Chunghwa Telecom HiPKI Certification Authority Certification Practice Statement

(HiPKICA CPS)

Version 0.97

Chunghwa Telecom Co., Ltd.

May 06, 2024

Contents

CPS Version Control

Version	Date	Revision Summary
0.95	May 12, 2023	(1) First Released. (2) This CPS states the practices of two CAs, including HiPKI RCA and HiPKI OV TLS CA.
0.97	May 06, 2024	Incrementing the version number.

1. Introduction

1.1 Overview

According to the HiPKI Certificate Policy (CP), HiPKI Root Certification Authority (HiPKI RCA) is a top-level CA and a trust anchor of HiPKI. HiPKI RCA must maintain a high level of credibility that relying parties can directly trust its certificates. This Certification Practice Statement (CPS) uses the brand name of Chunghwa Telecom HiPKI Certification Authority (HiPKICA) to refer to the HiPKI RCA and its subordinate CA, HiPKI OV Certification Authority (HiPKI OV CA), in HiPKI.

The SSL (Secure Sockets Layer) protocol has been replaced by the TLS (Transport Layer Security) protocol. Because SSL certificates and TLS certificates both refer to certificates that allow the TLS protocol to operate and comply with the X.509 standard, this CPS uses the term"TLS certificate" to replac the previous widely used one "SSL certificate".

1.1.1 Certification Practice Statement

This CPS describes the practices used to comply with the HiPKI CP, the R.O.C.

(1) Electronic Signatures Act and

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

and official versions of related international standards or regulations, including

(1) The Internet Engineering Task Force (IETF) request for comments (RFC) 3647, RFC 5280, RFC 6960, RFC 6962, RFC 5019, RFC 8659;

(2) ITU-T X.509;

(3) Baseline Requirements for the Issuance and Management of

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

to provide guidance and requirements for what HiPKICA should include in its CPS.

1.1.2 CPS Applicability

The practice statement stipulated in this CPS applies to CAs of HiPKICA, registration authority (RA), subscribers, relying parties, repository, and other participants.

1.2 Document Name and Identification

This document is Chunghwa Telecom HiPKi Certification Authority Certification Practice Statement. This CPS can be obtained at:

https://eca.hinet.net/repository-h/.

The assurance level and certificate policy object identifier (CP OID) defined in the HiPKI CP and descripted in this CPS are set forth in the following table:

Object Name	OIDs
This 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

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 {2.23.140.1.1} 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 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.

The HiPKI RCA certificate is a self-signed certificate. According to international standards and practices, the HiPKI RCA certificate does not indicate the CP OID to reflect its high-credibility of root CA and was operated with IAL 4.

The TLS certificates issued by HiPKI OV TLS CA conform to the requirements defined in the Baseline Requirements. HiPKI OV TLS CA may use the CP OIDs, defined by the CA/Browser Forum, ({joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline- requirements(2) organization-validated(2)} (2.23.140.1.2.2)) for organization validation (OV) TLS certificates.

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

1.3 PKI Participants

The key members of HiPKICA include:

(1) CAs of HiPKICA

(2) RAs

(3) Subscribers

(4) Relying Parties

1.3.1 Certification Authorities

The following CAs of HiPKICA are established and operated by Chunghwa Telecom Co., Ltd. (CHT), the relevant CPS shall be submitted to the Chunghwa Telecom Certificate Policy Management Authority (PMA)

for review and approve.

Certification Authority	Description
HiPKI RCA	Root certificate authority, which has been implanted in major Root Certificate Programs. https://eca.hinet.net/hrca.htm
HiPKI OV TLS CA	Responsible for issuing publicly-trusted TLS certificates. https://tls.hinet.net

HiPKICA's CA certificate information and applicable CP, CPS, external audit report and management statement are published at: https://eca.hinet.net/repository-h/index.htm.

1.3.2 Registration Authorities

The RA is responsible for collection and authentication of subscriber identity and certificate-related information. The RA is comprised of one or more RA counters authorized under the organization approved by HiPKICA. Each RA counter has an RA officer (RAO) who is responsible for the review of certificate application, revocation, and re-key for different certificate groups and types.

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

The RA of the subordinate CA can be directly established and maintained by the subordinate CA (known as internal RA), or may be established and maintained by the customer contracted by the CHT (known as external RA). RAs shall operate in accordance with this CPS, where internal RA may adopt stricter security control practices than this CPS.

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

1.3.3 Subscribers

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

Certificate Subject	Subscriber
Equipment	owner of the equipment
Application software	owner of the application software

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

In the HiPKI, a Subordinate CA is not called the subscriber because the Subordinate CA is capable of issuing certificates.

1.3.4 Relying Parties

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

1.3.5 Other Participants

No stipulation.

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, where the assurance level of subordinate CA certificates is level 3 and the others are level 4 (please refer to section 3.2.2 for authentication of organization identity). The types of certificates and their scope of application are shown as follows:

Cert. Type	Scope of Applications
Self-signed certificates	A self-signed certificate is used to establish the trust anchor of the HiPKI. The issuance subject of the self-signed certificate is the HiPKI RCA itself. The self-signed certificate contains the HiPKI RCA public key which can be used to verify the digital signatures on subordinate CA certificates, cross-certificates, self-issued certificates and certification revocation lists (CRLs) issued by HiPKI RCA.
Self-issued certificates	A self-issued certificate which is used for as the path for certificate policy mutual trust in case of the HiPKI RCA re-key or certificate policy update of the CA certificate.
Subordinate CA certificates	A subordinate CA certificate is used construct the trust path required for the interoperability of CAs. The issuance subject of the subordinate CA certificate is subordinate CA established under the HiPKI. The subordinate CA certificate contains the subordinate CA public key which can be used to verify the digital signatures on certificates and CRLs issued by the subordinate CA.
cross-certificates	A cross-certificate is used construct the trust path required for the interoperability of CAs under different PKIs. The issuance subject of the cross-certificate 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

Cert. Type	Scope of Applications
	key which can be used to verify the digital signatures on certificates and CRLs issued by that CA.

In compliance with the Chrome Root Certificate policy, the subordinate CAs of HiPKICA will only issue TLS certificates for equipments or application software that apply to the TLS communication protocol. Please refer to section 3.2.2 for assurance level and authentication of organization identity, and the types of certificates and their scope of application are shown as follows:

Cert. Type	Scope of Applications
Level 3 OV TLS certificates	Provides encryption of communication channels, and it is suitable for protecting network communication when it is necessary to identify which organization the domain name owner belongs to.

Subscribers and relying parties must carefully read and comply with this CPS before using and trusting the certificate service provided by HiPKICA, 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;
(4) Aviation flight and control systems; and
(5) Man-in-the-middle TLS traffic interception.

1.5 Policy Administration

1.5.1 Organization Administering the Document

Chunghwa Telecom Co., Ltd. (CHT).

1.5.2 Contact Person

1.5.2.1 CPS Related Issues

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

Email: caservice@cht.com.tw

Address: HiPKI Certification Authority (4F), Data Communication Building, No. 21, Sec.1, Hsinyi Rd., Taipei City 10048, Taiwan (R.O.C.)

1.5.2.2 Certificate Problem Report

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

HiPKICA may or may not revoke in response to this request. See Sections 4.9.3 and 4.9.5 for detail of actions performed by HiPKICA for making this decision.

1.5.3 Person Determining CPS Suitability for the Policy

HiPKICA shall first check whether this CPS conforms to the HiPKI CP regulations and then submit the CPS to the PMA for review and approval. After approval, HiPKICA is able to officially reference the HiPKI CP (https://eca.hinet.net/repository-h/en/index.htm).

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, Ministry of Digital Affairs.

HiPKICA conducts regular internal/external audits to demonstrate that it has operated with the assurance level under the HiPKI CP. In order

to ensure smooth operation of certificates by the CAs under HiPKI by operating systems, browsers, and software platforms, HiPKI has applied to the root certificate programs for operating systems, browsers and software platforms to include the self-signed certificates of HiPKI RCA in the CA trust lists of these platforms. According to the regulations of the root certificate program, the audits of HiPKICA are conducted annually and the latest CPS as well as the audit reports are submitted to the root certificate programs. HiPKICA also publishes the audit seals to the HiPKICA websites.

1.5.4 CPS Approval Procedures

This CPS is published by HiPKICA following approval by the PMA and Ministry of Digital Affairs. 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 Ministry of Digital Affairs 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

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

2. Publication and Repository Responsibilities

2.1 Repositories

The HiPKICA repository is responsible for the publication and storage of certificates and certificate revocation lists (CRLs) issued by HiPKICA and this CPS. HiPKICA provides availability of a 24x7 repository inquiry service to subscribers and relying parties. The URLs of the HiPKICA repositories are as follows:

Name of CAs	**URLs of the repositories**
HiPKI RCA	http://eca.hinet.net/repository-h/index.htm
HiPKI OV TLS CA	http://tls.hinet.net/

The repository will resume normal operation within two working days if unable to operate normally for some reason.

2.2 Publication of Certification Information

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

(1) The HiPKI CP and this CPS.

(2) All HiPKICA certificates, Cross-certificates, and CRLs

(3) Privacy protection policy.

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

HiPKICA hosts test Web pages (valid, expired, and revoked) that allow application software suppliers to test their software with subscriber certificates that chain up to each publicly trusted root certificate.

CAA (Certification Authority Authorization) issuer domain names (as specified in Section 4.2.1) of HiPKI OV TLS CA include ‘pki.hinet.net’ or ‘tls.hinet.net’.

2.3 Time or Frequency of Publication

(1) This CPS is reviewed and updated annually, and a dated changelog is state in the “Document History” section even if no other changes are 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 HiPKICA is published in the repository as soon as possible upon the approval of the PMA,

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

(4) HiPKICA certificates are published in the repository within seven working days after issuance.

2.4 Access Controls on Repositories

HiPKICA implements access control where it provides read-only access to prevent anyone from unauthorized writing operation, which would put repository security in risk.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

HiPKICA certificates are issued with the following types of names:

(1) The subject distinguished name (DN) shall comply with ITU-T X.500 standards.

(2) The subject alternative name extension for subscriber certificates must not be marked critical. When this extension contains a domain name syetem label, the domain name must be stored in the dNSName.

3.1.2 Need for Names to be Meaningful

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

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

Fully qualified domain names (FQDN) shall be appeared in the commonNames and Subject Alternative Name fields for TLS certificate. The DN for organization validation (OV) TLS certificate shall include the organization field verified in Section 3.2.2.

3.1.3 Anonymity or Psuedonymity of Subscribers

HiPKI OV TLS CA does not issue end entity pseudonymous

certificates.

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

3.1.4 Rules for Interpreting Various Name Forms

The rules for interpreting name forms follow the definition of name attribute type documented in ITU-T X.520.

3.1.5 Uniqueness of Names

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

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

3.1.6 Recognition, Authentication, and Role of Trademarks

The certificate subject name, including trademark or any name, business or company name or representation protected by law, provided by subscribers must comply with relevant regulations in our country's

Trademark Act, Fair-Trade Act, and other relevant laws and regulations. HiPKICA does not guarantee the recognition, verification, legality and uniqueness of the certificate subject name if it contains a trademark. Related disputes and arbitration shall not be the obligation of HiPKICA, the subscriber shall apply to relevant competent authorities, courts or arbitration institutions.

HiPKICA may reject any application or at its own discretion revoke certificates (refer to Section 4.9.1) that involves in a trademark dispute.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

HiPKICA shall verify that the entity (Subordinate CA or end entity) possesses the private key, which is paired with the public key to be contained in the certificate.

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

3.2.2 Authentication of Organization Identity

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

Assurance Level	Procedures for Authentication of Organization Identity
Level 1	There is no requirement to link the applicant to a specific real-life identity. Any attributes provided in conjunction with the

Assurance Level	Procedures for Authentication of Organization Identity
	authentication process are self-asserted. (1) No identity verification required. (2) The applicant is required to demonstrate control of their domain name to which the certificate relates. (3) In-person identity proofing at counter is not required.
Level 2	Evidence supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity. (1) No identity verification required. (2) In-person identity proofing at counter is not required. (3) The applicant is required to provide organization information such as organization ID number (i.e., withholding tax ID number) and organization name. HiPKICA may additionally cross-check the information provided by the applicant for consistency with available government or third-party data sources.
Level 3	HiPKICA allows the following methods for authentication of organization identity: (1) In-person (physically-present) identity proofing at counter, which can be one of the following means: a. A certification document or official document issued by government agency in the jurisdiction of the applicant; b. Public information obtained from a qualified government information source (QGIS) such as the MOEA industry and business registration database or a qualified government tax information source (QTIS) such as the Fiscal Information Agency of MOF; or c. Organizations belonging to CHT apply for the certificate with written application. (2) Remote identity proofing, which can be one of the following means and the detailed operating procedures are formulated in the internal control system of each RA: a. Application through an identity assurance level 3 organization certificate issued by the GPKI or ePKI; b. For those organization who has complete registration procedure with the competent authority, like (1)-a or (1)-b, mailing the copies of the certification documents is

Assurance Level	Procedures for Authentication of Organization Identity
	acceptable; c. A letter attesting that subject information is correct written by an accountant, lawyer, or notary; d. A site visit by CA personnel or a third party who is acting as an agent for the CA; or e. Organizations belonging to CHT apply for the certificate with e-form. For CAs: (1) The identity authentication of a CA established by CHT is reviewed by a PMA meeting convened by CHT. (2) For a CA not established by CHT, the CA shall submit an application of subordinate CA certificate, and a PMA meeting shall conven by CHT to review the application.
Level 4	(1) The identity authentication of a CA established by CHT is reviewed by a PMA meeting convened by CHT. (2) For a CA not established by CHT, the CA shall submit an application of cross-certificate, and a PMA meeting shall conven by CHT to review the application.
OV TLS certificates	In compliance with the Baseline Requirements and the provisions for assurance level 3.

3.2.3 Authentication of Individual Identity

No stipulation.

3.2.4 Non-verified Subscriber Information

All information provided by the subscriber to be listed in the certificates must be verified.

3.2.5 Validation of Authority

When a certificate lifecycle activity such as a certificate application or revocation request is submitted by an individual (an authorized representative) related to the certificate subject, HiPKICA or its RA shall

perform a validation of authority in accordance with Section 3.2.5 of the Baseline Requirements to verify that the individual can represent the certificate subject.

In addition, HiPKICA shall use one of the following methods (please refer to Section 3.2.5.1 to Section 3.2.5.7) set forth in the Baseline Requirements to validate the subscriber's right to use or control the domain name.

3.2.5.1 Validating the Applicant as a Domain Contact

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

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

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

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

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

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

SMS, or postal mail.

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

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

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

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

3.2.5.3 Constructed Email to Domain Contact

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

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

The Random Value SHALL be unique in each email.

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

The Random Value SHALL remain valid for use in a confirming

response for no more than 30 days from its creation.

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

3.2.5.4 Agreed-Upon Change to Website

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

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

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

The file containing the Request Token or Random Number:

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

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

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

(4) MUST be accessed over an Authorized Port.

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

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

Redirects MUST be the result of a 301, 302, or 307 HTTP status code response, as defined in RFC 7231, Section 6.4, or a 308 HTTP status code response, as defined in RFC 7538, Section 3. Redirects MUST be to the final value of the Location HTTP response header, as defined in RFC 7231, Section 7.1.2.

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

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

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

3.2.5.5 DNS Change

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

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

Once the FQDN has been validated using this method, HiPKICA MAY also issue TLS certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names. This method of validation confirms to Section 3.2.2.4.7 of the Baseline Requirements.

3.2.5.6 Email to DNS CAA Contact

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

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

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

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

3.2.5.7 Email to DNS TXT Contact

Confirming the Applicant's control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to a DNS TXT Record Email Contact for the Authorization Domain Name selected to validate the FQDN. Its format is defined in Baseline Requirements Section B.1.2.

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

The Random Value SHALL be unique in each email. The email MAY be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient(s) SHALL remain unchanged. The Random Value SHALL remain valid for use in a confirming response

for no more than 30 days from its creation.

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

If the FQDN portion of any Wildcard Domain Name is "registry-controlled" or is a "public suffix", HiPKICA refuses issuance unless the Applicant proves its rightful control of the entire Domain Namespace. (e.g. HiPKICA MUST NOT issue "*.com.tw" or "*.local"). If using the PSL, HiPKICA consults the "ICANN DOMAINS" section only, not the "PRIVATE DOMAINS" section.

3.2.6 Criteria for Interoperation

HiPKICA allows another root CA to interoperate with, see HiPKI CP for details.

3.2.7 Data Source Accuracy

Prior to using any data source as a Reliable Data Source, HiPKICA SHALL evaluate the source for its reliability, accuracy, and resistance to alteration or falsification. HiPKICA 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 HiPKICA, its owner, or its affiliated companies do not qualify as a Reliable Data Source, if the primary purpose of the database is to collect information according to the validation requirements in Section 3.2 of the Baseline Requirements.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

If the subscriber or CA's private key needs to be renewed upon expiry of the certificate period, certificate rekey work may be performed, and the subscriber may re-apply for certification. The RA may validate the subscriber's identity by using the subscriber's public key to verify the CSR, or conduct an initial identity validation in accordance with Section 3.2. The identification and authentication for routine re-key of TLS certificate are handled in accordance with the Baseline Requirements.

3.3.2 Identification and Authentication for Re-key after Revocation

If the subscriber or CA's private key needs to be re-keyed due to certificate revocation, the subscriber or CA shall re-apply for a new certificate with HiPKICA, and an initial identity validation shall be conducted in accordance with Section 3.2.

3.4 Identification and Authentication for Revocation Request

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

4. Certificate Life-cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Either the applicant or an individual authorized to request certificates on behalf of the applicant may submit certificate applications.

4.1.2 Enrollment Process and Responsibilities

The certificate application procedures are as follows:

(1) Use the appropriate secure platform to generate an appropriate key pair.

(2) Generate a PKCS#10 CSR using an appropriately tool.

(3) Fill out the information on the certificate application and agrees to a subscriber agreements or other applicable terms and conditions.

(4) Submit the certificate application request (including the CSR, the legal name of the organization or the website FQDN based on the type of the certificate applied for, etc.) and provide relevant identification documents to the RA, where the application information can be in electronic form.

The RA are responsible for ensuring the accuracy of the application request and performing the identification and authentication of the applicant before delivery the request to the issuing CA for issuance.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Upon receipt of the certificate request, HiPKICA and RAs shall verify the application information in accordance with Section 3.2. The certificate applicant shall submit correct and complete factual information. The

information required for the certificate application shall contain required and optional information. The information submitted by the certificate applicant and contact records kept by HiPKICA and RA during the application process shall be properly kept in a secure, auditable manner in accordance with the HiPKI CP and this CPS.

For TLS certificates, the RA system maintains an internal database of all previously revoked certificates and previously rejected certificate requests due to suspected phishing or other fraudulent usage. HiPKI OV TLS CA and its RA implements extra procedures that identify and require additional verification activity for High-Risk Certificate requests prior to the certificate's approval, as reasonably necessary to ensure that such requests are properly verified under the Baseline Requirements.

Prior to issuing a TLS certificate, HiPKI OV TLS CA checks the DNS for the existence of a CAA record for each dNSName in the subjectAltName extension of the certificate to be issued, as specified in RFC 8659, and in accordance with Section 3.2.2.8 of the Baseline Requirements. If the certificate is issued, it will be issued within the Time to Live (TTL) of the CAA record, or 8 hours, whichever is greater.

HiPKI OV TLS CA supports the "issue" CAA tag and logs all actions taken. If a CAA record exists that does not list "pki.hinet.net" or "tls. hinet.net" as a CAA Issuer Domain Name, HiPKI OV TLS CA will not issue the certificate. HiPKI OV TLS CA does not dispatch reports of issuance requests to the contact(s) listed in an "iodef" property tag.

4.2.2 Approval or Rejection of Certificate Applications

HiPKI OV TLS CA will not issue TLS certificates containing internal names or reserved IP addresses. The verification of the authorization domain name and the basic domain name must comply with the regulations as specified in Section 3.2.5.

If all identity authentication work follows relevant regulations and best practices can be successfully implemented, HiPKICA may approve the certificate application.

If the various identity authentication works cannot be successfully completed, HiPKICA may reject the certificate application. In addition to this reason, HiPKICA may refuse to issue certificates for other reasons. HiPKICA and its RA may also reject certificate application from applicants who have previously been rejected or have previously violated the subscriber agreements.

A PMA meeting is convened when any CA submits a Subordinate CA certificate or cross-certificate application. The PMA will review the related documents provided by the CAs to evaluate the appropriateness for becoming a subordinate CA or Cross-certified CA of HiPKI RCA. The PMA may decide that the application enters the next stage, supplemental information is required, or the application is rejected.

4.2.3 Time to Process Certificate Applications

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

Upon receiving the certificate application, the RAO will complete the review process, and the applicant will be asked to accept the certificate. The times when the issuing CA completes the issuance of the certificate are given as follows:

Type of Certificates	Time required for processing and issuance the Certificate
OV TLS Certificates	within 2 bussiness days

Issuance time frames are greatly dependent on when the applicant provides the details and documentation necessary to complete validation or complates the certificate acceptance.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

HiPKI RCA cannot automatically issue certificates and shall follow the regulations in Section 5.2.2.

Upon HiPKICA receive the certificate application, the relevant review procedures are enforced in accordance with Chapter 3 of this CPS to serve as a basis for determining whether approve the certificate issuance.

Certificate issuance steps are follows:

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

(2) When the issuing CA receives the certificate application submitted by the RA, the authorization status of the RA is first checked to confirm its authorized assurance level and scope, and then the certificate is issued according to the information of the certificate application submitted by the RA.

(3) If the authorized assurance level and scope of the RA does not comply with the certificate application, the issuing CA will response the error message to the RA and reject the request. If there are any questions, the RA may directly contact the issuing CA to understand where the problem is.

(4) The CA issuing TLS certificates provides the function of pre-issuance linting, which can check whether the format of the certificate to be issued complies with the requirements of the Baseline Requirements/RFC 5280. If it does not meet the

requirements, it will be rejected to prevent mis-issuance or false of the certificate.

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

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

HiPKICA shall notify the subscriber about the certificate issuance during the enrollment process by email or any other equivalent method. The email may contain the certificate itself or a link to download depending upon the workflow of the certificate requested.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Upon the issuance of the certificate, HiPKICA shall inform the certificate applicant, and the certificate is published to the repositoty after the certificate applicant verified the accuracy of the certificate content and accepts the certificate. If the certificate applicant refuses to accept the issued certificate after reviewing the content of the certificate, it should inform the RA to revoke the certificate.

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

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.

HiPKICA publishes end-entity certificates by delivering them to the Subscriber.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

If there are newly issued self-signed certificates, HiPKI RCA will submit the inclusion application in compliance with the root certificate program of operating system, browser, and software platform to include the certificate into the CA trust lists.

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 this CPS. Subscribers must be able to control the private keys, which must not be used to issue certificates.

Subscribers shall protect their private keys from unauthorized use or disclosure and shall use their private keys only for the correct key usage (i.e., the policy for key usage specified in the extension of the certificates). Subscribers shall use their certificates in accordance with the HiPKI CP and this CPS.

4.5.2 Relying Party Public Key and Certificate Usage

When relying parties use a certificate, they shall confirm its certificate usage and use it in accordance with this CPS. Relying parties may only use a tool or a method that is compliant with the ITU-T X.509, IETF RFCs or Baseline Requirements.

Prior to a certificate’s use, the tool or method selected by relying parties must verify each certificate in the certificate chain, including the accuracy of the content of specific fields, the integrity of the signature, and the validity of the certificate status, where the certificate status may be

obtained from a CRL or an online certificate status protocol (OCSP) service.

In addition, relying parties shall check the content of the certificate policies extension of the issuing CA and TLS certificates to confirm the assurance level of the certificates.

4.6 Certificate Renewal

HiPKICA does not allow certificate renewal.

4.6.1 Circumstances for Certificate Renewal

Not applicable.

4.6.2 Who May Request Renewal

Not applicable.

4.6.3 Processing Certificate Renewal Requests

Not applicable.

4.6.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Not applicable.

4.6.6 Publication of the Renewal Certificate by the CA

Not applicable.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.7 Certificate Re-Key

4.7.1 Circumstance for Certificate Re-key

Under the following circumstances, the subordinate CA/cross-certified CA will renew the key and ask HiPKI RCA to issue a new subordinate CA/cross-certified 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).

Subscribers whose certificates have not expired may request a re-key, and HiPKICA shall identify and authenticate them in accordance with Section 3.3.1. After the key pair is re-keyed, HiPKICA may revoke the old certificate and does not allow the modification or re-key of the old certificate.

4.7.2 Who May Request Certification of a New Public Key

The subject of the certificate or an authorized representative.

4.7.3 Processing Certificate Re-keying Requests

For subscriber certificate re-keying, HiPKICA shall validate the request in accordance with Sections 3.1, 3.2, 3.3, 4.1 and 4.2 and may re-validate the subscriber subject with any previously validated data when needed.

4.7.4 Notification of New Certificate Issuance to Subscriber

As stated in Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

As stated in Section 4.4.1.

4.7.6 Publication of the Re-keyed Certificate by the CA

As stated in Section 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.8 Certificate Modification

4.8.1 Circumstance for Certificate Modification

Certificate modification means creating a new certificate for the same subject, where authenticated information that slightly differs from the old certificate (e.g., changes to FQDN or other relatively attribute information). The new certificate has a new certificate serial number but with the same subject public key and 'NotAfter' date. After the certificate is modified, the old certificate shall be revoked.

4.8.2 Who May Request Certificate Modification

The subject of the certificate or an authorized representative.

4.8.3 Processing Certificate Modification Requests

(1) The application procedure for certificate modification is as Section 4.2.

(2) If there is any change to the important identity information such as the organization name, the original certificate must be revoked. The subscriber must submit a new certificate application with the modified organization name to obtain a new certificate.

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

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

4.9.1 Circumstances for Revocation

4.9.1.1 Circumstances for Revoking a Subscriber Certificate

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

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

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

(3) HiPKICA obtains evidence that the subscriber's private key corresponding to the public key in the certificate suffered a key compromise;

(4) HiPKICA is made aware of a demonstrated or proven method that can easily compute the subscriber's private key based on the public key in the certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys); or

(5) HiPKICA obtains evidence that the validation of domain authorization or control for any FQDN or IP address in the certificate should not be relied upon.

HiPKICA should revoke a certificate within 24 hours and must revoke a certificate within 5 days if one or more of the following occurs:

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

(2) HiPKICA obtains evidence that the certificate was misused;

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

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

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

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

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

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

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

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

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

4.9.1.2 Circumstances for Revoking a Subordinate CA Certificate

HiPKI RCA shall revoke a Subordinate CA certificate within seven (7)

days if one or more of the following occurs:

(1) The Subordinate CA requests revocation in writing to HiPKI RCA;

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

(3) HiPKI RCA obtains evidence that the Subordinate 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 has not complied with this document or the applicable CP/CPS;

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

(7) HiPKI RCA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the certificate;

(8) HiPKI RCA'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.

The issuing CA may at its own discretion revoke certificates, including subscriber certificates, subordinate CA certificates or cross-certificates, under the aforementioned circumstances.

4.9.2 Who Can Request Revocation

Subscribers or legally authorized third party (such as judicial or prosecution authorities, the subject of the certificate or an authorized

representative, and legal heirs of natural person) can request revocation.

In addition, a subscriber, relying party, application software suppliers or other third party may submit certificate problem report to advise HiPKICA a reasonable reason to revoke the certificate. HiPKICA shall take actions in accordance with Section 4.9.5 and confirm the validity of the certificate revocation request upon receiving the certificate problem report.

4.9.3 Procedure for Revocation Request

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

(2) After the RA completes the review work, the certificate revocation request is sent to HiPKICA;

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

(4) If the above checking does not comply with the revocation request, HiPKICA will response the error message to the RA and reject the request. If there are any questions, the RA may directly contact HiPKICA to understand where the problem is;

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

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

(7) HiPKICA receives certificate problem reports and provides 24x7 availability of certificate problem response mechanism, as specified in Section 4.9.3.1.

4.9.3.1 Mechanism for Responding the Certificate Problems

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

4.9.4 Revocation Request Grace Period

The certificate revocation request grace period refers to the time to submit a revocation request when the subscriber has confirmed the certificate revocation circumstances. When the subscriber's private key is lost or suspect or known to be compromised, the subscriber shall promptly submit a revocation request to the RA. The revocation request grace period is two working days. HiPKICA may extend the revocation grace period when deemed necessary.

If any of the circumstances described in Section 4.9.1 occurs, CAs or RAs shall submit the revocation request within 10 working days.

4.9.5 Time within Which CA Must Process the Revocation Request

Within 24 hours after receiving a Certificate Problem Report, HiPKICA shall investigate the facts and circumstances related to a

Certificate Problem Report and provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report.

After reviewing the facts and circumstances, HiPKICA shall work with the Subscriber and any entity reporting the Certificate Problem Report or other revocation-related notice to establish whether 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 HiPKICA shall consider the following criteria:

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

4.9.6 Revocation Checking Requirement for Relying Parties

Prior to relying on a certificate, relying parties must verify the accuracy and validity of each certificate in the certificate chain, including checking for the certificate validity, digital signature, issuer/subject name chaining, certificate policies, key usage, and certifciate status, where the certificate status may be checked through a CRL or an OCSP response.

Relying parties must also confirm the validity of the CRL or OCSP response prior to use it, such as verifying the digital signature, checking the validity period, and confirming the issuer/subject name chaining.

4.9.7 CRL Issuance Frequency

The CRL issuance frequency of HiPKICA is at least twice per day. Issued CRL are valid for no more than 36 hours. Before the CRL expires,

HiPKICA may issue a new CRL. The new CRL validity period may overlap the validity period of the old CRL. Even though the old CRL has not yet expired, relying parties still may obtain the new CRL from the HiPKICA repository to receive the updated certificate revocation information.

4.9.8 Maximum Latency for CRLs

Except for HiPKI RCA has pre-signed of CRLs, after a CRL is produced by other CAs, it will be released immediately.

4.9.9 On-line Revocation/Status Checking Availability

The status information for HiPKICA cerificates is availabe via CRLs, web-based certificate search/download function, and OCSP services.

HiPKICA uses an OCSP responder to provide OCSP responses complying with RFC 6960 and RFC 5019, where the OCSP responses are signed by the OCSP responder using a 2048-bit or greater RSA key (that modulus size in bits is divisible by 8) and a hash algorithm at least as strong as SHA-256. In addition, the OCSP responder also provides OCSP responder certificates, which are issued by HiPKICA and contain the extension of type id-pkix-ocsp-nocheck, as defined by RFC 6960.

4.9.10 On-line Revocation Checking Requirements

Relying parties must confirm the validity of a certificate in accordance with Section 4.9.6 before using it.

HiPKICA provides an OCSP service that an OCSP responder operated under the service supports the HTTP-based POST and GET methods, as described in RFC 6960 and RFC 5019. The certificate status information provided by the service shall meet the following requirements:

(1) For status of TLS certificates: HiPKICA updates an OCSP response prior to one-half of the validity period before the nextUpdate, and the validity interval of the OCSP response is

greater than or equal to 8 hours and less than 16 hours.

(2) For status of self-issued certificates, subordinate CA certificates, and cross-certificates: HiPKICA updates the information at least every twelve months and within 24 hours after any of these certificates is revoked.

A certificate serial number within an OCSP request is one of the following three options:

(1) “assigned” if a certificate with that serial number has been issued by HiPKICA; or

(2) “reserved” if a precertificate, which is required for issuing TLS certificates, with that serial number has been issued by HiPKICA; or

(3) “unused” if neither of the previous conditions are met.

If the OCSP responder receives a request for the status of a certificate serial number that is “assigned”, the responder shall respond with the current status of the certificate corresponding to 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. HiPKICA shall monitor the OCSP responder for requests of “unused” serial numbers 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 certificates status of high-traffic websites, HiPKICA supports OCSP stapling operation based on RFC 4366 and through the support of Certificate Transparency (CT) and technical review, or provision of relevant setting instructions to assist subscribers who own high-traffic websites to implement OCSP stapling.

4.9.12 Special Requirements Related to Key Compromise

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

In case of a compromise of CA's private key, HiPKI RCA will publish a CRL to inform software suppliers, subscribers, and relying parties about the private key compromise event.

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

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

(2) Submitting the private key itself.

4.9.13 Circumstances for Suspension

HiPKICA does not allow suspension of CA certificates and TLS certificates.

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.

4.9.17 Procedure for Certificate Resumption

Not applicable.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

HiPKICA provides CRLs and OCSP services. Revocation entries on a CRL or OCSP response must not be removed until after the expiry date of the revoked certificate. If a revocation entry contains the information of a suspended certificate, the entry can only be removed after the certificate has been resumed or expired.

4.10.2 Service Availability

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

HiPKICA maintains an online 24x7 repository that application software can use to automatically check the current status of all unexpired certificates issued by HiPKICA.

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

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

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

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

HiPKICA's private signing keys shall not be escrowed.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

HiPKICA does not currently support session key encapsulation and recovery.

5. Facility, Management, and Operation Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

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

5.1.2 Physical Access

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

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

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

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

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

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

5.1.4 Water Exposures

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

5.1.5 Fire Prevention and Protection

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

5.1.6 Media Storage

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

5.1.7 Waste Disposal

When the documents of HiPKICA detailed in Section 9.3.1 are no longer in use, it shall be shredded by the paper shredder. Any storage media that HiPKICA used shall be formatted to erase the information stored on it before scrapping, and discs shall be physically destroyed.

5.1.8 Off-site Backup

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

5.2 Procedural Controls

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

5.2.1 Trusted Roles

In order to make appropriate segmentation and assignment of the responsibility for performing system-related operations, to prevent someone from maliciously using the CA system without being noticed, the trusted role authorized to perform each system access task is clearly defined in HiPKICA.

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

The administrator is responsible for:

- Installation, configuration and maintenance of the HiPKICA system
- Creation and maintenance of system user accounts
- Generation and backup of HiPKICA keys
- Activation / deactivation of related keys of certificate manager
- System hardware and software updates
- System backup and recovery
- Website maintenance
- Patching the system vulnerabilities

The CA officer is responsible for:

- Generation and backup of HiPKICA keys
- Activation / deactivation of keys for certificate issuance
- Activation / deactivation of keys for certificate revocation
- Activation / deactivation of keys for CRL issuance

The internal auditor is responsible for:

- Generation and backup of HiPKICA keys
- Checking, maintenance and archiving of audit logs
- Conducting or supervising internal audits to ensure HiPKICA is operating in accordance with this CPS
- Patching the anti-virus and vulnerabilities of audit system

The system operator is responsible for:

- Archiving of audit logs
- Daily operation and maintenance of system equipment
- Storage media updating
- Set up protection mechanisms for system security and threats of virus or malware

The physical security controller is responsible for:

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

The cyber security coordinator is responsible for:

- Maintenance of the network and network facilities
- Patches management for the vulnerabilities of the network facilities
- The network security of HiPKICA
- The detection and report of the network security events

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

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

5.2.2 Number of Persons Required per Task

In accordance with security requirements, the number of persons

required for each trusted role is as follows:

- Administrator

  At least 3 qualified individuals are needed.

- CA Officer

  At least 3 qualified individuals are needed.

- Internal Auditor

  At least 2 qualified individuals are needed.

- System Operator

  At least 2 qualified individuals are needed.

- Physical security controller

  At least 2 qualified individuals are needed.

- Cyber security coordinator

  At least 1 qualified individual.

- Anti-virus and anti-hacking coordinator

  At least 1 qualified individual.

The number of persons 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 HiPKICA system	2				1		
Establishment and maintenance of system user accounts	2				1		
Generation and backup of HiPKICA keys	2	2	1		1		
Activation / deactivation of certificate issuance, certificate revocation and CRL issuance	2	2			1		

Assignments	Administrator	CA Officer	Internal Auditor	System Operator	Physical security controller	Cyber security coordinator	Anti-virus and anti-hacking coordinator
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		
Hardware and software updates outside the HiPKICA system	1				1		
Website maintenance	1				1		
Daily operation and maintenance of the network and network facilities				1	1	1	
Patching the vulnerabilities of the network facilities	1				1	1	
Reporting the threats and vulnerabilities of computer virus							1
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

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

HiPKICA utilizes user accounts, passwords, and groups for system account management and IC card to identify and authenticate administrator, CA officer, internal auditor and system operator. HiPKICA utilizes the authority setting function of the central access control system to identify

and authenticate physical security controllers.

HiPKICA utilizes user accounts, passwords, and groups for system account management, or other security mechanisms to identify the role of the cyber security coordinator.

5.2.4 Roles Requiring Separation of Duties

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

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

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

(1) Security evaluation for personnel selection

Personnel selection includes the following items:

(a) Personality evaluation;

(b) Applicant experience evaluation;

(c) Academic and professional skills and qualifications evaluation;

(d) Personal identity check; and

(e) Evaluation of personnel conduct.

(2) Management of Personnel Evaluation

All HiPKICA personnel performing certificate work shall have their qualifications reviewed at the initial time of employment to verify their reliability and work capabilities. After

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

(3) Appointment, Dismissal and Transfer

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

(4) Duty of Confidentiality Agreement

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

5.3.2 Background Check Procedures

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

5.3.3 Training Requirements

Trusted Role	Training Requirements
Administrator	(1) HiPKICA security principles and mechanism. (2) Installation, configuration, and maintenance of the HiPKICA operation procedures. (3) The use and operation procedures of HiPKICA system software and hardware. (4) Establishment and maintenance of system user accounts operation

Trusted Role	Training Requirements
	procedures. (5) Audit parameter configuration setting procedures. (6) HiPKICA key generation and backup operation procedures. (7) Procedure of disaster recovery & business continuity planning.
CA Officer	(1) HiPKICA security principles and mechanism. (2) HiPKICA key generation and backup operation procedures. (3) Activation/deactivation of certification issuance operation procedure. (4) Activation/ deactivation of certification revocation operation procedure. (5) Activation/ deactivation of certificate CRL issuance operation. (6) Procedure of disaster recovery & business continuity planning.
Internal Auditor	(1) HiPKICA security principles and mechanism. (2) The use and operation procedures of HiPKICA audit Server. (3) HiPKICA key generation and backup operation procedures. (4) Audit log check, maintain and archiving procedures. (5) Procedure of disaster Recovery & business continuity planning.
System Operator	(1) Daily operation and maintenance procedures for system equipment. (2) Upgrading of storage media procedure. (3) Procedure of disaster Recovery & business continuity planning. (4) Network and website maintenance procedure.
Physical security controller	(1) Physical access authorization setting procedure. (2) Procedure of disaster Recovery & business continuity planning.
Cyber security coordinator	(1) Network and network facilities maintain procedure. (2) Security mechanism for the network.
Anti-virus and anti-hacking coordinator	(1) Prevention to the threats and vulnerabilities of computer virus. (2) Security mechanism for the operating system and the network.

5.3.4 Retraining Frequency and Requirements

In case of software/hardware upgrades, working procedures changed, equipment replaced, or relevant regulations changed, relevant personnel will be arranged for retraining and the training situation will be recorded, so as to make the personnel understand the changes in relevant operating procedures and regulations.

5.3.5 Job Rotation Frequency and Sequence

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

(2) Personnel with a full two years of experience as a system operators, cyber security coordinator, or anti-virus and anti-hacking coordinator with the requisite training and review may be reassigned to the position of administrator, CA officer or internal auditor.

(3) Administrator, CA officer and internal auditor may be reassigned to the position of administrator, CA officer or internal auditor after they have been transferred from their original positions for one full year.

5.3.6 Sanctions for Unauthorized Actions

HiPKICA related personnel shall be subject to appropriate administrative and disciplinary actions for violations of the HiPKI CP, this CPS or other procedures announced by HiPKICA. 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

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

5.4 Audit Logging Procedures

HiPKICA shall keep security audit logs for all events related to HiPKICA 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 in accordance with the archive retention regulations stated in Section 5.5.2.

5.4.1 Types of Events Recorded

(1) Key generation
- Key generation of CAs

(2) Private key loading and storage
- Loading the private key into a system component.
- All access to private keys kept by HiPKICA for key recovery work.

(3) Certificate registration
- Certificate registration request process.

(4) Certificate revocation
- Certificate revocation request process.

(5) Account administration
- Add or delete roles and users.
- User account or role access authority revisions.

(6) Certificate profile management
- Certificate profile changes.

(7) CRL profile management
- CRL profile changes.

(8) Physical access / site security
- Known or suspect violation of physical security regulations.

(9) Anomalies
- Software defect.

- CPS violation.
- Reset system clock.

5.4.2 Frequency of Processing Log

HiPKICA shall routinely review audit logs to prevent possible malicious activity, and any significant operations should be further reviewed. Review work includes examining all log entries and conducting a final complete check for any warnings or anomalies. Audit checking results shall be documented.

5.4.3 Retention Period for Audit Log

Audit logs shall be retained on-site for two months, and the log retention management system shall be operated in accordance with Sections 5.4.4, 5.4.5, 5.4.6 and 5.5.

If the retention period of the audit record file expires, the auditor is responsible for removing the data and cannot be behalfed by other personnel.

5.4.4 Protection of Audit Log

Signature and encryption technology shall be used to protect the current and archived audit logs. A CD-R or other media storage that cannot change the audit logs is used, and only authorized personnels can access.

HiPKICA's audit system enforces resource control and identity identification security mechanisms, only authorized auditor has backup and read access to logs, and the system keeps a log file of access audit records to detect and prevent improper access.

5.4.5 Audit Log Backup Procedures

(1) HiPKICA shall routinely archive event logs, and electronic audit logs are backed up at least once a month.

(2) At least one copy of the media for storing audit logs shall be kept at an off-site location with proper security control measures.

5.4.6 Audit Collection System (Internal vs. External)

Audit systems are built in the HiPKICA system, and audit procedures are activated when the HiPKICA system is activated and only stops when the HiPKICA system is shut down.

If the automated audit system cannot operate normally, HiPKICA 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 status.

5.4.7 Notification to Event-causing Subject

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

5.4.8 Vulnerability Assessments

CAs that issuing TLS certificates shall follow the methods and frequency stipulated in the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security and Network and Certificate System Security Requirements to conduct the vulnerability assessments at least once per quarter and the penetration testing at least once per year. HiPKI OV TLS CA should perform a vulnerability assessment when identifying significant changes to a network or system. HiPKI OV TLS CA also must conduct penetration testing after it is determined that there is a significant upgrade or modification to the application program or infrastructure. HiPKICA shall implement the enhancement and correction measures after the penetration testing and the vulnerability assessment. HiPKICA shall record the skills, tools, followed ethics, competitive relations and independence guidelines for those personnel or groups capable of implementing reliable vulnerability scans, penetration testing, or information security diagnosis or security surveillance.

5.5 Records Archival

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

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

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

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

5.5.1 Types of Records Archived

HiPKICA retains the following information in its archives:

(1) HiPKICA accreditation information from competent authorities.
(2) CPS.
(3) Major contracts.
(4) System and equipment configuration settings.
(5) System and configuration setting modifications and updates.
(6) Certificate application information.
(7) Revocation request information.
(8) Subscriber identity identification information stipulated in Section 3.2.
(9) Issued and published certificates.
(10) HiPKICA re-key records.
(11) Issued or announced CRLs.
(12) Audit logs.

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

(14) Documents required by the auditor.

5.5.2 Retention Period for Archive

HiPKICA retains archived data for at least 2 years. The application programs used to process archived data are retained until all archived data is deprecated.

5.5.3 Protection of Archive

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

(2) The archived data can be moved to another storage medium after pass through the HiPKICA authorized procedures.

(3) The archived data is stored in a secure, protected location.

5.5.4 Archive Backup Procedures

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

5.5.5 Requirements for Time-stamping of Records

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

5.5.6 Archive Collection System (Internal or External)

There is currently no archive collection system.

5.5.7 Procedures to Obtain and Verify Archive Information

Only authorized HiPKICA personnel are allowed to access the archive.

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

5.6 Key Changeover

HiPKICA shall periodically change its private keys in accordance with Section 6.3.2 and shall change its key pair before the usage period of its private key issuing subscriber certificates has expired. After key changeover of Subordinate CAs, an application for a new CA certificate shall be submitted to HiPKI RCA is required and the new CA certificate shall be published in the HiPKICA repository.

After key changeover of HiPKI RCA, 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 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 the HiPKI RCA repository.

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

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

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

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

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

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

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

5.7.3 Entity Private Key Compromise Procedures

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

(1) Publish in the repository and notify subscribers and relying parties about the event of key compromise.
(2) Revoke the HiPKICA signature key certificate and issued subscriber certificates.
(3) Generate new key pairs in accordance with the procedures in Section 5.6 and the new certificates are published in the HiPKICA repository.

HiPKICA shall conduct the drills of CA private key compromise at least once a year.

5.7.4 Business Continuity Capabilities after a Disaster

HiPKICA has established a disaster recovery procedure and conducts

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

5.8 CA or RA Termination

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

(1) HiPKICA shall notify the competent authority, Ministry of Digital Affairs, and subscribers 30 days prior to of the scheduled termination of service.

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

- For certificates which are valid at the time of termination, arrangements shall be made for other CA to take over the service. Matters regarding service termination and service acceptance by other CAs shall be published in the repository and subscribers with valid certificates stall be notified. This shall not apply if notification cannot be made.
- All records and files during the operation period shall be handed over to the other CA that is taking over this service.
- If there is no CA willing to take over the HiPKICA service, a report shall be submitted to the competent authority to arrange for other CA to take over this service.
- If the competent authority arranges for other CA to take over the service but no other CA takes over the service, HiPKICA shall revoke the still valid certificates, publish the revoked certificates in the repository and notify all certificate-related persons 30 days prior to the scheduled termination of service. HiPKICA will refund the certificate issuance fee based on the propotion of the certificate validity.

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

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

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

According to the regulations in Section 6.2.2, HiPKICA generates key pairs within the hardware security module by using the algorithm and the procedures that meets NIST FIPS 140-2 standard.

HiPKICA key generation is witnessed and videotaped by those related personnel who need to sign key initiation witness document (the public key of the generated key pair is listed on it). The related personnel shall include the members of the PMA and/or the qualified auditors.

6.1.2 Private Keys Delivery to Subscriber

HiPKICA should not generate key pair of TLS or Subordinate CA certificates on behalf of the subscriber.

6.1.3 Public Key Delivery to Certificate Issuer

If a subscriber self-generates a key pair, the subscriber shall deliver the public key to the RA via a CSR file with PKCS# 10 format. The RA shall delivery the public key to HiPKICA via secure channels after it is verified that the subscriber is in possession of the corresponding private key in accordance with the regulations in Section 3.2.1.

Secure channels referred in this Chapter are the use of TLS or other equivalent or higher-level data encryption transmission protocols.

6.1.4 CA Public Key Delivery to Relying Parties

Commercial web browsers and platform operators are encouraged to embed Root Certificate Public Keys of HiPKICA into their root stores and operating systems. HiPKICA shall deliver the certificates containing the certificate chain of relevant CAs to the subscriber after certificate issuance.

Relying parties can also download the public key certificates of the relevant CAs through the repository operated by HiPKICA. Excepet for HiPKI RCA, HiPKICA notes the download location of the relevant public key certificates in the certificate chain through the Authority Information Access (AIA) extension of the issued certificate.

6.1.5 Key Sizes

HiPKICA complies with the regulations of the HiPKI CP in using key sizes, as described below:

(1) Root CAs shall use RSA keys with the modulus size of 4096 bits or ECDSA keys with a valid point on the NIST P-384 elliptic curve. The hash algorithm required to issue certificates depends on the Root CAs' key algorithm:

- RSA keys: SHA-256, SHA-384, or SHA-512;
- ECDSA keys: SHA-384 (with the P-384 curve).

(2) Subordinate CAs and cross-certified CAs shall choose RSA keys with the modulus size of 4096 bits or ECDSA keys with a valid point on the NIST P-256/NIST P-384 elliptic curve. The hash algorithm required to issue certificates depends on the aforementioned CAs' key algorithm:

- RSA keys: SHA-256, SHA-384, or SHA-512.
- ECDSA keys: SHA-256 (with the P-256 curve) or SHA-384 (with the P-384 curve).

(3) Subscribers shall use RSA keys with the modulus size of at least 2048 bits or ECDSA keys with a valid point on the NIST P-256/NIST P-384 elliptic curve.

(4) The modulus size of the aforementioned RSA key (in bits) must be divisible by 8.

6.1.6 Public Key Parameters Generation and Quality Checking

The public key parameter of the RSA algorithm is null.

HiPKICA shall use the ANSI X9.31 algorithm or the NIST FIPS 186-4 standard to generate the prime number needed for the RSA algorithm if a RSA key pair is selected and ensure that the prime number is a strong prime.

Cross-certified CAs must perform appropriate key parameter quality checking according to the selected algorithm.

There is no need to guarantee that the prime number, which is needed for the RSA algorithm and generated inside the software/hardware security modules, is a strong prime when subscribers use RSA key pairs.

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

In case certificates are issued with Elliptic Curve Cryptography (ECC) algorithm, HiPKICA shall follow the requirements of Sections 5.6.2.3.2 and 5.6.2.3.3 in NIST SP 800-56A Revision 2 to confirm the validity of all keys using either the ECC Full Public Key Validation Routine or the ECC Partial Public Key Validation Routine.

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

6.1.7.1 Key Usage Purposes of CAs

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

The content of the key usage extention in the self-signed certificates, self-issued certificates, subordinate CA certificates and cross-certificates issued by HiPKI RCA shall meet the requirements of Section 7.1.2.

6.1.7.2 Key Usage Purposes of Subscribers

The keyUsage extension of TLS certificates has two key usage bits set: keyEncipherment and digitalSignature. The extKeyUsage extension includes the values id-kp-serverAuth and id-kp-clientAuth.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

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

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

HiPKICA's private keys are controlled in accordance with the multi-person control process specified in the HiPKI CP, and this process can be used as the activation and deactivation methods for private keys as well as the backup and recovery methods for private key splitting.

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

6.2.3 Private Key Escrow

HiPKICA does not escrow its private signing keys. HiPKICA does not provide private key escrow services as well.

6.2.4 Private Key Backup

Backups of HiPKICA private keys are made according to private key multi-person control set forth in Section 6.2.2, and high-security IC cards are used as the storage media for secret sharing. HiPKICA does not provide additional private key backup services.

6.2.5 Private Key Archival

HiPKICA does not archive its private signing keys.

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 requirements of 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.

If HiPKICA becomes aware that its subordinate CA's or cross-certified CA's 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

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

Subscribers shall choose a secure computer environment and a trustworthy application system carefully and keep and use the private keys properly.

6.2.9 Method of Deactivating Private Key

When the private keys of HiPKICA is not in use, an appropriate deactivation method will be selected to deactivate the private keys in

compliance with HiPKI CP. HiPKICA does not provide the deactivate services of subscribe private keys.

6.2.10 Method of Destroying Private Key

In order to prevent the theft of HiPKICA private keys which could endanger the authenticity of the entire certificate, the private key must be destroyed at the end of the HiPKICA key lifecycle. Therefore, when HiPKICA completes the key renewal and HiPKI RCA issues a new HiPKICA certificate, after no additional certificates or CRL are issued, zeroization is done on the old HiPKICA private key stored inside the hardware security module to ensure that the old HiPKICA private key is destroyed. In addition to destroying the old HiPKICA private key in the hardware security module, physical destruction of the splitted IC cards with a backed-up key inside shall be done as well during the HiPKICA key renewal.

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

Subordinate CAs and cross-certified CAs must follow the HiPKI CP regulations when choosing an appropriate private key destruction method. The destruction method for subscriber private keys is not stipulated.

6.2.11. Cryptographic Module Rating

See Section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

HiPKICA archives certificates issued by it in accordance with Section 5.5.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

6.3.2.1 CA Certificate Operational Periods and Key Pair Usage Periods

Certificates and private keys of HiPKICA's issuing CAs have maximum validity periods of:

Type of CA	Private Key Usage	Certificate Term
Root CA	■ Issuing self-signed certificates: 15 years ■ Issuing self-issued certificates: no stipulation ■ Issuing cross-certificates: no stipulation ■ Issuing subordinate CA certificates: 15 years ■ Issuing CRLs, OCSP responder certificates or OCSP responses: 25 years	25 years
Subordinate CA / Cross-certified CA	■ Issuing subscriber certificates: 10 years ■ Issuing CRLs, OCSP responder certificates or OCSP responses: 20 years	20 years

The expiry date of subordinate CA certificates or cross-certificates issued by HiPKI RCA must not be greater than the end of HiPKI RCA's self-signed certificate's validity period.

The expiry date of HiPKI RCA's self-issued certificates cross-signed with old and new HiPKI RCA keys shall be equal to the expiry date of HiPKI RCA's self-signed certificate issued with the old HiPKI RCA key.

The validity period for private keys and certificates of an OCSP responder is 36 hours. An OCSP response signed by the OCSP reponder's private key includes the signature and the OCSP responder certifcate that can be used by relying parties to verify the signature of the OCSP response.

6.3.2.2 Subscriber Certificate Operational Periods and Key Pair Usage Periods

The maximum validity periods of the subscriber certificate and private key are:

Type of Cert.	Private Key Usage Period	Certificate Term
OV TLS Certificate	No stipulation	398 days

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The activation data of HiPKICA's private key is randomly generated and written to the hardware cryptographic module after completing identity verification for administrators of n-out-of-m control IC cards based on the access control list set during the generation of the afforementioned private key. Administrators must insert their n-out-of-m control IC cards into the card reader built in the hardware cryptographic module and enter the correct personal identification number (PIN) of IC cards when performing identity verification as mentioned above.

6.4.2 Activation Data Protection

Activation data is protected by the n-out-of-m control IC cards. Administrators who hold the IC cards are responsible for the safekeeping of the card PIN, which shall not be stored in any media. If the administrator enters the wrong PIN for more than 3 consecutive times, the IC card is locked. During IC card handover, a new PIN is set by the new administrator.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

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

(1) Trusted role or identity authentication login,
(2) Provide discretionary access control,
(3) Provide security audit capability, and
(4) Access control restrictions for certificate services and PKI trusted roles.

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

6.5.2 Computer Security Rating

HiPKICA servers use Common Criteria EAL 3 or above certified computer operating systems.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

Quality control for HiPKICA's system development complies with Capability Maturity Model Integration (CMMI) standards.

System development, test and production environments shall operate independently to prevent unauthorized access or changes. In addition, HiPKICA may only use dedicated and authorized hardware and software.

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

For each product or program delivered to HiPKICA, it is required to provide the delivery list, test report, and source code analysis report, as well as be under version control.

6.6.2 Security Management Controls

HiPKICA shall not install software, hardware or components that are not related to its operation. When installing software onto a CA system, HiPKICA shall first confirm the integrity and correctness of the version and check the integrity of CA software regularly or before each use. In addition, HiPKICA documents and controls any change to the system as well as detecting unauthorized modifications to system software or configurations.

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

6.6.3 Life Cycle Security Controls

HiPKICA shall conduct a risk assessment at least once a year to determine if there is any risk of compromise for existing keys.

6.7 Network Security Controls

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

The HiPKICA host and repository have firewalls and are connected to external networks. The repository is placed in the external service area of the firewall (de-militarized zone, DMZ) and connected to the Internet. Except during required maintenance or backup, the repository provides uninterrupted certificate and CRL inquiry services.

The certificates and CRLs issued by the HiPKICA are digitally signed and transmitted to the repository. The HiPKICA repository protects against denial of service and intrusion attacks by system patch updates, system vulnerability scans, intrusion defending/detection systems, firewall systems and filtering routers.

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

6.8 Time-stamping

HiPKICA 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. Automatic or manual procedures may be used to adjust the system time, and system clock synchronizations shall be auditable events.

(1) Time of certificate issuance,

(2) Time of certificate revocation,

(3) Time of CRL issuance, and

(4) Time of system event occurrence.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

The certificates issued by HiPKICA conform to the official versions of the ITU-T X.509, Baseline Requirements and RFC 5280.

HiPKICA 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)

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

7.1.2 Certificate Extensions

See Appendix 3 for details.

7.1.3 Algorithm Object Identifiers

HiPKICA uses the algorithms listed in the table below for signing certificates and generating key pairs.

Purpose	Algorithm	OID
Signature	sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}
	sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha384WithRSAEncryption(12)}
	sha512WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha512WithRSAEncryption(13)}
	ecdsaWithSHA256	{iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2)}
	ecdsaWithSHA384	{iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA384(3)}
	ecdsaWithSHA512	{iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA512(4)}

Key Generation	rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(1)}
	ecPublicKey	{iso(1) member-body(2) us(840) ansi-x962(10045) keyType(2) ecPublicKey(1)}

During ECC algorithm is used for generarting ECDSA key pairs, the OIDs of the elliptic curve parameter is set as follows according to the key size:

Key Size	Elliptic Curve Parameter	OID
P-256	secp256r1	{iso(1) member-body(2) us(840) ansi-x962(10045) curves(3) prime(1) prime256v1(7)}
P-384	secp384r1	{iso(1) identified-organization(3) certicom(132) curve(0) ansip384r1(34)}

7.1.4 Name Forms

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

7.1.4.1 Name Encoding

According to Section 7.1.4.1 of the Baseline Requirements, the encoded content of the issuer DN field of certificates issued by an issuing CA shall be byte-for-byte identical with the encoded form of the subject DN field of the issuing CA's certificate. If there are two or more CA certificates, including expired and revoked CA certificates, whose subject DNs can be compared as equal, the encoded content of the subject DN field of the aforementioned certificates shall be byte-for-byte identical.

7.1.4.2 Subject Information–CA Certificates

Certificates can be issued after issuing CAs followed the procedures

set forth in the HiPKI CP and this CPS to verify that all of the subject information was accurate. For self-signed certificates and subordinate CA certificates issued by HiPKI RCA, the subject DN field includes three attributes, namely “commonName”, “organizationName”, and “countryName”, described as follows:

(1) commonName

The name used to identify the issuing CA. It is the unique identifier of the certificate and can be used to distinguish the issuing CA’s certificate from other CA certificates.

(2) organizationName

The official name of the organization to which the issuing CA belongs. It can be adjusted according to the abbreviation method approved by our country. The authentication of this organization name shall be implemented in accordance with Section 3.2.2.

(3) countryName

The country where the place of business that the issuing CA locates. It shall be represented by the country codes specified in ISO 3166-1, which is “TW”.

7.1.4.3 Subject Information–Subscriber Certificates

By issuing the subscriber certificates, HiPKICA represents that they followed the procedures set forth in the HiPKI CP and/or this CPS to verify that, as of the subscriber certificate’s issuance date, all of the subject information was accurate. For TLS certificates, if the commonName field of subject DN is present, this field must contain exactly one entry that is one of the values contianed in the subject alternative name extension which contains the FQDNs validated by one of the methods stated in Section 3.2.5. In addition, subject attributes MUST NOT contain only metadata such as ‘.’, ‘-’, and ‘ ’ (i.e. space) characters, and/or any other indication that the

value is absent, incomplete, or not applicable.

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

For the certificate application that the entry in the subject alternative name extension of subscriber certificates will contain a FQDN, the RA officers shall validate the ownership or control of the domain name in compliance with Section 3.2.5.

7.1.5 Name Constraints

Name constraints are not applied to HiPKICA certificates. Self-signed certificates, self-issued certificates, subordinate CA certificates and cross-certificates, which are not technically constrained, will be disclosed publicly, such as being disclosed in the Common CA Database (CCADB) of Mozilla.

7.1.6 Certificate Policy Object Identifier

HiPKICA certificates, excluding self-signed certificates of HiPKI RCA, must include the certificate policies extension. In addition to the CP OID(s) defined in the HiPKI CP, this extension may also contain the CA/Browser Forum-assigned OID(s) referenced in the HiPKI CP according to the certificate purpose. With regard to the related statement of the CP OIDs, please refer to Section 1.2 of the HiPKI CP.

7.1.7 Usage of Policy Constraints Extension

The policy constraints extension may be used as required for subordinate CA certificates and cross-certificates issued by HiPKI RCA. Otherwise, certificates issued by HiPKICA do not contain this extension.

7.1.8 Policy Qualifiers Syntax and Semantics

The policy qualifier field in the certificate policies extension of HiPKICA certificates may be used as needed. When using this field, it may

contain a CPS pointer qualifier that points to this CPS.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

The certificate policies extension of the certificates issued by HiPKICA are not marked critical.

7.2 CRL Profile

7.2.1 Version Number(s)

HiPKICA issues CRLs complying with RFC 5280 and ITU-T X.509 version 2.

7.2.2 CRL and CRL Entry Extensions

The CRL and CRL entry extensions in the CRL issued by HiPKICA comply with the official versions of the ITU-T X.509, Baseline Requirements and RFC 5280. These extensions are described below.

(1) CRL Extensions

Extension	Criticality	Description
Authority Key Identifier	FALSE	The SHA-1 hash value of the CRL issuer's public key.
CRL Number	FALSE	A monotonically increasing sequence number for a given CRL scope and CRL issuer.
Issuing Distribution Point	TRUE	This extension is only applicable to a partitioned CRL. It is used to identify the CRL distribution point, indicate whether the CRL covers revocation for end entity certificates only, CA certificates only, attribute certificates only, or a limited set of reason codes, and state whether or not it is an indirect CRL. The scope of the CRL only includes certificates issued by HiPKICA, and thus the indirectCRL boolean must be set to FALSE.

(2) CRL Entry Extensions

Extension	Criticality	Description
Reason Code	FALSE	If this CRL entry extension is used to identify the revocation reason of self-signed certificates, self-issued certificates, subordinate CA certificates and cross-certificates, the reasonCode value can be the follows: ➢ caCompromise(2) ➢ affiliationChanged(3) ➢ superseded(4) ➢ cessationOfOperation(5) ➢ privilegeWithdrawn(9) If the CRL entry extension is used to identify the revocation reason of subscriber certificates, the reasonCode value is as follows. ➢ keyCompromise(1) ➢ affiliationChanged(3) ➢ superseded(4) ➢ cessationOfOperation(5) ➢ privilegeWithdrawn(9)

7.3 OCSP Profile

HiPKICA provides OCSP services in compliance with RFC 6960 and RFC 5019, and includes a HTTP URL of the issuing CA's OCSP responder in the authority Information access extension of HiPKICA certificates (excluding self-signed certificates of HiPKI RCA).

7.3.1 Version Number(s)

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

- Protocol version; and
- Target certificate identifier.

An OCSP response, issued by the OCSP responder, at a minimum consists of a responseStatus field indicating the processing status of the prior request. If the value of responseStatus is 'successful', the OCSP

response must further include the other fields as follows:

Field	Description
Version	v.1 (0x0)
OCSP Responder ID	The subject DN of OCSP responder
Produced Time	The time at which the OCSP response was signed
Target Certificate Identifier	The contents of this field include the hash algorithm, the hash of the issuer's DN, the hash of the issuer's public key and the serial number of the target certificate.
Certificate Status	The meaning of certificate status value is described below: ➢ 0: valid ➢ 1: 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 CRL (See Section 7.2.2). 2: unknown
ThisUpdate/NextUpdate	Recommended validity period for this OCSP response, including ThisUpdate and NextUpdate
Signature Algorithm	OCSP response signature algorithm, which can be either: ■ sha256WithRSAEncryption, or ■ ecdsaWithsha384
Signature	OCSP responder signature
Certificates	OCSP responder certificate

7.3.2 OCSP Extensions

The singleExtensions of an OCSP response MUST NOT contain the reasonCode (OID 2.5.29.21) CRL entry extension.

8. Compliance Audit and Other Assessments

8.1 Frequency or Circumstances of Assessment

HiPKICA 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

HiPKICA entrusts external audit operations to qualified auditors, who is familiar with the operations of HiPKICA and authorized by the WebTrust for CA program management unit to implement relevant WebTrust Principles and Criteria for Certification Authorities audit criteria 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. HiPKICA shall conduct identity identification of auditors during audits.

8.3 Assessor’s Relationship to Assessed Entity

CHT shall entrust an impartial third party to conduct audits of HiPKICA operations.

8.4 Topics Covered by Assessment

HiPKICA undergoes an audit in accordance with the scheme of “WebTrust for CAs”. For CAs issuing TLS certificates, they should also

undergoe additional audit scheme of "WebTrust for CAs SSL Baseline with Network Security v2.3 or newer".

The assessment shall include the following topics:

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

HiPKICA has the right to conduct the review and examination of following (but not limited to) items to ensure its trustworthiness:

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

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

and examination.

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

8.5 Actions Taken as a Result of Deficiency

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

(1) Note the discrepancy,

(2) Notify HiPKICA about the discrepancy, and

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

8.6 Communications of Results

Except for any audit findings that could result in system attacks and the stipulations in Section 9.3, HiPKICA shall make its audit report publicly available. Audit results are displayed with appropriate seals, including WebTrust for Certification Authorities and WebTrust for Certification Authorities – SSL Baseline Requirements seals, on HiPKICA's homepage. The audit report and management's assertions may

be viewed by clicking on the seals. HiPKICA 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, HiPKICA shall provide an explanatory letter signed by the qualified auditor.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

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

9.1.2 Certificate Access Fees

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

9.1.3 Revocation or Status Information Access Fees

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

9.1.4 Fees for Other Services

No stipulation.

9.1.5 Refund Policy

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

9.2 Financial Responsibility

9.2.1 Insurance Coverage

HiPKICA is owned and operated by CHT. Its financial responsibilities are the responsibilities of CHT.

9.2.2 Other Assets

HiPKICA 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. HiPKICA can provide self-insured asset prices based on CHT's financial reports. CHT's finances are sound and its ratio of current assets to current liabilities is no lower than 1.0 which meets the requirement of the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates.

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The following information generated, received and kept by HiPKICA

or its RA is deemed confidential information:

(1) Private keys and passphrases used for operations,

(2) Key splitting safekeeping information,

(3) Subscriber application information,

(4) Audit and tracking logs generated or kept by HiPKICA,

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

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

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

9.3.2 Information Not Within the Scope of Confidential Information

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

(2) Information of issued certificates, revoked certificates and CRLs published in the HiPKICA repository are not deemed confidential information.

9.3.3 Responsibility to Protect Confidential Information

HiPKICA shall handle subscriber application information in accordance with the Electronic Signatures Act, WebTrust Principles and Criteria for Certification Authorities audit criteria, Baseline Requirements, WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security audit criteria, and Personal Information Protection Act and its related sub-laws.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

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

9.4.2 Information Treated as Private

Private information includes:

(1) The personal information listed on certificate applications should not be disclosed without the subscriber's consent or in accordance with related laws,

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

(3) Personnel identifiable information in HiPKICA such as names together with palmprint or fingerprint biometrics, and

(4) Personal information on confidentiality agreements or contracts.

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

9.4.3 Information Not Deemed Private

The following information not deem as private:

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

(2) Information of issued certificates, revoked certificates and CRLs published in the HiPKICA repository are not private information.

9.4.4 Responsibility to Protect Private Information

The personal information required for the operation of HiPKICA, in either paper or digital form, must be handled in accordance with Personal Information Protection Act and its related sub-laws and privacy rights declaration posted on the website. HiPKICA shall negotiate the liability of protecting private information with its RA.

9.4.5 Notice and Consent to Use Private Information

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

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

If judicial, supervisory or law enforcement authorities need to check private information under Section 9.3.1 due to one of the following conditions, the matter shall be handled in accordance with law or regulation:

(1) The provisions of government decrees and the legal authorization of the competent authority; or
(2) The court handles disputes arising from the use of certificates and legal application needs for arbitration.

Otherwise, the registered personal information and identification-related information of subscribers will never be arbitrarily provided to the competent authority or any other person.

9.4.7 Other Information Disclosure Circumstances

Subscriber personal information obtained during HiPKICA operations

is handled in accordance with related laws and may not be disclosed externally, unless stipulated otherwise under the law.

9.5 Intellectual Property Rights

The following is the intellectual property of HiPKICA:

(1) Related documents or system development for certificate management of HiPKICA;

(2) Certificates and CRLs issued by HiPKICA; and

(3) This CPS.

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. This CPS can be used reasonably and no fee will be charged. HiPKICA reserves the right to pursue legal action for any violation of the use or dissemination of this CPS.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

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

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

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

the Certificate; and (iii) accurately described the procedure in this CPS (see Section 3.2);

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

(3) **Accuracy of Information**: That, at the time of issuance, HiPKICA (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);

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

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

(6) **Subscriber Agreement**: That, if HiPKICA and Subscriber are not Affiliated, the Subscriber and HiPKICA are parties to a legally valid and enforceable Subscriber Agreement that satisfies the Baseline Requirements, or, if HiPKICA and Subscriber are the same entity or are Affiliated, the Applicant Representative

acknowledged the Terms of Use;

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

(8) **Revocation**: That HiPKICA will revoke the Certificate for any of the reasons specified in the Baseline Requirements (see Section 4.9.1).

9.6.2 RA Representations and Warranties

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

RAs shall represent and warrant that:

(1) Certificate verification is performed in compliance with the HiPKI CP and this CPS;

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

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

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

(5) Identification and authentication procedures for RAO are implemented; and

(6) RA private keys are securely managed.

9.6.3 Subscriber Representations and Warranties

For the express benefit of HiPKICA and the Certificate Beneficiaries, the Applicant shall warrant that, prior to the issuance of a certificate, HiPKICA will obtain, either:

(1) The Applicant’s agreement to the Subscriber Agreement with

HiPKICA, or

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

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

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

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

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

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

(5) Promptly notify HiPKICA, cease using a certificate, and request revocation of the certificate, if

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

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

(6) Use the certificate only for legal and authorized purposes, consistent with the HiPKI CP, this CPS and Subscriber Agreement, i.e., only installing TLS certificates on servers accessible at the domain listed in the certificate, and

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

9.6.4 Relying Party Representations and Warranties

Each relying party represents and warrants to:

(1) Comply with the provisions of this CPS when using a certificate or querying the HiPKICA repository;

(2) Check the certificate assurance level before using it;

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

of certificates;

(4) Validate a certificate (issued by HiPKICA) by using a CRL or OCSP published by HiPKICA to confirm the validity;

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

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

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

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

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

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

HiPKICA will assume the compensation liability no more than the amount stipulated in Section 9.9 of this CPS.

9.9 Indemnities

9.9.1 Indemnification by HiPKICA

If subscribers or relying parties suffer damages due to the intentional or unintentional failure of HiPKICA to follow the HiPKI CP, this CPS, relevant laws or the provisions of contracts signed between HiPKICA and subscribers/relying parties when processing subscriber certificate-related work, HiPKICA shall be held liable. Subscribers may claim compensation for damages based on the related provisions of the contract set down between HiPKICA (or its RA) and subscribers. Relying parties shall request compensation in accordance with laws and regulations. The total compensation limit of HiPKICA for each subscriber or relying party is shown in the Table below. If the subscriber or relying party has signed a contract with HiPKICA, the certificate scope of use and transaction compensation limit shall be determined separately.

Certificate Assurance Level	Compensation Limit (NTD)
Level 1	3,000
Level 2	100,000
Level 3	3,000,000
Level 4	5,000,000

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

9.9.2 Indemnification by RA

If subscribers or relying parties suffer damages due to the RA intentional or unintentional failure to follow this CPS, related laws or the

provisions of contracts signed between the RA and subscribers/relying parties when processing subscriber certification registrations, HiPKICA is only responsible for compensation for the RA established by HiPKICA, and the compensation limits are detailed in Section 9.9.1. For other RA not established by HiPKICA, the RA takes the responsible of compensation. If the RA and subscribers or relying parties have a contract determing the usage of certificates and transaction compensation amounts, then the contract takes precedence. Compensation claims by subscribers shall be made in accordance with related provisions in the contract set down with the RA. Compensation claims by relying parties shall be made in accordance with relevant laws and regulations.

9.10 Term and Termination

9.10.1 Term

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

9.10.2 Termination

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

9.10.3 Effect of Termination and Survival

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

9.11 Individual Notices and Communications with Participants

HiPKICA, RAs, subscribers, relying parties shall adopt suitable methods for establishing mutual notification and communication channels

including but not limited to official document, letter, telephone, fax, email or secure email.

9.12 Amendments

9.12.1 Procedure for Amendment

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

9.12.2 Notification Mechanism and Period

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

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

9.12.3 Circumstances under which OID Must Be Changed

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

9.13 Dispute Resolution Provisions

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

9.14 Governing Law

For disputes involving HiPKICA issued certificates, the applicable ROC laws shall govern.

9.15 Compliance with Applicable Law

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

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

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

9.16.2 Assignment

The participants describes in this CPS may not assign or delegate their rights or obligations under this CPS to other parties in any form without a prior notice to HiPKICA.

9.16.3 Severability

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

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

domestic laws, this CPS will delete and amend the adjusted contents. The aforesaid actions shall be completed within 90 days.

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

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

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

9.16.5 Force Majeure

HiPKICA 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 HiPKICA, including natural disasters, wars, or terrorism which may cause the interruption of telecommunications network. HiPKICA has set clear limitations for certificate usage and is not bear any legal responsibility for damages caused by exceeding these usage limitations.

9.17 Other Provisions

No stipulation.

Appendix 1: Acronyms and Definitions

Acronyms	Full Name	Definition
AIA	Authority Information Access	See Appendix 2.
CA	Certification Authority	See Appendix 2.
CAA	Certification Authority Authorization	See Appendix 2.
CMMI	Capability Maturity Model Integration	See Appendix 2.
CP	Certificate Policy	See Appendix 2.
CPA	Chartered Professional Accountants Canada	See Appendix 2.
CP OID	CP Object Identifier	
CPS	Certification Practice Statement	See Appendix 2.
CRL	Certificate Revocation List	See Appendix 2.
DN	Distinguished Name	
DNS	Domain Name System	See Appendix 2.
HiPKI RCA	HiPKI Root Certification Authority	See Appendix 2.
EE	End Entities	See Appendix 2.
HiPKI	Chunghwa Telecom HiPKI	See Appendix 2.
FIPS	(US Government) Federal Information Processing Standard	See Appendix 2.
FQDN	Fully Qualified Domain Name	See Appendix 2.
IANA	Internet Assigned Numbers Authority, IANA	See Appendix 2.
IDN	Internationalized Domain Name	See Appendix 2.
IETF	Internet Engineering Task Force	See Appendix 2.

Acronyms	Full Name	Definition
NIST	(US Government) National Institute of Standards and Technology	See Appendix 2.
OCSP	Online Certificate Status Protocol	See Appendix 2.
OID	Object Identifier	See Appendix 2.
OV	Organization Validation	See Appendix 2.
PIN	Personal Identification Number	
PKCS	Public-Key Cryptography Standard	See Appendix 2.
PKI	Public Key Infrastructure	See Appendix 2.
QGIS	Qualified Government Information Source	See Appendix 2.
QTIS	Qualified Government Tax Information Source	See Appendix 2.
RA	Registration Authority	See Appendix 2.
RFC	Request for Comments	See Appendix 2.
SSL	Secure Sockets Layer	See Appendix 2.
TLS	Transport Layer Security	See Appendix 2.
UPS	Uninterrupted Power System	See Appendix 2.

Appendix 2: Glossary

Access	Use the information processing capabilities of system resources
Access Control	Authorization procedure for access to information system resources given to subscribers, programs, procedures and other systems.
Activation Data	Private data, other than keys, that are required to access cryptographic modules and that need to be protected (i.e., unlock private keys for signing or decryption events).
Applicant	Subscribers who request certificates from a CA and have not yet completed the certificate procedure.
Archive	A physically separate storage site for long-term information (storage site for important information) which can be used to support audit, usage and integrity services.
Assurance	A basis that the trusted entity has complied with certain security requirements. [Article 2-1, Chapter 1, Regulations on Required Information for Certification Practice Statements]
Assurance Level	A certain level in a relative assurance tier. [Article 2-2, Chapter 1, Regulations on Required Information for Certification Practice Statements]
Audit	Assessment of whether system controls are adequate and ensure conformance with existing policy and operation procedures, and independent checking and review of recommended required improvements to existing controls, policies and procedures.
Audit Data	Activity logs of a system organized in the order of time of occurrence that can be used to reconstruct or investigate the time sequence or changes that occurred during a certain event.
Authenticate	(1) Authentication is the process by which a claimed identity is verified. [A Guide to Understanding Identification and Authentication in Trusted Systems, National Computer Security Center]

	(2) Determination of identity authenticity when an identity of a certain entity is shown.
Authentication	(1) The process of establishing confidence in user identities electronically presented to an information system. [NIST.SP.800-63-2 Electronic Authentication Guideline] (2) Safety measures used to secure data transmission or ways to authorize the privilege of individuals upon receiving certain types of information. (3) Authentication is the process by which a claimed identity is verified. [A Guide to Understanding Identification and Authentication in Trusted Systems] Mutual authentication means that the authentication is performed between two parties during communication.
Authority Information Access (AIA)	Records extensions related to certificate authority information access. The content may include: OCSP service sites and certificate issuance authority certificate verification path downloading site.
Authorization Domain Name	The Domain Name used to obtain authorization for certificate issuance for a given FQDN. The CA may use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. If the FQDN contains a wildcard character, then the CA MUST remove all wildcard labels from the left most portion of requested FQDN. The CA may prune zero or more labels from left to right until encountering a Base Domain Name and may use any one of the intermediate values for the purpose of domain validation.
Backup	Information or program copying that can be used for recovery purposes when needed.
Base Domain Name	The portion of an applied-for FQDN that is the first domain name node left of a registry controlled or public suffix plus the registry-controlled or public suffix (e.g. "example.co.uk" or "example.com"). For FQDNs where the right-most domain name node is a gTLD having ICANN Specification 13 in its registry agreement, the gTLD itself may be used as the Base Domain Name.

Baseline Requirements	"The Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" issued by CA/Browser Forum, and all the amendments.
Binding	The process for binding (connecting) two related information elements.
CA Certificate	Certificates issued by CAs.
CA Key Pair	A Key Pair where the Public Key appears as the Subject Public Key Info in one or more Root CA Certificate(s) and/or Subordinate CA Certificate(s).
Capability Maturity Model Integration (CMMI)	CMMI is the successor of the Capability Maturity Model (CMM) and was developed by the Software Engineering Institute at Carnegie Mellon University. CMMI models provide guidance for developing or improving processes that meet the business goals of an organization. Its purpose is to help improve organizational performance.
Certificate	(1) Refers to verification information carrying a digital signature used to verify the identity and qualifications of the signer in electronic form [Article 2-6, Electronic Signatures Act] (2) Digital presentation of information. The contents include: A. Issuing certificate authority B. Subscriber name or identity C. Subscriber public key D. Certificate validity period E. Certification authority digital signature The term 'certificate' referred to this CPS specifically refers to ITU-T X.509 v.3 format certificates which states the certificate policy object identifier in the 'certificate policy' field.
Certification Authority (CA)	(1) The agency or natural person that issues certificate [Article 2-5, Electronic Signatures Act] (2) The competent body trusted by the subscriber. Its functions are the issuance and administration of ITU-T X.509 format public key certificates, and CRLs.
Certification	The certification authority authorization (CAA) DNS

Authority Authorization (CAA)	resource record allows a DNS domain name holder to specify one or more certification authorities (CAs) authorized to issue certificates for that domain. CAA resource records allow a public CA to implement additional controls to reduce the risk of unintended certificate mis-issue. [RFC 8659]
Certificate Policy (CP)	(1) Refers to a named set of rules that indicates the applicability to a certain community or class of application with common security requirements [Article 2-3, Chapter 1, Regulations on Required Information for Certification Practice Statements] (2) Certificate policy refers to the dedicated profile administration policy established for the electronic transactions performed through certificate administration. Certificate policy covers a variety of issues including the formation, generation, delivery, auditing, administration and restoration after compromise. Certificate policy indirectly controls the use and operation of certificate security systems to protect the transactions performed by the communication systems. The security services required for certain application are provided through control of the certificate extension methods, certificate policy and related technology.
Certification Practice Statement (CPS)	(1) External notification by the certificate authority used to describe the practice statement of the certificate authority governing certificate issuance and processing of other certification work. [Article 2-7, Electronic Signatures Act] (2) Announcement of a statement that certain procedures of the certificate authority for certificate work (including issuance, suspension, revocation, renewal and access) comply with certain requirements (listed in the certificate policy or other service contracts).
Certificate Profile	A set of documents or files that defines requirements for Certificate content and Certificate extensions in accordance with Section 7 of the Baseline Requirements. e.g. a Section in a CA's CPS or a certificate template file used by CA software.

Certificate Problem Reports	The complaints regarding suspected cracking of keys, certificate misused, or other types of fraud, cracks, abuse, or inappropriate behaviors related to certificates.
Certificate Revocation	Termination of a certificate prior to its expiry date.
Certificate Revocation List (CRL)	(1) The certificate revocation list digitally signed by the certification authority provided for relying party use. [Article 2-8, Chapter 1, Regulations on Required Information for Certification Practice Statements] (2) List maintained by the certificate authority. The expiry dates of the above revoked certificates issued by the certification authority are recorded on the list.
Chartered Professional Accountants Canada (CPA)	Institution which jointly drafted The Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy system standards with the American Institute of Certified Public Accountants (AICPA) and the management organization for WebTrust for CA and SSL Baseline Requirement & Network Security mark. Canadian Institute of Chartered Accountants is abbreviated as CICA.
Compromise	Information disclosed to unauthorized persons or unauthorized intentional or unintentional disclosure, modification, destruction or loss of objects which constitutes a violation of information security policy.
Confidentiality	Information which will not be known or be accessed by unauthorized entities or programs.
Cross-Certificate	A certificate used to establish a trust relationship between two root CA. This certificate is a type of CA certificate and not a subscriber certificate.
Cryptographic Module	A set of hardware, software, firmware or combination of the above used to run cryptologic or programs (including crypto algorithms) and included within the cryptographic boundaries of the module.
Data Integrity	Information that has been subjected to unauthorized

	access or accidental modification, damage or loss.
Digital Signature	An electronic signature generated by use of mathematic algorithm or other means to create a certain length of digital data encrypted by the signatory's private key and capable of being verified by the public key. [Article 2-3, Electronic Signatures Act]
Domain Contact	The Domain Name Registrant, technical contact, or administrative contract (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record.
Domain Name	A node label assigned by the domain name system. Converts the IP address into a text name that is easily remembered by humans.
Domain Name Registrant	Sometimes referred to as the domain name owner, but it is more appropriate to say a certain individual or entity who have registered with the Domain Name Registrar to have the right to use a domain name and the Domain Name Registrant or WHOIS has listed the 'registrant' as a natural person or legal person.
Domain Name Registrar	A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns).
Domain Name System (DNS)	A distributed database used to automatically convert the IP address to domain name.
DNS CAA Email Contact	The email address defined in BR Section A.1.1.
DNS TXT Record Email Contact	The email address defined in BR Section A.2.1.
Duration	A certificate field made up of two subfields "start time of the validity period" (notBefore) and "end time of the validity period" (notAfter).
E-commerce	Provision of goods for sale and other services through the use of network technology (specifically the

	Internet).
End Entity	The PKI includes the following two types of entities: (1) Those responsible for the safeguarding and use of certificate public keys. (2) Third parties who trust the certificates issued by the PKI (not holders of private keys and not a certificate authority). The end entities are subscribers and relying parties including personnel, organizations, accounts, devices and sites.
End-Entity Certificate	Certificates issued to end-entities.
Chunghwa Telecom HiPKI (HiPKI)	A hierarchical PKI established by CHT in compliance with Chrome Root Certificate policies and ITU-T X.509. The subordinate CA in this PKI will only issue TLS certificates for Transport Layer Security (TLS) communication protocol equipment or application software.
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.
HiPKI Root CA (HiPKI RCA)	The Root CA and top-level CA in HiPKI, and its public key is the trust anchor of HiPKI.
Federal Information Processing Standard (FIPS)	Except for military organizations in the US Federal Government System, information processing standard for all government organizations and government subcontractors. The security requirement standard for the cryptographic module is FIPS no. 140 standard (FIPS 140). FIPS 140-2 divides the cryptographic module into 11 types of security requirements. Each security requirement type is then divided into 4 security levels.
Firewall	An access restriction gateway between networks which complies with near-end (local area) security policy.
Fully Qualified	An unambiguous domain name that specifies the exact

Domain Name (FQDN)	location of a computer within the domain's hierarchy. The FQDN consists of two parts: the host name (service name) and domain name. For example, ourserver.ourdomain.com.tw, ourserver is the host name and ourdomain.com.tw is the domain name. In this name, ourdomain is the third-level domain, com is the second-level domain name and tw is the country code top-level domain (ccTLD). A FQDN always starts with a host name. For example, www.ourdomain.com，www is the host name. Ourdomain is the the second-level domain name. com is Generic Top-Level Domain, gTLD.
High Risk Certificate Request	The CA marks the request to be referred to the internal standards maintained by the CA and other database for reviewing. They may include the high-risk names used for phishing or other wrongful purposes, Miller Smiles phishing list, Google Safe Browsing list, or the names identified by the CA with the risk-reducing standards.
Identification	A statement of who the user is. [A Guide to Understanding Identification and Authentication in Trusted Systems] A way that can be used to describe or claim the identity of an individual or entity, e.g., user account, name or email.
Integrity	Protecting information so that it is not subject to unauthorized modification or damage. Preserve information in an untampered state during transmission and storage following generation at its source until receipt by the final recipient.
Internationalized Domain Name (IDN)	A kind of internet domain name, including at least one script or alphabetic character of one specific language, and then encoded with Punycode, and used for the domain name service only accepting ASCII codes.
Internet Assigned Numbers Authority (IANA)	An organization that oversees the allocation of global IP address, domain names and many other parameters used for Internet.
Internet Engineering Task Force (IETF)	Responsible for the development and promotion of Internet standards. Official website is at: https://www.ietf.org/. Its vision is the generation of high quality technical documents affects how man

	designs, uses and manages the Internet and allows the Internet to operate smoothly.
Issuing CA	For a particular certificate, the CA that issues the certificate is the issuing CA.
Key Escrow	Storage of related information using the subscriber's private key and according to the terms of the mandatory subscriber escrow agreement (or similar contract). The terms of this escrow agreement requires that one or more than one agencies have possession of the subscriber key provided it is beneficial to the subscriber, employer or another party in accordance with the provisions of the agreement.
Key Exchange	Mutual exchange of keys to establish a secure communication processing procedure.
Key Pair	Two mathematically related keys having the following properties: (1) One (public) key can be used to encrypt a message that can only be decrypted by using the other (private) key, and (2) It is computationally infeasible to determine one key from another.
Non-Repudiation	Provide proof of delivery to the information sender and proof of sender identity to the receiver so neither party may repudiate the processing of this information after the fact. Technically speaking, non-repudiation refers to the guarantee that this signature must be signed by the corresponding private key if a certain public key can be used to verify a certain digital signature for a trusted party. Legally speaking, non-repudiation refers to the establishment of a possession and control system for private signature keys.
Object Identifier (OID)	(1) One type of unique alphanumeric / numeric identified registered under the International Standard Organization registration standard which could be used to identify the uniquely corresponding certificate policy; where the certificate policy is modified, the OID is not changed accordingly. [Article 2-4, Chapter 1, Regulations on Required Information for Certification Practice Statements]

	(2) When a special form of code, object or object type is registered with the International Standard Organization (ISO), the unique code may be used as an identified. For example, this code can be used in the public key infrastructure to indicate what certificate policy and cryptographic algorithms are used.
Online Certificate Status Protocol (OCSP)	The Online Certificate Status Protocol is a type of online certificate checking protocol which lets the application software of relying parties to determine the status (such as revoked or valid) of a certain certificate.
OCSP Responder	The online server that is authorized, maintained, and operated by the CA, and connects to the repository to process the certificate status request.
OCSP Stapling	This is a form of TLS 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 certificate status from the CA when connecting to a high traffic TLS website, and thus to decrease the burden of the CA. This mechanism also prevents the privacy concern that the OCSP Responder knows which subscribers attempting to browsing that TLS website by having the TLS website referring the TLS certificate validity message issued regularly by the OCSP Responder to the CA.
Out-of-Band	Delivery method other than ordinary information delivery channels. If the delivery method is by electric cable, a special secure channel may be the use of physical registered mail.
Organization Validation, (OV)	In the TLS certificate approval process, except for identification and authentication of subscriber domain

	name control rights, following the certificate assurance level to identify and authenticate the identity of subscriber organizations. Therefore, connection to a website installed an Organization Validation TLS certificate is able to provide SSL encryption channels, in order to know who is the owner of the website and ensure the integrity of the transmitted information.
Private Key	(1) The key in the signature key pair used to generate digital signatures. (2) The key in the encryption key pair used to decrypt secret information. This key must be kept secret under these two circumstances.
Public Key	(1) The key in the signature key pair used to verify the validity of the digital signature. (2) The key in the encryption key pair used for encrypting secret information. These keys must be made public (usually in a digital certificate form) under these two circumstances.
Public-Key Cryptography Standard (PKCS)	In order to promote the use of public key technology, the RSA laboratory under the RSA Information Security Company has developed a series of public key cryptography standards that are widely used by the industry.
Public Key Infrastructure (PKI)	A set of law, policy, standards, personnel, equipment, facilities, technology, processes, audits and services developed on a broad scale and management of asymmetric cryptography and public key certificates.
Qualified Auditor	Accountant firms, entities, or individuals that satisfy the auditor qualification requirements specified in Section 8.2 of the Baseline Requirements, as well as independent from the audited parties.
Qualified Government Information Source (QGIS)	A regularly-updated and current, publicly available, database designed for the purpose of accurately providing the information for which it is consulted, and which is generally recognized as a dependable source of such information provided that it is maintained by a Government Entity, such as Ministry

	of Economic Affairs Bussiness & Factory Registration Database, the reporting of data is required by law, and false or misleading reporting is punishable with criminal or civil penalties. Nothing in the EV SSL Certificate Guidelines shall prohibit the use of third-party vendors to obtain the information from the Government Entity provided that the third party obtains the information directly from the Government Entity.
Qualified Government Tax Information Source (QTIS)	A Qualified Governmental Information Source that specifically contains tax information relating to Private Organizations, Business Entities, or Individuals. Such as Fiscal Information Agency, Ministry of Finance in Taiwan and IFS in USA.
Random Value	A value specified by a CA to the Applicant that exhibits at least 112 bits of entropy.
Registration Authority (RA)	(1) Responsible for checking the identity and other attributes of the certificate applicant but does not issue or administer certificates. The nature and scope of obligations borne by the registration authority are set down in the applicable certificate policy or agreement. (2) An entity responsible for the identity identification and authentication of the certificate subject which does not issue certificates.
Re-key	Changing the key values used in the cryptographic system application program. It is commonly achieved by issuing a new certificate for the new public key.
Relying Party	(1) Recipient of a certificate who acts in reliance of that certificate or a digital signature to verify the public key listed in the certificate, or the counterpart to identify (or its attributes) of the subject named in a trusted certificate and public key listed in the certificate. [Article 2-6, Chapter 1, Regulations on Required Information for Certification Practice Statements] (2) The individual or agency which receives information including a certificate and digital signature (the public key listed on the certificate may be used to verify the digital signature) and

	may rely on this information.
Repository	(1) A system for storing and retrieving certificates or other information relevant to certificates. [Article 2-7, Chapter 1, Regulations on Required Information for Certificate Practice Statements] (2) A database that contains information and data relating to certificates as specified in the CP/CPS.
Request Token	A value derived in a method specified by the CA which binds this demonstration of control to the certificate request. The Request Token SHALL incorporate the key used in the certificate request. A Request Token MAY include a timestamp to indicate when it was created. A Request Token MAY include other information to ensure its uniqueness. A Request Token that includes a timestamp SHALL remain valid for no more than 30 days from the time of creation. A Request Token that includes a timestamp SHALL be treated as invalid if its timestamp is in the future. A Request Token that does not include a timestamp is valid for a single use and the CA SHALL NOT re-use it for a subsequent validation. The binding SHALL use a digital signature algorithm or a cryptographic hash algorithm at least as strong as that to be used in signing the certificate request.
Required Website Content	Either a Random Value or a Request Token, together with additional information that uniquely identifies the Subscriber, as specified by the CA.
Reserved IP Addresses	IPv4 and IPv6 addresses reserved in the IANA setting. See: http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml and http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml
Request for Comments (RFC)	A series of memos issued by the Internet Engineer Task Force that include Internet, UNIX and Internet

	community standards, protocols and procedures for number assignment.
Secure Sockets Layer	Protocol issued by Netscape through introduction of their web browser which can encrypt network communication in the transport layer and ensure the integrity of transmitted information and perform identity authentication on the server and client. The advantage of the secure socket layer protocol is it is independent and separate from the application layer protocol. High level application layer protocol (such as: HTTP, FTP and Telnet) may be established on top of SSL. The SSL protocol completes encryption algorithm, communication secret key agreement and server authentication work before the application layer protocol communication. This protocol is a successor to the Transport Layer Security (TLS) protocol.
Signature Certificate	Public key certificates which contains a digital signature public key used for verification purposes (not used for data encryption or other cryptographic uses).
Subordinate CA	In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA.
Subscriber	An entity that (1) is the subject named or identified in a certificate issued to that entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual, an organization, an application or network device.
Technical Non-Repudiation	Technical evidence provided by the public key system to support non-repudiation security service.
Threat	Any status or event which may cause damage (including destruction, disclosure, malicious tampering or denial of service) to information systems. Can be divided into internal threats and outside threats. Internal threats are use of authorization to employ

	information destruction, disclosure, tampering or denial of service methods to damage the information system. Outside threats are an outside unauthorized entity which has the potential to damage the information system (including information destruction, tampering, disclosure and interruption of service).
Time-stamp	A digitally signed assertion by a trusted authority that a specific digital object existed at a certain time.
Transport Layer Security (TLS)	TLS 1.0 was first defined in RFC 2246 by the IETF based on the SSL 3.0 and updated in RFC 5246 and RFC 6176 as TLS 1.2. The current version is TLS 1.3 defined in RFC 8446 by the IETF in 2018.
Trust List	List of trusted certificates used by relying parties to authenticate certificates.
Trusted Certificate	Certificate trusted by relying party obtained through a secure and reliable transmission method. The public key contained in this type of certificate comes from a trusted path. Also called a trust anchor.
Trustworthy System	Computer hardware, software and programs which possess the following attributes: (1) Functions that protect again intrusion and misuse. (2) Provides reasonably accessible, reliable and accurate operations. (3) Appropriate implementation of preset function. (4) Security procedures uniformly accepted by the general public.
Uninterrupted Power System (UPS)	Provide uninterrupted backup power to loading equipment in the event of abnormal power conditions (such as power outage, interference or power surge) to allow uninterrupted operation of servers, switches and other critical equipment and precision instruments to prevent loss of calculation data, communication network interruption and loss of instrument control.
Validation	The process of identification of certificate applicants. Validation is a subset of identification and refers to identification in the context of establishment of the identity of certificate applicants. [RFC 3647]

WHOIS	Information retrieved directly from the Domain Name Registrar or registry operator via the protocol defined in RFC 3912, the Registry Data Access Protocol defined in RFC 7482, or an HTTPS website.
Zeroize	Method to delete electronically stored information. Storage of changed information to prevent information recovery.

Appendix 3: Certificate Extensions

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

HiPKICA shall not issue a certificate with:

(1) Extensions that do not apply in the context of the public internet;
(2) Semantics that will mislead a relying party about the certificate information verified by HiPKICA; and
(3) Internal name or reserved IP address that may be contained in the commonName field of subject DN or in the entry within the subject alternative name extension.

The subordinate CA of HiPKICA supports CT via X.509v3 extension in the certificate, as described below.

(1) A subordinate CA submits a precertificate as defined in RFC 6962 to several CT logs and waits for individual log to return a signed certificate timestamp (SCT).
(2) The CA attachs SCTs to a certificate using an X.509v3 extension, signs the certificate, and delivers the certificate to the applicant for completing the certificate issuance.
(3) The aforementioned precertificates shall not be considered to be a certificate subject to the requirements of RFC 5280.

Appendix 3-1: CA Certificates

CA certificates issued by HiPKICA include the self-signed certificate and self-issued certificate of root CA, subordinate CA certificate and cross-certificate. The certificate 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	Necessity	Criticality	Description
Subject Key Identifier	Required	FALSE	The SHA-1 hash value of the root CA's public key.
Basic Constraints	Required	TRUE	Subject Type=CA Path Length Constraint=None
Key Usage	Required	TRUE	The content in this extension can be one of the following: ➢ keyCertSign and cRLSign. (Default) ➢ digitalSignature, keyCertSign and cRLSign. (If the root CA uses the private signing key to issue OCSP responses, the bits of digitalSignature, keyCertSign, and cRLSign are asserted.)

(2) Self-issued Certificate

Extension	Necessity	Criticality	Description
Authority Key Identifier	Required	FALSE	The SHA-1 hash value of the new (old) root CA's public key.
Subject Key Identifier	Required	FALSE	The SHA-1 hash value of the old (new) root CA's public key.
CRL Distribution Points	Required	FALSE	The HTTP URL of the new (old) root CA's CRL service.
Authority Information Access	Required	FALSE	Two items of information included in this extension: ➢ The HTTP URL of the new (old) root CA's certificate. ➢ The HTTP URL of the new (old) root CA's OCSP responder.
Certificate Policies	Required	FALSE	The following two items of information shall be included in this extension. The

Extension	Necessity	Criticality	Description
			policy qualifier field in this extension may be used as needed. When using this field, it may contain a CPS pointer qualifier that points to this CPS. ➢ All CP OIDs defined in the HiPKI CP. ➢ All the CA/Browser Forum-assigned OID(s) referenced in the HiPKI CP.
Key Usage	Required	TRUE	The content in this extension shall be identical to the content of the key usage extension in the new (old) root CA's self-signed certificate.
Basic Constraints	Required	TRUE	Subject Type=CA Path Length Constraint=None

(3) Subordinate CA Certificate

Extension	Necessity	Criticality	Description
Authority Key Identifier	Required	FALSE	The SHA-1 hash value of the root CA's public key.
Subject Key Identifier	Required	FALSE	The SHA-1 hash value of the subordinate CA's public key.
CRL Distribution Points	Required	FALSE	The HTTP URL of the root CA's CRL service.
Authority Information Access	Required	FALSE	Two items of information included in this extension: ➢ The HTTP URL of the root CA's certificate. ➢ The HTTP URL of the root CA's OCSP responder.
Certificate Policies	Required	FALSE	This extension is used to indicate the certificate policies that the root CA approved and permitted the subordinate CA to use. The policy qualifier field in this extension may be used as needed. When using this field, it may contain a CPS pointer qualifier that points to this CPS. One or more of the following CP OIDs may be contained in this extension: ➢ CP OIDs defined in the HiPKI CP. ➢ the CA/Browser Forum-assigned OID(s) referenced in the HiPKI CP.
Extended Key Usage (EKU)	Required	FALSE	The subordinate CA certificate must include this extension specifying the

Extension	Necessity	Criticality	Description
			extended key usages to be used by the CA. According to Section 1.2 of the HiPKI CP, the subordinate CAs in HiPKI can only issue TLS certificates, thus the following rules must be followed: ➢ 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	Required	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	Required	TRUE	Subject Type=CA Path Length Constraint=Set according to the needed certificate path length of the subordinate CA.

(4) Cross-Certificate

Extension	Necessity	Criticality	Description
Authority Key Identifier	Required	FALSE	The SHA-1 hash value of the root CA's public key.
Subject Key Identifier	Required	FALSE	The SHA-1 hash value of the cross-certified CA's public key.
CRL Distribution Points	Required	FALSE	The HTTP URL of the root CA's CRL service.
Authority Information Access	Required	FALSE	Two items of information included in this extension: ➢ The HTTP URL of the root CA's certificate. ➢ The HTTP URL of the root CA's

Extension	Necessity	Criticality	Description
			OCSP responder.
Certificate Policies	Required	FALSE	This extension is used to indicate the certificate policies that the root CA approved and permitted the cross-certified CA to use. The policy qualifier field in this extension may be used as needed. When using this field, it may contain a CPS pointer qualifier that points to this CPS. One or more of the following CP OIDs may be contained in this extension: ➢ CP OIDs defined in the HiPKI CP. ➢ the CA/Browser Forum-assigned OID(s) referenced in the HiPKI CP.
Policy Mappings	Required	FALSE	This extension is used to indicate the correspondences between the certificate policies of the cross-certified CA and the ones of the root CA. It lists one or more pairs of CP OIDs. The pairing indicates the root CA considers its CP OID equivalent to the cross-certified CA's CP OID.
Key Usage	Required	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 OCSP responses, the bits of digitalSignature, keyCertSign, and cRLSign are asserted.)
Basic Constraints	Required	TRUE	Subject Type=CA Path Length Constraint= Set according to the needed certificate path length of the cross-certified CA.

Appendix 3-2: Subscriber Certificates

For TLS certificates issued by subordinate CAs of HiPKICA, the certificate extensions are described as follows.

Extension	Necessity	Criticality	Description
Certificate Policies	Required	FALSE	The policy qualifier field in this extension may be used as needed. When using this field, it may contain a CPS pointer qualifier that points to this CPS.
CRL Distribution Points	Required	FALSE	The HTTP URL of the subordinate CA's CRL service.
Authority Information Access	Required	FALSE	Two items of information included in this extension: ➢ The HTTP URL of the subordinate CA's OCSP responder. ➢ The HTTP URL of the subordinate CA's certificate.
Basic Constraints	Optional	TRUE	Subject Type=EE Path Length Constraint= None
Key Usage	Optional	TRUE	Bit positions for keyCertSign and cRLSign must not be set, but the keyEncipherment and digitalSignature bits may be set.
Extended Key Usage	Required	FALSE	The values id-kp-serverAuth and id-kp-clientAuth must be present. The value anyExtendedKeyUsage must not be present.
Authority Key Identifier	Required	FALSE	It must contain a keyIdentifier field and it must not contain an authorityCertIssuer or authorityCertSerialNumber field.