HiPKI Certificate Policy

Version 1.2

Chunghwa Telecom Co., Ltd.

August 29, 2023

Contents

Document History

Version	Release Date	Revision Summary
1.0	February 22, 2019	First Release.
1.05	March 2, 2020	(1) Admendation are made on Sections 1.5.2, 3.2.5, 4.2.1, 4.9, 6.2 and 9.6 according to BR v1.6.7; (2) Admendation are made on Sections 3.2.5 and 4.9 to reflect the revision of Mozilla Root Store Policy v2.7 regarding the validation of e-mail address and the revocation regulation, repectively; and (3) Admendation are made on Sections 1.1, 1.2, 1.6, 2.3, 3.1.1, 4.8.1, 5.7.1, 6.3.2, 7.1.3 and 7.2.2.
1.1	April 13, 2021	Amendments are made on Sections 1.1, 1.3.4, 1.3.5, 1.4.1, 1.4.2, 1.5.2.1, 1.6.1, 2.3, 2.4, 3.2.1, 3.2.2, 3.2.3, 3.2.5, 3.3.1, 5.5.2, 5.7.3, 6.1.1, 6.1.7, 6.2.6, 6.3, 6.3.2, 6.4.1, 6.4.2, 6.6.1, 6.6.2, 6.8, 7.1.3, 7.1.4, 7.3, 7.3.1, 9.10, 9.16.1 and 9.16.5 in compliance with the Baseline Requirements and our current practice.
1.15	June 17, 2021	(1) Delete the descriptions/regulations related to individuals, time stamp, Code Signing and EV Code Signing certificates in compliance with the Google Chrome Root Program Transition. (become a pure TLS Root CA/PKI). (2) Amendments are made on Sections 1.1, 1.2, 1.3.6, 1.4.1, 1.6.1, 1.6.2, 3.1.2, 3.1.3, 3.2.1, 3.2.2, 3.2.3, 3.2.4, 3.2.5, 3.3.1, 4.1.1, 4.2.1, 4.4.1, 4.5.2, 4.6, 4.9.1.1, 4.9.6, 4.9.7, 5.4.3, 5.4.8, 6.1.7, 6.2.2, 6.2.4, 6.3.2.2, 6.6.1, 8, 8.1, 9.5, 9.6.1, 9.6.3 and 9.12.1.

Version	Release Date	Revision Summary
1.16	August 30, 2021	Amendments are made on Sections 6.6.2 and 8 (in response to Mozilla public discussion issues).
1.17	August 30, 2022	Amendments are made on Sections 1.1, 1.3.1, 1.6.1, 1.6.2, 2.3, 3.1.1, 4.5.1, 4.5.2, 4.9.6, 4.9.10, 6.2.1, 6.2.6, 6.3.1, 6.4.1, 6.4.2, 6.6.1, 6.6.2, 7.1.2-7.1.4, 7.1.9, 7.2.1 and 7.2.2.
1.2	August 29, 2023	Amendments are made on Sections 1.1, 1.2, 1.3.2, 1.3.2.1, 1.3.2.2, 1.3.3, 1.4.1, 1.5.3, 1.5.4, 1.6.1, 1.6.2, 2.2, 3.1.2, 3.1.4, 3.2.2, 3.2.5, 3.3.1, 4.2.1, 4.4.1, 4.5.2, 4.6, 4.9, 4.9.6-4.9.9, 4.9.11, 4.9.13-4.9.16 4.10.1, 4.10.2, 5.1.3, 5.3.3, 5.4.1, 5.5.1, 5.6, 6.1.5, 6.1.7, 6.2.3, 6.2.5, 6.3.2.1, 6.3.2.2, 6.6.1, 6.6.2, 6.8, 7.1.4, 7.2.1, 7.2.2, 7.3.2, 8, 8.1, 8.2, 8.6, 9.2.1, 9.6.1, 9.6.3 and 9.16.3.

1. Introduction

A public key infrastructure (PKI) is a set of law, policy, rules, people, equipment, facilities, technology, processes, audits, and services used for the purpose of administering certificates and public/private key pairs. HiPKI is established in conjunction with the policies of Chunghwa Telecom Co., Ltd. (CHT) to promote electronic services and to create a sound e-commerce infrastructure environment. Certificates that issued by HiPKI are applicable to various applications of e-commerce and e-government to provide more secure, reliable, and fast network services.

1.1. Overview

This Certificate Policy (CP) conforms to the current versions of

(1) the Electronic Signatures Act and

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

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

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

(2) ITU-T X.509;

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

(4) Mozilla Root Store Policy;

(5) Microsoft Trusted Root Program Requirements;

(6) Apple Root Certificate Program; and

(7) Google Chrome Root Program,

to provide guidance and requirements for what a CA in HiPKI should include in its certification practice statement (CPS).

The SSL (Secure Sockets Layer) protocol has been replaced by the TLS

(Transport Layer Security) protocol because SSL certificates and TLS certificates all refer to certificates that can allow the TLS protocol to operate and comply with the ITU-T X.509, therefore we use “TLS certificates” in this CP.

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

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

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

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

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

CAs in HiPKI shall include appropriate CP OIDs when issuing certificates, such that interoperation with CAs that issue under same policies will be performed through policy mapping; or further cross-domain interoperation will be performed between HiPKI and other external PKI entries through the same means. Policy mapping can be confirmed if the issuing CA and subject CA have included the same CP OID.

1.1.1. Certificate Policy

CP is a guideline of information technology for network certification, which is a named set of rules that indicates the applicability of a certificate to a particular community or class of applications with common security requirements. The CP OIDs may be used by a relying party to decide whether a certificate is trusted for a particular purpose. CAs can directly include the registered CP OIDs in their issued certificates and its applicability can be confirmed by the relying party.

HiPKI RCA certificate is a self-signed certificate, which is also a trust anchor of HiPKI, that relying parties should trust. In accordance with international standards and practices, there are no CP OID listed in the certificate because HiPKI RCA must maintain a high level of credibility. HiPKI RCA shall operate with assurance level 4.

1.1.2. Relationship between the CP and the CPS

This CP states what assurance can be placed in a certificate issued by a CA. The CPS states how the CA establishes that assurance. Each CA that issues certificates under this CP shall have a corresponding CPS.

1.1.3. Certificate Policy Object Identifiers cited by Certification Authority

CAs in HiPKI shall follow this CP, any self-defined CP is not allowed. Citing CP OIDs by any CA must be approved by CHT, and readers are encouraged to contact us if there are any suggestions regarding this CP.

1.2. Document Name and Identification

This document is HiPKI Certificate Policy, the current version of this CP can be obtained at the website: https://eca.hinet.net. CAs shall put CP OIDs into the certificatePolicies extension of the certificates issued in accordance with this CP (not including self-signed certificates). CAs in HiPKI is authorized to issue the following certificates:

(1) Domain validation (DV) TLS certificates

(2) Organization validation (OV) TLS certificates

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

The following OIDs are reserved for use by CAs as an optional means of asserting compliance with various certificates and documents described in this CP.

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 certificates	2.23.140.1.2.1
OV TLS certificates	2.23.140.1.2.2

OIDs with a prefix of {2.23.140} are required and defined by CA/Browser Forum according to different documents and certificate usage scope. 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.

With regard to TLS certificates, if there is any inconsistency between the CP/CPS and the Baseline Requirements, then the Baseline Requirements takes precedence.

If any part is not regulated under the documents of CA/Browser Forum, the rule of assurance level 1 is applicable for CAs that issue DV TLS certificates, and the rule of assurance level 3 is applicable for CAs that issue OV TLS certificates. For CAs that issue self-signed, self-issued, and cross-certified certificates, the rule of assurance level 4 is always applicable.

1.3. PKI Participants

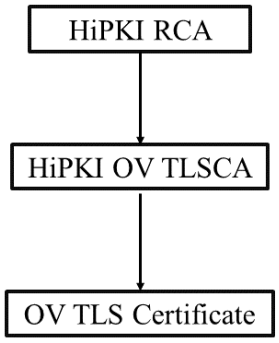
1.3.1. Policy Management Authority

The Chunghwa Telecom Certificate Policy Management Authority (PMA) was established by CHT to be responsible for the administration and to ensure the continued and regular operation of HiPKI. The PMA is formed by: one convener who shall be a Vice President or at an equivalent position; six to nine members; and one executive secretary who shall be the Managing Director of the Data Business Operation and Cybersecurity Applications Department; where the members are all assigned by the President of Information Technology Group of CHT. The PMA is responsible for:

(1) Authorizing and supervising key generation of CAs in HiPKI,
(2) Reviewing HiPKI CP,
(3) Reviewing related technical specifications used in HiPKI,
(4) Reviewing HiPKI CPS,
(5) Reviewing interoperation applications submitted by cross-certified CAs,
(6) Reviewing and approving the policy mapping for each incoming or cross-certified CA, and
(7) Supervising conformance of each cross-certified CA with the approved CP as a condition for allowing continued interoperation.

1.3.2. Certificate Authorities

HiPKI is a hierarchical PKI established in compliance with ITU-T X.509. The infrastructure includes a trust anchor, namely HiPKI RCA, and certain Subordinate CAs formed by CHT. Currently, HiPKI has only one Subordinate CA, namely HiPKI OV TLS CA. The architecture of HiPKI is as follows:



1.3.2.1. HiPKI RCA

HiPKI RCA is a Root CA as well as being a principal CA in HiPKI. HiPKI RCA is responsible for:

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

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

(3) Publishing the newly issued certificate revocation list (CRL) to the repository and ensure that the repository operates regularly.

HiPKI RCA shall establish the identification and authentication procedures for Subordinate CAs and the cross-certification procedures for external CAs in its CPS. After being approved by CHT, HiPKI RCA can perform cross-certification with any Root CA outside HiPKI.

The information, including certificate serial number and certificate thumbprint, of HiPKI RCA self-signed certificate are as follows:

(1) Self-signed certificate of HiPKI RCA – G1

Certificate Serial Number: 2d dd ac ce 62 97 94 a1 43 e8 b0 cd 76 6a 5e 60

Certificate Thumbprint (SHA-1): 6a 92 e4 a8 ee 1b ec 96 45 37 e3 29 57 49 cd 96 e3 e5 d2 60

Certificate Thumbprint (SHA-256): f0 15 ce 3c c2 39 bf ef 06 4b e9 f1 d2 c4 17 e1 a0 26 4a 0a 94 be 1f 0c 8d 12 18 64 eb 69 49 cc

Valid Period: February 22, 2019 to December 31, 2037

Key Type / Key Size: RSA 4096 with SHA-256

This information will be disclosed in the repository, external audit reports and management statements, registered in the common CA database (CCADB), and used to applying CA trusted list of application software suppliers (such as browsers or application system providers).

1.3.2.2. Subordinate CA

A Subordinate CA is another form of CA in HiPKI responsible for the issuance and administration of EE certificates. When necessary, the hierarchy of the Subordinate CA can be extended to multiple levels, i.e., a level 1 Subordinate CA can issue certificates to a level 2 Subordinate CA, or a level 2 Subordinate CA can issue certificates to a level 3 Subordinate CA and so on. However, any Subordinate CA is not allowed to cross-certify with any CA outside HiPKI directly.

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

The information, including certificate serial number and certificate thumbprint, of HiPKI OV TLS CA certificate is as follows:

(1) <u>CA certificate of HiPKI OV TLS CA – G1</u>

Certificate Serial Number: 2b ab a2 d6 e6 80 cc a5 94 e0 48 09 af 06 5d 42

Certificate Thumbprint (SHA-1): a5 84 71 e6 90 e4 17 e8 5d 1b 4f 38 7c 1d db 62 28 3e 9b e9

Certificate Thumbprint (SHA-256): d3 4a 5b 98 1a 85 ca 07 5d b6 2c ba c4 15 ef 65 9d 95 33 90 40 ca 47 68 68 62 5d 4a a2 3a 98 49

Valid Period: May 18, 2023 to December 31, 2037

Key Type / Key Size: RSA 4096 with SHA-256

This information will be disclosed in the repository, external audit reports, and management statements, as well as registered in the CCADB.

1.3.2.3. Cross-Certified CA

HiPKI RCA does not cross certify with any CA outside HiPKI currently.

1.3.3. Registration Authorities

Registration Authorities (RAs) collect and verify each subscriber's identities, attributes and contact information in order to facilitate CAs' administration work, including certificate issuance, revocation, re-key and modification.

HiPKI RCA itself serves the role of RA and performs RA's operation in accordance with its CPS approved by the PMA.

Subordinate CAs may establish respective RAs and shall specify their duties in the CPS. A RA may be directly established and operated by a Subordinate CA or independently established and operated by customers who have signed contracts with CHT. In any case, these RAs must be operated in accordance with this CP and their CPS. RAs in latter case may adopt a security control practice stricter than this CP or their CPS according to their internal requirements and regulations.

1.3.4. Subscribers

A subscriber is a certificate subject who is not capable of issuing certificates and the entity who possesses the private key that corresponds with a certificate's public key. A Root CA, Subordinate CA or cross-certified CA is not called the "subscriber" because they are capable of issuing certificates.

1.3.5. Relying Parties

A relying party is the entity that relies on the validity of the binding of the certificate subject name to a public key. The relying party must check the validity of the received certificate by checking the appropriate certificate status information.

The relying party can use the certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the certificate subject. A relying party may use information in the certificate (such as CP OID) to determine the suitability of the certificate for a particular use.

1.3.6. Other Participants

CAs may select other related authorities, e.g., an audit authority or data archiving service authority, which provide trust services as collaborative partners. In that case, CAs shall specify the mutual operation mechanisms and the rights and obligations of each other in their CPS to ensure the efficiency and reliability of the service quality provided by CAs.

1.4. Certificate Usage

CAs shall evaluate associated risks, application environment, possible vulnerability, and certificate usage prior to determining an appropriate assurance level for CA operation and certificate issuance and administration.

1.4.1. Appropriate Certificate Uses

The applicable scope for TLS certificates in this CP is described as follows:

Cert. Type	Scope of Applications
DV	• Only provide communication channel encryption and protection. (Communication channel encryption refers to 'through the exchange of encryption key to encrypt the transmitted information between the subscriber's browser and websites). • Scope of application includes: (1) Provide an encryption protection to the non-monetary or non-property applications, where the probability of occurring malicious actions is low.
OV	• Provide communication channel encryption and protection. • Require verifying the identity of the organization that owns the domain name (website). • Scope of application includes: (1) e-commerce transactions, (2) e-government, and (3) The environment where the probability of occurring malicious actions is moderate.

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

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

1.4.2. Prohibited Certificate Uses

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

(1) Crime,
(2) Military command and nuclear, biological and chemical weapons control,
(3) Operation of nuclear equipment,
(4) Aviation flight and control systems, and
(5) Man-in-the-middle TLS traffic interception.

1.5. Policy Administration

1.5.1. Organization Administering the Document

Chunghwa Telecom Co., Ltd.

1.5.2. Contact Person

1.5.2.1. CP Related Issues

Any suggestion regarding this CP, please contact us by the following information.

Tel: +886 2-2344-4820

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

E-mail: caservice@cht.com.tw

Other information can be found at https://eca.hinet.net/repository-h/en/index.htm.

1.5.2.2. Certificate Problem Report

CAs shall provide the information of their contact window that is responsible for certificate problem report in their CPS.

1.5.3. Person Determining CPS Suitability for the Policy

CAs shall inspect whether the CPS conforms to this CP first and submit this CP to the PMA for review and approval. After approved, CAs can then quote this CP formally.

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.

CHT has the right to assess (see Chapter 8) whether CAs are complied with this CP. CAs shall conduct regular self-audits to demonstrate that they have operated with the assurance levels under this CP.

HiPKI has applied to the root certificate programs of most operating systems, web browsers, and software platforms to include our root certificate, the self-signed certificate of HiPKI RCA, into their CA trust list. This makes the program can use our root certificate to anchor a chain of trust for certificates used by TLS servers and other applications without having to ask users for further permission or information. According to the criteria of each program, full-surveillance period-of-time audits must be conducted and updated audit information provided no less frequently than annually. That is, successive audits must be contiguous (no gaps). In addition, CAs must submit the current CPS and audit report to each program every year.

1.5.4. CPS Approval Procedures

The CPS of CAs must obey relevant laws, comply with this CP and obtain approval from the PMA and Ministry of Digital Affairs, the competent authority of the Electronic Signatures Act. The CPS must be revised in

response to any revision of this CP, and the revised CPS must be submitted to the PMA and Ministry of Digital Affairs for approval.

1.6. Definitions and Acronyms

1.6.1. Definitions

Term	Definition
Access	Ability to make use of any information system (IS) resource.
Access Control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems.
Activation Data	Private data, other than keys, that are required to access cryptographic modules and that need to be protected (i.e., unlock private keys for signing or decryption events).
Applicant	The subscriber who requests a certificate from a CA and has not yet completed the certificate issuance procedure.
Archive	A long-term, physically separate storage which can be used to support audit, availability and integrity services.
Assurance	A basis that the trusted entity has complied with certain security requirements. [Article 2-1, Regulations on Required Information for Certification Practice Statements]
Assurance Level	A certain level in a relative assurance tier. [Article 2-2, Regulations on Required Information for Certification Practice Statements]
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend

Term	Definition
	necessary changes in controls, policies, or procedures.
Audit Data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event.
Authenticate	To confirm the identity of an entity when that identity is presented.
Authentication	(1) The process of establishing confidence in user identities electronically presented to an information system. [NIST.SP.800-63-2 Electronic Authentication Guideline] (2) Safety measures used to secure data transmission or ways to authorize the privilege of individuals upon receiving certain types of information. (3) Authentication is the process by which a claimed identity is verified. [A Guide to Understanding Identification and Authentication in Trusted Systems] Mutual authentication means that the authentication is performed between two parties during communication.
Authority Information Access (AIA)	An extension that indicates how to access information and services with regard to the issuer of a certificate, including the address of the OCSP responder and the URL pointing to the location where issuer of this certificate is located.
Authorization Domain Name	The Domain Name used to obtain authorization for certificate issuance for a given FQDN. The CA may use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of

Term	Definition
	domain validation. If the FQDN contains a wildcard character, then the CA MUST remove all wildcard labels from the left most portion of requested FQDN. The CA may prune zero or more labels from left to right until encountering a Base Domain Name and may use any one of the intermediate values for the purpose of domain validation.
Backup	Copy of files and programs made to facilitate recovery if necessary.
Binding	Process of associating two related information elements.
Biometrics	A physical or behavioral characteristic of a human being.
CA Certificate	Certificates that is issued to certification authorities.
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) An electronic certification on certification material with signature for use in confirming identity and qualification of the signature party. [Article 2-6, Electronic Signatures Act] (2) Digital presentation of information, the content

Term	Definition
	includes at least: a. information of issuing CA, b. names or identities its subscriber, c. the subscriber's public key, d. operational period, and e. digital signature of issuing CA The term "certificate" referred to this CP shall be a certificate with the format of ITU-T X.509 version 3 and has asserted the OIDs of this CP in the certificate policy extension.
Certification Authority (CA)	(1) A government agency or a juristic person that issues certificates [Article 2-5, Electronic Signatures Act] (2) An authority trusted by one or more users that issues and manages X.509 public key certificates and CRLs.
Certification Authority Authorization (CAA)	The certification authority authorization (CAA) DNS resource record allows a DNS domain name holder to specify one or more certification authorities (CAs) authorized to issue certificates for that domain. CAA resource records allow a public certification authority to implement additional controls to reduce the risk of unintended certificate mis-issue. [RFC 8659]
Certificate Policy (CP)	(1) A named set of rules that indicates the applicability of a certificate to a particular community or class of application with common security requirements. [Article 2-3, Regulations on Required Information for Certification Practice Statements] (2) A certificate policy is a specialized form of administrative policy tuned to electronic

Term	Definition
	transactions performed during certificate management. A certificate policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates. A certificate policy can also indirectly govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.
Certification Practice Statement (CPS)	(1) A practice statement published by a certification service provider to specify the practices that the certification service provider employs in issuing certificates and managing other certification-related services. [Article 2-7, Electronic Signatures Act] (2) A statement of the practices that a certification authority employs in issuing, suspending, revoking, and renewing or re-keying certificates and that complies with certain particular requirements specified in its CP or other service contracts.
Certificate 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 Re-key	Changing the key pair used in a cryptographic system application. It is commonly achieved by issuing a new certificate that contains the new

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

Term	Definition
	CAs and that of CPS.
Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes.
Contract Signer	Applicant, personnel employed by the applicant, an authorized representative who can make a declaration on behalf of the applicant or a natural person who can sign the purchase agreement on behalf of the applicant.
Cross-certificate	A certificate that is used to establish a trust relationship between two Root CAs. The certificate is a type of CA certificates and not a subscriber certificate.
Cross-Certification Agreement (CCA)	An agreement between a Root CA and cross-certified CAs that includes the items and individual liability and obligation which must be followed during the period of joining the PKI where the Root CA is established.
Cryptographic Module	A set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module.
Data Integrity	Assurance that the data are unchanged from creation to reception.
Digital Signature	An electronic signature generated by the use of mathematic algorithm or other means to create a

Term	Definition
	certain length of digital data encrypted by the signatory's private key, and capable of being verified by the public key. [Article 2-3, Electronic Signatures Act]
Domain Name	An ordered list of one or more Domain Labels assigned to a node in the Domain Name System, i.e., translates an IP address into a text name that is easily remembered.
Domain Name System (DNS)	An Internet service that translates domain names into IP addresses.
Domain Validation (DV)	Prior to issuance of a DV TLS certificate, only a subscriber's ownership or control of the domain is validated, but identification or authentication of the subscriber's affiliate or identity is exclude from the validation. Therefore, anyone links to a website installed a DV TLS certificate can get a TLS encryption channel but knows nothing about who owns the website.
Duration	A certificate field that contains two subfields, a start time "notBefore" and an end time "notAfter."
E-commerce	Provision of goods for sale and other services through the use of network technology (specifically the Internet).
End-Entity Certificate	A certificate in which the subject is not a CA.
Federal Information Processing Standards (FIPS)	The standards developed by the U.S. federal government for use in computer systems by non-military government agencies and government contractors. The 140 series of FIPS are U.S. government computer security standards that specify requirements for cryptographic modules. As of December 2016, the current version of the

Term	Definition
	standard is FIPS 140-2. FIPS 140 imposes requirements in eleven different areas and FIPS 140-2 defines four levels of security.
Firewall	Gateway that limits access between networks which complies with local security policy.
Fully-Qualified Domain Name (FQDN)	An absolute domain name that specifies its exact location in the DNS hierarchy. A FQDN consists of two parts, a host name (service name) and a domain name. For example, a website with the hostname *ourserver* in the parent domain *ourdomain.com.tw* has the FQDN *ourserver.ourdomain.com.tw*, where *ourdomain* is the third-level domain, *.com* is the second-level domain and *.tw* is the country code top-level domain (ccTLD). In addition, a website with the hostname *www* in the parent domain *ourdomain.com* has the FQDN *www.ourdomain.com*, where *ourdomain* is the second-level domain and *.com* is the generic top-level domain (gTLD). A FQDN always starts with a host name.
HiPKI	In order to promote electronic services, CHT builds a hierarchical PKI for issuing TLS certificates in accordance with the ITU-T X.509 standard.
HiPKI Root Certification Authority (HiPKI RCA)	The Root CA and top-level CA in HiPKI, and its public key is the trust anchor of HiPKI.
Integrity	Protection against unauthorized modification or destruction of information. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.

Term	Definition
Internet Assigned Numbers Authority (IANA)	An organization that oversees the allocation of global IP address, domain names and many other parameters used for Internet.
Internet Engineering Task Force (IETF)	An organization that develops and promotes Internet standards concerned with the evolution of the Internet architecture and the smooth operation of the Internet to make the Internet work better. Official website is at: https://www.ietf.org/.
Issuing CA	For a particular certificate, the issuing CA is the CA that issued the certificate. This could be either a Root CA or a Subordinate CA.
Key Compromise	A private key is said to be compromised if its value has been disclosed to an unauthorized person or an unauthorized person has had access to it.
Key Escrow	A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer, or other party, upon provisions set forth in the agreement.
Key Pair	Two mathematically related keys having the following properties: (1) One (public) key can be used to encrypt a message that can only be decrypted by using the other (private) key, and (2) It is computationally infeasible to determine one key from another.
National Institute of Standards and Technology	Official website is at http://www.nist.gov/. Its mission is to promote U.S. innovation and industry competitiveness by advancing measurement science, standards, and technology in ways that

Term	Definition
(NIST)	enhance economic security and improve our quality of life. The hardware cryptographic module standards and certification, key security assessment and U.S. federal government civil servant and contractor identity card standards defined by NIST are widely referenced and employed.
Non-Repudiation	Technical evidence provided by the public key cryptosystem to support non-repudiation security service. Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. Technical non-repudiation refers to the guarantee that if a public key is used to validate a digital signature, that signature must be signed by the corresponding private key for a relying party.
Object Identifier (OID)	(1) A unique alphanumeric/numeric identifier registered under the International Standard Organization (ISO) registration standard, and which could be used to identify the uniquely corresponding CP; where the CP is modified, the OID is not changed accordingly. [Article 2-4, Regulations on Required Information for Certification Practice Statements] (2) A specialized formatted and unique identifier that is registered with an ISO and refers to a specific object or object class. For example, OIDs can be used to uniquely identify the CP and cryptographic algorithms of PKIs.
Online Certificate Status Protocol (OCSP)	An online certificate-checking protocol that enables relying party application software to determine the status of an identified certificate, e.g.,

Term	Definition
	revoked or valid.
OCSP Responder	An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.
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.
Organization Validation (OV)	Prior to issuance of an OV TLS certificate, not only a subscriber's ownership or control of the domain is validated, but also identification or authentication of the subscriber's affiliate or identity is made according to the assurance level of the certificate. Therefore, anyone links to a website installed an OV TLS certificate can get a TLS encryption channel and know who owns the

Term	Definition
	website that provides integrity of data transmission.
Out-of-Band	A communication method (between parties) that differs from the current on-line methods and can be regarded as a special secure channel, e.g., one party uses physical registered mail to communicate with another party.
Private Key	(1) The key of a signature key pair that is used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.
Public Key	(1) The key of a signature key pair that is used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is publicly available and is normally made in the form of a digital certificate.
Public Key Infrastructure (PKI)	A set of law, policy, rules, people, equipment, facilities, technology, processes, audits, and services used for the purpose of administering certificates and public/private key pairs.
Public-Key Cryptography Standards (PKCS)	These are a group of public-key cryptography standards devised and published by RSA Security LLC. The company published the standards to promote the use of the cryptography techniques.
Registration Authority (RA)	An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates. An RA is not a CA but can be part of CAs.
Relying Party	A recipient of a certificate who acts in reliance on

Term	Definition
	that certificate. [Article 2-6, Regulations on Required Information for Certification Practice Statements]
Repository	(1) A system for storing and retrieving certificates or other information relevant to certificates. [Article 2-7, Regulations on Required Information for Certification Practice Statements] (2) A database that contains information and data relating to certificates as specified in the CP/CPS.
Request for Comments (RFC)	A series of memos issued by IETF that include standards, protocols and procedures with reference to Internet, UNIX, and Internet community and are scheduled by numbers.
Reserved IP Addresses	An IPv4 or IPv6 address that the IANA has marked as reserved: http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml
Root Certification Authority (Root CA)	The top-level certification authority in a hierarchical PKI that issues Subordinate CA certificates and self-signed certificates.
Secure Sockets Layer (SSL)	Protocol issued by Netscape through promotion of their web browser which can encrypt network communication in the transport layer, ensure the integrity of transmitted information, and perform identity authentication on the server and client. The SSL protocol is independent of the application layer protocol, such that high level application layer protocols, e.g., HTTP, FTP and Telnet, may be

Term	Definition
	established based on SSL. The SSL protocol completes encryption by algorithm, secret key agreement for a communication and server certification prior to the communication with the application layer protocol. This protocol is a predecessor of the Transport Layer Security (TLS) protocol.
Self-issued Certificate	Self-issued certificates may be generated to implement a key change-over or to support changes in policy. The certificates, including the old-with-new certificate, new-with-old certificate and new-with-new certificate, are signed by the Root CA with new/old private keys to establish a trusted path between the old and new keys or the certificate policies.
Self-signed Certificate	(1) Self-issued certificates are CA certificates in which the issuer and subject are the same entity. In other words, it is a certificate containing the corresponding public key or other information signed with the private key. (2) A self-signed certificate in a PKI may serve as a trust anchor for a certification path. The subject of certificate is the Root CA itself. (3) Self-issued certificates can be used by relying parties to validate the self-issued certificates, Subordinate CA certificates, cross-certificates and CRLs issued by a Root CA.
Subject CA	In the context of a particular CA certificate, the subject CA is the CA whose subject is certified in the certificate.
Subordinate CA	In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose

Term	Definition
	activities are constrained by that other CA.
Subscriber	An entity that (1) is the subject named or identified in a certificate issued to that entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual, an organization, an application or network device.
Threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. The threat may be internal or external. An internal threat refers to the aforementioned circumstance or event was caused by an entity with authorized access; an external threat refers to the aforementioned circumstance or event was caused by an unauthorized entity from outside the domain perimeter.
Time-stamp	A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.
Transport Layer Security (TLS)	TLS 1.0 was first defined in RFC 2246 by the IETF based on the SSL 3.0 and updated in RFC 5246 and RFC 6176 as TLS 1.2. The current version is TLS 1.3 defined in RFC 8446 by the IETF in 2018.
Trust List	List of trusted certificates used by relying parties to authenticate other certificates.
Trusted Certificate	A certificate that is trusted by the relying party on the basis of secure and authenticated delivery. The

Term	Definition
	public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor."
Uninterrupted Power System (UPS)	Provide emergency power to a load in the event of abnormal power conditions (such as power outage, noise or sustained overvoltage) to allow continual operation of critical equipment or precision instruments (e.g., servers or switches) and to prevent loss of calculation data, interruption of communication network and loss of instrument control.
Validation	The process of identification of certificate applicants. Validation is a subset of identification and refers to identification in the context of establishing the identity of certificate applicants. [RFC 3647]
WebTrust	The current version of CPA Canada's WebTrust Program(s) for Certification Authorities.
Zeroize	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. [FIPS 140-2]

1.6.2. Acronyms

Acronyms	Full Name	Definition
AIA	Authority Information Access	See Section 1.6.1
CA	Certification Authority	See Section 1.6.1
CAA	Certification Authority Authorization	See Section 1.6.1
CCA	Cross-Certification Agreement	See Section 1.6.1

Acronyms	Full Name	Definition
CMMI	Capability Maturity Model Integration	See Section 1.6.1
CP	Certificate Policy	See Section 1.6.1
CPS	Certification Practice Statement	See Section 1.6.1
CRL	Certificate Revocation List	See Section 1.6.1
CT	Certificate Transparency	See Section 1.6.1
DN	Distinguished Name	
DNS	Domain Name System,	See Section 1.6.1
DV	Domain Validation	See Section 1.6.1
EE	End Entities	
FIPS	(U.S. Government) Federal Information Processing Standard	See Section 1.6.1
FQDN	Fully-Qualified Domain Name	See Section 1.6.1
HiPKI RCA	HiPKI Root Certification Authority	See Section 1.6.1
IANA	Internet Assigned Numbers Authority	See Section 1.6.1
IETF	Internet Engineering Task Force	See Section 1.6.1
NIST	(U.S. Government) National Institute of Standards and Technology	See Section 1.6.1
OCSP	Online Certificate Status Protocol	
OID	Object Identifier	See Section 1.6.1
OV	Organization Validation	See Section 1.6.1
PIN	Personal Identification Number	
PKCS	Public Key Cryptography Standards	See Section 1.6.1

Acronyms	Full Name	Definition
RA	Registration Authority	See Section 1.6.1
RFC	Request for Comments	See Section 1.6.1
SSL	Secure Sockets Layer	See Section 1.6.1
TLS	Transport Layer Security	See Section 1.6.1
UPS	Uninterrupted Power System	See Section 1.6.1

2. Publication and Repository Responsibilities

2.1. Repositories

CAs that issue certificates under this CP are obligated to provide inquiry and download of all certificates issued by or to the CA and CRLs issued by the CA in a repository, as well as to publish CPs and CPSs.

Repositories may be operated by CAs or other parties. One CA is not limited to having one repository, but it must have at least one primary repository for external operations. CAs shall specify related information of their repositories in their CPS and also ensure the availability of the repositories, suitability of access controls and data integrity.

2.2. Publication of Certificate Information

CAs shall take responsibility for making the following information publicly accessible in their repositories:

(1) CP and CPS,

(2) Certificate revocation information,

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

(4) All issued certificates including certificates issued to other CAs,

(5) Privacy protection policy,

(6) The latest result of the external audit, and

(7) Related latest news.

In addition to the above information, CAs shall publish information required to verify digital signatures. CAs shall specify the repository service suspension time limits and the regulations of publication and notification in their CPS.

CAs under HiPKI that issue TLS certificates shall specify CAA Issuer Domain Names in the CPS.

2.3. Time or Frequency of Publication

Publication requirements for CRLs are provided in Sections 4.9.7. This CP is reviewed and updated annually. New or modified version of this CP is published in the CA repository as soon as possible upon the approval of the PMA. CAs shall publish their new or modified CPS to their repositories as soon as possible upon receiving the approval letter from the competent authority.

CAs SHALL indicate conformance with the Baseline Requirements by incrementing the version number and adding a dated changelog entry.

2.4. Access Controls on Repositories

(1) Write access control is made when acquiring CP and CPSs.

(2) CAs shall decide whether to set up access controls for certificates.

(3) CAs shall protect repository information from malicious dissemination or modification. The public key and certificate status information in the repository shall be publicly available through the Internet.

3. Identification and Authentication

3.1. Naming

3.1.1. Types of Names

CAs shall issue certificates with a non-null subject distinguished name (DN) that complies with ITU-T X.500 standards.

For certificate applications, the issuing CA has the right to decide whether to accept the subject alternative name. If the subject alternative name is included in the certificate, the subject alternative name extension must be marked non-critical.

3.1.2. Need for Names to be Meaningful

For OV TLS certificates, the subject names of equipment or servers shall be the organization name who administers or owns them, and the naming shall conform to the subject naming regulations under the Jurisdiction country's law of the applicant organization.

CAs SHALL NOT issue publicly trusted TLS certificates with a subjectAltName extension or subject field containing a Reserved IP Address or Internal Name in compliance with CA/Browser Forum guidelines.

3.1.3. Anonymity or Pseudonymity of Subscribers

Subscribers are not identified in DV certificates, which have subject fields identifying only domain names (not people or organizations). Subordinate CA may issue end-entity anonymous certificates if (i) such certificates comply with the Baseline Requirements and certificate profile and (ii) with name space uniqueness.

3.1.4. Rules for Interpreting Various Name Forms

CAs should state the rules for interpreting various name forms in their CPS.

3.1.5. Uniqueness of Names

Name uniqueness for certificates issued by each CA must be enforced. Each CA and its associated RAs shall enforce name uniqueness within the X.500 name space. CAs shall specify how to use X.500 name space in their CPS and ensure the uniqueness of the subject name when multiple certificates are issued to the same entity.

Name ownership is carried out in accordance with the naming rules in relevant laws and regulations of our country (e.g., the Company Act). CAs shall detail the dispute resolution procedures of naming in their CPS.

CHT is the arbitration authority for PKI naming disputes.

3.1.6. Recognition, Authentication, and Role of Trademarks

If the subject name contains a trademark, its naming shall conform to relevant trademark laws and regulations of our country.

3.2. Initial Identity Validation

3.2.1. Method to Prove Possession of Private Key

Prior to issuing a certificate to an applicant, issuing CA shall verify that the applicant possesses the private key corresponding to the public key in the certificate request.

Different methods shall be used by those who generate different keys to prove possession of the private key. HiPKI allows only the following one method:

- Key pairs are generated by subscribers:

  Subscribers can use their private keys to create signatures which are provided to CAs or RAs in accordance with Section 6.1.3. CAs or RAs then uses subscribers' public keys to validate the signature and the fact that subscribers indeed possess the corresponding private keys. This CP allows use of other methods, e.g., the methods listed in RFC 2510 and RFC 2511, in equivalent security levels to prove possession of the private keys.

3.2.2. Authentication of Organization Identity

According to different assurance levels, the procedures of organization identity authentication are listed as follows:

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 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. CAs may additionally cross-check the information provided by the applicant for consistency with available government or third-party data sources.
Level 3	CAs in HiPKI are allowed to use 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

Assurance Level	Procedures for Authentication of Organization Identity
	formulated in the internal control system of each RA: a. Application through an identity assurance level 3 organization certificate issued by the GPKI or ePKI; b. For those organization who has complete registration procedure with the competent authority, like (1)-a or (1)-b, mailing the copies of the certification documents is acceptable; c. A letter attesting that subject information is correct written by an accountant, lawyer, or notary; d. A site visit by CA personnel or a third party who is acting as an agent for the CA; or e. Organizations belonging to CHT apply for the certificate with e-form. 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 convene 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 convene by CHT to review the application.
DV TLS certificates	The same as level 1.
OV TLS certificates	In compliance with the Baseline Requirements and the provisions for assurance level 3.

3.2.3. Authentication of Individual Identity

CAs under HiPKI do not issue certificate to individuals.

3.2.4. Non-verified Subscriber Information

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

3.2.5. Validation of Authority

CAs shall specify a reliable method of communication by which the CA or the RA performs validation of authority in their CPS. One of the following methods may be used to verify the authenticity of the Applicant Representative's certificate request:

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

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

Subordinate CAs shall specify the methods used to validate the applicant's authority for various TLS certificate in their CPS:

Type of TLS Certificates	**Methods for Authority Validation**
DV	■ Validating the applicant's ownership or control of the domain in accordance with the Baseline Requirements.
OV	■ Validating the applicant's ownership or control of the domain in accordance with the Baseline Requirements, and ■ Performing identification and authentication of organization identity and confirmation of authorization in accordance with the Baseline Requirements and Sections 3.2.2 or 3.2.3 for assurance level 3 of the CPS.

3.2.6. Criteria for Interoperation

CAs shall disclose related information of a Root CA in their CPS in the case of applications by the Root CA wishing to interoperate with.

3.2.7. Data Source Accuracy

Prior to using any data source as a reliable data source, CAs shall evaluate the source for its reliability, accuracy, and resistance to alteration or falsification. CAs shall consider the following terms during its evaluation:

(1) The age of the provided information,

(2) The update frequency of the information source,

(3) The data provider and the purpose of data collection,

(4) The public accessibility of the data availability, and

(5) The relative difficulty in falsifying or altering the data.

Databases maintained by the CA, its owner, or its affiliated companies do not qualify as a reliable data source, if the primary purpose of such 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

Certificate re-key is the issuance of a new certificate possessing the same characteristics and assurance level as an old certificate. Besides the different public key (corresponding to a new and different private key) and different serial number, the new certificate may also be assigned a different validity period.

When a Subordinate CA renews the key pair, identification and authentication of the Subordinate CA to which the CA certificate is issued shall be performed in accordance with Section 3.2 before the new CA certificate is issued to the Subordinate CA.

Each subscriber of DV and OV TLS certificates shall re-establish its identity using the initial registration processes of Section 3.2 in accordance with the Baseline Requirements and Section 6.3.2.2 of this CP if the identity has been validated for 398 days from the time of initial registration.

3.3.2. Identification and Authentication for Re-key after Revocation

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

3.4. Identification and Authentication for Revocation Request

CAs or RAs shall conduct identification and authentication for certificate revocation request. CAs shall specify the methods for validating the identities of applicants in their CPS that comply with Section 4.9 to ensure that the applicants have the rights to submit the revocation request.

Requests to revoke a certificate may be authenticated using that certificate's public key, regardless of whether the associated private key has been compromised.

4. Certificate Life-cycle Operational Requirements

4.1. Certificate Application

4.1.1. Who Can Submit a Certificate Application

Applicants, including the HiPKI RCA, Subordinate CAs established by CHT or Root CAs outside HiPKI, may apply for a certificate. An application for a subordinate CA certificate issued by HiPKI RCA shall only be submitted by an organization (or an authorized representative).

An application for a computer and communication equipment (such as routers, firewalls and load balancers) or a server software (such as web server or application server) shall be submitted by the organization or individual who administers the equipment.

4.1.2. Enrollment Process and Responsibilities

The issuing CA is responsible for ensuring that the identity of each certificate applicant is verified in accordance with this CP and the applicable CPS prior to the issuance of a certificate. Applicants are responsible for submitting sufficient information and documentation for the issuing CA or the RA to perform the required verification of identity prior to issuing a certificate. Subscribers who accepted certificates shall have the following obligations:

(1) Follow the regulations and procedures in Chapters 3 and 4,

(2) Use the certificate in a correct manner,

(3) Properly safeguard and use the private keys, and

(4) Notify the CA immediately in the event of private key compromise.

4.2. Certificate Application Processing

CAs shall specify the application procedures, locations and websites regarding initial registration, certificate renewal and certificate re-key in their CPS.

HiPKI RCA may accept certificate application that a CA established by

CHT requests to become a level 1 Subordinate CA in HiPKI or a Root CA outside HiPKI requests to cross-certify with HiPKI RCA. The application procedure shall be determined separately by the PMA.

Subordinate CAs at each level in HiPKI shall not accept other CA applications to become Subordinate CA unless permission is given by a superior CA. A negotiation between the PMA and HiPKI RCA shall be conducted prior to the issuance of a cross-certificate issued by HiPKI RCA to a Root CA outside HiPKI.

4.2.1. Performing Identification and Authentication Functions

The issuing CA shall ensure that the system and procedures for authenticating subscriber identity conform to this CP and its CPS. The initial registration procedures must meet the requirements specified for subscriber authentication as specified in Sections 3.2 of this CP. Certificate applicants (Subscribers) are responsible for providing accurate information on their certificate applications. The information required for certificate applications includes both required and optional information, but only the information listed on the certificate profile is recorded in the certificate to be issued. The issuing CA shall ensure that all communication between the issuing CA and an RA regarding information provided by the applicant and certificate issuance or changes in the status of a certificate are made using secure and auditable methods in accordance with this CP and the CPS.

CAs shall maintain an internal database of all previously revoked certificates and previously rejected certificate requests due to suspected phishing or other fraudulent usage or concerns. CAs shall use this information to identify subsequent suspicious certificate requests.

Prior to issuing a certificate, the RAOs shall check the DNS for the existence of a CAA DNS resource record (CAA record) for each dNSName (i.e., FQDN) in the subjectAltName extension of that certificate, according to the procedure in RFC 8659.

The issuer domain names, that is, the Certification Authority CAA identifying domains for CAs, within HiPKI's operational control are "pki.hinet.net", "tls.hinet.net" and "eca.hinet.net". The issuing CA shall

specify in its CPS its practices on processing CAA records for FQDNs with "issue" or "issuewild" property tags. For example, the issuing CA will issue a TLS certificate to an applicant having FQDNs with "issue" or "issuewild" property tags only when the applicant has designated any of HiPKI's issuer domain names as the issuer in the CAA records.

4.2.2. Approval or Rejection of Certificate Applications

If all identity authentication works followed related regulations and best practices can be successfully completed, the issuing CA may approve the certificate application; otherwise, the issuing CA may reject any certificate application.

The issuing CA may also reject a certificate application on any reasonable basis, including the concerns about previous rejection of certificate application or violation of subscriber terms and conditions.

4.2.3. Time to Process Certificate Applications

If an applicant has provided sufficient information on their certificate applications that conforms to this CP and the CPS, CAs and RAs shall verify the applicant's information and issue a certificate within a reasonable time frame. The time to process certificate applications may be stated in their CPS, subscriber terms and conditions or the certificate applicant contract.

4.3. Certificate Issuance

4.3.1. CA Actions during Certificate Issuance

Personnel in CAs shall perform the tasks related to certificate issuance in accordance with Section 5.2 and the CPS. After certificate issuance, CAs or RAs shall notify the applicant in a suitable manner.

HiPKI RCA shall issue one self-signed certificate for each key lifecycle to establish a trust anchor. Several self-issued certificates shall also be issued in response to the changes in the key pair and policy. The PMA must check the content of the aforementioned certificates prior to their issuance. Newly issued self-issued certificate is delivered to relying parties in accordance with Section 6.1.4 and the self-issued certificates are published in the repository to allow downloading by relying parties.

When cross-certificates are issued, HiPKI RCA shall specify the path length constraint in the basicConstraints extension to ensure that the path for certificate interoperation is permitted. The value of path length is set depending on the path length that allows for certificate interoperation.

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

CAs shall specify the methods used to notify the applicants (subscribers) after the issuance of certificates in their CPS.

If CAs or RAs does not approve the certificate issuance, the certificate application shall be notified in a suitable method and the reason for refusing to issue the certificate shall be clearly stated. CAs shall specify the notification methods for certificate issuance refusal in their CPS.

4.4. Certificate Acceptance

4.4.1. Conduct Constituting Certificate Acceptance

The CA that operates with assurance level 2 or higher or issues TLS certificates shall publish an issued certificate in the repository and deliver the certificate to an applicant after the certificate applicant has (i) reviewed the content of the certificate to be issued or (ii) reviewed the content of the certificate after it is issued. That is, the certificate is deemed to be accepted by the applicant. The certificate is not issued if the certificate applicant refuses to accept the certificate information listed in the certificate to be issued after reviewing its contents; and the certificate shall be revoked if the certificate applicant refuses to accept the issued certificate after reviewing the content of the issued certificate.

The CA that operates with assurance level 2 or higher or issues TLS certificates shall specify the following items in its CPS:

(1) Certificate applicant’s method to accept or to refuse a certificate,

(2) The certificate fields need to be reviewed by the certificate applicant before deciding whether to accept the certificate, and

(3) Method to process certificate refusal.

The above certificate fields that certificate applicant shall first review must include, at least, the subject name field. Before acceptance of the certificate, the applicant shall also review the subject alternative name field of the certificate.

If the method to process certificate refusal involves fee collection and return issues, it shall be determined in accordance with Consumer Protection Act and fair-trade principles of our country.

4.4.2. Publication of the Certificate by the CA

CA repository service shall routinely publish the issued certificates. RAs can deliver the certificate to the subscriber directly if RAs and CAs agree on it.

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

No stipulation.

4.5. Key Pair and Certificate Usage

4.5.1. Subscriber Private Key and Certificate Usage

Key pairs of subscribers shall be generated in compliance with Section 6.1.1 of this CP. Subscribers must be able to control the private keys corresponding to the public key of their certificates and do not issue certificates to others.

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

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 CP and each 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

CAs in HiPKI does not allow renewal of TLS certificate.

4.6.1. Circumstance for Certificate Renewal

Not applicable.

4.6.2. Who May Request Renewal

Not applicable.

4.6.3. Processing Certificate Renewal Requests

Not applicable.

4.6.4. Notification of New Certificate Issuance to Subscriber

Not applicable.

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

Not applicable.

4.6.6. Publication of the Renewal Certificate by the CA

Not applicable.

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

Not applicable.

4.7. Certificate Re-key

4.7.1. Circumstance for Certificate Re-key

(1) CA private keys shall be regularly renewed in accordance with Section 6.3.2.

(2) Certificate re-key is required under the following cases (but not limited to):

(a) A certificate is revoked for reasons of key compromise, and

(b) A certificate has expired, and the usage period of the key pair has also expired.

4.7.2. Who May Request Certification of a New Public Key

CAs may accept a re-key request provided that it is authorized by either the original subscriber, or an authorized representative who retains responsibility for the private key on behalf of a subscriber through a suitable certificate lifecycle account challenge response. A certificate signing request file for certificate re-key is mandatory with any new public key.

4.7.3. Processing Certificate Re-keying Requests

CAs may request additional information before processing a re-key or reissue request and may re-validate the subscriber subject to re-verification of any previously validated data. In the case of a reissuance, authentication through a suitable challenge response mechanism is acceptable. The related procedures must be implemented in accordance with Sections 3.1, 3.2, 3.3, 4.1 and 4.2.

4.7.4. Notification of New Certificate Issuance to Subscriber

As stated in Section 4.3.2.

4.7.5. Conduct Constituting Acceptance of a Re-keyed Certificate

As stated in Section 4.4.1.

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

As stated in Section 4.4.2.

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

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. The new certificate has a new certificate serial number but with the same subject public key and 'NotAfter' date.

4.8.2. Who May Request Certificate Modification

The subscriber certificate subject or an authorized representative of the certificate subject may request modification of the certificates.

4.8.3. Processing Certificate Modification Requests

As stated in Section 4.2.

4.8.4. Notification of New Certificate Issuance to Subscriber

As stated in Section 4.3.2.

4.8.5. Conduct Constituting Acceptance of Modified Certificate

As stated in Section 4.4.1.

4.8.6. Publication of the Modified Certificate by the CA

As stated in Section 4.4.2.

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

No stipulation.

4.9. Certificate Revocation and Suspension

CAs shall specify the mechanism to accept and respond to revocation requests and certificate problem reports in their CPS and decide whether to

provide certificate suspension services depending on certificate usage and service quality.

For expired certificates, CAs may not accept certificate revocation or suspension requests and/or list the information of revocation or suspension on the CRLs. For revoked or suspended certificates prior to expiry, CAs shall list the information of revocation or suspension on the CRLs. After that, the information shall be removed.

4.9.1. Circumstances for Revocation

4.9.1.1. Reasons for Revoking a Subscriber Certificate

CAs 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 the CA that the original certificate request was not authorized and does not retroactively grant authorization;

(3) The CA obtains reasonable evidence that the subscriber's private key (corresponding to the public key in the certificate) suffered a key compromise or is suspected of compromise;

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

CAs 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) The CA obtains evidence that the certificate was misused;

(3) The CA is made aware that a subscriber has violated one or more of

its material obligations under the Subscriber Agreement or Terms of Use;

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

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

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

(7) The CA is made aware that the certificate was not issued in accordance with these requirements or the CA's CP/CPS;

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

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

(10) Revocation is required by the CA's CP and/or CPS; or

(11) The CA 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. Reasons for Revoking a Subordinate CA Certificate

The Issuing CA 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 the Issuing CA;

(2) The Subordinate CA notifies the Issuing CA that the original

certificate request was not authorized and does not retroactively grant authorization;

(3) The Issuing CA 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) The Issuing CA obtains evidence that the certificate was misused;

(5) The Issuing CA 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) The Issuing CA determines that any of the information appearing in the certificate is inaccurate or misleading;

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

(8) The Issuing CA's or Subordinate CA's right to issue certificates under these Requirements expires or is revoked or terminated, unless the issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository; or

(9) Revocation is required by the Issuing CA's CP and/or 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

Subscriber or entities, possessing a private key that corresponds to the public key in a certificate, may request revocation of the certificate to the issuing CA or the RA. Additionally, subscribers, relying parties, application software suppliers, and other third parties may submit certificate problem reports informing the issuing CA of reasonable cause to revoke the certificate.

4.9.3. Procedure for Revocation Request

CAs shall disclose the instructions and specify a continuous 24x7 ability to accept and respond to revocation requests and certificate problem reports

in their CPS. After receiving the certificate revocation request or certificate problem reports, the issuing CA or the RA shall identify and authenticate the applicant in advance according to the regulations in Section 4.9 and its CPS.

CAs shall specify the manner of notifying the subscriber about the decision whether to revoke the certificate in their CPS. If the revocation request has been approved, the issuing CA or the RA shall assign suitable personnel to perform the revocation in accordance with Section 5.2 and the CPS.

4.9.4. Revocation Request Grace Period

The revocation request grace period is the time available to the subscriber within which the subscriber must submit a revocation request after reasons for revocation have been identified. The CA and RA are required to report the suspected compromise of their CA or RA private key and request revocation to the issuing CA within one hour of discovery. The issuing CA may extend revocation grace periods on a case-by-case basis.

4.9.5. Time within Which CA Must Process the Revocation Request

CAs shall begin investigating the facts and circumstances related to a certificate problem report and shall provide a preliminary report on its findings to both the subscriber and the entity who filed the problem report within 24 hours of receipt of the report.

CAs shall specify the criterions and procedures used to establish whether the certificate will be revoked in their CPS. The period from receipt of the certificate problem report or revocation request to published revocation must not exceed the time frame set forth in Section 4.9.1.

4.9.6. Revocation Checking Requirement for Relying Parties

Prior to relying on a certificate, relying parties must check the certificate status via CRLs or OCSP services. The matter of how often new certificate revocation data should be obtained is a determination to be made by the relying party, considering the risk, responsibility, and consequences for using a certificate that the certificate status cannot be guaranteed.

CAs shall specify the requirements for relying parties to check CRLs in their CPS.

4.9.7. CRL Issuance Frequency

The accuracy of CRLs shall be checked by the issuing CA prior to issuance. CRLs shall be issued periodically, even if there are no changes to be made, to ensure timeliness of information. Certificate status information shall be published not later than the next scheduled update. The expired information of certificate status shall be removed from the repository. The regulations regarding issuance frequency of CRLs are described in the following Table:

Assurance Level	CRL
Level 1	At least once every 7 days
Level 2	At least once every 3 days
Level 3	At least once a day
Level 4	At least once a day

4.9.8. Maximum Latency for CRLs

Each CRL should be published no later than the time specified in the nextUpdate field of the previously issued CRL for same scope.

4.9.9. On-line Revocation/Status Checking Availability

CAs shall at least provide CRLs and specify whether OCSP services are supported in their CPS. If a CA does support an OCSP service, its OCSP service must conform to RFC 6960 and RFC 5019.

4.9.10. On-line Revocation Checking Requirements

CAs shall specify the requirements of on-line revocation checking for relying parties in their CPS. If a CA does support an OCSP service, the OCSP responder operated by the CA shall at least support the HTTP GET method, as described in RFC 6960 and/or RFC 5019.

4.9.11. Other Forms of Revocation Advertisements Available

CAs that issue TLS certificates shall support the operation of OCSP stapling for checking the revocation status of certificates. CAs shall ensure that the subscriber "staples" the OCSP response for the certificate in its TLS handshake.

CAs may use other methods to publicize the revoked certificates. Any alternative method must meet the following requirements:

(1) The alternative method is described in CAs' approved CPS;

(2) The alternative method must provide authentication and integrity services commensurate with the assurance level of the certificate being verified; and

(3) The alternative method must meet the issuance and latency requirements for CRLs stated in Sections 4.9.7 and 4.9.8.

4.9.12. Special Requirements Related to Key Compromise

As stated in Sections 4.9.1, 4.9.2 and 4.9.3.

4.9.13. Circumstances for Suspension

Certificate suspension is strictly forbidden for TLS certificates in accordance with Section 4.9.13 of the Baseline Requirements. CAs shall specify whether to provide the service of certificate suspension and resumption in their CPS.

4.9.14. Who Can Request Suspension

For TLS certificates, suspension is not allowed.

4.9.15. Procedure for Suspension Request

For TLS certificates, suspension is not allowed.

4.9.16. Limits on Suspension Period

For TLS certificates, suspension is not allowed.

4.10. Certificate Status Services

4.10.1. Operational Characteristics

CAs shall provide a certificate status service either in the form of CRLs

or OCSP services or both. The public information of certificate status shall contain the ones of revoked certificates and must not be removed until the expiry date of the revoked certificates.

4.10.2. Service Availability

Under normal operating conditions, the response time of the CRL and OCSP services provided by CAs is at most 10 seconds.

CAs shall maintain 24x7 availability of certificate status service that application software can use to automatically check the current status of all unexpired certificates issued by CAs.

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

4.10.3. Optional Features

No stipulation.

4.11. End of Subscription

End of subscription signifies that subscribers stop using CAs' services. CAs shall allow 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

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

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

CAs that support session key encapsulation and recovery shall specify their practices in their CPS.

5. Facility, Management, and Operational Controls

5.1. Physical Controls

5.1.1. Site Location and Construction

The site location and construction requirements for CAs must comply with provisions for hosting highly important and sensitive data and other physical security mechanisms, including access control, security, intrusion detection and video monitoring, to prevent unauthorized access.

5.1.2. Physical Access

CAs shall protect its equipment from unauthorized access and shall implement physical controls after the installation and activation of cryptographic module. Even though the cryptographic module is not installed or activated, the physical controls shall also be implemented to reduce the risk of unauthorized tampering or equipment damage. CAs shall meet the following security mechanisms for various assurance levels:

For the CA operating with assurance levels 1 and 2:

(1) Prevent unauthorized intrusion; and

(2) Portable storage media and documents containing sensitive data shall be kept in a secure location.

For the CA operating with assurance levels 3 and 4:

(1) 24-hour manual or electronic monitoring system;

(2) Maintain and review access log periodically; and

(3) At least two persons jointly when performing physical control over computer system and cryptographic module.

Because HiPKI RCA must issue certificates of all assurance levels, the security system of its facility must be in compliance with the above requirements of assurance level 4.

The following security checks must be done in case of personnel leave the facilities:

(1) The security containers are properly secured; and

(2) Physical security systems (e.g., door locks, vent covers) are functioning properly.

5.1.3. Power and Air Conditioning

CAs shall provide sufficient backup power, i.e., a UPS, to support the operation of the CA system and to avoid a lack of power or air conditioning causes a shutdown. Meanwhile, the UPS must provide at least 6 hours of power for backup of repository data, including issued certificates and CRL.

5.1.4. Water Exposures

CAs shall protect the facility of its CA equipment from water exposure.

5.1.5. Fire Prevention and Protection

The facilities that CAs located must have automatic fire detection and alarm functions and systems which include automatic fire extinguishing equipment. Manual switches should be placed on major entrances and exits to allow manual operation by on-site personnel during emergencies.

5.1.6. Media Storage

CAs shall protect relevant storage media from accidental damage.

5.1.7. Waste Disposal

No stipulation.

5.1.8. Off-site Backup

CAs shall specify whether off-site backup is provided, the distance from CA hosts to the backup site, and the backup items in their CPS.

5.2. Procedural Controls

5.2.1. Trusted Roles

CAs and RAs must assign trusted roles to be responsible for performance of related task to serve as a foundation of trust. The fairness of the CAs may be reduced if security goals cannot be reached due to an accident or human error. CAs may adopt the following two methods to

enhance security:

(1) Guarantee that the personnel performing each role have received appropriate training and is completely trustworthy.

(2) Appropriately separate each task. Each task shall be assigned to more than one person to prevent one person from having the opportunity to perform malicious activities.

Trusted roles include the following:

(1) **Administrator**
Responsible for installing, configuring and maintaining CA system and software, including CA and user accounts, audit parameters and generation of component keys.

(2) **CA Officer**
Activate/deactivate the certificate issuance or revocation service of CA HSM.

(3) **Internal Auditor**
Check and maintain audit logs as well as execute internal audits.

(4) **System Operator**
Perform system backup and troubleshooting.

(5) **Physical security controller**
Physical security controls.

(6) **Cyber security coordinator**
Security protection of the network and network equipment.

(7) **Anti-virus and anti-hacking coordinator**
Provide technologies or measures of anti-virus, anti-hacking, and/or anti-malware.

(8) **RA Officer (validation and vetting personnel, RAO)**
Responsible for processing certificate requests of issuance, revocation and re-key, including enrollment, identity identification and authentication.

5.2.2. Number of Persons Required per Task

CAs shall specify the number of persons required per task in their CPS.

5.2.3. Identification and Authentication for Each Role

Not required for the CA operating with assurance level 1. For the CA operating with assurance level 2 or higher, personnel appointed to trusted roles must undergo identification and authentication before performing the tasks.

5.2.4. Roles Requiring Separation of Duties

In order to optimize the security of CA equipment and operations, CA roles requiring separation of duties are described as follows:

Assurance Level	Regulations
Level 1	No stipulation
Level 2	Individual CA personnel shall be specifically designed the trusted roles defined in Section 5.2.1 and shall follow the regulations below: (1) An individual may assume only one of the administrator, CA officer, internal auditor, or cyber security coordinator roles. (2) Individuals designated as administrator, CA officer or internal auditor may also assume the system operator role. (3) Individuals designated as physical security controller may not assume any of the administrator, CA officer, internal auditor, or system operator role. (4) Individuals designated as RAO may not assume any of the administrator, internal auditor, or system operator role. (5) Any individual designated as trusted role is allowed to perform self-audit.
Level 3	Same as Level 2
Level 4	Same as Level 2

5.3. Personnel Controls

5.3.1. Qualifications, Experience, and Clearance Requirements

Prior to the engagement of any person in the certificate management process, whether an employee or an independent contractor of CAs, CAs shall verify the identity and trustworthiness of such person. Required qualifications for person selected for trusted roles are loyalty, integrity and ROC citizenship. CAs shall specify regulations concerning personnel qualifications, selection, supervision and audit in their CPS.

5.3.2. Background Check Procedures

CAs shall specify background check procedures in their CPS.

5.3.3. Training Requirements

CAs shall provide all personnel performing information verification duties with skills-training that covers:

(1) Basic Public Key Infrastructure knowledge,

(2) Authentication and vetting policies and procedures (including issuing CA's CP and/or CPS),

(3) Common threats to the information verification process (including phishing and other social engineering tactics),

(4) Disaster recovery and business continuity procedures,

(5) CA/RA security principles and mechanisms, and

(6) Baseline Requirements (only for the CA that issues TLS certificates).

CAs shall require RAO to pass an examination provided by the CAs on the information verification requirements outlined in the Baseline Requirements. CAs shall maintain records of such training and ensure that personnel entrusted with RAO maintain a skill level that enables them to perform such duties satisfactorily. CAs shall document that each RAO possesses the skills required by a task before allowing the RAO to perform that task.

5.3.4. Retraining Frequency and Requirements

All personnel acting in trusted roles must maintain skill levels consistent with CAs' training and performance programs. CAs shall make the personnel aware of any changes to the issuing CA's operations, such as software/hardware upgrades, work procedure changes or equipment replacement. If such operations change, the issuing CA shall provide documented retraining, in accordance with an executed training plan, to all trusted roles.

New personnel shall also take the training to meet the requirement of training programs. CAs shall review the training status of all personnel every year.

5.3.5. Job Rotation Frequency and Sequence

No stipulation.

5.3.6. Sanctions for Unauthorized Actions

CAs shall establish appropriate management rules and publish the rules in their CPS to prevent unauthorized or inappropriate actions. CAs shall take appropriate administrative and disciplinary actions against personnel failed to comply with the CP or CPS.

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

CAs shall provide personnel in trusted roles with the documentation, including the CP, CPS, regulations and contracts, necessary to perform their duties.

5.4. Audit Logging Procedures

5.4.1. Types of Events Recorded

CAs shall ensure that all events relating to the certificate administration system and its operating system are logged to establish the accountability of the operators who initiate such actions. Regardless of manual or automatic generation, each audit log should contain the following elements:

(1) Type of event (relating to CAs key life cycle management, CAs and subscriber certificate life cycle management, or security);

(2) The identity of the entity and/or operator that caused the event;

(3) The identity to which the event was targeted;

(4) The date and time the event occurred;

(5) The cause of the event; and

(6) Log (success or failure) of performing certificate issuance or revocation procedure by CAs

Audit logs shall be automatically generated by the system whenever possible. If not possible, logs may be made in work logbooks, paper or other physical form. When an event occurs, CAs shall decide to record the audit logs in the form of electronic or physical. According to different assurance levels, the audit events (or called auditable events) recorded by CAs are stated in the following Table:

Auditable Event/Assurance Level	Level 1	Level 2	Level 3	Level 4
A.1 Security Audit				
A.1.1 Any changes to the audit parameters, e.g., audit frequency, type of event audit and new/old parameter contents		✓	✓	✓
A.1.2 Any attempt to delete or modify the audit logs		✓	✓	✓
A.2 Identification and Authentication				
A.2.1 Successful and fail attempts		✓	✓	✓

Auditable Event/Assurance Level	Level 1	Level 2	Level 3	Level 4
to assume a role				
A.2.2 Change in the maximum value of authentication		✓	✓	✓
A.2.3 Maximum value of fail authentication		✓	✓	✓
A.2.4 Administrator unlocks an account that has been locked as a result of a number of fail authentication		✓	✓	✓
A.2.5 Administrator changes the method of authentication, e.g., from password to biometrics		✓	✓	✓
A.3 Key Generator				
A.3.1 When the CA generates a key (not limited to the key generation of single session or single use)	✓	✓	✓	✓
A.4 Load and Storage of Private Key				
A.4.1 Loading private key to system component	✓	✓	✓	✓
A.4.2 Access of private keys stored in CAs for key recovery	✓	✓	✓	✓
A.5 Creation, Deletion and Storage of Trusted Public Key				
A.5.1 All changes to the trusted public keys, including creation and deletion	✓	✓	✓	✓
A.6 Export of Private Key				
A.6.1 Export of private key (exclusive of single session or single use key)	✓	✓	✓	✓
A.7 Certificate Registration				

Auditable Event/Assurance Level	Level 1	Level 2	Level 3	Level 4
A.7.1 Processes of all certificate registration	✓	✓	✓	✓
A.8 Certificate Revocation				
A.8.1 Processes of all certificate revocation		✓	✓	✓
A.9 Approval of Certificate Status Change				
A.9.1 Approval or rejection of a certificate status change		✓	✓	✓
A.10 CA Configuration				
A.10.1 Any change to CAs' configuration		✓	✓	✓
A.11 Account Administration				
A.11.1 Addition or deletion of roles or users	✓	✓	✓	✓
A.11.2 Alteration of access privilege of roles or users	✓	✓	✓	✓
A.12 Management of Certificate Profile				
A.12.1 Any change to certificate profile	✓	✓	✓	✓
A.13 Management of CRL Profile				
A.13.1 Any change to CRL profiles		✓	✓	✓
A.14 Miscellaneous				
A.14.1 Installation of operating system		✓	✓	✓
A.14.2 Installation of CA system		✓	✓	✓
A.14.3 Installation of HSM			✓	✓
A.14.4 Removal of HSM			✓	✓
A.14.5 Destruction of HSM		✓	✓	✓

Auditable Event/Assurance Level	Level 1	Level 2	Level 3	Level 4
A.14.6 System startup		✓	✓	✓
A.14.7 Applications attempted to login CA system		✓	✓	✓
A.14.8 Receipt of hardware / software			✓	✓
A.14.9 Attempt of setting password		✓	✓	✓
A.14.10 Attempt of altering password		✓	✓	✓
A.14.11 Backup of CA data		✓	✓	✓
A.14.12 Restoration of CA data		✓	✓	✓
A.14.13 File manipulation (e.g., create, rename, or move)			✓	✓
A.14.14 Delivery of any information to repository			✓	✓
A.14.15 Access to internal database of CA			✓	✓
A.14.16 Notification of certificate compromise		✓	✓	✓
A.14.17 Loading token with certificate			✓	✓
A.14.18 Transmission of token			✓	✓
A.14.19 Zeroization of token		✓	✓	✓
A.14.20 CA Re-keying	✓	✓	✓	✓
A.15 Configuration Changes to CA Server				
A.15.1 Hardware		✓	✓	✓
A.15.2 Software		✓	✓	✓
A.15.3 Operating system		✓	✓	✓
A.15.4 Patches		✓	✓	✓

Auditable Event/Assurance Level	Level 1	Level 2	Level 3	Level 4
A.15.5 Security profiles			✓	✓
A.16 Physical Access / Site Security				
A.16.1 Personnel getting in and out of CA facility			✓	✓
A.16.2 Access of CA server			✓	✓
A.16.3 Known or suspected violation of physical security regulations		✓	✓	✓
A.17 Anomalism				
A.17.1 Software errors		✓	✓	✓
A.17.2 Failure of software integrity check		✓	✓	✓
A.17.3 Receipt of improper messages			✓	✓
A.17.4 Misrouted messages			✓	✓
A.17.5 Network attacks (suspected or confirmed)		✓	✓	✓
A.17.6 Breakdown of equipment	✓	✓	✓	✓
A.17.7 Power outage			✓	✓
A.17.8 Breakdown of UPS			✓	✓
A.17.9 Failure of obvious and significant network service or access			✓	✓
A.17.10 Violation of CP	✓	✓	✓	✓
A.17.11 Violation of CPS	✓	✓	✓	✓
A.17.12 Reset of operating system clock		✓	✓	✓

5.4.2. Frequency of Processing Log

Audit logs shall be reviewed periodically according to the Table below and explanations shall be added to the major events in the audit reports. Review work shall include verification of record tampering, inspection of all log entries and investigation of any detected anomalies or irregularities.

Assurance Level	Frequency of Processing Log
Level 1	Not stipulated
Level 2	Not stipulated
Level 3	(1) At least once every two months. (2) CAs shall reinforce the review on audit logs regarding security event after the previous audit review. (3) CAs shall make an investigation for any evidence of malicious activity and shall document any actions taken as a result of a review.
Level 4	(1) At least once a month. (2) CAs shall reinforce the review on audit logs regarding security event after the previous audit review. (3) CAs shall make an investigation for any evidence of malicious activity and shall document any actions taken as a result of a review.

5.4.3. Retention Period for Audit Log

Audit logs of CAs shall be retained in compliance with the retention period specified in Section 5.5.2.

Prior to save audit logs to a secure off-site location, the audit logs shall be retained at the site of CAs for at least two months. CAs shall make these audit logs available to its qualified auditor upon request. After the end of the audit log retention period, the removal task shall be performed only by the internal auditor.

5.4.4. Protection of Audit Log

CAs shall protect archived data from unauthorized access, alteration, and destruction prior to the end of the audit log retention period.

5.4.5. Audit Log Backup Procedures

Assurance Level	Audit Log Backup Procedures
Level 1	No stipulated.
Level 2	Backup of audit logs shall be done at least once a month.
Level 3	
Level 4	Backup of audit logs shall be done and saved to a secure off-site location at least once a month. Related off-site backup procedures shall be specified in the issuing CA's CPS.

5.4.6. Audit Collection System (Internal vs. External)

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

5.4.7. Notification to Event-causing Subject

No stipulated.

5.4.8. Vulnerability Assessments

CAs that issue TLS certificates shall perform regular vulnerability assessment and penetration testing in compliance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security (WebTrust for CA – SSL BR) and Network and Certificate System Security Requirements.

5.5. Records Archival

5.5.1. Types of Records Archived

CAs shall archive the following information upon the security requirements of various assurance levels.

Archived Information / Assurance Level	**Level 1**	**Level 2**	**Level 3**	**Level 4**
Any accreditation of the CA (If applicable)	✓	✓	✓	✓
CPS	✓	✓	✓	✓
Important contractual	✓	✓	✓	✓
System and equipment configurations, modifications, and updates	✓	✓	✓	✓
Certificate issuance requests	✓	✓	✓	✓
Certificate revocation requests		✓	✓	✓
Identity authentication data		✓	✓	✓
Document receipt or acceptance of a certificate or token		✓	✓	✓
Token activation log		✓	✓	✓
Issued or published certificates	✓	✓	✓	✓
A record of certificate re-keys	✓	✓	✓	✓
Issued and/or published CRLs		✓	✓	✓
Audit logs	✓	✓	✓	✓
Any data or applications necessary to verify an		✓	✓	✓

Archived Information / Assurance Level	Level 1	Level 2	Level 3	Level 4
archive's contents				
Document requests by Auditors		✓	✓	✓

5.5.2. Retention Period for Archive

According to various assurance levels, the retention periods for archived data that, at a minimum, the CA shall retain are specified in the following Table:

Assurance Level	Retention Period
Level 1	2 years
Level 2	2 years
Level 3	2 years
Level 4	20 years

If the stored media cannot retain the data for the required period, a mechanism that regularly transfers the archived data to new media must be established. Meanwhile, the application used to process the archive data shall also be retained until the data is either destroyed or transferred to a newer medium.

5.5.3. Protection of Archive

CAs shall store archived data at an off-site location providing proper protection. The protection class of the location may not be lower than that of the CAs located.

5.5.4. Archive Backup Procedures

No stipulation.

5.5.5. Requirements for Time-stamping of Records

No stipulation.

5.5.6. Archive Collection System (Internal or External)

No stipulation.

5.5.7. Procedures to Obtain and Verify Archive Information

CAs shall specify the procedures to obtain and verify archive information in their CPS.

5.6. Key Changeover

CAs shall periodically change its private keys in accordance with Section 6.3.2. After key changeover, CAs shall sign certificates using only the new key and shall notify all entities relying on the CAs certificate about the fact.

HiPKI RCA shall change its key pair before the usage period of its private key has expired. After key changeover, HiPKI RCA shall sign a new self-signed certificate (by using the new private key) and mutually sign a new self-issued certificate (by using the new and old private keys, separately). The issuance procedures for these three new certificates need to comply with Section 4.3.

The Subordinate CA shall change its key pair before the usage period of its private key has expired. After key changeover, the Subordinate CA shall apply for a new CA certificate from the superior CA in accordance with Section 4.1. The superior CA must issue and publish the new CA certificate before the old CA certificate of the Subordinate CA has expired.

For Root CA that is cross-certified with HiPKI RCA, the time to change its key pair depends on the CP that the Root CA complied with. After key changeover, whether the Root CA shall continue to request a cross-certificate to HiPKI RCA is determined by the agreement or contract between the Root CA and CHT. If this is the case, it shall be carried out in accordance with Section 4.2. In addition, an enough time is required to allow the PMA and HiPKI RCA to process the request and to ensure that HiPKI RCA is able to issue and publish the new cross-certificate before the Root CA's old cross-certificate has expired.

The CA shall still maintain and protect its old private keys and shall

make the old certificate available to verify CRL or OCSP until all of the subscriber certificates signed with the private key have expired.

5.7. Compromise and Disaster Recovery

5.7.1. Incident and Compromise Handling Procedures

CAs shall establish incident and compromise reporting and handling procedures. Required documentation includes, but is not limited to, an incident response plan and business continuity plan, which shall be reviewed, drilled, and updated at least annually.

CAs shall make its incident response plan and business continuity plan available to CAs' auditors upon request.

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

CAs shall make regular system backup in accordance with the CP and CPS to minimize disaster losses in the event of computer resources, software or data corruption. After ensuring the integrity of the CA systems, CAs shall give priority to restoring the capacity of repository and to reestablishing the generation of certificate status information.

CAs operating with assurance levels 3 and 4 shall hold a drill of recovery procedures if computing resources, software, and/or data are corrupted at least annually.

5.7.3. Entity Private Key Compromise Procedures

The CA operating with assurance level 2 or higher shall specify the procedures and appropriate actions taken in the event that a CA private key is compromised in its CPS, in order to restore the operation of certificate issuance and administration as soon as possible.

The CA operating with assurance levels 3 and 4 shall hold a drill of CA private key compromise at least annually.

When the private key of the CA is compromised, the application software supplier, subscriber, and relying party should be notified immediately.

5.7.4. Business Continuity Capabilities after a Disaster

The CA operating with assurance level 2 or higher shall specify the steps of resuming CA facilities operation following a disaster in its CPS.

The CA operating with assurance levels 3 and 4 shall hold a drill of its disaster recovery plan at least annually.

5.8. CA or RA Termination

CAs shall terminate all or a portion of its digital certificate issuance and management operations subject to the Electronic Signatures Act.

6. Technical Security Controls

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

Key pairs must be generated in a secure cryptographic module or physically secure environment that meets FIPS 140-2 using key generation algorithm and key size as specified in Sections 6.1.5 and 6.1.6.

If a private key is generated in the cryptographic module, that key shall always be kept in that cryptographic module or encrypted and stored in the host. If the private key is generated outside the cryptographic module, that key shall be imported into the cryptographic module without leaving the key generation environment. The environment should assure that no personnel may use any method to obtain generated private keys without being detected. After the private key is stored in the cryptographic module, that key shall immediately be deleted from the key-generation environment.

CAs shall take appropriate measures to ensure that the uniqueness of the subscriber's public key in HiPKI.

Any pseudo-random number used for key generation must be approved by CHT. With regard to validated hardware or software cryptographic module that CAs shall use when generating subscriber's pseudo-random numbers and key pair is listed in the following Table and is classified according to assurance level that CAs operated:

Assurance Level	Key Generation Mechanism
Level 1	Software or hardware
Level 2	Software or hardware
Level 3	Software or hardware
Level 4	Limited to hardware

6.1.2. Private Key Delivery to Subscriber

If a CA, RA or trusted third-party generates private keys on behalf of any subscriber, then the entity generating the key shall deliver the private key securely to the subscriber via a cryptographic module, and the subscriber shall acknowledge receipt of the private key. If a mechanism of secret sharing (such as code or PIN) is used, either the subscriber or the entity shall be the only entity who knows the secret.

The entity shall perform the following tasks:

(1) Protect the private key from activation, compromise, or modification during the delivery process;

(2) Not retain a copy of the subscriber's private key after delivery;

(3) Ensure that the correct tokens and activation data are provided to the correct subscribers;

(4) Maintain a record of the subscriber's acknowledgement of receipt of the cryptographic module containing the subscriber's private key; and

(5) Maintain accountability for the location and state of the cryptographic module until the subscriber acknowledges acceptance of the device.

If private keys are generated and stored inside the subscriber's cryptographic module, there is no need to deliver its private key.

6.1.3. Public Key Delivery to Certificate Issuer

The subscriber shall deliver its public key to the CA for identity authentication. Delivery methods include:

(1) Electronic message for certificate application sent by the RA;

(2) When keys are generated by a third-party, CA or RA must obtain the subscriber's public key through auditable secure channels;

(3) Other secure electronic mechanisms; or

(4) Secure non-electronic methods, e.g., delivering media stored the subscriber's public key via registered or express mail.

6.1.4. CA Public Key Delivery to Relying Parties

The Root CA (i.e., HiPKI RCA) must make its public key available at all times. The Subordinate CA must deliver the Root CA's self-signed certificate or public key to the relying party in a reliable manner, include:

(1) CAs stores the Root CA's self-signed certificate or public key into a token and delivers it to the relying party in a secure fashion;

(2) Out-of-band delivery of the Root CA's self-signed certificate or public key;

(3) Out-of-band delivery of the hash value or fingerprint of the Root CA's self-signed certificate or public key provided for user comparison; or

(4) Other methods approved by the PMA.

The above out-of-band channels shall be specified in the Root CA's CPS. The Root CA shall publish the issued Subordinate CA certificates in its repository.

6.1.5. Key Sizes

Certificates issued under this CP must meet the following requirements for algorithm and key size.

(1) Root CA certificates:

Digest algorithm	SHA-256, SHA-384 or SHA-512
RSA modulus size (bits)	4096
ECC curve	NIST P-384

(2) Subordinate CA certificates:

Digest algorithm	SHA-256, SHA-384 or SHA-512
RSA modulus size (bits)	4096
ECC curve	NIST P-256 or P-384

(3) Subscriber certificates:

Digest algorithm	SHA-256, SHA-384 or SHA-512
RSA modulus size (minimum bits)	2048
ECC curve	NIST P-256 or P-384

6.1.6. Public Key Parameters Generation and Quality Checking

For RSA algorithm, public key parameters must be null. CAs need not perform parameter quality checking while a primality test is required. CAs shall specify how to accomplish the related test in their CPS.

For other algorithms, public key parameters shall be set and parameter quality checking shall be done by CAs in accordance with relevant international standards, e.g., NIST SP 800-89.

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

The key usage extension of CA certificates must be set to keyCertSign and cRLSign. If the CA will use its private signing keys to sign a OCSP response, then the digitalSignature bit must also be set.

CAs must set the content of the key usage extension for TLS certificates depending on the algorithm used for key pair generation and the intended application of the key pairs, but bit positions for keyCertSign and cRLSign must not be set.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

The CA shall implement physical and logical safeguards to prevent unauthorized certificate issuance. Protection of the CA private key outside the validated system or device specified above must consist of physical security, encryption, or a combination of both, implemented in a manner that prevents disclosure of the CA private key. The CA shall encrypt its private

key with an algorithm and key-length that, according to the state of the art, are capable of withstanding cryptanalytic attacks for the residual life of the encrypted key or key part.

6.2.1. Cryptographic Module Standards and Controls

The PMA shall ensure that the cryptographic module used in HiPKI meets the requirements of FIPS 140-2 series or equivalent international standard.

Cryptographic module requirements for each entity in HiPKI are shown in the following table. Each entity except the subscriber shall deem these requirements as the minimum level of cryptographic module protection. The levels listed in this table are defined referring to the FIPS 140-2 series.

Assurance Level / Entity	HiPKI RCA	Subordinate CA	RA	Subscriber
Level 1	N/A	Level 1 (Hardware or Software)	Level 1 (Hardware or Software)	Not stipulated
Level 2	N/A	Level 2 (Hardware)	Level 1 (Hardware or Software)	Level 1 (Hardware or Software)
Level 3	N/A	Level 3 (Hardware)	Level 2 (Hardware)	Level 1 (Hardware or Software)
Level 4	Level 3 (Hardware)	Level 3 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)

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

The CA private signing keys must comply with the multi-person control specified in Chapter 5.

6.2.3. Private Key Escrow

CAs shall not escrow their private signing keys.

6.2.4. Private Key Backup

CAs shall backup their private signing keys under multi-person control and shall store the backup at a secure off-site location. CAs must specify the procedures of key backup in their CPS.

6.2.5. Private Key Archival

CAs shall not archive their 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 shall be controlled complying with the requirements specified in Section 6.2.2. The private keys shall be encrypted or split by CAs and its RAs when they are 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 the Issuing CA becomes aware that a Subordinate CA private key has been communicated to an unauthorized person or an organization not affiliated with the Subordinate CA, then the CA shall revoke all certificates that include the public key corresponding to the communicated private key.

6.2.7. Private Key Storage on Cryptographic Module

As stated in Sections 6.1.1 and 6.2.1.

6.2.8. Method of Activating Private Key

The activator shall authenticate itself to the cryptographic module before activating its private key. Acceptable authentication methods include (but are not limited to) pass-phrase, personal tokens, personal identification number (PIN) or biometric, and disclosure must be avoided when the activation data is input, i.e., activation data shall not be displayed.

CAs shall prevent unauthorized access to any activated private keys.

6.2.9. Method of Deactivating Private Key

The cryptographic module must stop operation when not in use by means of the manual logout procedure or automatically stop operation after a period of non-operation (length of time shall be stipulated in the issuing CA's CPS). If the hardware cryptographic module is no longer being used, it must be separated from the server and stored in a secure location.

6.2.10. Method of Destroying Private Key

When a private signing key and its backup is no longer needed or the certificate has expired and been revoked, the key must be destroyed. For software cryptographic modules, CAs may destroy the private signing keys by overwriting the data. For hardware cryptographic modules, CAs may destroy the private signing keys by executing a "zeroize" command, but physical destruction of hardware is not required.

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

Public key archival is not required anymore after the corresponding certificate is archived in compliance 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

All CAs in HiPKI 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	30 years

Type of CA	Private Key Usage	Certificate Term
	years ■ Issuing CRLs, OCSP responder certificates, or OCSP responses: 30 years	
Subordinate CA / Cross-certified CA	■ Issuing end-entity certificates: 10 years ■ Issuing CRLs, OCSP responder certificates, or OCSP responses: 20 years	20 years

The validity of Subordinate CA certificates or cross-certificates issued by a Root CA shall not exceed the validity of the Root CA's self-signed certificate.

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

6.3.2.2. Subscriber Certificate Operational Periods and Key Pair Usage Periods

TLS certificates in HiPKI have a maximum validity period of:

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

The validity of TLS certificates shall not exceed the validity of their issuing CA certificates.

6.4. Activation Data

6.4.1. Activation Data Generation and Installation

The activation data of the CA private keys shall be generated by appropriate security mechanisms and managed by appropriate individuals in trusted roles.

6.4.2. Activation Data Protection

The activation data used to activate the private keys must be protected by appropriate security mechanisms after the risk assessment. If the activation data needs to be transmitted, it should be transmitted through an appropriate secure channel.

CAs shall specify the method for protecting the activation data in their CPS.

6.4.3. Other Aspects of Activation Data

No stipulation.

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

The CA operating with assurance levels 3 and 4 and its ancillary parts must include the following computer security functions. These functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards:

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

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

(3) Provide security audit capability,

(4) Require use of cryptography for session communication and database security, and

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

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

6.5.2. Computer Security Rating

No stipulation.

6.6. Life Cycle Technical Controls

6.6.1. System Development Controls

The system development controls for CAs are as follows:

Assurance Level	System Development Controls
Level 1	No stipulation.
Level 2 Level 3 Level 4	(1) Must ensure the software is developed with software engineering development methods. (2) The hardware and software must be dedicated and authorized. (3) Malicious software must be prevented from being installed on the CA equipment. (4) For software used by the RA, it must check for malicious code before the first use or version update and perform a security scan periodically. (5) System development environment and test environment shall be separated from the on-line environment. (6) Research and development units of CAs shall exercise the due care of a good management responsibility (e.g., signing a guaranteed agreement of security compliance to ensure that there are no back doors or malicious programs installed in the CA systems) and provide program or hardware handover lists, test reports, and administration manuals.

6.6.2. Security Management Controls

The security management controls for CAs are as follows:

Assurance Level	Security Management Controls
Level 1 Level 2 Level 3	(1) No software or hardware unrelated to the operation shall be installed. (2) The CA system configurations and their modification history must be documented and controlled. (3) There must be a mechanism for detecting unauthorized

Assurance Level	Security Management Controls
	modification to the CA software or configuration. (4) The CA software, when installing, must be verified with no modifications, and be the version intended for use. (5) CAs shall perform security management controls in compliance with WebTrust for CA audit scheme.
Level 4	(1) No software or hardware unrelated to the operation shall be installed. (2) The CA system configurations and their modification history must be documented and controlled. (3) There must be a mechanism for detecting unauthorized modification to the CA software or configuration. (4) The CA software, when installing, must be verified with no modifications, and is the version intended for use. (5) Perform an integrity check of CA software is required before each execution. (6) CAs shall perform security management controls in compliance with WebTrust for CA audit scheme.

6.6.3. Life Cycle Security Controls

CAs shall determine lifecycle security controls according to their demand and shall specify these controls in the CPS.

6.7. Network Security Controls

CA hosts are not connected to external networks while their repositories are connected to the Internet to provide uninterrupted services (except during required maintenance or backup). CAs shall specify network security controls in their CPS.

6.8. Time-stamping

CA systems shall regularly synchronize with a reliable time service to ensure the accuracy of system clocks and that of the following items:

(1) Time of certificate issuance,

(2) Time of certificate revocation,

(3) Time of CRL issuance, and

(4) Time of system event occurrence.

Clock adjustments shall be auditable events (see Section 5.4.1).

7. Certificate, CRL, and OCSP Profiles

7.1. Certificate Profile

CAs shall generate 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)

CAs shall issue ITU-T X.509 version 3 certificates.

7.1.2. Certificate Extensions

CAs must set certificate extensions in accordance with the ITU-T X.509, Baseline Requirements, and RFC 5280. Any CA is allowed to set other extensions, and the detail of these extensions including which ones shall be marked as critical shall be stated in its CPS.

7.1.3. Algorithm Object Identifiers

CAs shall sign certificates using one of the following algorithms and their corresponding OIDs:

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)}

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

When the aforementioned ECC algorithm is used to generate ECDSA keys, the OID of the elliptic curve domain parameter that the algorithm uses must be set as follows according to its key size:

Key Size	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

CAs shall use ITU-T X.500 distinguished names in the subject and issuer fields of certificates. The attribute types of the distinguished names must be composed in accordance with the ITU-T X.509, Baseline Requirements, and RFC 5280.

As specified in Baseline Requirements Section 7.1.4.1, the encoded content of the issuer distinguished name field of each certificate in the certification path shall be byte-for-byte identical with the encoded form of the subject distinguished name field of the issuing CA certificate. In addition, the encoded content of the subject distinguished name field of the aforementioned CA certificate SHALL be byte-for-byte identical among all certificates whose subject distinguished names can be compared as equal, and including expired and revoked certificates.

7.1.5. Name Constraints

No stipulation.

7.1.6. Certificate Policy Object Identifier

When CAs issue a certificate containing one of the CP OIDs set forth in Section 1.2, it asserts that the certificate was issued and is managed in

accordance with the requirements applicable to that CP OID.

7.1.7. Usage of Policy Constraints Extension

No stipulation.

7.1.8. Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

Processing semantics for the critical certificate policies extension must be in accordance with the ITU-T X.509, Baseline Requirements, and RFC 5280.

7.2. CRL Profile

7.2.1. Version Number(s)

CRLs MUST be of type X.509 v2.

7.2.2. CRL and CRL Entry Extensions

The CRL and CRL entry extensions in the CRLs MUST comply with the ITU-T X.509, Baseline Requirements, and RFC 5280.

7.3. OCSP Profile

The CA providing an OCSP service shall specify the OCSP version number and the used standards of OCSP extensions in its CPS. The URL of the OCSP service shall be able to be obtained from the authority information access (AIA) extension of certificates issued by that CA.

7.3.1. Version Number(s)

CAs shall provide OCSP services in compliance with RFC 5019 and RFC 6960.

7.3.2. OCSP Extensions

CAs shall provide OCSP extensions in accordance with the Baseline Requirements, RFC 5019, and RFC 6960.

8. Compliance Audit and Other Assessments

CAs shall conduct a compliance audit in accordance with WebTrust for CA to ensure that the requirements of this CP and their CPS are being implemented and enforced. The CA that issues OV or DV TLS certificates must undergo an extra WebTrust for CA – SSL BR audit.

If a CA does not have a currently valid audit report indicating compliance with one of the aforementioned audits, then the CA shall successfully complete a point-in-time readiness assessment before issuing TLS certificates.

8.1. Frequency or Circumstances of Assessment

CAs shall conduct routine external audits at least once per year and the audit period must not exceed 12 months in duration.

CAs shall conduct routine and non-routine audits on its Subordinate CAs and RAs to ensure that the Subordinate entities are operating in compliance with their CPS.

According to the Baseline Requirements and WebTrust for CA – SSL BR, the CA that issues TLS certificates also must assign auditors to perform self-audits on at least a quarterly basis against a randomly selected sample of the greater of one certificate or at least three percent of the certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.

8.2. Identity/Qualifications of Assessor

Audit personnel shall be independent from the audited CA and may be performed by a qualified auditor that possesses the following qualifications:

(1) Impartial third parties, or

(2) An entity which is independent from the audited CA in organization division.

Audit personnel shall submit an impartial and independent assessment. CHT retains the qualified auditor who is familiar with CA operations and is

authorized by WebTrust for CA program as a licensed WebTrust practitioner that can perform WebTrust for CA-related audits in R.O.C., and 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 and be familiar with CA certificate issuance and administration regulations. CAs shall conduct identity identification of auditors during auditing.

8.3. Assessor's Relationship to Assessed Entity

The audit personnel shall be independent from the audited CA, as specified in Section 8.2.

8.4. Topics Covered by Assessment

The assessment shall include the following topics:

(1) Whether a CA is operating in accordance with the CPS,

(2) Whether the requirements of the CA's CPS are being implemented and enforced subject to this CP,

(3) Whether all RAs of that CA comply with this CP and their CPS, and

(4) If a Cross-Certification Agreement (CCA) is signed between the CA and other root CA, that Root CA shall be considered in the assessment to ensure that the Root CA's compliance with the CCA.

8.5. Actions Taken as a Result of Deficiency

If audit personnel find a discrepancy between the requirements of this CP or the stipulations in the CCA and the design, operation, or maintenance of a CA, the following actions shall be performed:

(1) Note the discrepancy, and

(2) Notify the responsible authority promptly about the discrepancy, and if the discrepancy is a critical fault, the PMA shall be notified as well.

The CA where the discrepancy occurred shall make improvements based on the audit report and the stipulations in this CP or the CCA.

8.6. Communication of Results

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

9. Other Business and Legal Matters

9.1. Fees

9.1.1. Certificate Issuance or Renewal Fees

No stipulation.

9.1.2. Certificate Access Fees

No stipulation.

9.1.3. Revocation or Status Information Access Fees

No stipulation.

9.1.4. Fees for Other Services

No stipulation.

9.1.5. Refund Policy

No stipulation.

9.2. Financial Responsibility

9.2.1. Insurance Coverage

No stipulation.

9.2.2. Other Assets

See Section 9.2.1.

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

CAs shall specify the scope of confidential information in their CPS.

9.3.2. Information Not Within the Scope of Confidential Information

CAs shall specify the information not within the scope of confidential in their CPS.

9.3.3. Responsibility to Protect Confidential Information

CAs shall specify the responsibility to protect confidential information in their CPS.

9.4. Privacy of Personal Information

9.4.1. Privacy Plan

CAs shall protect personal information in accordance with the police of personal information protection and privacy on their website.

9.4.2. Information Treated as Private

CAs shall specify the information treated as privacy in their CPS.

9.4.3. Information Not Deemed Private

CAs shall specify the information not deemed privacy in their CPS.

9.4.4. Responsibility to Protect Private Information

CAs shall specify the responsibility to protect privacy information in their CPS.

9.4.5. Notice and Consent to Use Private Information

CAs shall specify the related stipulations with respect to the use of private information in their CPS.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

CAs shall specify the related stipulations with respect to the disclosure pursuant to judicial or administrative process in their CPS.

9.4.7. Other Information Disclosure Circumstances

CAs shall specify the related stipulations with respect to other information disclosure, which shall be disclosed only in accordance with the relevant laws.

9.5. Intellectual Property Rights

This CP is available for free download from the repository or reasonable use according to the relevant provisions in the Copyright Act of R.O.C. No one can charge for the distribution of this CP. CHT reserves the right to pursue legal action for any violation of the use or dissemination of this CP.

9.6. Representations and Warranties

9.6.1. CA Representations and Warranties

The issuing CA shall represent and warrant to the Certificate Beneficiaries including Subscribers, Relying Parties, and Application Software Suppliers that, during the period when the Certificate is valid, the issuing CA has complied with this CP and/or its 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, the issuing CA (i) implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the Domain Name(s) listed in the Certificate's subject field and subjectAltName extension (or, only in the case of Domain Names, was delegated such right or control by someone who had such right to use or control); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CP and/or its CPS (see Section 3.2);

(2) **Authorization for Certificate**: That, at the time of issuance, the issuing CA (i) implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate

on behalf of the Subject; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CP and/or its CPS (see Section 3.2.5);

(3) **Accuracy of Information**: That, at the time of issuance, the issuing CA (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 CP and/or its CPS (see Sections 3.2.2, 3.2.3 and 3.2.7);

(4) **No Misleading Information**: That, at the time of issuance, the issuing CA (i) implemented a procedure for reducing the likelihood that the information contained in the Certificate's subject:organizationalUnitName attribute would be misleading; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CP and/or its 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, the issuing CA (i) implemented a procedure to verify the identity of the Applicant in accordance with Sections 3.2.2 and 3.2.3; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CP and/or its CPS;

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

(7) **Status**: That the issuing CA shall maintain a 24x7 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 the issuing CA 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

RAs shall represent and warrant that:

(1) Certificate management is performed in compliance with this CP and the issuing CA's 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 the issuing CA's 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 the issuing CA and the Certificate Beneficiaries, the Applicant shall warrant that, prior to the issuance of a certificate, the issuing CA will obtain, either:

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

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

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

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

(2) Provide accurate and complete information to the issuing CA and RA,

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

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

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

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

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

(6) Use the certificate only for legal and authorized purposes, consistent with this CP, the issuing CA's 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

Relying Parties must follow the procedures and make the representations required by the relevant CPS and in the applicable Relying Party Agreement prior to relying on or using a certificate.

9.6.5. Representations and Warranties of Other Participants

No stipulation.

9.7. Disclaimers of Warranties

Except as otherwise in the CPS expressly provided or as limited by law, HiPKI disclaims all warranties and obligations related to this CP. If any problem results from the citation of this CP by other CA outside HiPKI, that CA shall shoulder the responsibility.

9.8. Limitations of Liability

CAs shall specify the limitations of liability in their CPS.

9.9. Indemnities

As stated in Article 14 of the Electronic Signatures Act, "A certification service provider shall be liable for any damage caused by its operation or other certification-related process to the parties, or to a bona fide person who relies on the certificate, unless the certification service provider proves that it has not acted negligently. Where a certification service provider clearly specifies the limitation for the use of the certificate, it shall not be liable for any damage arising from a contrary use."

CAs shall specify the compensation responsibility to subscribers and relying parties in their CPS. For example,

(1) CAs shall include any indemnification requirements for a subscriber's fraudulent misrepresentations on the certificate application under which the issuing CA issued the subscriber an inaccurate certificate in their Subscriber Agreements, and

(2) CAs shall include any indemnification requirements for relying parties' use of a certificate without properly checking revocation information or use of a certificate for purposes beyond what the CA permits in a Relying Party Agreement.

9.10. Term and termination

9.10.1. Term

This CP is effective when published to HiPKI RCA's repository.

9.10.2. Termination

The new version of this CP is announced after being approved by the PMA, and the current version is terminated.

9.10.3. Effect of Termination and Survival

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

9.11. Individual Notices and Communications with Participants

CHT accepts digitally signed or paper notices related to this CP that are addressed to the locations specified in Section 1.5.2 of this CP. Notices are deemed effective after the sender receives a valid and digitally signed acknowledgment of receipt from CHT. If an acknowledgement of receipt is not received within five days, the sender must resend the notice in paper form using either an express delivery or a registered mail.

CAs shall specify the way of individual notices and communications with the participants prior to implementation of any planned change to the infrastructure in their CPS.

9.12. Amendments

9.12.1. Procedure for Amendment

The PMA shall review this CP at least annually. CAs shall review their CPS at least once a year. The new versions of the CP/CPS will publish according to the regulations stated in Section 2.3.

9.12.2. Notification Mechanism and Period

CAs shall post appropriate notice on its websites of any major or significant changes that could have a significant impact to subscribers. CAs shall specify the notification mechanism and period for change items in their CPS.

9.12.3. Circumstances under which OID Must Be Changed

CP OIDs will be changed if a change in the 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 the issuing CA's CPS accordingly.

9.13. Dispute Resolution Provisions

The parties to the dispute arising out of the use of certificates issued under this CP shall strive in their negotiations to reach a consensus. If negotiation fails, CHT may establish dispute settlement procedures to

secure an interpretation. CAs shall specify the procedures utilized to resolve disputes in their CPS.

9.14. Governing Law

The interpretation and enforcement of this CP or agreements as well as the validity and effect with regard to certificates issued under this CP shall be governed by the laws of R.O.C.

9.15. Compliance with Applicable Law

All CAs operating under this CP are required to comply with applicable laws and regulations of R.O.C.

9.16. Miscellaneous Provisions

9.16.1. Entire Agreement

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

CAs shall obligate RAs by contracts or agreements to comply with this CP and applicable industry standards and guidelines. CAs shall obligate subscribers or relying parties using its products and services to enter into an agreement that delineates the terms associated with the product or service.

9.16.2. Assignment

The participants as stated in Section 1.3 may not assign or delegate their rights or obligations under this CP to other parties in any form without a prior written notice to CHT.

9.16.3. Severability

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

The requirements regarding CAs in this CP comply with the Baseline

Requirements; however, if there is any inconsistency between the related domestic laws followed by this CP and the Baseline Requirements, this CP 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 CP will delete and amend the adjusted contents. The aforesaid actions shall be completed within 90 working days.

9.16.4. Enforcement (Attorneys' Fees and Waiver of Rights)

In the event that HiPKI suffers damages attributable to an intentional or unintentional violation of this CP by a subscriber or relying party, HiPKI may seek compensation for damages and indemnification and attorneys' fees from the responsible party related to the dispute or litigation. HiPKI's failure to assert rights with regard to the violation of this CP to the party does not waive HiPKI's right to pursue the violation of this CP later or in the future.

9.16.5. Force Majeure

CAs are not liable for any delay or failure to perform an obligation under this CP to the extent that the delay or failure is caused by a force majeure or other circumstances not attributable to CAs, including natural disasters, wars, or terrorism which may cause the interruption of telecommunications network. CAs may specify other exemption provisions in their CPS but may not exclude mistakes arising from self-negligence.

9.17. Other Provisions

No stipulation.