPKI CP regulations to choose an appropriate private key importation method when they need to transfer a private key into a cryptographic module, HiPKI RCA shall examine whether the CA has chosen an appropriate

private key importation method prior to the issuance of the subordinate CA certificates or cross-certificates.

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

6.2.7. Private Key Storage on Cryptographic Module

As stated in Sections 6.1.1 and 6.2.1.

6.2.8. Method of Activating Private Key

The activation of RSA private key in HiPKI RCA is controlled by multi-person control IC cards. Different usage control IC cards are kept separately by the administrator and CA officer.

The subordinate CA and cross-certified CA must follow the CP regulations when choosing an appropriate private key activation method. HiPKI RCA shall examine whether the CA has chosen an appropriate private key activation method before the subordinate CA certificate or cross-certificate is issued by HiPKI RCA.

6.2.9. Method of Deactivating Private Key

As HiPKI RCA utilizes an offline operation mode, the HiPKI RCA keys are normally in a deactivated state in order to prevent illegal use of the private key.

Once certificate issuance and other related administrative work is completed, HiPKI RCA uses the n-out-of-m method to deactivate the private key. The subordinate CA and cross-certified CA must follow CP regulations when choosing an appropriate private key deactivation method.

HiPKI RCA shall examine whether the CA has chosen an appropriate private key deactivation method before the subordinate CA certificate or cross-certificate is issued by HiPKI RCA.

6.2.10. Method of Destroying Private Key

In order to prevent the theft of old HiPKI RCA private keys which influences the correctness of issued certificates, HiPKI RCA private keys are destroyed at the end of their lifecycle. Therefore, after HiPKI RCA completes key renewal and issuance of a new HiPKI RCA self-signed certificate and no other certificates or CARL will be issued, zeroization of the memory locations of the old HiPKI RCA private key stored in the hardware cryptographic module is conducted to destroy the old private key in the hardware cryptographic module. Split old private keys are also physically destroyed.

If a hardware cryptographic module will cease to provide the demanded services to HiPKI RCA but still is accessible, all the private keys (including these used or probably used private keys) stored in this hardware cryptographic module shall be destroyed. After destroying all the private keys in this hardware cryptographic module, it is necessary to verify that all the aforesaid private key do not exist anymore with the key management tools provided by the hardware cryptographic module.

The subordinate CA and cross-certified CA must follow CP regulations when choosing an appropriate private key destruction method. HiPKI RCA shall examine whether the CA has chosen an appropriate private key destruction method before the subordinate CA certificate or cross-certificate is issued by HiPKI RCA.

6.2.11. Cryptographic Module Rating

See Section 6.2.1.

6.3. Other Aspects of Key Pair Management

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

6.3.1. Public Key Archival

HiPKI RCA shall conduct certificate archiving and follow the regulations in Section 5.5 to perform security control for the archival system. No addition archiving is done for public keys because certificate archiving can replace public key archiving.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

HiPKI RCA only provides the issuance of self-signed certificates, self-issued certificates, subordinate CA certificates, cross-certificates, CARLs, OCSP responder certificates, or OCSP responses, but not the issuance of TLS/SSL certificates. For the related requirements for issuing TLS/SSL certificates, please refer to the CPS of the subordinate CAs under HiPKI or the cross-certified CAs.

6.3.2.1. HiPKI RCA Certificate Operational Periods and Key Usage Periods

HiPKI RCA certificate operational periods and key usage periods are up to 30 years. The maximum usage period of using private keys to issue subordinate CA certificates is 15 years; but the usage period of using private keys to issue CARLs, OCSP responder certificates, or OCSP responses is valid until self-issued certificates, subordinate CA certificates, or cross-certificates expired. In addition, it may be necessary to re-issue the self-issued certificate due to the modification of HiPKI CP or to issue the cross-certificate due to the cross-certification with a root CA outside

HiPKI. Therefore, the usage period of private keys of HiPKI RCA to issue self-issued certificates or cross-certificates is 30 years at maximum.

The usage period for private keys and certificates of OCSP responders is 36 hours. A new certificate for the OCSP responder is published daily. (The OCSP responses signed by the new private key of the OCSP responder will contain the new OCSP responder certificate for relying parties to verify the signature of OCSP responses).

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

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

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

Subordinate CAs and cross-certified CAs certificate operational periods and key usage periods are up to 20 years. The maximum usage period of using private keys to issue TLS/SSL certificates is 10 years, but the usage period of using private keys to issue CRLs, OCSP responder certificates or OCSP responses is not subject to these restrictions.

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

6.3.2.3. Hash Function Algorithm Validity Period

HiPKI RCA uses SHA-256 hash function algorithm to issue self-signed certificates, self-issued certificates, subordinate CA certificates, cross-certificates, and CARLs.

The OCSP responder of HiPKI RCA uses 2048-bit RSA keys and

SHA-256 hash function algorithm to issue OCSP responses.

Subordinate CAs under HiPKI or CAs cross-certified with HiPKI shall apply SHA-256 or other hash function algorithms with higher security level to issue TLS/SSL certificates, CRLs, and OCSP responses.

6.4. Activation Data

6.4.1. Activation Data Generation and Installation

The activation data of HiPKI RCA is generated by the hardware cryptographic module and then written in the n-out-of-m control IC cards. The activation data within the IC cards is directly accessed by the built-in card readers inside the hardware cryptographic module. The IC card personal identification number (PIN) is directly input from the built-in keyboard in the hardware cryptographic module.

The subordinate CA and cross-certified CA must follow the HiPKI CP regulations when choosing an appropriate activation data generation method. HiPKI RCA shall examine whether the CA has chosen an appropriate activation data generation method before the subordinate CA certificate or cross-certificate is issued by HiPKI RCA.

6.4.2. Activation Data Protection

The activation data of HiPKI RCA is protected by the n-out-of-m control IC cards. Administrators are responsible for safekeeping of the IC card PIN. The PIN shall not be stored in any media. If there are over three failed login attempts, the controlled IC card is locked. During IC card handover, a new PIN is set by the new administrator.

The subordinate CA and cross-certified CA must follow the HiPKI CP regulations when choosing an appropriate activation data protection method. HiPKI RCA shall examine whether the CA has chosen an

appropriate activation data protection method before the subordinate CA certificate or cross-certificate is issued by HiPKI RCA.

6.4.3. Other Aspects of Activation Data

HiPKI RCA shall not archive the activation data of its private key.

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

HiPKI RCA and its ancillary parts include the following computer security functions. These functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards:

- Authenticate the identity of users before permitting access to the system or applications,
- Manage privileges of users to limit users to their assigned roles,
- Provide security audit capability,
- Require use of cryptography for session communication and database security, and
- Support protection of process integrity and security control.

HiPKI RCA equipment must be 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 RCA enforces multi-factor authentication for all accounts capable of directly causing certificate issuance.

6.5.2. Computer Security Rating

HiPKI RCA servers use Common Criteria EAL 4 certified computer operating systems.

6.6. Life Cycle Technical Controls

6.6.1. System Development Controls

Quality control for HiPKI RCA system development complies with the requirements of Capability Maturity Model Integration (CMMI).

System development environments, test environments, and production environments must be separated to prevent unauthorized access and changes. In addition, malicious software shall also be prevented from being installed on the HiPKI RCA's equipment, and only components authorized by security policy may be used for HiPKI RCA's operations.

For hardware and software used by HiPKI RCA, it must check for malicious code before the first use or version update and perform a security scan periodically.

The products or programs delivered to HiPKI RCA should provide the guarantee agreement of security compliance, which ensures that there are no back doors or malicious programs, product or program handover lists, test reports, system management manuals, and reports of source code analysis. The version controls for the programs should be also conducted.

6.6.2. Security Management Controls

The HiPKI RCA hardware and software are dedicated to supporting the operation of HiPKI RCA. There shall be no other applications, hardware devices, network connections, or component software installed that are not parts of the HiPKI RCA's operation.

When installing software used by HiPKI RCA to the system for the first time, HiPKI RCA verifies that the software is the correct version without any modifications and is supplied by the software vendor. After the installation is complete, HiPKI RCA shall check the integrity of CA software before each use and shall regularly perform a scan by using tools

including anti-virus software and malware removal tool.

HiPKI RCA documents and controls the system configurations and their modification and the upgrade of functions as well as detecting unauthorized modifications to system software or configurations.

HiPKI RCA references the methodologies and standards in the ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, ISO/IEC 31000, WebTrust Principles and Criteria for Certification Authorities (WebTrust for CA), and Baseline Requirements for risk assessment, risk management, and security management controls.

6.6.3. Life Cycle Security Controls

Assessment shall be conducted at least once a year to determine whether the current key is at risk of being compromised.

6.7. Network Security Controls

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

The HiPKI RCA servers are not connected to external networks. The repository is connected to the Internet to provide uninterrupted certificate and CARL inquiry services (except during required maintenance or backup).

The certificates and CARLs issued by the HiPKI RCA servers are protected with digital signature and sent to the repository from the HiPKI RCA servers manually.

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

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

6.8. Time-stamping

HiPKI RCA 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 certificate issuance,

(2) Time of certificate revocation,

(3) Time of CARL issuance, and

(4) Time of system event occurrence.

Automatic or manual procedures may be used by HiPKI RCA to adjust the system time. Clock synchronizations shall be auditable events.

7. Certificate, CRL, and OCSP Profiles

7.1. Certificate Profile

HiPKI RCA issues certificates in compliance with the ITU-T X.509, Baseline Requirements, and RFC 5280.

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

7.1.2. Certificate Extensions

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

There are four kinds of certificates issued by HiPKI RCA, namely self-signed certificate, self-issued certificate, subordinate CA certificate, and cross-certificate. The necessary extensions and the criticality of these extensions are described below. Other optional extensions may be used as applicable, and the methods shall comply with the aforesaid regulations.

(1) Self-signed Certificate

Extension	Criticality	Description
Subject Key Identifier	FALSE	The SHA-1 hash value of the subject public key
Basic Constraints	TRUE	Subject Type=CA Path Length Constraint=None
Key Usage	TRUE	The content in this extension can be one of the following: ■ keyCertSign and cRLSign. (Default) ■ digitalSignature, keyCertSign and cRLSign. (If HiPKI RCA uses the private signing key to issue OCSP responses, the bits of digitalSignature, keyCertSign, and

Extension	Criticality	Description
		cRLSign are asserted.)

(2) Self-issued Certificate

Extension	Criticality	Description
Authority Key Identifier	FALSE	The SHA-1 hash value of the issuer public key
Subject Key Identifier	FALSE	The SHA-1 hash value of the subject public key
CRL Distribution Points	FALSE	The URL to the CARL announced by HiPKI RCA
Authority Information Access	FALSE	Two items included in this extension: ■ The URL to download the self-signed certificate of HiPKI RCA ■ The URL of OCSP services provided by HiPKI RCA
Certificate Policies	FALSE	The following two items shall be included in this extension. The policy qualifier in this extension may be used to mark the published URL of this CPS as needed: ■ All CP OIDs defined in the HiPKI CP. ■ All CP OIDs defined by CA/Browser Forum referenced in the HiPKI CP.
Key Usage	TRUE	The content in this extension shall be identical to the content of the key usage extension in the self-signed certificate.
Basic Constraints	TRUE	Subject Type=CA Path Length Constraint=None

(3) Subordinate CA Certificate

Extension	Criticality	Description
Authority Key Identifier	FALSE	The SHA-1 hash value of the issuer public key
Subject Key Identifier	FALSE	The SHA-1 hash value of the subject public key
CRL Distribution Points	FALSE	The URL to the CARL announced by HiPKI RCA
Authority Information Access	FALSE	Two items included in this extension: ■ The URL to download the self-signed certificate of HiPKI RCA ■ The URL of OCSP services provided by HiPKI RCA
Certificate Policies	FALSE	This extension is used to indicate the certificate policies that used by the subordinate CA and approved and permitted to use by HiPKI RCA. The policy qualifier in this extension may be used to mark the published URL of this CPS as needed. One or more of the following CP OIDs may be contained in this extension: ■ CP OIDs defined in the HiPKI CP. ■ CP OIDs defined by CA/Browser Forum referenced in the HiPKI CP.
Extended Key Usage (EKU)	FALSE	Key purpose OID(s) used by the subordinate CA shall be included in this extension. According to Section 1.2 of HiPKI CP, subordinate CAs under HiPKI RCA will only

Extension	Criticality	Description
		be used to issue TLS/SSL certificates. Therefore, the following requirements shall be met in this extension: ■ The value id-kp-serverAuth must be present. ■ The value listed below must not be present. ➢ id-kp-codeSigning ➢ id-kp-timeStamping ➢ id-kp-emailProtection ➢ anyExtendedKeyUsage ■ The value id-kp-clientAuth may be present. Other values should not be present.
Key Usage	TRUE	The content in this extension can be one of the following: ■ keyCertSign and cRLSign. (Default) ■ digitalSignature, keyCertSign and cRLSign. (If the subordinate CA uses the private signing key to issue OCSP responses, the bits of digitalSignature, keyCertSign, and cRLSign are asserted.)
Basic Constraints	TRUE	Subject Type=CA Path Length Constraint=Set according to the needed certificate path length of subordinate CAs.

(4) Cross-Certificate

Extension	Criticality	Description
Authority Key Identifier	FALSE	The SHA-1 hash value of the issuer public key
Subject Key Identifier	FALSE	The SHA-1 hash value of the subject public key
CRL Distribution Points	FALSE	The URL to the CARL announced by HiPKI RCA
Authority Information Access	FALSE	Two items included in this extension: ■ The URL to download the self-signed certificate of HiPKI RCA ■ The URL of OCSP services provided by HiPKI RCA
Certificate Policies	FALSE	This extension is used to indicate the certificate policies that used by the cross-certified CA and approved and permitted to use by HiPKI RCA. The policy qualifier in this extension may be used to mark the published URL of this CPS as needed. One or more of the following CP OIDs may be contained in this extension: ■ CP OIDs defined in the HiPKI CP. ■ CP OIDs defined by CA/Browser Forum referenced in the HiPKI CP.
Policy Mappings	FALSE	This extension is used to indicate the correspondences between the certificate policies of the cross-certified CA and the ones of HiPK RCA. It lists one or more pairs of CP OIDs. The pairing indicates HiPKI RCA considers its CP OID equivalent to the cross-certified CA's CP OID.
Key Usage	TRUE	The content in this extension can be one of the following: ■ keyCertSign and cRLSign. (Default) ■ digitalSignature, keyCertSign and cRLSign. (If the cross-certified CA uses the private signing key to issue

Extension	Criticality	Description
		OCSP responses, the bits of digitalSignature, keyCertSign, and cRLSign are asserted.)
Basic Constraints	TRUE	Subject Type=CA Path Length Constraint= Set according to the needed certificate path length of cross-certified CAs.

In addition, HiPKI RCA 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 RCA.

HiPKI RCA does not issue TLS/SSL certificates. In other words, HiPKI RCA does not implement the issuance of pre-certificates defined by RFC 6962.

7.1.3. Algorithm Object Identifiers

The algorithm OIDs used for signatures within the HiPKI RCA 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 OIDs used to identify the algorithm of the subject key generation within the HiPKI RCA issued certificates 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)

Where the certificate contains an elliptic curve public key, the parameters shall be specified as one of the following named curves:

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 distinguished name and issuer distinguished name fields of the certificates comply with ITU-T X.500 distinguished name and the attribute types of the distinguished name comply with the ITU-T X.509, Baseline Requirements, and RFC 5280.

The encoded content of the issuer distinguished name field of self-

signed certificates, self-issued certificates, subordinate CA certificates, and cross-certificates issued by HiPKI RCA shall be byte-for-byte identical with the encoded form of the subject distinguished name field of the HiPKI RCA self-signed certificate. If there are two or more certificates, including expired and revoked certificates, whose subject distinguished names can be compared as equal, the encoded content of the subject distinguished name field of the aforementioned certificate shall be byte-for-byte identical.

In the HiPKI RCA self-signed certificates, the subject distinguished name field includes three attributes, namely "commonName", "organizationName", and "countryName", described as follows:

(1) commonName

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

(2) organizationName

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

The organization name may be a little bit different from the name used to verify the identity. Take the abbreviation as an example, a part of the text of the organization name can be adjusted by the abbreviation recognized domestically, such as changing "Chunghwa Telecom Company Limited" to "Chunghwa Telecom Co., Ltd."

(3) countryName

To record the country where the place of business that HiPKI RCA locates and shall be represented by the country codes specified in ISO 3166-1.

By issuing self-issued certificates, subordinate CA certificates and

cross-certificates, HiPKI RCA represents that it followed the procedure set forth in the HiPKI CP and/or this CPS to verify that, as of the certificate's issuance date, all of the subject information was accurate.

7.1.5. Name Constraints

No name constraints are used in HiPKI RCA. Self-signed certificates, self-issued certificates, subordinate CA certificates, and cross-certificates, which are not technically constrained, will be disclosed via Mozilla's Common CA Database (CCADB) and other public channels.

7.1.6. Certificate Policy Object Identifier

HiPKI RCA's self-signed certificates do not contain the certificate policies extension.

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

7.1.7. Usage of Policy Constraints Extension

If necessary, subordinate CA certificates and cross-certificates issued by HiPKI RCA may use the policy constraints extension.

7.1.8. Policy Qualifiers Syntax and Semantics

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

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

The certificate policies extension contained in the certificates issued by HiPKI RCA is not marked critical.

7.2. CARL Profile

7.2.1. Version Number(s)

HiPKI RCA issues CARLs complying with RFC 5280 and ITU-T X.509 version 2.

7.2.2. CRL and the CRL Entry Extensions

The CRL and CRL entry extensions in the CARL issued by HiPKI RCA comply with the ITU-T X.509, Baseline Requirements, and RFC 5280.

The necessary CRL and CRL entry extensions and the criticality of these extensions are described below. Other optional extensions may be used as applicable, and the methods shall comply with the aforesaid regulations.

(1) CRL Extensions

Extension	Criticality	Description
Authority Key Identifier	FALSE	The SHA-1 hash value of the issuer public key
CRL Numbers	FALSE	The sequence number of the CARL

(2) CRL Entry Extensions

Extension	Criticality	Description
Reason Code	FALSE	This extension field is used to indicate the most appropriate reason code selected when HiPKI RCA revokes the certificate. The reason codes that can be used and their applicable scenarios are described as follows: ■ caCompromise(2): Use this CRLReason if it is suspected or confirmed that the CA's private signing key is stolen or compromised. ■ affiliationChanged(3): This CRLReason is used when

Extension	Criticality	Description
		there is a change in the subject information noted in the CA certificate. For example, the organization to which the CA belongs changes its name. ■ superseded(4): Use this CRLResaon to revoke the original certificate when the certificate needs to be reissued for some reason such as updating the CP OID(s) contained in the certificate policies extension of the certificate. ■ cessationOfOperation(5):The CRLReason is used when the CA does not issue certificates, CRL, and OCSP responses any longer. ■ privilegeWithdrawn(9): The CRLReason is used when the privilege contained within the certificate has been withdrawn. For example, the business license or registration of the organization to which the CA belongs has been revoked.

7.3. OCSP Profile

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

7.3.1. Version Number(s)

An OCSP request accepted by HiPKI RCA shall contain the following information:

Protocol version, and

Target certificate identifier

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

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

Field	Description
Version	v.1 (0x0)
OCSP Responder ID	The subject distinguished name of

Field	Description
	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 distinguished name, the hash of the issuer's public key, and the serial number of the target certificate.
Certificate Status	The meaning of certificate status value is described below: ■ 0: The status of the certificate is valid. ■ 1: The certificate has been revoked. When this status value is used, this field shall also contain the revocation time and reason of that certificate. The revocationReason field within the RevokedInfo of the CertStatus shall be identical to the CRLReason of the revoked certificate noted in the CARL. ■ 2: The status of the certificate is unknown.
ThisUpdate / NextUpdate	Recommended validity period for this OCSP response, including ThisUpdate and NextUpdate
Signature Algorithm	OCSP response signature algorithm, which can be sha256WithRSAEncryption
Signature	OCSP responder signature
Certificates	OCSP responder certificate

7.3.2. OCSP Extensions

The OCSP responses issued by HiPKI RCA include the following extensions:

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

also contain the same nonce field.

8. Compliance Audit and Other Assessments

8.1. Frequency or Circumstances of Assessment

HiPKI RCA 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.

8.2. Identity/Qualifications of Assessor

CHT retains a qualified auditor, who is familiar with the operations of HiPKI RCA and its subordinate CAs 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. HiPKI RCA 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 RCA operations.

8.4. Topics Covered by Assessment

HiPKI RCA undergoes an audit in accordance with the schemes of WebTrust for CA, WebTrust for CA – SSL BR, and WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL (WebTrust for CA – EV SSL).

The assessment shall include the following topics:

(1) Whether HiPKI RCA is operating in accordance with this CPS,
(2) Whether the regulations of this CPS comply with the HiPKI CP, and
(3) If a Cross-Certification Agreement (CCA) is signed between HiPKI RCA and other root CA, that Root CA shall be considered in the assessment to ensure that the Root CA's compliance with the CCA.

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 RCA, the following actions shall be performed:

(1) Note the discrepancy, and
(2) Notify HiPKI RCA about the discrepancy, and if the discrepancy is a critical fault, the PMA shall be notified as well.

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

8.6. Communications of Results

Except for any audit findings that could result in system attacks and the stipulations in Section 9.3, HiPKI RCA shall make its audit report publicly available. Audit result are displayed with appropriate seals, including WebTrust for CA, WebTrust for CA – SSL BR or WebTrust for CA – EV SSL seals, on HiPKI RCA's homepage. The audit report and management's assertions may be viewed by clicking on the seals. HiPKI RCA 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 RCA shall provide an explanatory letter signed by the qualified auditor.

9. Other Business and Legal Matters

9.1. Fees

HiPKI RCA reserves the right to collect fees from subordinate CAs and CAs which request cross-certificates. These fees are limited to fees which apply to HiPKI RCA operation.

If HiPKI RCA collects fees from subordinate CAs and CAs which request cross-certificates, this CPS will be revised, and related fee inquiry methods and fee refund procedures shall be established.

9.1.1. Certificate Issuance or Renewal Fees

There is currently no charge.

9.1.2. Certificate Access Fees

There is currently no charge.

9.1.3. Revocation or Status Information Access Fees

There is currently no charge.

9.1.4. Fees for Other Services

There is currently no charge.

9.1.5. Refund Policy

No refund policy because there is currently no charge.

9.2. Financial Responsibility

9.2.1. Insurance Coverage

HiPKI RCA is owned and operated by CHT, its financial responsibilities are the responsibilities of CHT. No insurance policies have

been taken out yet for the HiPKI RCA certificate business. Insurance will be added in the future as required by the competent authority.

9.2.2. Other Assets

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

9.2.3. Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3. Confidentiality of Business Information

9.3.1. Scope of Confidential Information

The information generated, received and kept by HiPKI RCA is deemed confidential information. Personnel currently and previously employed by HiPKI RCA and various audit personnel shall bear the duty of confidentiality towards confidential information. Confidential

information includes:

(1) Private keys and passphrases used in HiPKI RCA operations,
(2) HiPKI RCA key splitting safekeeping information,
(3) The application information of subordinate CAs, which may be disclosed only with the permission of the subordinate CAs or in compliance with relevant laws and regulations,
(4) The application information of cross-certified CAs, which may be disclosed only with the permission of the cross-certified CAs or in compliance with relevant laws and regulations,
(5) Audit and tracking logs generated and kept by HiPKI RCA,
(6) Audit logs and reports made by audit personnel during the audit process, which may not be fully disclosed, and
(7) Operation-related documents listed as confidential level.

9.3.2. Information Not Within the Scope of Confidential Information

(1) Identity information and information listed in certificates are not deemed confidential information unless stipulated otherwise, and
(2) Issued certificates, revoked certificates and CARLs published in the HiPKI RCA repository are not deemed confidential information.

9.3.3. Responsibility to Protect Confidential Information

HiPKI RCA shall handle the application information of subordinate CAs and cross-certified CAs in accordance with the Electronic Signatures Act, Baseline Requirements, EV SSL Certificate Guidelines, WebTrust for CA criterion, WebTrust for CA – EV SSL criterion, WebTrust for CA – SSL BR criterion and Personal Information Protection Act.

HiPKI RCA implements security measures to prevent confidential information from disclosure or leakage.

9.4. Privacy of Personal Information

9.4.1. Privacy Plan

HiPKI RCA has posted its personal information statement and privacy declaration on its website. HiPKI RCA implements privacy impact analysis, personal information risk assessments and related measures for its privacy protection plan.

9.4.2. Information Treated as Private

Private information includes:

(1) The personal information listed on any certificate application may only be disclosed with the consent of the applicant and authorized representative or in accordance with related law and regulation;

(2) Identifiable information of personnel in HiPKI RCA, such as names together with palmprint or fingerprint biometrics; and

(3) Personal information on confidentiality agreements or contracts.

HiPKI RCA implements security control measures to prevent personally identifiable information from unauthorized disclosure or leakage.

9.4.3. Information Not Deemed Private

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

9.4.4. Responsibility to Protect Private Information

The personal information required for the operation of HiPKI RCA, in either paper or digital form, must be securely stored and protected in accordance with the personal information protection and privacy rights declaration posted on the website and must comply with the Electronic

Signatures Act, WebTrust for CA standards and Personal Information Protection Act.

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 the party involved or unless stipulated otherwise in the personal information protection and privacy rights declaration posted on the HiPKI RCA website and in this CPS.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

If judicial, supervisory or law enforcement authorities need to check private information under Section 9.4.2 for investigation or evidence collection requirements, the matter shall be handled in accordance with law or regulation. However, HiPKI RCA reserves the right to collect a reasonable fee from the authorities requesting access to the information.

9.4.7. Other Information Disclosure Circumstances

Subordinate CAs may check the application information under Section 9.3.1 paragraph (3). However, HiPKI RCA reserves the right to collect a reasonable fee from the subordinate CA requesting access to the information.

Cross-certified CAs may check the application information under Section 9.3.1 paragraph (4). However, HiPKI RCA reserves the right to collect a reasonable fee from the cross-certified CA requesting access to the information.

Other information disclosure circumstances are handled in accordance with related laws and regulations.

9.5. Intellectual Property Rights

The HiPKI RCA key pairs and split keys are the property of HiPKI RCA. Subordinate CA or cross-certified CA key pairs are the property of that CA; however, its certificates are the property of HiPKI RCA when their public keys are issued in a certificate by HiPKI RCA.

Certificates and CARLs issued by HiPKI RCA are the property of HiPKI RCA.

Subject name in self-signed and self-issued certificates issued by HiPKI RCA are the property of HiPKI RCA.

HiPKI RCA shall ensure the correctness of the name of subordinate CAs and cross-certified CAs as far as possible, but not the trademark ownership. If there is a trademark dispute over a subordinate CA or cross-certified CA name, the subordinate CA and cross-certified CA shall handle the matter in accordance with legal procedures and submit the results to HiPKI RCA to protect their rights.

This CPS is available for free download from the repository or reasonable use according to the relevant provisions in the Copyright Act of R.O.C. No one can charge for the distribution of this CPS. 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. HiPKI RCA Representations and Warranties

HiPKI RCA represents and warrants to the Certificate Beneficiaries including Subordinate CAs, Relying Parties, and Application Software Suppliers that, during the period when the Certificate is valid, HiPKI RCA 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) **Authorization for Certificate**: That, at the time of issuance, HiPKI RCA (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);

(2) **Accuracy of Information**: That, at the time of issuance, HiPKI RCA (i) implemented a procedure for verifying the accuracy of all of the information contained in the Certificate; (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);

(3) **No Misleading Information**: That, at the time of issuance, HiPKI RCA (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);

(4) **Identity of Applicant**: That, if the Certificate contains Subject Identity Information, HiPKI RCA (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;

(5) **Subscriber Agreement**: That, if HiPKI RCA and Subordinate CA

are not Affiliated, the Subordinate CA and HiPKI RCA are parties to a legally valid and enforceable Subscriber Agreement that satisfies the Baseline Requirements, or, if HiPKI RCA and Subordinate CA are the same entity or are Affiliated, the Applicant Representative acknowledged the Terms of Use;

(6) **Status**: That HiPKI RCA 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

(7) **Revocation**: That HiPKI RCA 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).

9.6.2. RA Representations and Warranties

HiPKI RCA does not establish registration authorities.

9.6.3. Subordinate CA and Cross-certified CA Representations and Warranties

9.6.3.1. Subordinate CA Representations and Warranties

Subordinate CAs represent and warrant that they will:

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

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

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

(4) Accept the certification in accordance with Section 4.4, after a

subordinate CA certificate application is approved and HiPKI RCA has issued the certificate;

(5) Check the accuracy of the information contained in the certificate prior to the acceptance of a subordinate CA certificate issued by HiPKI RCA, and the certificate shall be used in accordance with Section 1.4.1;

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

(7) Properly safeguard and use their private keys;

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

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

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

9.6.3.2. Cross-certified CA Representations and Warranties

Cross-certified CAs represent and warrant that they will:

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

(2) State the assurance level of the requested certificate when submitting a cross-certificate application, because the

certificates issued by HiPKI RCA have different assurance levels and different usages as stipulated in the CP;

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

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

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

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

(7) Properly safeguard and use their private keys;

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

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

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

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 RCA repository;

(2) Obtain a trusted HiPKI RCA public key or self-signed certificates through secure distribution channels described in Section 6.1.4;

(3) Check the certificate assurance level prior to the use of certificates;

(4) Check the keyUsage field prior to using a certificate to confirm that the certificate usage meets the usage restrictions set down by HiPKI RCA;

(5) Validated a certificate (issued by HiPKI RCA) by using a CARL or OCSP published by HiPKI RCA in accordance with the proper certificate path validation procedure;

(6) Obtain the self-issued certificate from the HiPKI RCA repository after HiPKI RCA re-keyed prior to using a certificate to establish a certificate trust path between HiPKI RCA and CAs;

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

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

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

9.6.5. Representations and Warranties of Other Participants

No stipulation.

9.7. Disclaimers of Warranties

Except to the extent prohibited by law or as otherwise provided herein, 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 subordinate CAs, cross-certified CAs 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 the CPS Section 9.9.

9.9. Indemnities

9.9.1. Indemnification by HiPKI RCA

(1) If subordinate CAs, cross-certified CAs or relying parties suffer damages due to intentional or accidental failure of HiPKI RCA work personnel to follow CPS regulations when performing self-signed certificate, self-issued certificate, CA certificate, and cross-certificate issuance and revocation work or violation of related laws and regulations which caused HiPKI RCA, subordinate CAs, cross-certified CAs or relying parties to suffer damages, HiPKI RCA shall compensate for the direct damages.

(2) In the event of damages caused by certificates issued by HiPKI RCA due to force majeure factors under Section 9.16.5, HiPKI

RCA shall not bear any liability.

(3) If a CA certificate is used for illegal transactions during the period that a CA or another entitled party submits a certificate termination request and HiPKI RCA actually completes the termination of that CA certificate, HiPKI RCA shall not bear any liability in accordance with this CPS and related work regulations.

(4) If damages are incurred due to the failure of a subordinate CA, cross-Certified CA or relying party to use the certificate in accordance with the appropriate scope as described in Section 1.4.1, HiPKI RCA shall not bear any liability.

(5) The limitation period for damage claims is set in accordance with the provisions of the Electronic Signatures Act and related laws and regulations.

9.9.2. Indemnification by Subordinate CAs and Cross-certified CAs

Under legal standards, HiPKI RCA may request that a subordinate CA and cross-certified CA be liable for the direct damages which were caused by the following circumstances:

(1) False or fraudulent reporting during certificate application by the subordinate CA or cross-certified CA results in the issuance of inaccurate CA certificates or cross-certificates by HiPKI RCA.

(2) Improper safekeeping of the private key by the subordinate CA or cross-certified CA that results in the compromise, disclosure, alteration or unauthorized use of the private key.

(3) The subordinate CA or cross-certified CA violates the law, CP or CPS (such as failure to issue proper certificates according to the assurance level in CPS regulations) or cross-certificate agreement regulations.

(4) The subordinate CA or cross-certified CA violates the agreements signed with HiPKI RCA for participation in the root certification programs of operation systems, browsers and software applications which could affect the trusted CA list that HiPKI RCA has built in or applied for built in the above application software suppliers.

HiPKI RCA may stipulate the liability of subordinate CAs or cross-certified CAs in the CCA.

9.10. Term and Termination

9.10.1. Term

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

9.10.2. Termination

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

9.10.3. Effect of Termination and Survival

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

9.11. Individual Notices and Communication with Participants

HiPKI RCA, subordinate CAs, cross-certified CAs and relying parties shall adopt suitable methods for establishing mutual notification and communication channels including but not limited to official document, letter, telephone, fax, e-mail or secure e-mail.

9.12. Amendments

9.12.1. Procedure for Amendment

This CPS is reviewed annually, and an assessment is made to determine if this CPS needs to be amended to maintain its assurance level. This CPS shall be amended accordingly if the HiPKI CP is amended or the OID is changed, and if so, changes to this CPS are indicated by appropriate numbering. 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. The new version of this CPS will publish according to the regulations stated in Section 2.3.

9.12.2. Notification Mechanism and Period

HiPKI RCA 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. HiPKI RCA will notify subordinate CAs and cross-certified CAs not owned by CHT through official letter or email to provide notice of proposed amendments. If CAs or relying parties have any comment on the change items, they can submit the comment within the comment period. Reassess to the changes and response may or may not be made by HiPKI RCA 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 CAs belonging to CHT and HiPKI

RCA, the dispute shall be resolved by a joint superior competent authority according to CHT's organization and management system. If there is a dispute between the Cross-certified CAs not established by CHT and HiPKI RCA, a consensus shall first be reached through negotiation. If negotiation fails, the parties shall handle the dispute according to the dispute resolution procedures provided in the contract. In the event of litigation, the Taiwan Taipei District Court shall be the court of first instance.

9.14. Governing Law

For disputes involving HiPKI RCA 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 the HiPKI CP and this CPS.

9.16. Miscellaneous Provisions

9.16.1. Entire Agreement

The commitments set forth in this CPS constitute the final and entire agreement between the participants (as stated in Section 1.3).

9.16.2. Assignment

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

9.16.3. Severability

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

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

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

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

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

9.16.5. Force Majeure

HiPKI RCA 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 RCA, including natural disasters, wars, or terrorism which may cause the interruption of telecommunications network.

9.17. Other Provisions

No stipulation.