RAFFTECH

Certification Authority

Certificate Policy (CP)

Version 1.3

Effective Date: 18 February 2023

Raffcomm Technologies Sdn Bhd
Company No. 201001015771 (1000449-W)
Lot 32.02, Level 32, Sunway Putra Tower
No. 100, Jalan Putra, 50350 Kuala Lumpur
Wilayah Persekutuan Kuala Lumpur, Malaysia
Tel: +603 4040 0091
www.rafftech.my

REVISION HISTORY

Date	Version	Changes	Author
02nd January 2018	1.0	Certificate Policy	Internal Audit Department
28th January 2019	1.1	To amend the document format and make changes on the RAFFTECH's logo	Internal Audit Department
29th November 2021	1.2	To update the details of the email address, website address and the location of the Repository to reflect the domain shifting from cyphersign.my to rafftech.my To rectify clerical errors and make refinements	Business Compliance Department
18th February 2023	1.3	To refine the document format. To add OID details. To update sections 1.2, 7.1.3, 7.2.1 and 9.4.1	Business Compliance Department

TABLE OF CONTENTS

1. INTRODUCTION

RAFFCOMM TECHNOLOGIES SDN. BHD. ("RAFFTECH") operates as a Digital Certificate services provider pursuant to the Digital Signature Act 1997 ("DSA") and Digital Signature Regulations 1998 ("DSR") .

This documentation named Certificate Policy ("CP") has been prepared by RAFFTECH, in order to identify the policies and rules to be followed in the course of activities of RAFFTECH certificate services, follows the framework and structure outlined in the Internet Engineering Task Force ("IETF") RFC3647 .

This document describes the administrative, technical and legal requirements related with qualified Digital Certificate applications, issuance, management, renewal and revocation procedures and specifies the implementation responsibilities of RAFFTECH as certification authority ("CA"), (or, certificate service provider), Subscribers and relying parties.

1.1 Overview

The purpose of this CP is to describe the practices and operational specifications of certificates issued by RAFFTECH, which includes the following:

a. The CA, registration authorities ("RA"), Subscribers and relying parties;
b. The primary obligations of the parties governed by this CP;
c. The requirements for issuance of certificates and management of certificates lifecycle (including the issued Subordinate CA) for verification of certificates and for ensuring confidentiality of communications; and
d. The categories of electronic messages, communications and data for which this CP is applicable.

This CP is intended to be a framework for certificate policies. Part of the requirements of this CP will be reflected in the CPS, which is a public information document.
Readers should refer to the Certification Practice Statement ("CPS") for the detailed practices performed by RAFFTECH.

1.2 Document Name and Identification

This CP is named as the "RAFFTECH Certificate Policy". The version number and date of the document is provided herein on the cover page.

Object Identifier ("OID") for this CP is as follows:

OID	Description
1.3.6.1.4.1.51215.1	Certificate Policy (CP)

1.3 PKI Participants

This subcomponent describes the identity or types of entities that fill the roles of participants within a PKI.

1.3.1 Certification Authorities (Issuing CA)

The certification authorities are entities that issue certificates. A CA is the issuing CA with respect to the certificates it issues and is the subject CA with respect to the CA certificate issued to it. CAs may be organized in a hierarchy in which an organization's CA issues certificates to CAs operated by subordinate organizations, such as a branch, division, or department within a larger organization.

1.3.2 Registration Authorities

The registration authorities are entities that establish enrolment procedures for end-user certificate Applicants, perform identification and authentication of certificate Applicants, initiate or pass along revocation requests for certificates, and approve applications for renewal or re-keying certificates on behalf of a CA. Subordinate organizations within a larger organization can act as RA for the CA serving the entire organization, but RAs may also be external to the CA.

1.3.3 Subscribers (End Entities)

Subscribers, refer to both the subject of the certificate and the entity that contracted with RAFFTECH for the certificate's issuance. Prior to the verification of identity and issuance of a certificate the subscriber is classified as an Applicant.

Verification of identity or name is performed in accordance with the relevant party's legislation and standards. Consequences due to the use of a certificate and liability of the Subscribers are qualified by relevant legislation and the Subscriber's commitment.

1.3.4 Relying Parties

Relying parties are entities that act in reliance on a certificate and/or Digital Signature issued by RAFFTECH. Relying parties must check the appropriate CRL or OCSP response prior to relying on information featured in a certificate.

1.3.5 Other Participants

All Digital Certificates services provided by RAFFTECH such as Digital Certificate issuance, renewal, revocation, Repository publication, and other similar services provided by CA.

In order to provide reliable and proper Digital Certificate services, the issuing CA engages with a cooperating and service providing participant.

1.4 Certificate Usage

A certificate (or Digital Certificate) is formatted data that cryptographically binds an identified Subscriber with a Public Key. A Digital Certificate allows an entity taking part in an electronic transaction to prove its identity to other participants in such a transaction. Digital Certificates are used in commercial environments as a digital equivalent of an identification card.

1.4.1 Appropriate Certificate Uses

Certificates issued under this CP may be used for the purposes designated in the key usage and extended key usage fields found in the certificate.

However, the sensitivity of the information processed or protected by a certificate varies greatly, and each relying party must evaluate the application environment and associated risks before deciding on whether to use a certificate issued under this CP.

This CP covers different types of end entity certificates with varying levels of assurance. The following table provides a brief description of the appropriate uses of each Certification Type. The descriptions are for guidance only and are not binding.

Certification Type	Certification Usage
CLASS 1 Individual Certificate	Provides the lowest degree of assurance concerning identity of the individual and is generally used only to provide data integrity to the information being signed. These certificates should only be used where the risk of malicious activity is low and if an authenticated transaction is not required.
CLASS 2 Individual Certificate	Used in environments where there are risks and consequences of data compromise, but such risks are not of major significance. Users are assumed not likely to be malicious.
CLASS 2 Organization Certificate	Used in environments where there are risks and consequences of data compromise, but such risks are not of major significance. Users are assumed not likely to be malicious.
CLASS 2 Device Certificate	This level is relevant to environments where risks and consequences of data compromise are moderate.
Time Stamping Certificate	Used to identify the existence of data at a set period of time.

1.4.2 Prohibited Certificate Uses

Certificates use is restricted by using certificate extension on key usage and extended key usage. Certificates do not guarantee that the subject is trustworthy, honest, reputable in its business dealings, compliant with any laws, or safe to do business with. A certificate only establishes that the information in the certificate was verified as reasonably correct when the certificate is issued.

Certificates issued pursuant to this CP may not be used:

a) for any application requiring fail-safe performance such as: (i) the operation of nuclear power facilities; (ii) air traffic control systems; (iii) aircraft navigation systems; (iv) weapons control systems; (v) any other system whose failure could lead to injury, death or environmental damage; or

b) where prohibited by law.

1.5 Policy Administration

1.5.1 Organization Administering the Document

All rights and responsibilities associated with this CP and document referenced are maintained by RAFFTECH.

1.5.2 Contact Person

Company	Raffcomm Technologies Sdn. Bhd. – 201001015771 (1000449-W)
Address	32.03, Level 32, Sunway Putra Tower, 100, Jalan Putra, 50350 Kuala Lumpur, Malaysia
Telephone	Corporate Office: 03-4040 0091 Operation Office: 03-2787 2010
Fax	03-4040 0095
E-mail	hello@raffcomm.my
Website	https://www.rafftech.my

1.5.3 Person Determining CP Suitability for the Policy

Changes to this CP shall take into account all modifications made to the Malaysian legislation, namely, the DSA and the DSR.

1.5.4 CP approval procedures

RAFFTECH's Board of Management approved this CP document. Approved CP documents shall be used to regulate the policies and the rules related to CA operations and certificate services.

1.6 Definitions and Acronyms

This subcomponent contains a list of definitions for defined terms used in this CP, as well as a list of acronyms used in this CP and their meanings.

1.6.1 Definitions

Term	Description
Applicant	An individual or legal entity that applies for a certificate. Once the certificate is issued, that individual or legal entity is referred as a Subscriber.
Certificate Policy (CP)	A set of rules that indicates the applicability of named certificate and PKI requirement with common security requirements.
Certificate Revocation List (CRL)	A periodically issued list, digitally signed by Certification Authority of identified certificates that has been revoked prior to its expiry dates.
Certification Authority (CA)	An organization that is trusted and authorized to provide Digital Certificates. CA verifies identity and legitimacy of company or individual that requested a certificate and if the verification is successful, CA issues a signed certificate.
Certification Practice Statement (CPS)	A document from a Certification Authority which describes its practice for issuing and managing certificates through its lifecycle.

Term	Description
Digital Certificate	Digital record that associates the Public Key and identity information of the Subscriber by using Private Key of the Certification Authority.
Digital Signature	Digital signatures are based on Public Key cryptography, also known as asymmetric cryptography. Using a Public Key algorithm such as RSA, one can generate two keys that are mathematically linked: one private and one public.
Hardware Security Module (HSM)	A secure cryptographic device used to securely manage the keys, accelerate cryptographic processes and a strong authentication mechanism.
Key Pair	The Private Key and its associated Public Key.
Online Certificate Status Protocol (OCSP)	An online certificate checking protocol for providing the relying parties with real-time certificate status information.
Private Key	The key of the Key Pair that is kept secret by the Subscriber, and that is used to generate Digital Signature or to decrypt electronic data that were encrypted with corresponding Public Key.
Public Key	The key of the Key Pair that is publicly disclosed by the Subscriber that is used to verify Digital Signature created using corresponding Private Key or to encrypt data so that they can be decrypted using corresponding Private Key.
Repository (REPO)	An online database contained publicly disclosed PKI governance documents and certificates status information either in form or CRL or OCSP response.
Root CA (RCA)	The top-level CA whose root certificate is distributed and issue Subordinate CA certificate.
Subordinate CA (ICA)	A certification authority whose certificates are signed and issued by RAFFTECH Root CA, in representing that the CA has followed the procedure stipulated in this CP and in verifying that all the information contained in the certificates are correct and complete as of the certificates' issuance date.

Term	Description
Subscriber	A natural person or legal entity to whom the certificate is issued by Certification Authority. A subscriber is capable of using and is authorized to use the Private Key that corresponds to the Public Key listed in the certificate.
x.509	A digital certificate based on the widely accepted International Telecommunications Union ("ITU") x.509 standard, which defines the format of Public Key Infrastructure (PKI) certificates. Used to manage identity and security in internet communications and computer networking.

1.6.2 Acronyms

Acronyms	Description
AD	Active Directory
CA	Certification Authority
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
DRC	Disaster Recovery Center
DSA	Digital Signature Act 1997
DSR	Digital Signature Regulations 1998
HSM	Hardware Security Module
IETF	Internet Engineering Task Force
LDAP	Lite Directory Access Protocol
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OU	Organizational Unit
PKCS	Public Key Cryptographic Standards
PKI	Public Key Infrastructure
RA	Registration Authority

Acronyms	Description
RFC	Request for Comment (document published by IETF for guidelines)
TSA	Time Stamping Authority

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

RAFFTECH will operate the Repository and publish the relevant documents and records. RAFFTECH's legal Repository for most services is located at https://www.rafftech.my/wp/knowledge .

RAFFTECH's publicly trusted root certificates and its CRLs and OCSP responses are available through online resources 24 hours a day, 7 days a week with systems described in section 5 to minimize downtime.

2.2 Publication of Certification Information

Information in RAFFTECH Repository regarding the conduct of the Digital Certificate services are kept public except for the institutional procedures and instructions specific to the operation of the CA and confidential commercial information. This includes this CP, the supporting CPS, the certificates issued under this CP and the CRL of certificates issued under this CP or some subset of this information are published for internal/external use within the CA and for the use of its customers.

2.3 Time or Frequency of Publication

RAFFTECH will publish certificates and on-line certificate status inquiry log constantly upon acceptance. The CRL will be published once a day. If the Subscriber's certificate is revoked, online certificate status will be updated in real time but a new CRL will be created during the time schedule.

RAFFTECH operates and maintains its CRL and OCSP capability with resources sufficient to provide response time of less than 20 seconds under normal operating conditions.

2.4 Access Controls on Repositories

RAFFTECH makes the information described in the Repository available to the Subscribers and the relying parties at all times, with reasonable provisions for scheduled maintenance. RAFFTECH shall take all security measures necessary to ensure the authenticity of the published information.

3. IDENTIFICATION AND AUTHENTICATION

RAFFTECH authenticates based on official sources together with all information in accordance with legal and technical requirements the identification of the first time certificate enrolment or renewal request.

3.1 Naming

3.1.1 Types of Names

RAFFTECH shall issue certificates with a non-null subject Distinguished Name (DN) that complies with ITU x.500 standards. Subject Alternate Name forms may be included in certificates if they are marked non-critical. When DNs are used, Common Names must respect name space uniqueness and must not be misleading.

3.1.2 Need for Names to be Meaningful

Digital Certificate under this CP should contain names with commonly understood semantics permitting the determination of the identity of the organization or individual that is subject of the certificate. For such certificate pseudonyms of the Subscribers (names other than the Subscriber's true organizational or personal name) are not permitted.

3.1.3 Anonymity or Pseudonymity of Subscribers

Where not otherwise prohibited by applicable policy (e.g. for certificate type, assurance level, or certificate profile), end-entity anonymous or pseudonymous certificates are not prohibited by this CP, as long as the name space uniqueness is preserved.

3.1.4 Rules for Interpreting Various Name Forms

Distinguished Names in certificates are interpreted using x.500 standards and ASN.1 syntax. See RFC 2253 and RFC 2616 for further information on how x.500 Distinguished Names in certificates are interpreted as Uniform Resource Identifiers (URI) and HTTP references.

3.1.5 Uniqueness of Names

Certificates issued by RAFFTECH shall have unique identification of Subscribers with information contained in subject Distinguished Names.

3.1.6 Recognition, Authentication, and Role of Trademarks

Subscribers are prohibited from using names in their certificates that infringe upon the intellectual property rights of others. However, RAFFTECH does not verify whether the Subscribers have the intellectual property rights in the name appearing in a certificate application or arbitrate, or otherwise resolve any dispute concerning the ownership of any domain trade name, trademarks or service marks. RAFFTECH will be entitled, without any liability to any Subscriber to reject or revoke any Subscriber's certificate because of such dispute.

3.2 Initial Identity Validation

RAFFTECH may use any legal means of communication or investigation to ascertain the identity of an organization or individual Applicant. RAFFTECH may refuse to issue a certificate in its sole discretion.

3.2.1 Method to Prove Possession of Private Key

RAFFTECH as a CA verifies the Subscriber possession of key through the use of a digitally signed certificate request pursuant to PKCS #10, another

cryptographically equivalent demonstration, or another approved method which is compliant with DSR.

3.2.2 Authentication of Organization Identity

For any certificate that includes an organization identity, the Applicants shall provide the organization's name and registered or business address. RAFFTECH and RA shall verify information about the organization and its legal existence using reliable third party and government databases or through direct means of communication with the entity or jurisdiction governing the organization's legal creation, existence or recognition.

RAFFTECH and RA shall identify high risk certificate requests and shall conduct additional verification activity and take additional precautions necessary to ensure that high risk requests are properly verified.

3.2.3 Authentication of Individual Identity

RAFFTECH and RA shall authenticate an individual's identity in accordance with the procedures described as below:

Certificate	Description
CLASS one (1) Individual – Personal (email certificates)	Applicant demonstrates control over the email address to which certificate is related. RAFFTECH or RA`s are not required to verify any other information provided.
CLASS one (1) Customized – Individual and Organization (email certificates)	This level requires the Applicant to demonstrate control over the email address to which certificate is related. RAFTTECH also acquires other documents such as copy of MyKad, copy of passport or any other related documents to prove identity of the Applicant.

CLASS two (2) Individual and Organization	Applicant's required to submit a legal copy of valid government issued identity document or photo ID (valid driving license, military ID or equivalent). Identity verification shall be performed using one of the following methods: 1) In person verification by presenting the valid government issued identity document that contains a picture and either address of record and nationality. 2) Remote verifying information by record check with the specified issuing CA or through a similar database to establish existence of such records with matching name and reference number (identification number) and to corroborate date of birth.

RAFFTECH may also be required to authenticate the Applicant's authority to represent the organization wishing to be named as a subject Distinguished Names in the certificate according to section 3.2.2.

3.2.4 Non-Verified Subscriber Information

RAFFTECH is not required to verify that the Common Name in a CLASS one (1) certificate is the legal name of the Subscriber. Any other non-verified information included in a certificate shall be designated as such in the certificate. No unverified information as a subject Distinguished Names shall be included in any Level two (2), code signing and device certificate.

3.2.5 Validation of Authority

RAFFTECH or the RA shall verify the authorization of a certificate request as follows:

Certificate	Validation
CLASS one (1) Individual – Personal (email certificates)	An individual with control over the email address listed in the certificate or with a person who has technical or administrative control over the domain or the email address to be listed in the certificate.
CLASS one (1) Customized – Individual and Organization (email certificates)	RAFFTECH or the RA conducts cross checking with an individual or an organization which controls over the email address listed in the certificate or possesses technical or administrative control over the domain or the email address to be listed in the certificate.
CLASS two (2) Individual and Organization	Individuals and organizations affiliated with the organization who confirm the Applicant's authority to obtain a certificate indicating the affiliation and who agree to request revocation of the certificate when that affiliation ends.
SSL Certificate and Device Certificate	An authorized contact listed with the Domain Name Registrar, a person with control over the domain name, or through communication with the Applicant using a reliable method of communication, as defined in the baseline requirements.

3.2.6 Criteria of Interoperation

No stipulation.

3.3 Identification and Authentication for Re-Key Requests

RAFFTECH or the RA may support re-key requests from the Subscribers prior to expiry of the Subscriber's existing certificate. RAFFTECH may also support reissue at any time during the lifetime of the certificate.

3.3.1 Identification and Authentication for Routine Re-Key

RAFFTECH may allow the Subscribers to authenticate themselves over SSL session with username and password. RAFFTECH requires the Subscribers to establish the identity through use of the current Subscriber's Private Key. Each Subscriber shall re-establish its identity using the initial registration process of section 3.2.

Certificate	Re-Key Authentication	Re-Verification Period
CLASS one (1) Individual Certificates	Username and Password	At least every one (1) year
CLASS one (1) Customized – Individual and Organization Certificates	Username and Password	At least every one (1) year
CLASS two (2) Individual and Organization Certificates	Username and Password or client authentication with current unexpired and unrevoked certificate	At least every five (5) years
SSL Certificates and Device Certificates	Username and Password	At least every six (6) years

3.3.2 Identification and Authentication for Re-Key after Revocation

RAFFTECH requires the Subscribers of certificates that have been revoked to undergo the initial registration process as described under section 3.2 to obtain a new certificate.

3.4 Identification and Authentication for Revocation Request

RAFFTECH or the RA should perform authentication as below after received revocation requests from the Subscribers. The Subscribers, by using credentials given to them at the application phase, authenticate themselves on the web or other RAFFTECH's CA software to revoke their certificates.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

RAFFTECH generates certificates and manages the certificate life-cycle in accordance with the policies and rules set forth in this CP.

4.1 Certificate Application

4.1.1 Who can Submit a Certificate Application

Any real person free of any legal obstacles may apply for the Digital Certificate. RAFFTECH and the RA has the right to retain all necessary information submitted during certificate application for a period of seven (7) years.

RAFFTECH maintains its own blacklists for individuals from whom or entities which do not accept Digital Certificate applications. Blacklist may be based on past history or other sources. In addition, other external sources such as government lists or internationally recognized denied person lists which are applicable to Malaysia's jurisdiction may be used for unwanted Applicants.

4.1.2 Enrollment Process and Responsibilities

RAFFTECH maintains systems and processes that sufficiently authenticate the Applicant's identity for all certificates under this CP. Applicants must submit sufficient information to allow RAFFTECH and RA successfully perform required verifications. RAFFTECH and RA shall protect and securely store information presented by Applicants.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

RAFFTECH shall maintain systems and processes to authenticate the Applicant's identity in compliance with this CP. Initial validation shall be performed by the validation team or by the RA appointed by RAFFTECH. RAFFTECH and the RA shall ensure all communication and information regarding certificate issuance are made secure and auditable.

4.2.2 Approval or Rejection of Certificate Applications

RAFFTECH and the RA shall reject applications where validation of all items cannot be verified.

Based on the following conditions, a certificate application is approved:

a) According to the principle of section 3.2 and relevant RAFFTECH procedures, required documentation are completed;

b) Contact is made by the RAFFTECH's validation team or by RA appointed by RAFFTECH; and

c) Payment is made.

Based on the following conditions, a certificate application is rejected:

a) According to the principle of section 3.2 and relevant RAFFTECH procedures, required documentation are not completed;

b) Contact is not made by the RAFFTECH's validation team or the RA appointed by RAFTTECH or application is not verified; and

c) Payment is not made.

RAFFTECH may also reject certificate application on any reasonable basis, including if the certificate could damage the RAFFTECH's business and reputation.

4.2.3 Time to Process Certificate Applications

RAFFTECH and the RA shall ensure that all reasonable methods are used in order to process and evaluate certificate applications. Certificate

applications submitted to RAFFTECH or the RA with accurate and complete information are processed within at most 3 working days.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

Accepted certificate applications as described in section 4.2.2 are processed by RAFFTECH. The RA that performs validation shall ensure that all information is verified and authenticated in a secure manner when submitting to RAFFTECH.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

After certificate issuance is completed, RAFFTECH shall notify the Subscribers through appropriate and convenient ways based on the information submitted during application request. Generally, RAFFTECH delivers certificates via email to the email address designated by the Subscriber during the application process.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The Subscribers are under obligation to review and verify the accuracy of the data in the certificate before using the certificate and notify RAFFTECH and request revocation of the certificate if the data is inaccurate with the certificate application.

The Subscribers are solely responsible for installing the issued certificate on the Subscribers' computer or Hardware Security Module (HSM). The certificates are considered accepted 30 days after the certificates issuance,

or earlier upon use of the certificates when evidence exists that the Subscribers have used the certificates.

4.4.2 Publication of the Certificate by the CA

RAFTECH may publish a certificate issued in the web or suitable directory servers.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

a) The notification of certificate issuance shall be through emails.

b) Upon the user's identity including its attributes are verified for registration by the RA and such registration is recognized as valid by the CA, the CA shall generate a certificate and such certificate shall first be validated by the CA before issuance.

For the issuance purposes, the validated certificate shall be emailed to the subscriber whereby the information that the certificate is approved and ready to be installed and used by the subscriber shall be contained therein.

The details of the password for the purposes to open and the procedures to install the certificate (as attached in the earlier email) will be sent through subsequent email.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

The Subscribers are required to use a Private Key and certificate only for appropriate applications as set forth in this CP and in consistency with applicable certificate content (e.g. key usage field).

The Subscribers must protect their Private Keys to avoid disclosure or misuse by third parties. Use of a Private Key and certificate are subject to the terms of the Subscriber Agreement and using the certificate within the

scope and authority defined in the legal regulations, this CP and the CPS documents.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties are obligated to check the validity of certificates only for appropriate applications as set forth in this CP and in consistency with applicable certificate content (e.g. key usage field), successfully perform Public Key operations as a condition of relying on a certificate, assume responsibility to check the status of a certificate using appropriate mechanism available to verify the certificate.

Relying parties are under obligation to use a trustworthy system defined under the legislation and standard during these operations. RAFFTECH will not be responsible for the relying parties not fulfilling the conditions stated above before relying on the certificates.

4.6 Certificate Renewal

4.6.1 Circumstance for Certificate Renewal

A certificate shall be renewed upon request from the Subscriber where period of time remains before the expiry and no changes occur in the information included in the certificate.

An expired certificate cannot be renewed. The renewal operation is done within at most 30 days, otherwise the renewal request is rejected.

4.6.2 Who May Request Renewal

The Subscriber may request for renewal.

4.6.3 Processing Certificate Renewal Requests

A new Key Pair should be generated during the renewal process. The Subscriber is required to sign the renewal request, as well as to demonstrate possession of the Private Key based on the existing certificate. RAFFTECH may require reconfirmation of the information in a certificate during renewal.

4.6.4 Notification of New Certificate Issuance to Subscriber

Refer to section 4.3.2

4.6.5 Conduct constituting acceptance of a renewal certificate

Refer to section 4.4.1

4.6.6 Publication of the renewal certificate by the CA

Refer to section 4.4.2

4.6.7 Notification of certificate issuance by the CA to other entities

a) The notification of certificate issuance shall be through emails.

b) Upon the user's identity including its attributes are verified for registration by the RA and such registration is recognized as valid by the CA, the CA shall generate a certificate and such certificate shall first be validated by the CA before issuance.

For the issuance purposes, the validated certificate shall be emailed to the user whereby the information that the certificate is approved and ready to be installed and used by the user shall be contained therein.

The details of the password for the purposes to open and the procedures to install the certificate (as attached in the earlier email) will be sent through the subsequent email.

4.7 Certificate Re-Key

4.7.1 Circumstance for Certificate Re-Key

Within 3 months of the certificate validity period, a new certificate is issued with re-key without any documentation of verification if the certificate has been erased from medium storage such as smart card or crypto token or lost or device malfunction.

The Subscribers may require RAFFTECH or the RA to check the information. The Subscriber should identify themselves as described in section 3.3.1.

4.7.2 Who May Request Certification of a New Public Key

The Subscriber of the issued certificate may request for re-key.

4.7.3 Processing Certificate Re-Keying Requests

In case of any indication or doubt about the information submitted during enrolment process, the related information may be taken again.

4.7.4 Notification of New Certificate Issuance to Subscriber

Refer to section 4.3.2

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

Refer to section 4.4.1

4.7.6 Publication of the Re-Keyed Certificate by the CA

Refer to section 4.4.2

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

a) The notification of certificate issuance shall be through emails.

b) Upon the user's identity including its attributes are verified for registration by the RA and such registration is recognized as valid by

the CA, the CA shall generate a certificate and such certificate shall first be validated by the CA before issuance.

For the issuance purposes, the validated certificate shall be emailed to the user whereby the information that the certificate is approved and ready to be installed and used by the user shall be contained therein.

The details of the password for the purposes to open and the procedures to install the certificate (as attached in the earlier email) will be sent through the subsequent email.

4.8 Certificate Modification

4.8.1 Circumstance for Certificate Modification

Certificate modification occurs where there are any changes in the data included in the certificate issued by RAFFTECH. Such a certificate shall be revoked and certificate application shall be filed for a new certificate with new information.

4.8.2 Who May Request Certificate Modification

Refer to section 4.6.2 and section 4.7.2

4.8.3 Processing Certificate Modification Requests

Refer to section 4.1.1

4.8.4 Notification of New Certificate Issuance to Subscriber

Refer to section 4.3.2

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Refer to section 4.4.1

4.8.6 Publication of the Modified Certificate by the CA

Refer to section 4.4.2

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

a) The notification of certificate issuance shall be through emails.

b) Upon the user's identity including its attributes are verified for registration by the RA and such registration is recognized as valid by the CA, the CA shall generate a certificate and such certificate shall first be validated by the CA before issuance.

For issuance purposes, the validated certificate shall be emailed to the user with the information that the certificate is approved and ready to be installed and used by the user shall be contained therein.

The details of the password for the purposes to open and the procedures to install the certificate (as attached in the earlier email) will be sent through the subsequent email.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

The certificate of the Subscriber is revoked if:

a) The Subscriber has reason to believe or suspects that there has been compromise of Subscriber's Private Key;

b) RAFFTECH or the RA has reason to believe that the Subscriber has materially breached an obligation, representation, or warranty under the applicable Subscriber Agreement;

c) Certificate application submitted to RAFFTECH or the RA is false;

d) If an evidence is obtained that certificate was misused; or

e) The Private Key has been lost, stolen, disclosed or risk of access or use by a third party arises;

f) The disappearance of the right to give certificate under the law;

g) The Private Keys of RAFFTECH for Root CA and Subordinate CA certificates are out of suspicion or compromised; or

h) Revocation is required by the local CA regulator.

4.9.2 Who can Request Revocation

Below are the entity or people who may request for revocation:

a) The Subscribers who may request to revoke their own certificates;

b) Authorized personnel for all certificates under RAFFTECH CP and Root CA and sub root certificates where security concern is necessity; and

c) An authorized representative of the organization is entitled to request the revocation issued to the organization.

4.9.3 Procedure for Revocation Request

The entity or the Subscribers must list out their identities and explain the reason for requesting the revocation. RAFFTECH and the RA authenticate and log each revocation request.

RAFFTECH or the RA shall revoke the certificate if the request is authenticated as originated from the Subscriber or authorized personnel in the organization listed in the certificate.

RAFFTECH may revoke the certificate of its own volition without reasons, even if no other entity has requested revocation.

Where the Root CA and the Subordinate CA certificates of the issuing CA are revoked, the status shall be notified in electronic media to all related parties urgently in the shortest possible time. All certificates that are issued under revoked Root CA or sub-root certificates shall also be revoked and the Subscribers shall be notified via e-mail.

4.9.4 Revocation Request Grace Period

The Subscribers should take necessary action after discovery to revoke their certificates within a commercially reasonable period of time.

4.9.5 Time Within which CA Must Process the Revocation Request

RAFFTECH or the RA shall begin investigating certificate revocation immediately upon receiving the request.

4.9.6 Revocation Checking Requirement for Relying Parties

Relying parties must verify the relevant certificate for its intended purposes and to ensure the certificate is valid. To verify the certificate status, an updated CRL is published or OCSP, the online certificate status inquiry service, should be used.

4.9.7 CRL Issuance Frequency

RAFFTECH shall issue a new CRL at least once a day even if there is no change in the status of the Subscriber's certificates. For RAFFTECH Root CA that is operated in an offline manner, the routine CRLs publish upon the Root CA revocation.

4.9.8 Maximum Latency for CRLs

All CRLs shall be published within one (1) hour after generation. Furthermore, each CRL shall be published no later than the time specified in the next update field of the previous issued CRL for the same scope.

4.9.9 On-Line Revocation or Status Checking Availability

RAFFTECH shall provide online certificate status checking service through OCSP protocol. OCSP services provide real time certificate status inquiry and are more reliable than CRL. By using appropriate software at the relying parties site, it is possible to obtain information about the certificate status at any specific time.

4.9.10 On-Line Revocation Checking Requirements

It is recommended that relying parties when inquiring the status of certificates should prefer OCSP if their technical capabilities allow or opt for CRL as an alternative.

4.9.11 Other Forms of Revocation Advertisements Available

RAFFTECH does not offer other methods other than OCSP and CRL.

4.9.12 Special Requirements Re-Key Compromise

When key compromise, all certificates affected by the incident shall be revoked by RAFFTECH. If RAFFTECH's Root CA or Subordinate CA certificate needs to be revoked, all Subscribers' certificates issued under such certificates shall also be revoked and the same shall be informed to the Subscribers.

RAFFTECH may report suspected compromise of its Root CA or Subordinate CA Private Key to the local CA regulator within four (4) hours of discovery.

4.9.13 Circumstances for Suspension

Not Applicable

4.9.14 Who can Request Suspension

Not Applicable

4.9.15 Procedure for Suspension Request

Not Applicable

4.9.16 Limits on Suspension Period

Not Applicable

4.10 Certificate Status Services

4.10.1 Operational Characteristics

RAFFTECH shall make certificate status information available via CRL and/or OCSP. RAFFTECH shall list revoked certificates on the appropriate CRL where they remain until one additional CRL is published after the end of the certificate's validity period.

4.10.2 Service Availability

RAFFTECH shall provide certificate status services 24x7 without interruption.

4.10.3 Optional Features

OCSP responders may not be available for all certificate types.

4.11 End of Subscription

The subscription shall end upon the expiry or revocation of the Subscriber's certificate.

4.12 Key Escrow and Recovery

RAFFTECH does not offer Key Escrow and Recovery services.

4.12.1 Key Escrow and Recovery Policy and Practices

Not Applicable

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not Applicable

5. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

5.1 Physical Controls

5.1.1 Site Location and Construction

RAFFTECH CA operation shall be performed in secured facilities protected against external threats and high security areas and various security areas have been designated and equipped with logical and physical controls to make CA operations accessible by authorized personnel only.

The site location combined with other physical security protection mechanisms such as biometric access, door locks and intrusion sensors shall protect from unauthorized access to CA equipment and data records. The RA must protect their equipment from unauthorized access in a manner to the level of threat to the RA including implementing physical access controls to reduce equipment and records tampering.

5.1.2 Physical Access

Physical access such as mechanisms to control access from one area of the facility to another or access into high-security zones, such as locating CA operations in a secure computer room monitored by guards, surveillance system or security alarms and requiring movement from zone to zone shall be accomplished using a token, biometric readers, and access control lists.

5.1.3 Power and Air Conditioning

RAFFTECH's CA facilities have primary and backup power supplies to operate the equipment which is critical to run the CA critical operations. Particularly, in areas where computer hardware and CA equipment are concentrated and adequate and uninterrupted air conditioning systems are provided.

5.1.4 Water Exposures

RAFFTECH's CA facilities are equipped with raised flooring and monitoring systems to protect the CA equipment from water exposures.

5.1.5 Fire Prevention and Protection

RAFFTECH's CA facilities are equipped with a fire suppression system.

5.1.6 Media Storage

Backup of all records including the cryptographic key material of RAFFTECH's CA operations are kept in appropriate secure media.

5.1.7 Waste Disposal

All information and documents relating to certificate services stored in electronic or paper based shall be destroyed and disposed of pursuant to relevant procedures if no longer be used or no need to be stored. Cryptographic equipment shall be reset to clear all key material according to the manufacturer's instruction manual before its being disposed of.

5.1.8 Off-Site Backup

RAFFTECH shall keep the backup of electronic records in Disaster Recovery Center and secure safe off-site which include the key material related to its CA operations.

5.2 Procedural Controls

5.2.1 Trusted Roles

RAFFTECH shall ensure that all operators and administrators directly related in CA operations should act as a trusted role. RAFFTECH shall ensure that there is no conflict of interest that might prejudice the security of its CA operations. The functions and duties performed by persons in trusted roles are distributed so that no single person can circumvent security and trustworthiness of its CA operations.

a) Customer Services Officers

Person responsible for certification services such as customer services, document control, processes relating to certificate registration, generation, renewal and revocation.

b) System Administrators

Person in charge of the installation, configuration and maintaining the CA system, viewing and maintenance of CA system archives and audit logs.

c) Security Managers

Person responsible for administering and monitoring the implementation of security policies and practices.

d) Key Managers

Person responsible for managing the CA cryptographic key lifecycle in the CA system.

e) Security Officers

Person responsible for the physical security of the entire RAFFTECH's CA facilities.

5.2.2 Number of Persons Required per Task

Dual access controlled system has been established at RAFFTECH to perform critical tasks in CA operation.

All generation, renewal, revocation, disposal including backup activities related to RAFFTECH Root CA and Subordinate CA certificate can be performed by at least five (5) authorized personnel present during the key ceremony event.

5.2.3 Identification and Authentication for Each Role

RAFFTECH's personnel shall be authenticated and authorized into the security system before being allowed access to the system necessary to perform their trusted roles.

5.2.4 Roles Requiring Separation of Duties

RAFFTECH shall enforce role separation either by the CA equipment or procedure or by both means. The personnel are specifically designated to the roles defined in section 5.2.1. It is not permitted for any one person to serve the following roles.

a) Security Officer or Security Personnel and System Administrator;

b) Security Officer or Security Personnel and Key Manager;

c) System Administrator and Customer Service Officer or Key Manager;

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

RAFFTECH shall have a sufficient number of personnel that have appropriate educational levels (high school, bachelor degree, master degree etc.) with proper security clearance, training and qualifications to perform its CA operation in accurate and reliable manner.

5.3.2 Background Check Procedures

All RAFFTECH personnel shall undergo identity verification, background checks and adjudication prior acting in the role, including verification of employment history, education and criminal background.

RAFFTECH shall not appoint trusted roles to any person who has been convicted for any serious crime or another offense.

5.3.3 Training Requirements

All RAFFTECH personnel undergo training for their responsibilities prior to commencing their works. Employees shall be trained and informed in detail, throughout the training period, on basic certification business processes, customer services, procedures and instructions related to CA

operation, information security policy and procedures and CA software employed.

5.3.4 Retraining Frequency and Requirements

RAFFTECH provides the training to its personnel and shall be repeated periodically and as necessary after the initial training has been conducted.

5.3.5 Job Rotation Frequency and Sequence

RAFFTECH shall ensure that any change in its personnel will not affect the effectiveness of CA operation and security of the system.

5.3.6 Sanctions for Unauthorized Actions

Appropriate disciplinary actions shall be applied to RAFFTECH personnel attempting unauthorized actions.

5.3.7 Independent Contractor Requirements

For operations and services carried out by contractors within certification services, RAFFTECH shall sign a Service Agreement with the contractor. The Service Agreement stipulates the security clauses and service principles required by RAFFTECH.

5.3.8 Documentation Supplied to Personnel

RAFFTECH should make available to its personnel this CP, any corresponding CPS and any related policies and procedures. Other technical and administrative documents (system manual, user manual, etc.) are provided in order to trusted personnel who perform their duties.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

Audit logs shall be kept for all security and services of CA operation by RAFFTECH. Where possible, the security logs shall be automatically generated. If it is not possible, a log book, part form or other physical mechanism shall be applied. All security audit logs, both electronic or non-electronic shall be retained and made available during compliance audit.

RAFFTECH shall ensure all events related to the certificate lifecycle are recorded to ensure the traceability to a person in a trusted role for any action for CA operation.

5.4.2 Frequency of Processing Log

Audit logs should be reviewed periodically for any event of malicious activities and following each critical operation.

5.4.3 Retention Period for Audit Log

Audit logs for RAFFTECH CA operations shall be retained in the system at least as long as the transaction replying on the valid certificate can be questioned.

5.4.4 Protection of Audit Log

Audit logs are protected by physical and electronic security measures, and can be accessed by authorized personnel by configuring its system and established operational procedures. The records of the event shall be protected from alteration and data tempering and separate from its originally generated.

5.4.5 Audit Log Backup Procedures

At least on a monthly basis, RAFFTECH shall make backups of audit logs and audit log summaries and store in a secure location (example fire proof safe) which shall be controlled by authorized trusted personnel only.

5.4.6 Audit Collection System (Internal vs. External)

The audit shall be generated and recorded automatically from the application, network and operating system level. Audit processes must be initiated at system start up and finish only at system shut down. The audit collection system shall ensure the integrity and availability of the data collected. If the automated audit system fails, RAFFTECH may consider suspending its operation until it is remedied. Manually recorded audit data is recorded by authorized personnel in the issuing CA's trusted role.

5.4.7 Notification to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

Audit logs reported in the system will be analyzed and security gaps in the system including fault points in certification processes shall be identified and measure shall be taken.

5.5 Records Archival

5.5.1 Types of Records Archived

RAFFTECH includes reasonably sufficient detail of the records to show validity of the proper operation of the CA system and of generated certificates according to this CP and the corresponding CPS.

5.5.2 Retention Period for Archive

The retention period of the archive related to RAFFTECH CA operation shall be at least seven (7) years.

5.5.3 Protection of Archive

Archives records shall be protected by physical and electronic measures, and can be accessed by RAFFTECH authorized personnel only.

5.5.4 Archive Backup Procedures

Backups of electronic archives are retained pursuant to the related procedures. No backup is made to achieve on paper documents.

5.5.5 Archive Collection System (Internal or External)

Archive information is collected internally by RAFFTECH authorized personnel.

5.5.6 Procedures to Obtain and Verify Archive Information

Only RAFFTECH authorized personnel under trusted roles are allowed to access the archive.

5.6 Key Changeover

RAFFTECH shall perform key changeover procedures to ensure smooth transition from expiring Root CA and Sub Root CA certificate to the new one. Toward the expiring of Root CA Private Key, RAFFTECH no longer uses these expiring Root CA's Private Key to sign certificates but still be used to sign CRLs and OCSP responder certificates.

A new Root CA Key Pair is commissioned and all subsequent certificates, CRLs and OCSP are signed with the new Root CA Private Key. The new corresponding Root CA Public Key certificate shall be provided to the Subscribers and the Relying Parties.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

When an event of security incident or system compromise occurs that would prevent CA operations, RAFFTECH shall carry out a risk assessment

to evaluate the business risk and impact before determining the necessary security requirement and the operation procedure to be taken as a consequence of its disaster recovery procedures and business continuity plans.

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

If damage on computing equipment, software units and operational data causes CA operation to become inoperative, RAFFTECH shall ensure the integrity of its CA system and reinitiate its operation by replacement of hardware, using backup copies of its software, data and key material at the issuing CA's secure facility.

5.7.3 RAFFTECH CA Private Key Compromise Procedures

In the event where security of a Root CA Private Key is compromised or lost, RAFFTECH shall immediately assess the situation, determine the degree and scope of the incident, and evaluate the business risk to take appropriate action.

RAFFTECH personnel shall report the results of the investigation. The report must detail the cause of the compromise or loss and the measures should be taken to prevent a reoccurrence.

If a key is compromised, RAFFTECH shall decide to revoke the Root CA certificate. Following revocation of Root CA certificate, RAFFTECH shall notify at earliest feasible opportunity to all Subscribers that the certificate has been issued. The newly generated Root CA Key Pair shall then be used to generate a new Subscriber certificate.

5.7.4 Business Continuity Capabilities after a Disaster

RAFFTECH establishes and manages Disaster Recovery Center (DRC) apart from its primary RAFFTECH CA site. Data stored at the primary RAFFTECH site are backed up to ensure business continuity after a disaster.

5.8 CA or RA Termination

In the event of CA termination, RAFFTECH shall notify the local CA regulatory body and announce to the public at least three (3) months in advance. RAFFTECH and the RA shall not be issuing and delivery certificates according to this CP and also destroy all Root CA and Subordinate CA Private Keys prior to the termination.

RAFFTECH shall archive all audit logs and other records prior to the termination. RAFFTECH shall ensure the archive records are transferred to the appropriate CA upon approval from the local CA regulatory body.

6. TECHNICAL SECURITY CONTROLS

This component is used to define the security measures taken by RAFFTECH to protect its cryptographic keys and activation data (e.g., PINs, passwords, or manually-held key shares). This component may also be used to impose constraints on Repositories, subject CAs, Subscribers, and other participants to protect their Private Keys, activation data for their Private Keys, and critical security parameters. Secure key management is critical to ensure that all secret and Private Keys and activation data are protected and used only by authorized personnel.

This component also describes other technical security controls used by RAFFTECH to perform securely the functions of key generation, user authentication, certificate registration, certificate revocation, auditing, and archiving. Technical controls include life-cycle security controls (including software development environment security, trusted software development methodology) and operational security controls.

This component can also be used to define other technical security controls on Repositories, subject CAs, RAs, Subscribers, and other participants.

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Root and Subordinate CA Key Pairs shall be generated in a physically secured environment by authorized personnel in the trusted roles under at least dual control. The issuing CA shall create auditable evidence to show the enforcement of role separation and follow its key generation process. Private Keys are protected against unauthorized access by physical and technical security measures.

Root and Subordinate CA Key Pairs are generated within Hardware Security Module (HSM) which at least certified to Federal Information Processing Standards ("FIPS") 140-2 level three (3).

Subscribers key generation shall be performed in secure cryptographic devices that have at least FIPS 140-2 level three (3) using key algorithm and key size specified under section 6.1.5.

6.1.2 Private Key Delivery to Subscriber

The Private Key that is created by RAFFTECH may be delivered when sufficient security is maintained within the key generation and issuance process to the Subscribers. The Key Pair shall be encrypted with PIN code which shall be provided by RAFFTECH to the Subscribers.

The encrypted Key Pairs shall be delivered through a Transport Layer Security ("TLS") session, authenticating the password provided to the Subscribers. RAFFTECH or the RA shall not retain Subscriber's Private Keys after it has been delivered.

6.1.3 Public Key Delivery to Certificate Issuer

The Public Key shall bind the Subscriber's identity when it is delivered to RAFFTECH. RAFFTECH shall only accept once the authenticity and integrity has been verified. The certificate request process shall ensure the Applicant possesses the Private Key associated with Public Key presented for certification.

6.1.4 CA Public Key Delivery to Relying Parties

The Root CA and Subordinate CA certificates will be published at RAFFTECH's web site. The relying parties may be able to download and use it for certificate verification. RAFFTECH may deliver its Root CA and Subordinate CA Public Keys as specified in the certificate validation path or discovery policy file.

6.1.5 Key Sizes

RAFFTECH shall select the following key sizes and hash algorithms for self-signed Root CA, Subordinate CA certificates, Subscriber's certificates as well as CRL and/or OCSP certificate status responders.

Key Algorithm	Key Sizes	Secure Hash Algorithm
RSA	2048 bit RSA	SHA-1
RSA	2048 bit RSA	SHA-256
RSA	4096 bit RSA	SHA-256
ECC	256 bit ECDSA	SHA-256
ECC	384 bit ECDSA	SHA-256
ECC	512 bit ECDSA	SHA-512

6.1.6 Public Key Parameters Generation and Quality Checking

RAFFTECH shall generate Key Pair and shall perform parameter quality checking according to FIPS 186.

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

RAFFTECH shall include key usage extension fields that specify the intended use of the certificate and technically limit the certificate's functionality in x.509 v3 compliant software.

Private Key of Root and Sub Root certificates of RAFFTECH shall be used for signing certificates and CRLs.

Private Key of OCSP certificate, RAFFTECH shall be used for signing OCSP response. The use of a specific key shall be determined by the key usage extension in x.509 certificate.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

Key Pair generation, certificate and CRL signing including OCSP responses at RAFFTECH are performed in secure cryptographic Hardware Security Module ("HSM"), complying to the FIPS 140-2 level three (3) as the minimum level of security protection.

The minimum requirement for a cryptographic module for the Subscribers is FIPS 140 Level one (1) for software based certificate and FIPS 140 Level two (2) for hardware based certificate.

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

RAFFTECH ensures that multiple trusted personnel are required to access and use Root CA and Subordinate CA Private Keys including any backup key.

6.2.3 Private Key Escrow

RAFFTECH does not allow any key escrow except for Private Key for encryption in order to provide key recovery as described in section 4.12.1.

6.2.4 Private Key Backup

RAFFTECH Private Key for Root CA and Subordinate CA certificate are backed up under the same multi authorized person control and store at least one backup offsite.

RAFFTECH may provide backup service for Private Keys that are not required to be stored in cryptographic devices. Access to the Private Key shall be secured in a manner only the owner or Subscriber can control the Private Key.

6.2.5 Private Key Archival

RAFFTECH does not allow archival of Private Keys.

6.2.6 Private Key Transfer into or from a Cryptographic Module

All Private Keys exported from the cryptographic module must be encrypted and never exist in plain text format.

6.2.7 Private Key Storage on Cryptographic Module

RAFFTECH shall store its Root CA and Subordinate CA on cryptographic hardware modules which conform to at least FIPS 140 Level three (3).

6.2.8 Method of Activating Private Key

RAFFTECH shall activate Private Key for the Root CA and the Subordinate CA according to the specification of the manufacturer of the cryptographic module and performed by two authorized personnel under the trusted roles.

Subscribers are solely responsible for protecting their Private Keys and shall protect from unauthorized access. The Subscribers shall authenticate themselves before activating their Private Keys.

6.2.9 Method of Deactivating Private Key

RAFFTECH shall deactivate its Root CA and Subordinate CA Private Keys and store it in secure containers when not in use. RAFFTECH shall prevent unauthorized access to any activated cryptographic modules.

6.2.10 Method of Destroying Private Key

All copies of RAFFTECH Private Keys for the Root CA and the Subordinate CA certificate shall be destroyed when no longer in need. RAFFTECH may destroy the Private Key, deleting it from all known cryptographic modules

and shall be performed by two authorized personnel under the trusted roles. RAFFTECH also zeroizes the cryptographic devices and associated backup according to the specifications of the cryptographic hardware manufacturer.

6.2.11 Cryptographic Module Rating

Please refer to section 6.2.1.

6.3 Other Aspects of Key Pair Management

Other aspects of key management need to be considered for RAFFTECH, Repositories, subject CAs, RAs appointed by RAFFTECH, Subscribers and other participants.

6.3.1 Public Key Archival

RAFFTECH shall archive a copy of each Public Key of the certificates Digital Signatures.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

All certificates, including renewed certificates, have maximum validity period based on the type of certificate below:

Type	Private Key Use	Max Certificate Validity
Root CA	20 Years	25 Years
Subordinate CA	12 Years	15 Years
CRL and OCSP responder signing	6 Years	15 Years
CLASS 1 Individual	3 Years	3 Years
CLASS 2 Individual	3 Years	3 Years
CLASS 2 Organization	3 Years	3 Years
Time Stamping Authority	3 Years	3 Years

Private Keys associated with self-signed Root CA certificates that are distributed as trust anchors are used for a maximum of 20 years. RAFFTECH may retire its Root CA and Subordinate CA Private Keys before the periods listed above to accommodate key changeover processes.

RAFFTECH shall not issue a Subscriber certificate with an expiration date that is past its Public Key's expiration date or exceed the routine re-key identification requirement specified in section 3.3.1.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Activation data (Secret Shares) used to protect the tokens containing RAFFTECH Root CA and Subordinate CA Private Key is generated in accordance with section 6.2.2. The creation and distribution is logged.

The Subscribers are recommended to choose strong passwords to protect their Private Keys.

6.4.2 Activation Data Protection

The activation data (Secret Shares) shall be protected from disclosure through a combination of cryptographic and physical access control mechanisms.

6.4.3 Other Aspects of Activation Data

No stipulation

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

RAFFTECH configured its CA systems and components, including any remote workstations to:

a) Authenticate the identity of users before permitting access to the system or applications;
b) Manage the privileges of users and limit users to their assign roles;
c) Generate and archive audit records for all transactions;
d) Enforce domain isolation for security critical processes; and
e) Support recovery from system failure.

6.5.2 Computer Security Rating

No stipulation

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

RAFFTECH system development consist of only:

a) Commercial off-the-shelf software that was designed and developed under a formal and documented development methodology;
b) Hardware and software developed specifically for the issuing CA by verified personnel, using a structured development approach and a controlled development environment; and
c) Hardware and software purchased and shipped in a process that reduces the likelihood of tempering.

RAFFTECH takes proper care to prevent malicious software from being loaded onto the CA equipment. Any update modifications and upgrades to CA components or equipment are documented and controlled.

6.6.2 Security Management Controls

Appropriate tools are used and security procedures are implemented to ensure the security of the CA system and computer network used in RAFFTECH.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 Network Security Controls

RAFFTECH and the RA component shall implement appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Such measures shall include security guards, firewall and filtering routers. Unused network ports and services are turned off. Any boundary control devices used to protect the network on which PKI equipment are hosted deny all but necessary services to the RAFFTECH CA equipment.

6.8 Time-Stamping

RAFFTECH CA components are regularly synchronized with a time service such as an atomic clock or Network Time Protocol (NTP) service. A dedicated authority such as Time Stamping Authority, may be used to provide this trusted time.

7. CERTIFICATE, CRL AND OCSP PROFILES

7.1 Certificate Profile

7.1.1 Version Number(s)

RAFFTECH issues x.509 version three (3) standard to construct the certificates.

7.1.2 Certificate Extensions

RAFFTECH uses certificate extensions in accordance with the applicable industry standards, including RFC 3280 and RFC 5280 . RAFFTECH follows best practice and where possible prevent unnecessary risks to the relying parties when applied to name constraints.

7.1.3 Algorithm Object Identifiers

RAFFTECH signs certificates using one of the following algorithms and OIDs.

Algorithm Name	OID
SHA256WithRSAEncryption	1.2.840.113549.1.1.11
SHA384WithRSAEncryption	1.2.840.113549.1.1.12
SHA512WithRSAEncryption	1.2.840.113549.1.1.13
ECDSA-With-SHA1	1.2.840.10045.4.1
ECDSA-With-SHA256	1.2.840.10045.4.3.2
ECDSA-With-SHA384	1.2.840.10045.4.3.3
ECDSA-With-SHA512	1.2.840.10045.4.3.4

7.1.4 Name Forms

RAFFTECH follows name forms according to RFC 5280.

RAFFTECH includes a unique serial number in each certificate.

7.1.5 Name Constraints

RAFFTECH may include name constraints in the name constraints field when appropriate.

7.1.6 Certificate Policy Object Identifier

No stipulation.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

RAFFTECH may issue certificates with a policy qualifier and suitable text to aid the relying parties in determining applicability.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2 CRL Profile

7.2.1 Version Number(s)

RAFFTECH issues x.509 version two (2) standard to construct the CRL.

7.2.2 CRL and CRL Entry Extensions

RAFFTECH uses extension according to RFC 5280.

7.3 OCSP Profile

RAFFTECH provides an Online Certificate Status Protocol (OCSP) service in accordance with RFC 6960.

7.3.1 Version Number(s)

The OCSP service provided by RAFFTECH supports version one (1) under RFC 6960 .

7.3.2 OCSP Extensions

No stipulation.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

This CP is designed to meet the requirements of generally accepted and developing industry standards, including WebTrust for Certification Authorities, DSA, DSR or International Organization for Standardization (ISO).

8.1 Frequency or Circumstances of Assessment

At least on an annual basis, RAFFTECH retains an independent auditor listed by the local CA regulation body who assesses CA's compliance with this CP and its CPS. The independent auditor shall submit the results of the issuing CA's compliance audit to the local CA regulation body on annual basis for review and approval.

8.2 Identity/Qualifications of Assessor

The audit shall be performed by a qualified auditor listed under the local CA regulation body. The auditor shall be neutral person/entity that possesses the following qualifications and skills:

a) Independences from the subject of audit;
b) Familiar with Public Key Infrastructure certificate system, and information security tools and techniques;
c) Ability to conduct an audit that addresses criteria and audit scheme specified in section 8.;
d) Conform to applicable standards, rules and best practices under the Malaysia DSA and DSR; and
e) Certified, accredited, licensed or otherwise assessed as meeting qualification requirements of auditors under the audit scheme.

8.3 Assessor's Relationship to Assessed Entity

The auditor shall be completely independent from RAFFTECH and the RA.

8.4 Topics Covered by Assessment

The audit must meet the audit scheme under which assessment is being made. These requirements may vary as audit schemes are updated.

8.5 Actions Taken as a Result of Deficiency

If an audit reports non-compliance with the applicable law, this CP and corresponding CPS, or any contractual obligations related to the RAFFTECH certificate services and CA operation, then:

a) The auditor shall document the discrepancy;
b) The auditor shall promptly notify the issuing CA's management and the local CA regulation body; and
c) The issuing CA shall submit the plan of action to the local CA regulation body on how to rectify the non-compliance issues.

The local CA regulation body may require additional action if necessary to rectify any significant issues created by non-compliance, including requiring suspension of certificate issuance to the Subscribers.

8.6 Communication of Results

The results of each audit shall be reported to the local CA regulation body for review and resolution of any deficiency through subsequent corrective action plan. The results shall also be communicated to any third party entities entitled by law, regulation or agreement to receive a copy of the audit results.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

RAFFTECH shall charge reasonable fees for certificate issuance and renewal. RAFFTECH may charge for reissuance or re-key. Fees and any associated terms and conditions shall be made clear to Applicants.

9.1.2 Certificate Access Fees

RAFFTECH may charge a reasonable fee for access to a database which stores issued certificates.

9.1.3 Revocation or Status Information Access Fees

RAFFTECH may charge additional fees to the Subscribers who have a large relying community and to use OCSP service.

9.1.4 Fees for Other Services

RAFFTECH may charge for other additional services such as time stamping.

9.1.5 Refund Policy

RAFFTECH does not practice a refund policy. However, if the certificate contains information different than that on the application due to RAFFTECH or the RA, a new certificate shall be issued free of charge.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

A statement that the participant maintains a certain amount of insurance coverage for its liabilities to other participants.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

Insurance coverage for end-entities is specified in RAFFTECH's Relying Party Agreement.

A statement that a participant has a program that offers first-party insurance or warranty protection to other participants in connection with their use of the PKI.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

All confidential commercial information and documents related to the RAFFTECH certification services, Private Key of the Root CA and Sub Root certificates, software and hardware information, operational records, audit reports, access to onsite and offsite area and devices, facility layout, system manual, business continuity plans, business plans, and information of business partner should be kept confidential.

9.3.2 Information Not Within the Scope of Confidential Information

Information and documents of RAFFTECH which are not confidential and which should be kept public pursuant to the law and practices shall be excluded from the scope of confidential information. Certificate issued, CRLs, customer guides related to certificate lifecycle, this CP and its CPS document are deemed public.

9.3.3 Responsibility to Protect Confidential Information

RAFFTECH's employees shall be responsible to protect confidential information. No person or third party other than authorized personnel in RAFFTECH is allowed to access any confidential information.

9.4 Privacy of Personal Information

9.4.1 Privacy Policy

RAFFTECH recognises the importance of maintaining the privacy, confidentiality and security of the information received during the course of its business and is committed to protecting the privacy of all personal information entrusted to RAFFTECH in accordance with the applicable personal data protection laws in Malaysia, including but not limited to the Personal Data Protection Act 2010.

9.4.2 Information Treated as Private

RAFFTECH treats all personal information about an individual or entity that is not publicly available in the contents of the certificate, OCSP or CRL as private information. RAFFTECH and the RA shall protect private information in its possession using reasonable degree of care and appropriate safeguards.

9.4.3 Information not Deemed Private

Private information does not include certificates, CRLs, OCSP or its content.

9.4.4 Responsibility to Protect Private Information

RAFFTECH 's employees are responsible for securely storing and protecting private information.

9.4.5 Notice and Consent to use Private Information

The Subscribers must consent to any transfer or publication of any private information.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

RAFFTECH may disclose private information without notice when required to do so by law or regulation.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

RAFFTECH holds the intellectual property rights on the certificate issued, CRLs, customers guideline relating to the certificate services, CP and CPS documents, all internal and external documents related to certificate services, operation data, databases and websites.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

RAFFTECH warrants that the contents of all issued certificates are accurate, validation of identity performed accurately and reliable, the right certificate has been issued to the right Applicant and delivery to the right person, published certificate status information is updated and accurate and shall perform all practice and obligation in this CP and its CPS.

9.6.2 RA Representations and Warranties

RAFFTECH RA represents and warrants that identity validation has been performed accurately and reliably for the applications, records are kept securely, certificate issuing, renewal and revocation requests transmitted to the RAFFTECH CA system are accurate and complete.

9.6.3 Subscriber Representations and Warranties

The Subscribers represent and warrant that all information and documents are accurate and updated when submitted to RAFFTECH during certificate application, renewal and revocation requests and fulfill all obligations stipulated under this CP and its CPS.

The Subscribers shall ensure that each Digital Signature created using the Private Key corresponding to the Public Key listed in the certificate has been

accepted and not expired or not been revoked at the time the Digital Signature is generated.

The Subscribers or someone explicitly authorized by the Subscribers, have been and remain the only person in possession of Subscriber's Private Key and all material and information protecting the Subscriber's Private Key and no unauthorized person has access to such material and information.

9.6.4 Relying Party Representations and Warranties

The relying parties shall follow the procedures and make the representations required by this CP, CPS and in the applicable Relying Party Agreement prior to relying on or using certificates.

9.6.5 Representations and Warranties of other Participants

No stipulation.

9.7 Disclaimers of Warranties

Except as expressly stated otherwise herein or as limited by law, RAFFTECH disclaims all warranties and obligations related to this CP and its CPS.

9.8 Limitations of Liability

RAFFTECH may limit its liability to any extent not otherwise prohibited by this CP, provided that the remain responsible for this CP and CPS.

9.9 Indemnities

RAFFTECH indemnification obligations must be set forth in the CPS, this CP, Subscriber Agreement and Relying Party Agreement including any obligation to third party beneficiaries.

9.10 Term and Termination

9.10.1 Term

This version of the CP is valid until a new version is available.

9.10.2 Termination

This CP and any amendments remain in effect until replaced by a newer version.

9.10.3 Effect of Termination and Survival

RAFFTECH communicates the validity of present CP version termination via the RAFFTECH Repository.

9.11 Individual Notices and Communications with Participants

Available contact information of Subscribers is used for all individual notices from RAFFTECH. Notice from RAFFTECH to relying people shall be published over the web or press media.

9.12 Amendments

9.12.1 Procedure for Amendment

Changes to this CP are indicated by appropriate numbering.

9.12.2 Notification Mechanism and Period

RAFFTECH posts appropriate notice on the website of any major or significant changes to this CP as well as any appropriate period by when the newer CP is available to be accepted.

9.12.3 Circumstances Under Which OID must be changed

No stipulation.

9.13 Dispute Resolution Provisions

Parties are required to notify RAFFTECH and attempt to resolve disputes directly before resorting to any dispute mechanism.

9.14 Governing Law

The law of Malaysia governs the interpretation, construction, and enforcement of this CP and all proceedings related to RAFFTECH certificate services.

Every party, including RAFFTECH partners, Subscribers and relying parties, shall submit to the jurisdiction of the Malaysia court of law.

9.15 Compliance with Applicable Law

RAFFTECH provides Digital Certificate services in accordance with Malaysia Digital Signature Act 1997 and Digital Signature Regulations 1998.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

RAFFTECH contractually obligates each RA involved in certificate issuance to comply with this CP, CPS and applicable industry guidelines. RAFFTECH contractually obligates other parties using products and services issued under this CP, such as Subscribers and relying parties, to the relevant provision herein.

9.16.2 Assignment

Entities operating under this CP may not assign their rights obligations without prior written consent from RAFFTECH.

9.16.3 Severability

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

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

RAFFTECH may seek indemnification and attorney's fees from a party for damages, losses and expenses related to that party's conduct. RAFFTECH's

failure to enforce a provision of this CP does waive its right to enforce the same provision later or right to enforce any other provision of this CP.

9.16.5 Force Majeure

RAFFTECH is not liable for a delay or failure to perform obligation under this CP to the extent that the delay or failure is caused by an occurrence beyond the reasonable control.

9.17 Other Provisions

No stipulation.