RAFFTECH

RAFFTECH CERTIFICATION AUTHORITY

Certification Practice Statement (CPS)

VERSION	**2.3**
EFFECTIVE DATE	**01st Aug 2024**

RAFFCOMM TECHNOLOGIES SDN BHD 201001015771 (1000449-W)
LOT 32.02, LEVEL 32, SUNWAY PUTRA TOWER
NO. 100, JALAN PUTRA, 50350 KUALA LUMPUR
WILAYAH PERSEKUTUAN KUALA LUMPUR, MALAYSIA
TELEPHONE: +603 4040 0091
www.rafftech.my

REVISION HISTORY

DATE	VER	CHANGES	AUTHOR
02nd Jan 2018	1.0	Certification Practice Statement	Internal Audit Department
28th Jan 2019	1.1	To amend the document format and make changes on the RAFFTECH's logo	Internal Audit Department
29th Nov 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 Feb 2023	1.3	Refine the document format; Added OID details in Sections 1.2, 7.1.3, 7.2.1 and 9.4.1.52;	Business Compliance Department

01st May 2024	2.0	Major revamp of document structure to comply with RFC 3647;
		Updated Section 5.4.3, 5.4.5, 5.5.2: Retention Period 10 Years [DSR-80];
		Updated Section 9.1: Fees imposed for RAFFTECH services;
		Updated Section 1.4.1.1.: Level of Assurance;
			Business Compliance Department

25th June 2024	2.1	Addition of Class 3 Digital Signature Certificates Updated Section 1.4, 1.4.1.1, 3.2.3, 3.2.5, Updated Figure 1.4b, 3.2.3c	Business Compliance Department
24th July 2024	2.2	Refined wordings containing subordinate-ca (sub-ca) to intermediate/issuing-ca (ica)	Business Compliance Department
01st Aug 2024	2.3	Refined Section 3.2.3. to include Class 3 requirement Updated Figure 1.4.1.1.A , Figure 1.4.1.1.b, Table 3.2.3c	Business Compliance Department

TABLE OF CONTENT

1. INTRODUCTION

1.1. OVERVIEW

i. This document is the Certification Practice Statement (CPS) for RAFFTECH Public Key Infrastructure (RPKI). This CPS is associated with RAFFTECH Certificate Policy (CP) serves as a comprehensive document outlining the practices and procedures employed by RAFFTECH Certification Authority (RAFFTECH-CA) to ensure the highest level of security and transparency in its issuance, management, and revocation of Certificates. As the reliance on Certificates continues to rise, the need for a standardised practice statement becomes critical to maintain trust among all parties involved, RPKI is operated and owned by Raffcomm Technologies Sdn. Bhd. ("RAFFTECH")

ii. RAFFTECH's CP and CPS incorporates RFC3647 framework and contains detailed information on the specifications, certification procedures and security measures for the issuance of Certificates by RAFFTECH-CA. This CPS is placed into operation with reasonable assurance that it is consistent with the CP.

iii. RAFFTECH CPS is divided into nine parts that covers security controls, procedures and practices concerning Certificate lifecycle services in addition to Certificate issuance, such as Certificate management (including publication and archiving), revocation, and renewal or re-keying practices.

iv. This CPS is intended to apply to and is a legally binding document between the Certification Authority (CA), Registration Authority (RA), Applicants/ Subscribers, Relying Parties, employees, and contractors (if any). Additionally, it shall also serve as notice to all parties within the context of this CPS.

v. This document outlines the contents of CPS provisions, in terms of nine primary components, as follows:

1. Introduction
2. Publication and Repository
3. Identification and Authentication
4. Certificate Life-Cycle Operational Requirements
5. Facilities, Management, and Operational Controls
6. Technical Security Controls
7. Certificate, CRL, and OCSP Profile
8. Compliance Audit
9. Other Business and Legal Matters

vi. RAFFTECH currently offers the following ranges of products and services:

a. **PRODUCTS**:

- **CypherSign Personal Individual Certificate**
  - CypherSign Personal Certificate is a Class-1 Digital Certificates issued to private subscriber individuals and primarily used for securing email communication.
  - Class-1 Digital Certificates are issued upon validation of the user's name and email address constitute a clear topic inside the Certifying Authorities database.

- **CypherSign PRO Individual Certificate**
  - CypherSign Pro is a Class-2 Digital Certificates issued for both business professionals and private individuals. They are used in situations where there is a moderate risk of data tampering.

- **CypherSign Organisational Certificate**
  - CypherSign Organisational is a Class-2 Digital Certificate issued to registered organizations that cater to the specific needs of businesses, offering greater security and functionality, non-repudiation via digital signatures (document signing).

- **CypherSign Pro Max Certificate**
  - CypherSign Pro Max is a Class-2 Digital Certificate issued to individuals/organizations for non-repudiation, Long-Term Validation (LTV) via digital signatures (document signing).
  - Class-2 Digital Certificates require thorough authentication of identity due to the high level of reliability, security and financial liability that the Certificate carries.

- **CypherSign Device Certificate**

  CypherSign Device Certificate is a Class-2 Device Certificate that enables the following:
  - Secure authentication through the use of verified organizational identity;
  - Device identity via the common name registered on the certificate;
  - Data security through the use of encryption and integrity through cryptographic signatures and hashing; and
  - Mutual authentication and secure connections between two devices.

b. **SERVICES**:

- **CypherSign Digital Signing Solution Platform**
  - Centralised digital document signing service platform for businesses and individuals to securely sign regardless of the place and time using web browsers, smartphones, or tablets.

- **CypherSign Sign Server**
  - Auditable digital signing solution server for businesses and individuals to securely sign documents, regardless of the place and time.

- **RAFFTECH PKI Enterprise**
  - Provides a Certificate lifecycle management system of Certificates equipped with strong authentication, encryption and digital signing applications with an advanced web-based configuration wizard, administration and support tools, report generators and application integration tools.

- **RAFFTECH Web Authentication and Verification**
  - Facilitates a safe environment for applying e-signature. It is also an advanced method of authentication of Certificates and verification of the validity of electronic signatures online. Certificate validation, Certificate revocation list (CRL) and real-time online Certificate status query (OCSP) checks can be performed during signing and signature verification processes through the functions provided by software libraries.

- **Time-Stamping Authority Services**
  - RAFFTECH Timestamping Authority Server is a service that binds the digital certificate used to sign a digital file with the data being signed, creating a unique sequence of characters or encoded information known as hash, and also identifies when a certain event has occurred. The result is a trusted accurate digital date and time stamp seal embedded within the digital file that contains X.509 digital signatures
  - RAFFTECH offers Timestamping Service that adds long-term integrity and non-repudiation validation for up to 10 years after the PDF signing certificate has expired or has been revoked

- **PKI Security Professional Services**

  RAFFTECH as a Public Key Infrastructure (PKI) Security Professional Service provides technical assistance to companies in designing and deploying systematic self-managed PKIs to meet growing demands-with customised services to meet specific operational needs.

1.2. DOCUMENT NAME AND IDENTIFICATION

i. This document is formally titled "Certification Practice Statement for RAFFTECH Public Key Infrastructure" and is referred to in this document as the ("CPS"). This CPS is published as a pdf document and made available online to the public via RAFFTECH Repository through HTTPS, or secure web interface at https://www.rafftech.my/repository.

ii. This CPS is structured according to the framework defined in IETF RFC 3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

iii. The Object Identifier (OID) registered for this CPS is as following:

NAME	RAFFTECH CERTIFICATION PRACTICE STATEMENT (CPS)
DOCUMENT ID	RFCA-RFDC-2200-CPS
DOT NOTATION	1.3.6.1.4.1.51215.3.2
ASN.1 NOTATION	{iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) 51215 cpCps(3) certificationPracticeStmt(2)}
OID-IRI NOTATION	/ISO/Identified-Organization/6/1/4/1/51215/3/2

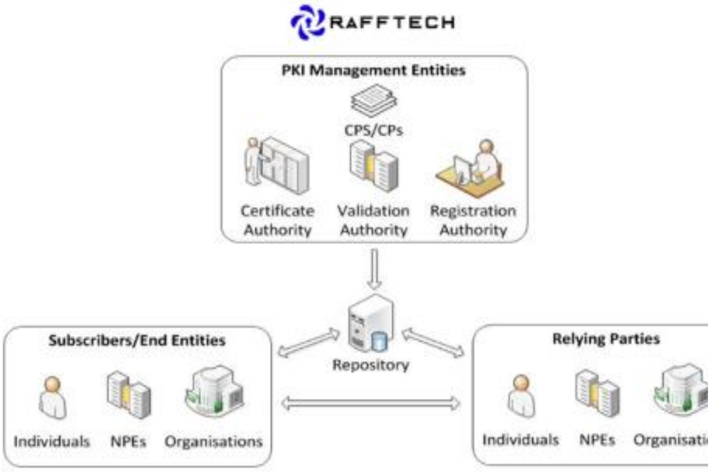
Figure 1.2

1.3. PKI PARTICIPANTS

i.
- In the context of issuing Certificates, RAFFTECH assumes the role of a Trust Service Providers (TSP) that verifies the identity of users, customers and businesses as well as approves electronic signature operations through the issuance and storage of digital certificates.
- As Trust Service Provider, and subject to other PKI Participants complying with their respective obligations and responsibilities, RAFFTECH Management Authority has the final and overall responsibility for the provision of the Digital Certificates offering, namely the Certificate generation services through the RAFFTECH PKI Certification Authority (RFCA), the registration services through the RAFFTECH PKI Registration Authority (RA), the Revocation Management Services, the Revocation Status Information Service (providing Certificate validity status information), and the Dissemination Services. Other PKI participants include the Subscribers, the Relying Parties (RP) and the Trusted Agents (TA).

ii.
- The RAFFTECH Certification Authority is built on a 3-Tier hierarchical PKI structure comprising of 4096-bit key Offline Root CA at the top serving as a secure trust anchors with two levels chaining of online intermediate/Issuing CAs.
- The Offline RAFFTECH Root CA (RCA) is hosted in multi-tier caged environment at a tier 3 accredited data centres operated by third party contractors that meets all technical, policy, and security requirements.

iii.



- Validation Authority (**VA**) Entities Authorized to perform Identity Proofing
- Registration Authority (**RA**) Entities responsible for subscriber registration, certificate registration & revocation.
- Certificate Authority (**CA**) manages certificate lifecycle.
- Non-Person Entity (**NPE**) Non-Natural Person e.g. devices, processes, e-mail addresses.

Figure 1.3

1.3.1. CERTIFICATION AUTHORITIES (CA)

i. RAFFTECH operates 5 Issuing CA as follows:

ISSUING CA	OID	CLASS
CypherSign Personal	1.3.6.1.4.1.51215.2.1	Class (1) One
CypherSign Pro	1.3.6.1.4.1.51215.2.2	Class (2) Two
CypherSign Organizational	1.3.6.1.4.1.51215.2.3	Class (2) Two
CypherSign Pro Max	1.3.6.1.4.1.51215.2.4	Class (2) Two
RAFFTECH Time Stamping Authority	1.3.6.1.4.1.51215.2.5	Class (2) Two

Table 1.3.1.a

ii. RAFFTECH-CA facilitates the following Certificate services:

- Subscriber Registration
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation
- Certificate Renewal

iii. In addition, RAFFTECH-CA roles and obligations are described in the following:

- Certificate Key Generation and Storage
- Certificate Generation
- Certificate Publication
- CRL and/or OSCP Generation and Issuance
- System Management Functions (e.g., security audit, configuration management, archive).

1.3.2. REGISTRATION AUTHORITIES (RA)

i. A Registration Authority (RA) is an entity that assists to verify applicant identity is legitimate and authorizes creation of a certificate by providing the validated user information to CA.

ii. In order to provide reliable and proper Digital Certification services, RAFFTECH-CA MAY performs the RA functions internally or make use of external registration authorities for specific subscriber registration activities and in some cases, an Intermediate/Issuing CA may act as RA for RAFFTECH. External RA agents are required to enter into an agreement with CA to collect and verify subscribers' identity and information that is to be entered into the digital certificates.

iii. Entities operating or intending to operate as a Registration Authorities (RA) body are required to meet all relevant evaluation requirements as set out by RAFFTECH. The specific privileges, duties and responsibilities of these RAs within RPKI are identified in the Registration Authority Policy Statement (RPS) as well as Registration Authority Practices Guideline (RAPG).

iv. RAFFTECH-RA facilitates the following certificate services:

- Subscriber Registration;
- Digital Certificate Revocation;
- Digital Certificate Renewal

v. RAFFTECH-RA rights and obligations are described in the following:

- Verifying the identity of entities applying for a digital certificate;
- Perform Identity-Proofing and Approve applications for Certificate renewal on behalf of RAFFTECH-CA;
- Initiate or pass along revocation requests for Certificates
- Manage and store registration data in a safe and secure environment

1.3.3. SUBSCRIBERS

i. The subject of a Certificate is the party named in the Certificate. A subscriber, as used herein, may refer to both the subject of the Certificate and/or the entity that contracted with RAFFTECH for the Certificate's issuance. Prior to verification of identity and/or issuance of a Certificate, a subscriber is defined as an applicant.

ii. RAFFTECH SHALL make its services accessible to all Applicants/Subscribers whose activities fall within its declared field of operation and who agree to abide by obligations specified in the following:
   - RAFFTECH Certificate Policy (CP) and Certification Practice Statement (CPS);
   - Subscriber Agreement (SA);
   - Terms of Use/Service.

1.3.4. RELYING PARTIES (RP)

i. A relying party verifies a digital signature from the Certificate's subject where the digital signature is associated with an email, web form, electronic document, or other data. Other examples of relying parties are such as an entity operating a server that controls access to online information using client Certificates as an access control mechanism. In summary, a relying party is an entity that uses a public key in a Certificate (for signature verification and/or encryption).

ii. A Relying Party must take notice and is bound by the following: -
   - RAFFTECH Certificate Policy (CP) and Practice Statement (CPS);
   - Relying Party Agreement (RPA);
   - Terms of Use/Service

iii. A Relying Party rights and obligations are described in the following:
   - Verify a Certificate identity and/or validity;
   - Perform Certificate path validation;
   - Processing Certificates and Certificate Revocation Lists (CRLs); and
   - Fetching and Caching RPKI Repository Objects.

1.3.5. OTHER PARTICIPANTS

i. RAFFTECH operates a licensed repository system that conforms to the structure described in RFC 6481, supporting the ongoing administration, maintenance, and preservation activities of RAFFTECH Public Key Infrastructure (RPKI).

1.3.5.1. TRUSTED AGENTS (TA)

i. RAFFTECH may choose to use the services of Trusted Agents to assist RFCA in performing any identity verification and authorization verification tasks. Trusted Agents are entities authorized to act as a representative of a RFCA in providing identity verification during the registration process. Trusted Agents may have automated interfaces with RFCA; they act on the behalf of the CA or the RA to only verify the identity and/or authority of the Subscriber. Trusted Agents do not have privileged access to RFCA functions, are considered agents of RFCA.

ii. A Trusted Agents (TA) must take notice and is bound by the following: -
   - RAFFTECH Certificate Policy (CP) and Practice Statement (CPS);
   - Relying Party Agreement (RPA).
   - Subscriber Agreement (SA);
   - Terms of Use/Service.

1.4. CERTIFICATE USAGE

i. Subscribers may use RAFFTECH certificates issued pursuant to this CP/CPS for all legal authentication, encryption, access control, and digital signature purposes, as designated by the key usage and extended key usage fields found within the certificate.

ii. The Certificates issued under RPKI provides assurance of the identity of the Subscriber, and are for use in conjunction with specific RAFFTECH services and products allowing use of such Certificates as documented in the relevant service documentation.

Certificate Type	Certification Usage
Class-One [1]	
Individual	Issued to an individual used to: Digitally sign email - Subscribers can digitally sign email messages so that the recipient is assured that the email has come from you.
Class-Two [2] and Class-Three [3]	
Individual	Issued to an individual intended for the signing of business documents such as sales contracts, invoice processing, vendor agreements. It is also intended for encrypting e-mails and files.
Device	Issued to an individual/organization use to control which endpoints access the networks and resources for authenticating distributed hardware
Organizational	issued to an organization to employ authentication, secure electronic mail file exchange and for signing business documents for message integrity, authentication, privacy via data encryption, and non-repudiation
Time-Stamping	Issued to an individual/organization used to identify the existence of data at a set period of time.

Figure 1.4

1.4.1. Appropriate Certificate Uses

i. RAFFTECH PKI is intended to support the following security services: confidentiality, integrity, authentication and technical non-repudiation. RAFFTECH PKI supports these security services by providing identification and authentication, integrity, technical non-repudiation through digital signatures, and confidentiality through key exchange.

ii. RAFFTECH PKI provides support of security services to a wide range of applications that protect various types of information. A single solution providing support to every application would appear to be desirable but because of different legal, security and national policy requirements for protection of the different categories of information, the most cost-effective solution is one that supports multiple assurance levels.

iii. RAFFTECH Digital Signature Certificates are issued with varying levels of assurance. Figure 1.4 provides a brief description of the appropriate uses of each Certification Type. The descriptions are for guidance only and are not binding.

iv. Some of the Certificates that may be issued under this PKI could be used to support operation of this infrastructure, e.g., access control for the repository system as described in Section 2.4. Such uses also are permitted under the RPKI Certificate policy. Additional uses of the Certificates, consistent with the basic goals cited above, are also permitted under RFC 6484.

1.4.1.1. Level of Assurance

i. Levels of Assurance (LoA) is the certainty with which a claim to a particular identity during authentication can be trusted to actually be the claimant's "true" identity. At its simplest, LoA is a standard for establishing with a high degree of confidence that someone is who they claim to be.

Class	Description
Class (1) one	Class 1 Digital Certificate Assurance Level is LOW
Digital Certificate	● Class 1 Certificates should not be used for authentication purposes and for supporting non-repudiation. The digital signature provides simple (modest) assurances that the e-mail originated from a sender with a certain e-mail address; ● Class 1 Certificates are suitable for document signing, encryption, and electronic access control for non-commercial transactions where proof of identity is not required.
Class (2) two	Class 2 Digital Certificate Assurance Level is MEDIUM
Digital Certificate	● Class 2 Certificates are used for securing e-mails of some inter- and intra-organizational, commercial, and personal for which proof of identity is required; ● Class 2 Certificates are suitable for digital signatures, encryption, and electronic access control in transactions where proof of identity based on information in the validating database is sufficient.
Class (3) Three	Class 3 Digital Certificate Assurance Level is HIGH
Digital Certificate	● Class 3 Digital Signature Certificates [DSC] ensures the highest level of security, assurance of its subscriber's identity compared to its Class 1 and Class 2; ● Class 3 DSC is mainly used in scenarios where the danger and effects of data manipulation or identity theft are serious. Examples include financial transactions, government applications, and e-commerce platforms.

Figure 1.4.1.1.a

ii. Identity Proofing Level and Verification-Validation Methods

Proofing Level	Verification-Validation Methods
BASIC ONE (1) OR MORE LEVEL OF VERIFICATION-VALIDATION METHODS	1. Verify e-mail address through an email challenge process; 2. Verify applicant identity against governmental database records; and 3. Remote Identity Validation through e-KYC, Telephone or Video Call.
STANDARD TWO (2) OR MORE LEVEL OF VERIFICATION-VALIDATION METHODS	1. Verify e-mail address through an email challenge process; 2. Verify applicant identity against governmental database records; 3. Verify business registration against governmental database records; 4. Verify submitted letter of Authorization; 5. Remote Identity Validation through e-KYC, Telephone or Video Call; and 6. Validate online through KYC identity verification.
ENTERPRISE THREE (3) OR MORE LEVEL OF VERIFICATION-VALIDATION METHODS	1. Verify e-mail address and validated through an email challenge process; 2. Verify applicant identity against governmental database records; 3. Verify business registration against governmental database records; 4. Verify submitted letter of Authorization; 5. in-person identity proofing; and 6. Certified by a notary public duly appointed under Notaries Public Act 1959.

Figure 1.4.1.1.b

ii. RAFFTECH Certificates Assurance Level and Key Usage

Certificate		Assurance Level			Key Usage		
Intermediate CA	**Class**	**Low**	**Medium**	**High**	**1**	**2**	**3**
CypherSign Personal	**One (1)**	✓			✓		✓
CypherSign Pro	**Two (2)**		✓		✓	✓	✓
CypherSign Organizational	**Two (2)**		✓		✓	✓	✓
CypherSign Pro Max	**Two (2)**		✓		✓	✓	✓
RAFFTECH Time Stamping Authority	**Two (2)**		✓		✓	✓	✓

ID	Key Usage
1	**Document Signing**
2	**Encryption**
3	**Authentication**

Figure 1.4.1.1.c

1.4.2. Prohibited Certificate Uses

i. When a RAFFTECH Certificates expires or is revoked, the subscriber must no longer use the associated private key after the expiry or revocation date, or have the private key signed or certified by another trust service provider.

ii. RAFFTECH Certificates does not assure that subject remains trustworthy, 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 as and when the certificate issued.

iii. The subscriber shall not make use of RAFFTECH certificate for other usage than what is included in the certificate extension on key usage and extended key usage.

1.5. POLICY ADMINISTRATION

1.5.1. Organization Administering the Document

i. Raffcomm Technologies Sdn. Bhd. [RAFFTECH] via a special committee called Management Authority [RAFFTECH-MA] owns this CPS and represents the interest of its members in developing the policies that govern RAFFTECH-PKI. RAFFTECH-MA made up of top-level management with full financial and administrative authority are responsible for the security, operation, and maintenance of RAFFTECH-PKI components, including:

- Maintaining RAFFTECH CP/CPS;
- Governing and operating the PKI according to RAFFTECH CP/CPS;
- Approving the CPS for CAs that issue Certificates under RAFFTECH CP/CPS; and
- Approving the Audit for CAs operating under this CPS.

ii. The RAFFTECH-MA has the responsibility for continually and effectively managing RPKI related risks. This includes a responsibility to periodically re-evaluate risks to ensure that the controls that have been defined remain appropriate, and a responsibility to periodically review the controls as implemented, to ensure that they continue to be effective. This is covered by the Information Security Risk Management framework at RAFFTECH.

1.5.2. CONTACT PERSON

i. All questions and comments regarding this Certification Practice Statement should be addressed to the representative of the RAFFTECH PKI Management Authority (MA):

ATTENTION	RAFFTECH Management Authority
COMPANY	Raffcomm Technologies Sdn. Bhd. [201001015771 (1000449-W)]
ADDRESS	32.03, Level 32, Sunway Putra Tower, 100, Jalan Putra, 50350 Kuala Lumpur, Malaysia
CORPORATE OFFICE	+603-4040 0091
FAX	+603-4040 0095
E-MAIL	business.compliance@raffcomm.my
WEBSITE	https://www.rafftech.my

Figure 1.5.2a

ii. All Certificate revocation requests or security issues such as suspected key compromise, Certificate misuse, fraud or other matters should be reported/addressed to the representative of the RAFFTECH PKI Registration Authority (RA):

ATTENTION	RAFFTECH Registration Authority
OPERATION OFFICE	03-2787 2010
FAX	03-4040 0095
E-MAIL	ra@raffcomm.my
WEBSITE	https://www.rafftech.my

Figure 1.5.2b

1.5.3. PERSON DETERMINING CPS SUITABILITY FOR THE POLICY

i. The RAFFTECH PKI Management Authority (RAFFTECH-MA) determines Certification Practice Statement (CPS) suitability for the related RAFFTECH Certificate Policy (CP).

1.5.4. CPS APPROVAL PROCEDURES

i. The RAFFTECH PKI Management Authority (RAFFTECH-MA) approves this Certification Practice Statement (CPS) and any subsequent changes before being published online. The "Version Control" mechanism will be used to trace all identified changes to the content of this document.

ii. Comments, questions, and change requests to this Certification Practice Statement document should be addressed accordingly as specified in section 1.5.2.

1.6. DEFINITIONS AND ACRONYMS

i. Please refer to Appendix 1 and Appendix 2

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

i. RAFFTECH-CA operates a licenced publication repository system that adheres to the structure outlined in RFC 6481, supporting the ongoing administration, maintenance, and preservation activities within RPKI.

ii. RAFFTECH Repository comprises the current (non-expired and non-revoked) digital signature Certificates issued by RAFFTECH-CA, the most recent CRL issued by RAFFTECH-CA, the current manifest, and all other current RPKI objects that can be verified using an EE Certificate RFC 6487 issued by RAFFTECH.

2.1. REPOSITORIES

i. RAFFTECH-CA publishes Certificates, CRLs, and RPKI objects (intended for public consumption), making it available for downloading by all parties relying, enabling them to validate this data.

2.2. PUBLICATION of CERTIFICATES and CERTIFICATE STATUS

i. RAFFTECH-CA is responsible to publish information regarding its practices, Certificates, and the current status of such Certificates in its repository publicly available in a read-only manner to subscribers and/or relevant parties through HTTPS server at https://www.rafftech.my/repository.

ii. CRL distribution points are included in intermediate and end-entity Certificates. OCSP services are publicly available online for real-time verification meanwhile CRL is published once a day. Access to OCSP, CRLs, CA Certificates, Certificate download, Certificates status is provided through the RAFFTECH PKI network and related hardware and software configuration required for connectivity. CRLs are made available to public via https://www.rafftech.my/crl/.

2.3. TIME or FREQUENCY of PUBLICATION

i. The information published in RAFFTECH repository is updated following specific events like:
- RAFFTECH legally bindings document updates;
- After issuing a new Certificate;
- CRL is updated either periodically or when a Certificate is revoked;
- Fixing of non-conformities found by audits; or
- Additional information – after every update.

ii. RAFFTECH SHALL develop, implement, enforce, and annually update a Certificate Policy and/or Certification Practice Statement that describes in detail how the CA implements the latest version of these requirements.

2.4. ACCESS CONTROLS on REPOSITORIES

i. Published information is public in nature and freely accessible. Write access to repository is limited to RAFFTECH authorized personnel only:
- Only the RAFFTECH-CA team has write access to the public repository of the PKI related objects/documents.
- Only the RAFFTECH-CA team has write access to OCSP responder environments, Certificate, and CRLs.

ii. RAFFTECH-CA is responsible to publish information regarding its practices as well as the current status of Certificates. RAFFTECH operates physical and logical security controls to protect the repository from unauthorized modification or deletion. In case of voluntary or involuntary alteration or compromise of information in RAFFTECH repository, appropriate actions will be taken to re-establish the repositories' data integrity. Actions (if appropriate) will be taken against those responsible for these acts. The affected relying parties will be notified.

3. IDENTIFICATION and AUTHENTICATION

i. RAFFTECH-CA or its appointed RA SHALL verify the identity of the applicant and/or the authenticity of the applicant representative's Certificate request using a verification process meeting the requirements described in the RAFFTECH Certificate Policy and/or Certification Practice Statement. RAFFTECH-CA SHALL inspect any document relied upon under this section for alteration or falsification.

ii. RAFFTECH-CA or RA verifies the identity of the person whose personal information is to be included in the subscriber distinguished name field of the Certificate. Only authenticated information is included in the subscriber distinguished name.

iii. For organisational Certificates (including role based, server, network resource, code signing, etc.), RAFFTECH-CA or RA verifies the legal existence of the organisation's name and the authority of the requesting party to be included in the organisation attribute in the subscriber distinguished name field of the Certificate. An unauthenticated organisation name is not included in a Certificate.

3.1. NAMING

i. Before issuing a Certificate, RAFFTECH-CA ensures that all subject organization information in the Certificate conforms to the requirements of, and has been verified in accordance with the procedures prescribed in the applicable CP/CPS and matches the information confirmed and documented by the RA pursuant to its verification processes.

ii. RAFFTECH Certificates are issued with a unique, non-null subject Distinguished Name (DN) which conforms to ITU X.500 standards for subjectName. RAFFTECH-RA provides naming elements pertaining to subscribers in accordance with RAFFTECH CP & CPS.

3.1.1. TYPES OF NAMES

i. The RAFFTECH-CA assigns each entity a X.509 Distinguished Name (DN) which serves as a unique identifier of the entity. The DN is inserted in the subject field of the Certificate(s) issued to the entity to bind the entity to the Certificate(s). The DN MUST be a non-empty printable String.

ii.

DEFAULT CERTIFICATE FIELDS			
CN = CypherSign Class 1 Root CA	**C** = MY	**O** = Raffcomm Technologies Sdn Bhd	**OU** = 1000449-W
CN = CypherSign Class 2 Root CA	**C** = MY	**O** = Raffcomm Technologies Sdn Bhd	**OU** = 1000449-W
CN = RAFFTECH Class 2 ECC Root CA	**C** = MY	**O** = Raffcomm Technologies Sdn Bhd	**OU** = 1000449-W
CN = RAFFTECH Class 2 RSA Root CA	**C** = MY	**O** = Raffcomm Technologies Sdn Bhd	**OU** = 1000449-W
CN = CypherSign Organizational	**C** = MY	**O** = Raffcomm Technologies Sdn Bhd	**OU** = 1000449-W
CN = CypherSign Personal	**C** = MY	**O** = Raffcomm Technologies Sdn Bhd	**OU** = 1000449-W

Figure 3.1.1.a

iii. The default subject attributes for RAFFTECH Certificate issued under this CPS SHALL consist the following elements:

ATTRIBUTES	DEFINITION	EXAMPLE
C = Country	Country of Certificate	"MY"
O = Organization	SSM Business Registration Name	"Raffcomm Technologies Sdn. Bhd."
OU = Organization Unit	SSM Business Registration Number	"201001015771(1000449-W)"
CN = Common Name	Full Name (as per MyKad/Passport).	"Ahmad bin Shukor"
SERIALNUMBER	MyKad/Passport Identification Number	"123456-78-9101 / A39231048"

Figure 3.1.1.b

iv. Distinguished name for an X.509 certificate consists of a sequence of relative distinguished names (RDN) where each RDN is expressed as an attribute type/value pair. The subject distinguished name is the name of the subscriber of the certificate. The distinguished name in the certificate is a textual representation of the subject or issuer of the certificate.

3.1.2. NEED FOR NAMES TO BE MEANINGFUL

i. Names shall identify the person or object to which they are assigned**.** The subject and issuer names contained in RAFFTECH Certificate shall be meaningful and associated with the authenticated names of the end-entities.

- The organisation name maps to SSM registered business name;
- The name used for a natural person maps to the Full Name as per MyKad/Passport; and
- The name used for equipment maps the model name and/or serial number, or an application process (e.g., Organization X Mail List or Organization Y Multifunction Interpreter).

ii. RAFFTECH Validation Authorities (VA) determines the proper elements for a given Subscriber based on validated supporting documents, establishing authority for the creation of the DNs.

3.1.3. ANONYMITY OR PSEUDONYMITY OF SUBSCRIBERS

i. RAFFTECH-CA does not issue anonymous or pseudonymous Certificates thus no explicit support for this feature is provided.

3.1.4. RULES FOR INTERPRETING VARIOUS NAME FORMS

i. RAFFTECH-CA issues digital signature Certificates with a non-null subject Distinguished Name ("DN"). When DN's are used, common names shall respect namespace uniqueness and shall not be misleading.

3.1.5. UNIQUENESS OF NAMES

i. RAFFTECH-CA verifies Certificate request submission with the use of CA public key. This is done to verify the uniqueness of the subscriber's distinguished name within its authorized X.500 name space.

ii. RAFFTECH-RA is responsible for the assignment of unique subject names are among all the Certificates issued. RAFFTECH-RA may append additional attributes to make the DN unique for its subscriber names.

3.1.6. RECOGNITION, AUTHENTICATION, AND ROLE OF TRADEMARKS

i. RAFFTECH does not make any provision to recognize nor authenticate trademarks, service marks, etc.

3.2. INITIAL IDENTITY VALIDATION

i. Initial validation is performed by the RAFFTECH Validation Authority personnel or by a third-party application to perform such operations. Before issuing an RAFFTECH Digital Signature Certificate, the Validation Authority are obligated to ensure that all information in the Certificate conforms to the requirements of and verified in accordance with the procedures prescribed in RAFFTECH CP/CPS.

3.2.1. METHOD TO PROVE POSSESSION OF PRIVATE KEY

i. RAFFTECH establishes Proof of Possession (PoP) that the subscriber holds or controls the private key by performing signature verification or decryption on data purported to have been digitally signed or encrypted. The means by which PoP is achieved is determined by RAFFTECH and MUST be declared. In the future RAFFTECH MAY determine other mechanisms that are at least as secure as those cited here to be acceptable.

3.2.2. AUTHENTICATION OF ORGANIZATION IDENTITY

i. Organisation identity proofing requires applicants to provide legal or regulatory documents as evidence of the organisation's identity and existence. These documents presented for establishing the organisation identity MUST identify the organisation and attest that the Authoriser is a member of the organisation.

ii. RAFFTECH validation team SHALL perform some if not all of the following: -

- Validate business name and details matches against recognised governmental database records;
- Verify the identity of the authorized personnel affiliated with the organization;
- Perform call and/or conduct visit the registered business premise.

iii. RAFFTECH may determine other mechanisms that are at least as secure as those cited here to be acceptable.

3.2.3. AUTHENTICATION OF INDIVIDUAL IDENTITY

i. The validation requirements are categorized following subscriber type and types of Certificates applied.

- In case the entity is a natural person, the initial authentication will be based on suitable identification documents and appearance of the applicant before the RAFFTECH-CA or RA.
- In case the entity to be certified is a machine or software component, the requester (a natural person) shall prove to the satisfaction of the Validation Authority that the binding will be to the service or system defined in the subject and that the requester is adequately authorised.

ii. Applications for Class 1 and 2 certificates are exempted to be certified by a notary public as per P.U.(A) 352/98 - Digital Signature (Certification by Notary Public) (Exemption) Order 1998. However for the purpose of identifying and validating foreign applicants, RAFFTECH requires the supporting documents to be attested.

iii. RAFFTECH Class 3 Digital Signature Certificates [DSC] ensures the highest level of security and assurance of its subscriber's identity hence all Class 3 certificate application are required to be certified by a notary public duly appointed under the Notaries Public Act 1959.

iii. External Registration Authorities may implement alternative identity vetting mechanisms that are at least as secure as the method described above.

iv. RAFFTECH-CA shall ensure that the applicant's identity is verified in accordance with this CP/CPS. Information exchange prior to Certificate issuance shall be validated by strong cryptographic means, or by means that constitute valid legal evidence, or shall be verified by out-of-band methods in a phone conversation or video call with firm positive identification by all parties involved.

v.

Class	Description	Proofing	Usage
RAFFTECH offers Basic level of Security and Assurance for Class 1 Digital certificates **Applicants for Class 1 certificates are required demonstrate authority over the e-mail address**			
Class One (1) **Basic Validation**	**Class 1 Individual certificates**: binds a valid email address	**Verify** • E-mail address **Validated trough** • E-mail challenge process	• Personal E-Mail Certificates that allows subscriber to secure email messages[s/mime] **Table 3.2.3a**

RAFFTECH offers Medium level of Security and Assurance for Class 2 Digital certificates **Applicants require to undergo a medium level of identity verification**			
Class Two (2) **Standard Validation** *For medium-value transactions*	**Class 2 Individual certificates**: binds entity to verified identity details	**Verify** • E-Mail Address • Subscriber Identity **Validated trough** • Remote/In-Person proofing before the CA/RA; [Telephone/Video Call]	• Online registration through the web; • Online transactions (e-banking, e-government services etc.); • Organizational Seal; • Document Signing - Digital Signature under Digital Signature Act 1997 ("DSA 1997") • Client-Server Authentication • Data Encryption **Table 3.2.3b**
	Class 2 Organization certificates: binds legal entity name of the organization	**Verify** • E-Mail Address • Subscriber Identity • Organization BRN • Department **Validated trough** • Site Visitation • Authorization Letter • Remote/In-Person proofing before the CA/RA;[Telephone/Video Call]	
	Class 2 Device Certificates: binds device to its serialnumber	**Verify** • Device Ownership • Serialnumber **Validated trough** • Authorization Letter	

Class	Description	Proofing	Usage
RAFFTECH offers highest level of security and assurance for Class 3 Digital certificates **Applicants require to undergo a high level of identity verification, includes in-person and/or supervised remote proofing**			
Class Three (3) **Extended Validation** *For high-value transactions*	**Class 3 Professional Certificates**: Binds legal entity to a professional title or department in an organization	**Verify** • E-Mail Address • Applicant Identity • Applicant Profession; • Telephone Number • Organization BRN **Validated trough** • Site Visit • Registered professional bodies • Authorization Letter • in-person proofing before the CA/RA • Certified by a notary public duly appointed under the Notaries Public Act 1959.	• For industry professional such as doctors, lawyers; • For e-government related programs such as e-tender and e-procurement • Online transactions (e-banking etc.). • Document Signing - Digital Signature under Digital Signature Act 1997 ("DSA 1997") **Table 3.2.3c**
	Class 3 Organization Certificates: binds the entity to its registered organization records		

3.2.3.1. IN-PERSON AUTHENTICATION

i. For Class 3 certificates, identity is established by in-person proofing before the CA/RA, to confirm identities; supporting documents provided shall be verified to ensure legitimacy.

ii. Minors and others not competent to perform face-to-face registration alone shall be accompanied by an authorized person whom endorses applicant providing sufficient supporting document for registration at the level of the Certificate being requested, for both himself and the person accompanied.

iii. RAFFTECH specifies in its Certificate Policy and Practices (CP/CPS), Registration Authority Practice Guideline (RAPG) procedures for authenticating a subscriber's identity. RAFFTECH-CA or the RA shall also verify the identity of each applicant for all Certificates so that identity details can be included in the Certificate. Finally, RAFFTECH-CA or the RA shall record the process that was followed for each Certificate, including the mechanism used to verify applicant identity. At a minimum, process documentation must include:
- The identity of the person performing the identification, including date and time of the verification;
- Signed declaration by that person that he/she verified the identity of the Subscriber as required by RAFFTECH CP/CPS;
- The method used to authenticate the individual's identity, including identification type and unique numeric or alphanumeric identifier, if appropriate;
- The identity of the person performing the authentication, including date and time of the validation;
- A signed declaration by that person that he or she validated the verification request performed as required by RAFFTECH CP/CPS;
- The method used to verify the identity of the applicant, including identification type and unique numeric or alphanumeric identifier, if appropriate;
- Additionally, the process documentation must include declaration of identity. The declaration shall be signed with a handwritten signature by the Certificate applicant in the presence of the person performing the identity authentication

iv. Foreign individuals requires the applicant to submit certified identity documents attested by a notary public.

3.2.3.2. ELECTRONIC AUTHENTICATION

i. RAFFTECH-CA shall ensure that the applicant's identity is verified in accordance with this CP/CPS. Information exchange prior to Certificate issuance shall be validated by strong cryptographic means, or by means that constitute valid legal evidence, or shall be verified by out-of-band methods in a phone conversation or video call with firm positive identification by all parties involved.

ii. RAFFTECH Certificates may be issued on the basis of electronically authenticated (e.g. E-KYC) Subscriber requests, subject to the following restrictions:
- Mobile application requires the collection of electronic images, fingerprints at the time of the applicant's registration;

3.2.3.3. AUTHENTICATION OF COMPONENT IDENTITIES

i. Some computing and communications components (e.g., routers, firewalls) may be named as Certificate subjects.

3.2.4. NON-VERIFIED SUBSCRIBER INFORMATION

i. Non-verified subscriber data SHALL not be included in Certificates issued under RAFFTECH Certificate policies.

3.2.5. VALIDATION OF AUTHORITY

i. Validation of Authority for Subscriber Certificates is the responsibility of RAFFTECH-CA or the appointed RA whom follows established, documented, standard operating procedure for identity proofing SHALL determine whether the Individual described in the Letter of Authorization (LoA) has the permission to act on behalf of an applicant or an organization to obtain Digital Signature Certificate on behalf of the subscriber.

ii.

CERTIFICATE	VALIDATED AGAINST
Class 1 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 email address to be listed in the Certificate.
CLASS 1 Customized Individual and Organization	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 email address to be listed in the Certificate.
CLASS 2 Certificates Individual & Organization	Individuals affiliated with an organization 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.
CLASS 2 Certificates SSL/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.

Figure 3.2.5.a

3.2.6. CRITERIA FOR INTEROPERATION

i. RAFFTECH does not practise / facilitate interoperability which MAY include cross-certification, unilateral certification, or other forms of interoperation

3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

i. This control is not applicable as RAFFTECH-CA does not practice Certificate rekey in business

3.3.1. IDENTIFICATION AND AUTHENTICATION FOR ROUTINE RE-KEY

i. This control is not applicable as RAFFTECH-CA does not practice routine re-keying before expiration of the subscribers' current Certificate.

3.3.2. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY AFTER REVOCATION

i. Revoked, suspended or expired Certificates shall not be rekeyed. Upon revocation of a Certificate, the subscriber shall immediately cease using such Certificate and shall remove such Certificate from any devices and/or software in which it has been installed. This control is not applicable as RAFFTECH-CA does not re-certify Certificates after revocation.

3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS

i. RAFFTECH-CA identifies supporting conditions eligible to request for Certificate revocation: -

- The Subscriber notifies the CA that the original Certificate request was not authorised and does not retrospectively grant authorisation;
- RAFFTECH obtains credible evidence that the Subscriber had misused the Certificate or suffered a key compromise or no longer complies with RAFFTECH PKI requirements;
- RAFFTECH is made aware that a Subscriber has violated one or more of its material obligations.

ii. Authentication of a subscriber requesting revocation of its Certificate may be accomplished by:

- Revocation request is digitally signed with the private key which needs to be revoked; and/or
- Revocation request is digitally signed by the authorized RA.

iii. If an authorized party other than the subscriber, requests revocation of a Certificate, authentication shall be done via a valid formal consent, as described by the applicable CP, of a representative of that party, or one formally appointed for such purpose.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

i. This chapter describes operational requirements imposed upon RAFFTECH PKI participants with respect to the RAFFTECH digital Certificate life-cycle. All entities within the RAFFTECH PKI including subscribers or other participants have a continuous duty to inform the RAFFTECH-CA of all changes in the information featured in a Certificate during the operational period of such Certificate and until it expires or revoked.

ii. The subscriber is required to accept the issuance terms by a subscriber agreement that will be executed with the RAFFTECH-CA. The subscriber agreement incorporates by reference this CPS.

iii. To carry out its tasks RAFFTECH may use third party agents for which RAFFTECH-CA assumes responsibility.

4.1 CERTIFICATE APPLICATION

i. RAFFTECH-CA acts upon a Certificate application to validate the submitted information. Subsequently, the application is either approved or rejected. Such approval or rejection does not necessarily have to be justified to the applicant or any other party.

ii. For rejected applications of Certificate requests, RAFFTECH-CA notes the reason for rejecting the application.

iii. Application for Certificates issued under this CPS MAY be submitted via: -

- Electronic submission means (e.g. secure email, website, and mobile application).
- Physical submission means signed copy of the application form.

4.1.1. WHO CAN SUBMIT A CERTIFICATE APPLICATION

i. The following entities can submit RAFFTECH Digital Certificate Application: -

- The entity who is the subscriber himself
- The authorized representative requesting Certificates on behalf of the subscriber or organization
- The entity which can prove its current responsibility for a certified machine or service
- The associated RA or the Trusted partner

4.1.2. ENROLMENT PROCESS AND RESPONSIBILITIES

i. RAFFTECH enrolment process are conducted according to its' established, documented, standard operating procedure for identity proofing. All any electronic transmission of shared secrets among CAs/RAs supporting the Certificate Application and issuance process SHALL be authenticated and protected from modification; Communications MAY be electronic or out-of-band and SHALL protect confidentiality and integrity of the data.

ii. The Certificate subscribers SHALL undergo an enrolment process that requires:

- Accepting RAFFTECH Subscriber Agreement (SA) and/or Terms of Use/Service
- Submitting completed RAFFTECH digital Certificate application form (individual/organizational);
- Providing the requested supporting documents/information;
- Responding to authentication requests in a timely manner; and
- Submitting required payment; and
- Any other relevant information that RAFFTECH MAY requests.

iii. The subscriber is required to accept the issuance terms by a subscriber agreement that will be executed with the RAFFTECH-CA. The subscriber agreement incorporates by reference this CPS.

4.2. CERTIFICATE APPLICATION PROCESSING

i. Trusted Agents and/or the Applicant MAY submit Certificate applications to RAFFTECH-CA and/or its appointed RA whom SHALL perform identification and authentication procedures to validate the Certificate application adhering to the established practices and procedures defined in the following documents: -

- RAFFTECH Certificate Policy (CP) and /or Certification Practice Statement (CPS)
- RAFFTECH Registration Authorities Policy Statement (RPS) and/or Registration Authority Practices Guideline (RAPG).

4.2.1. PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS

i. Prior to Certificate issuance, the applicant SHALL sign RAFFTECH Subscribers Agreement (SA) detailing subscriber's right and obligations, regarding the issuance and management of Certificates. This includes the requirement that the applicant SHALL protect the private keys and use the Certificates and private keys for authorized purposes only.

4.2.2. APPROVAL OR REJECTION OF CERTIFICATE APPLICATIONS

i. RAFFTECH-CA and/or its appointed RA SHALL approve or reject the Certificate application. RAFFTECH at its' discretion MAY reject any Certificate application that cannot be verified or incomplete.

ii. RAFFTECH-CA or its appointed RA SHALL approve a Certificate Application if all the following criteria/condition are met:

- Receipt of a fully executed subscriber agreement;
- Receipt of a signed Certificate Application;
- Receipt of all requested supporting documentation;
- Successful identification and authentication of all required information;
- Acceptance of the Certificate application would not cause a violation of the CPS or the CP; and
- Receipt of proof of Payment (if applicable) has been received; and
- RAFFTECH-CA approves the Certificate Application.

4.2.3. TIME TO PROCESS CERTIFICATE APPLICATIONS

i. Certificate applications submitted to RAFFTECH with accurate and complete information are expected to be processed within at most within 5 business working days.

4.3. CERTIFICATE ISSUANCE

i. Prior to the issuance of RAFFTECH digital signature Certificate, RAFFTECH-CA SHALL verify the identity and/or authority of the subscriber and the integrity of the information in the Certificate request.

ii. RAFFTECH-CA SHALL implement procedures to identify suspicious Certificate requests.

iii. RAFFTECH-CA may issue a Certificate to a subscriber only after all of the following conditions are satisfied:

a. RAFFTECH-CA has received a request for issuance signed by the validation authority; and

b. RAFFTECH-CA has confirmed that: -

- the prospective subscriber is the person to be listed in the certificate to be issued and the information in the certificate to be issued is accurate;
- if the prospective subscriber is acting through one or more agents, the subscriber duly authorized the agent or agents to have custody of the subscriber's private key and to request issuance of a certificate listing the corresponding public key;
- the prospective subscriber rightfully holds the private key listed in the certificate capable of creating a digital signature;
- the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the prospective subscriber; and
- Payment was done and proof of purchase was submitted and verified.

4.3.1. CA ACTIONS DURING CERTIFICATE ISSUANCE

i. At a high level, the following steps are taken during issuance of a subscriber Certificate. RAFFTECH-CA generates Certificate and ensures all details which will appear in the Certificate against the information provided during Certificate request are EXACTLY identical. The Certificate is then signed with RAFFTECH-CA public key loaded onto a protected HSM environment. RAFFTECH-CA stores the Certificate in an X.500/LDAP-compliant directory and makes notification on its availability for the subscriber to perform the final verification before publication.

ii. Upon receiving an issuance request, RAFFTECH-CA SHALL:

- Verify the identity of the applicant including the integrity of the information in the Certificate request;
- Verify authority of the representative and integrity of the business details provided in the Certificate request;
- Generate, sign and store a Certificate upon meeting all MANDATORY requirements;
- Make the Certificate available once subscriber formally acknowledges their obligations.

iii. Certificates will not be signed until all verifications and modifications, if any, have been completed to RAFFTECH-CA's satisfaction.

4.3.2. NOTIFICATION TO SUBSCRIBER BY THE CA OF ISSUANCE OF CERTIFICATE

i. RAFFTECH SHALL notify subscribers upon the Certificate availability and provide the means for obtaining the Certificate on its' publication to RAFFTECH repository.

ii. The notification of Certificate issuance shall be through emails.

4.4. CERTIFICATE ACCEPTANCE

i. RAFFTECH deems that the Certificates are valid five (5) days after issuance unless the subscriber explicitly rejects it in an authenticated communication with RAFFTECH-CA or its appointed RA.

ii. Certificate Acceptance implies that the subscriber: -

- Verified the information published;
- Acknowledged the Certificate is accurate; and
- Accepted the issued Certificate.

4.4.1. Conduct constituting Certificate acceptance

i. The following conduct constitutes Certificate acceptance by the subscriber:

- Download of the Certificate from the given source; and
- Failure to object to the Certificate or its content within five (5) days after issuance.
- Prior certificate acceptance, subscribers are advised to verify and confirm that the certificate is valid and not revoked or suspended.

4.4.2. Publication of the Certificate by the CA

i. RAFFTECH Certificates SHALL be published in a publicly available repository.

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

i. RAFFTECH MAY include RA when sending notification on issuance of the Certificate.

4.5. KEY PAIR AND CERTIFICATE USAGE

i. Authorized RAFFTECH personnel acting in the role of CA SHALL generate and store Certificate key pairs exclusively using a trustworthy method within a protected HSM environment.

4.5.1. Subscriber Private Key and Certificate Usage

i. Subscribers are contractually obligated to protect their Private Keys from unauthorized use or disclosure, discontinue using a Private Key after expiration or revocation of the associated Certificate, and use Certificates in accordance with their intended purpose.

ii. End entity/Leaf Certificate key pairs are always generated and stored within a protected HSM environment during the key generation process.

4.5.2. Relying Party Public Key and Certificate Usage

i. The relying party SHALL be solely responsible for determining whether reliance on a digital signature to be verified by the Certificate in question is acceptable. Any such reliance is made solely at the risk of the relying party. If a relying party determines that use of the Certificate is appropriate, the relying party must utilize appropriate software and/or hardware to perform digital signature verification as a condition of relying on the Certificate.

ii. Unless otherwise stated in this CPS, before any act of reliance, relying parties MUST independently:

- Verify the Certificate are used for an appropriate purpose that is not prohibited or otherwise restricted by this CPS;
- Assess the status of the Certificate and all the Certificates in the chain that issued the Certificates relevant to the Certificate in question;
- Rely on a RAFFTECH Certificate ONLY for legal and authorized purposes that are consistent with the values listed under key usage field in the Certificate;
- Assume responsibility to check the status of RAFFTECH Certificate using one of the required or permitted mechanisms set forth in the CP/CPS (see Section 4.9), and agreeing to terms of RAFFTECH Relying Party Agreement (RPA) as a condition of relying on the Certificate.

iii. Unless otherwise stated in this CPS, before any act of reliance on a time stamp token, relying parties MUST independently:

- Verify that the time stamp token has been correctly signed and that the private key used to sign the time stamp token has not been compromised prior to the time of the verification;
- Take into account any limitations on the usage of the time stamp token indicated by the time stamp policy; and
- Take into account any other precautions prescribed in this CPS or elsewhere.

4.6. CERTIFICATE RENEWAL

i. This section describes the procedures for Certificate renewal. Certificate renewal is the issuance of a new Certificate to replace an old one prior to its expiration. Only the validity dates and the serial number (the field in the Certificate, not the DN attribute) are changed. The public key and all other information remain the same.

4.6.1. CIRCUMSTANCE FOR CERTIFICATE RENEWAL

i. Revoked, suspended or expired Certificates shall not be renewed. The subscriber must apply for a new Certificate and replace the Certificate that has been revoked.

ii. A Certificate may be renewed if the public key has not reached the end of its validity period, the associated private key has not been compromised, and the subject name and attributes are unchanged. The new validity period of the renewed Certificate will not extend past the maximum lifetime of the original key.

iii. RAFFTECH initiates Certificate renewal process based on the Certificate expiration date and to ensure uninterrupted coverage, the validity interval of the new (renewed) Certificate SHALL overlap that of the previous Certificate by one (1) week.

iv. Certificate renewal will incorporate the same public key as the previous Certificate, unless the private key has been reported as compromised (see Section 4.9.1). If a new key pair is being used, the stipulations of Section 4.6 will apply.

4.6.2. WHO MAY REQUEST RENEWAL

i. The subscriber or RAFFTECH may initiate the renewal process. RAFFTECH adheres to the procedures listed in Section 3.2.1 ensuring that the requester is the legitimate entity who owns the private key of the Certificate being renewed.

ii. A natural person or Legal Entity to whom a RAFFTECH Certificate is issued and who is legally bound by RAFFTECH Subscriber Agreement (SA) or Terms of Use/Service under which an individual or organization acts as a subscriber MAY request for Certificate renewal at least Thirty (30) days before its expiration date.

4.6.3. Processing Certificate Renewal Requests

i. RAFFTECH Certificate renewal procedures are the same as the initial Certificate issuance;

4.6.4. Notification of New Certificate Issuance to Subscriber

i. The procedure in Section 4.3.2 applies here.

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

i. The procedure in Section 4.4.1 applies here.

4.6.6. Publication of the Renewal Certificate by the CA

i. As specified in Section 4.4.2, all certificates SHALL be published in RPKI Repository.

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

i. Notification of certificate issuance is provided to all entities by methods included in Section 4.4.3

4.7. CERTIFICATE RE-KEY

i. No stipulation.

4.7.1. Circumstance for Certificate Re-Key

i. No stipulation.

4.7.2. Who May Request Certification of a New Public Key

i. No stipulation.

4.7.3. Processing Certificate Re-Keying Requests

i. No stipulation.

4.7.4. Notification of New Certificate Issuance to Subscriber

i. No stipulation.

4.7.5. Conduct Constituting Acceptance of A Re-Keyed Certificate

i. No stipulation.

4.7.6. Publication of The Re-Keyed Certificate by the CA

i. No stipulation.

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

i. No stipulation.

4.8. CERTIFICATE MODIFICATION

i. This control is not applicable as RAFFTECH does not practice Certificate modification in RPKI.

4.8.1. Circumstance for Certificate Modification

i. No stipulation.

4.8.2. WHO MAY REQUEST CERTIFICATE MODIFICATION

i. No stipulation.

4.8.3. PROCESSING CERTIFICATE MODIFICATION REQUESTS

i. No stipulation.

4.8.4. NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

i. No stipulation.

4.8.5. CONDUCT CONSTITUTING ACCEPTANCE OF MODIFIED CERTIFICATE

i. No stipulation.

4.8.6. PUBLICATION OF THE MODIFIED CERTIFICATE BY THE CA

i. No stipulation.

4.8.7. NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

i. No stipulation.

4.9. CERTIFICATE REVOCATION AND SUSPENSION

i. RAFFTECH shall use reasonable efforts to publish clear guidelines for revoking Certificates, and maintain a 24/7 ability to accept and respond to revocation requests. The identification of the subscriber who applies for a revocation or suspension of a Certificate is carried out according to an internal documented procedure.

4.9.1. CIRCUMSTANCES FOR REVOCATION

i. RAFFTECH Certificate SHALL be revoked when the information in the Certificate is known to be suspected or compromised or at the request of the authorized entity. It includes following situations:
   - The associated private key is known to be compromised or misused.
   - The associated private key is suspected to be compromised or misused.
   - The subscriber's information in the Certificate has changed.
   - The subscriber is known to have violated his obligations.
   - The authenticated requester requested the Certificate revocation.

4.9.2. WHO CAN REQUEST REVOCATION

i. The following entities can request the revocation of a Certificate:
   - The entity who originally made the Certificate request.
   - The entity which can prove its current responsibility for a certified machine or service.
   - Any entity which demonstrates the compromise or misuse of a Certificate.
   - Any entity which demonstrates the change of subscriber's data.
   - The issuing CA or the associated RA.

4.9.3. PROCEDURE FOR REVOCATION REQUEST

i. In case where RAFFTECH-CA can independently confirm that the Certificate has been compromised or misused, RAFFTECH-CA SHALL revoke the compromised Certificate, even if the request to do so comes from an unauthenticated source and/or the holder of the Certificate is unreachable.

ii. Subscriber MAY submit a request to RAFFTECH-CA or its appointed RA for a Certificate revocation. RAFFTECH-CA SHALL authenticate the revocation request and try to contact the subscriber before revoking the Certificate. If the subscriber is temporarily unreachable, the Certificate SHALL be temporarily suspended.

iii. If the revoked Certificate is a CA Certificate, RAFFTECH-CA SHALL inform the subscribers and in addition SHALL terminate the Certificate and CRLs distribution service for Certificates/CRLs issued using the compromised private key.

4.9.4. REVOCATION REQUEST GRACE PERIOD

i. A subscriber is required to request revocation as soon as possible after the need for revocation has been identified.

ii. RAFFTECH-CA or its appointed RA SHALL respond within three (3) business working days (excluding weekends and public holidays) to revocation requests. It SHALL however handle revocation requests with the highest priority as soon as the request is recognized as such.

4.9.5. TIME WITHIN WHICH CA MUST PROCESS THE REVOCATION REQUEST

i. RAFFTECH-CA SHALL process a revocation request within 24 Hours.

4.9.6. REVOCATION CHECKING REQUIREMENT FOR RELYING PARTIES

i. As per RFC 6484, a relying party is responsible for acquiring and checking the most recent, scheduled CRL from the issuer of the Certificate, whenever the relying party validates a Certificate.

4.9.7. CRL ISSUANCE FREQUENCY

i. CRLs issued by RAFFTECH-CA are renewed every 24 hours even when there are no change in the status of a subscriber's Certificates.

ii. Each CRL SHALL contains a nextUpdate value. A new CRL SHALL be published at or before that time. RAFFTECH-CA will set the nextUpdate value when it issues a CRL, to signal when the next scheduled CRL will be issued.

4.9.8. MAXIMUM LATENCY FOR CRLS

i. RAFFTECH CRLs shall be published within one (1) hour after generation to its RPKI repository.

4.9.9. ON-LINE REVOCATION/STATUS CHECKING AVAILABILITY

i. On-line revocation/status checking of Certificates is available on a continuous basis by CRL and optionally OCSP. RAFFTECH-CA SHALL provide online Certificate status checking service through OCSP protocol. RAFFTECH-OCSP services provide a real time Certificate status inquiry. By using appropriate software at the relying parties' site, it is possible to obtain information about the Certificate status at any specific time.

ii. RAFFTECH-OCSP responses conforms to RFC 6960 and/or RFC 5019. RAFFTECH-OCSP responses shall be signed by RAFFTECH-CA that issues the Certificates whose revocation status is being checked either.

4.9.10. ON-LINE REVOCATION CHECKING REQUIREMENTS

i. RAFFTECH-CA SHALL support OCSP capability using the GET and POST methods for Certificates issued in accordance with this CPS. Should the OCSP responder receives a request for status of a Certificate serial number that is "unused", then the responder will not respond with a "good" status.

ii. The CRL and the OCSP response are included in the Certificate to support software applications that perform automatic Certificate status checking.

4.9.11. Other Forms of Revocation Advertisements Available

i. RAFFTECH does not provide any other forms of Certificate status service other than CRL and Online Certificate Status Protocol (OCSP).

4.9.12. Special Requirements Related to Key Compromise

i. No stipulation.

4.9.13. Circumstances for Suspension

i. This control is not applicable as RAFFTECH does not support Certificate suspension under this CPS.

4.9.14. Who Can Request Suspension

i. This control is not applicable as RAFFTECH does not support Certificate suspension under this CPS.

4.9.15. Procedure for Suspension Request

i. This control is not applicable as RAFFTECH does not support Certificate suspension under this CPS.

4.9.16. Limits on Suspension Period

i. This control is not applicable as RAFFTECH does not support Certificate suspension under this CPS.

4.10. CERTIFICATE STATUS SERVICES

i. RAFFTECH-CA only issue CRLs and supports Online Certificate Status Protocol (OCSP) but doesn't not support the Server-Based Certificate Validation Protocol (SCVP).

4.10.1. Operational Characteristics

i. RAFFTECH Certificate status information is available via CRL and OCSP responder RFC 2560. The serial number of a revoked Certificate remains on the CRL until one additional CRL is published after the end of the Certificate's validity period. Revocation entries on a CRL or OCSP Response SHALL NOT be removed until after the Expiry Date of the revoked Certificate

4.10.2. Service Availability

i. RAFFTECH-CA operates and maintains its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions. Certificate status services are available on a continuous basis.

4.10.3. Optional Features

i. No stipulation.

4.11. END OF SUBSCRIPTION

i. RAFFTECH subscriber's subscription service ends if its Certificate expires or is revoked or if the applicable subscriber agreement expires without renewal.

4.12. KEY ESCROW AND RECOVERY

i. This control is not applicable as RAFFTECH does not practice key escrow and recovery under this CPS.

4.12.1. Key Escrow and Recovery Policy and Practices

i. This control is not applicable as RAFFTECH does not practice key escrow for recovery under this CPS.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

i. This control is not applicable as RAFFTECH does not practice session key recovery under this CPS.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

i. WebTrust and MCMC guideline are incorporated by reference as if fully set forth herein. RAFFTECH SHALL develop, implement, and maintain a comprehensive security program designed to:

- protect the confidentiality, integrity, and availability of Certificate data and Certificate management processes;
- protect against anticipated threats or hazards to the confidentiality, integrity, and availability of the data;
- protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of any Certificate data;
- protect against accidental loss or destruction of, or damage to, any Certificate data; and
- comply with all other security requirements applicable to RAFFTECH by law.

5.1. PHYSICAL CONTROLS

i. The RAFFTECH-CA infrastructure is located in a selected set of locations and operates from secure high computing cloud data centre facility. Detailed security procedures are set in place and followed that prohibit unauthorized access and entry into the areas of the facilities in which CA systems reside.

ii. RAFFTECH HSM unit's sits within a security cage in Tier III datacentres, Activation Data are stored in a fireproof safe within the CA containment to which only RAFFTECH-authorized personnel have access. Access to these facilities is restricted to personnel in Trusted Roles.

5.1.1. Site Location and Construction

i. RAFFTECH-PKI systems are located in a selected set of locations which have been evaluated for their physical security, as well as local legal considerations that may affect RAFFTECH-CA operations. RAFFTECH-PKI systems are operated within a physically protected environment to deter, detect, and prevent unauthorized use of, access to, or disclosure of sensitive information.

ii. RAFFTECH-RA operates within a secured environment protecting their equipment and/or system from unauthorized access. RA SHALL implement physical access controls to reduce equipment and records tampering.

5.1.2. Physical Access

i. RAFFTECH CA systems are afforded physical security by virtue of being located within Maxis data centre. Only selected RAFFTECH staff have access to the data centre. The RAFFTECH staff responsible for CA operation are issued key cards that grant access to RAFFTECH-CAGE in the data centre.

ii. RAFFTECH has in place appropriate physical security controls to restrict access to all sensitive hardware and software used for providing PKI Services. Access to such hardware and software is limited to those personnel performing in a trusted role as described in Section 5.2.1 Access to the server room is controlled by badge and/or biometric readers restricted by security doors that can only be accessed by the authorized personnel followed by two layers of biometric locks to reach Root CA containment. Finally, the security of all the server rack is maintained using a physical lock. Such access controls are electronically monitored for unauthorized intrusion at all times. Only authorized personnel will be allowed access, either physical or logical, to RAFFTECH-PKI systems.

iii. RAFFTECH-PKI System operates virtually on Maxis HDC Cloud. Within the same datacentre, a 3-layer secure Cage protected by dual physical access controls and anti-pass back holds cryptographic module HSM units and remote terminal for the CA system.

5.1.3. POWER AND AIR CONDITIONING

i. The external data centres that host the RAFFTECH CA servers and cryptographic module are powered by a UPS (uninterruptible power supply) system and a backup generator system, guaranteeing at least 96 hours of power in the event of loss of power. The room containing this equipment makes use of N+1 Computer Room Air Conditioning (CRAC) systems to control temperature and relative humidity.

5.1.4. WATER EXPOSURES

i. RAFFTECH SHALL take necessary measures such as raised flooring and humidity monitoring system to protect critical systems for the PKI operation premises from any kind of water damage or water exposure.

5.1.5. FIRE PREVENTION AND PROTECTION

i. RAFFTECH SHALL ensure that the facility is equipped with fire detection alarms and protection equipment. Fire suppression for the external data centre that hosts the RAFFTECH CA computers and cryptographic modules is provided by an inert gas suppression system.

5.1.6. MEDIA STORAGE

i. All media containing production software and data, audit, archive, or backup information are stored securely within RAFFTECH-Cage in a safety box and/or in a secure off-site storage facility with appropriate physical and logical access controls designed to limit access to authorized personnel and protect such media from accidental damage (e.g., water, fire, and electromagnetic/static).

ii. System backup is via VM-level snapshots, which are performed once every twenty-four (24) hours, seven days, and four weeks. Access to the backup infrastructure are restricted to selected staff of the cloud service provider.

5.1.7. WASTE DISPOSAL

i. RAFFTECH takes reasonable steps to ensure that all media used for the storage of information such as keys, or its files are sanitized or destroyed before they are released for disposal. Sensitive documents and materials are shredded before disposal. Cryptographic devices (tokens) are zeroed in accordance with the manufacturers' guidance prior to disposal.

5.1.8. Off-Site Backup

i. RAFFTECH maintains backup facilities for its public key infrastructure systems which also hold copies of the CA private keys for redundancy. RAFFTECH appointed Cloud Service Provider (CSP) performs continuous, offsite backups of critical system data, audit log data, and other information via network-accessible storage. Within 24 hours, all data are replicated and sent to the offsite backup facility. The backup facilities have security controls which are equivalent to those operated at the primary facility.

5.2. PROCEDURAL CONTROLS

i. RAFFTECH follows established, documented procedures and management practices implemented for all trusted and administrative personnel that provide reasonable assurance of the trustworthiness and competence of the members of the staff and of the satisfactory performance of their duties in the fields of the electronic signature-related technologies.

5.2.1. Trusted Roles

i. Any personnel who has access to or control over cryptographic operations of RAFFTECH PKI that involve issuance, use, and management of Certificates are considered as serving in a trusted role (“Trusted Role”). Such personnel include, but are not limited to, members of RAFFTECH-CA Operation Team. RAFFTECH designated several trusted roles for Certificate Authority operations listed below:

- **System Administrators: –** has full access to the CA server and the associated cryptographic module.
- **CA Engineer:** – authorized to design, operate, and maintain the PKI systems supporting the execution of PKI business and ensuring efficient and effective PKI operation.
- **RA Administrator: –** authorized to design, implement, operate, and maintain the customer & Certificate lifecycle processes.
- **Security Officer: –** authorized to design, implement, and maintain a secure PKI operation ensuring customer trust.
- **Key Manager: –** authorized to maintain and manage RAFFTECH-PKI CA cryptographic key lifecycle.
- **Customer Services Officers: –** authorized to design, develop / acquire, implement, operate and maintain the business applications, databases and reporting systems ensuring efficient and effective PKI business.

5.2.2. Number of Persons Required per Task

i. RAFFTECH implements dual custody control for critical CA functions which requires at least that two (2) people personnel in trusted roles using, at least, dual control in a physically secured environment.

5.2.3. Identification and Authentication for Each Role

i. RAFFTECH maintains controls to provide reasonable assurance that:

- A documented procedure for appointing individuals to Trusted Roles and assigning responsibilities to them is followed.
- Only personnel assigned to Trusted Roles have access to RAFFTECH-CA network system. Access to the RAFFTECH-CA network system are controlled via password-protected login over an SSH connection on the RAFFTECH VPN.
- Access to the CA server and cryptographic module using a combination of physical security key and password provided by Key Manager.
- Individuals in a Trusted Role act within the scope of such role when required for performing administrative tasks.
- Employees and contractors SHALL observe the principle of “least privilege” when accessing, or when configuring access privileges on, Certificate Systems.
- Trusted Roles use unique credential assigned to a single person for authentication to Certificate Systems.

5.2.4. ROLES REQUIRING SEPARATION OF DUTIES

i. RAFFTECH enforces "separation of duties" on the roles defined in Section 5.2.1 It is not permitted for any one person to serve the same following roles.

- System Administrator and CA Engineer.
- System Administrator and Key Manager.
- System Administrator and Security Officer.

5.3. PERSONNEL CONTROLS

i. Full-Time RAFFTECH staff may fulfil the trusted roles described in Section 5.2.1. Staff members are assigned to the roles only if supervisory personnel deem them to be sufficiently trustworthy and only after they have undergone in-house training for the role.

5.3.1. QUALIFICATIONS, EXPERIENCE, AND CLEARANCE REQUIREMENTS

i. RAFFTECH SHALL implement policies for verifying the identity and trustworthiness of its personnel. Furthermore, RAFFTECH evaluates the performance of its personnel to ensure that they perform their duties in a satisfactory manner.

ii. Prior to the engagement of a trusted personnel, initial investigation of all candidates is conducted to verify qualifications, experience, and clearance as per HR recruitment procedure. RAFFTECH SHALL make reasonable attempt to determine their trustworthiness and competence.

5.3.2. BACKGROUND CHECK PROCEDURES

i. RAFFTECH SHALL conduct background checking as per HR recruitment procedure. This includes the following:

- Confirmation of previous employment.
- Check of professional reference.
- Confirmation of the highest or most relevant educational degree obtained.
- Search of criminal records (if applicable).
- Check of credit/financial/insolvency records.

5.3.3. TRAINING REQUIREMENTS

i. RAFFTECH SHALL provide all its personnel with skills-training that covers basic PKI knowledge, authentication and vetting policies and procedures (including the CA's CP and/or CPS), common threats (including phishing and other social engineering tactics).

ii. RAFFTECH SHALL maintain records of such training and ensure that personnel entrusted with PKI duties maintains a skill level that enables them to perform such duties satisfactorily;

iii. RAFFTECH SHALL document that each Validation Authority personnel possesses the skills required by a task before allowing the Validation Authority personnel to perform that task; and

iv. RAFFTECH SHALL require all Validation Authority personnel to undergo security awareness training provided by the IT Security Officer on the information verification requirements outlined in these requirements.

5.3.4. Retraining Frequency and Requirements

i. Training awareness is conducted to make the trusted personnel aware of any significant change to the operations, and the executions of such plans are documented. Such changes are CA software or hardware upgrade, changes in automated security systems, and relocation of equipment.

ii. Periodic training, security awareness and any new technological changes training MAY also be conducted to establish continuity and updates in the knowledge of the personnel and procedures.

5.3.5. Job Rotation Frequency and Sequence

i. RAFFTECH personnel MAY undergo job rotation practices as per the Human Resources Policy & Procedure.

5.3.6. Sanctions for Unauthorized Actions

i. RAFFTECH MAY impose sanction on personnel for unauthorized actions, unauthorized use of authority, and unauthorized use of systems for the purpose of imposing accountability on a participant's personnel, as it might be appropriate under the circumstances. RAFFTECH MAY apply disciplinary measures on personnel violating provisions and policies within the CP, this CPS or CA related operational procedures.

5.3.7. Independent Contractor Requirements

i. Delegated third-party and contractors acting on behalf of RAFFTECH-PKI SHALL be subjected to the same process, procedure, assessment, security control and training as permanent RAFFTECH employees.

5.3.8. Documentation Supplied to Personnel

i. Documentation are made available to personnel, during initial training, retraining, or otherwise. Training are provided to RAFFTECH employees as necessary for them to perform competently in their job role.

5.4. AUDIT LOGGING PROCEDURES

i. Audit log files are generated for all events relating to the security of the CAs. The security audit logs are automatically collected or if not possible, a logbook, paper form, or other physical mechanism are used. All security audits logs, both electronic and non-electronic, are retained and made available during compliance audits. The security audit logs for each auditable event defined in this section shall be maintained in accordance with Section 5.5.2.

5.4.1. Types of Events Recorded

i. Audit logging procedures include event logging and audit systems, implemented for the purpose of maintaining a secure environment. Audit records events include but are not limited to the following:
   - Issuance of a Certificate
   - Renewal of a Certificate
   - Revocation of a Certificate
   - Publishing of a CRL

ii. RAFFTECH audit trail records SHALL contain:
   - The identification of the operation;
   - The data and time of the operation;
   - The identification of the Certificate involved in the operation;
   - The identification of the person that performed the operation; and
   - A reference to the request of the operation.

iii. Documents available include:

- Infrastructure plans and descriptions;
- Physical site plans and descriptions;
- Configuration of hardware and software; and
- Personnel access lists.

iv. Only authorized trusted personnel are allowed to perform archival. The log files should be properly protected by an access control mechanism. Backed up Log files and audit trails are made be available to independent auditors upon request.

5.4.2 FREQUENCY OF PROCESSING LOG

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

5.4.3. RETENTION PERIOD FOR AUDIT LOG

i. RAFFTECH SHALL retain audit logs for not less than ten (10) years from the date of the last entry or the date of issue, as stipulated in DSR 1998.

5.4.4. PROTECTION OF AUDIT LOG

i. RAFFTECH-CA Audit logs, whether in production or archived, are protected using both physical and logical access controls.

5.4.5. AUDIT LOG BACKUP PROCEDURES

i. The offsite backup capabilities described in Section 5.1.8 applies to audit logs with a retention period of 10 years. RAFFTECH maintains formal procedures to ensure that audit logs are backed up and retained for not less than ten years from the date of the last entry or the date of issue as stipulated in DSR 1998.

5.4.6. AUDIT COLLECTION SYSTEM (INTERNAL VS. EXTERNAL)

i. Audit processes are initiated at system start up and finish only at system shutdown. The audit collection system ensures the integrity and availability of the data collected. If necessary, the audit collection system protects data confidentiality. In the case of a problem occurring during the process of the audit collection RAFFTECH determines whether to suspend CA operations until the problem is resolved.

5.4.7. NOTIFICATION TO EVENT-CAUSING SUBJECT

i. Events that are deemed potential security issues involving the RAFFTECH-PKI are reported and investigated.

5.4.8. VULNERABILITY ASSESSMENTS

i. Anomalies indicating attempted breaches of RAFFTECH-PKI security are reported and investigated. From time to time, RAFFTECH security team SHALL perform Risk Assessment that:

- Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data.
- Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
- Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that RAFFTECH has in place to counter such threat

5.5. RECORDS ARCHIVAL

i. RAFFTECH archives all types of audit logs as set forth in Section 5.5.1, including other documents and information critical to understanding the historical security and performance of the CA's duties.

5.5.1. Types of Records Archived

i. RAFFTECH archives auditable data, Certificate application information including documentation supporting Certificate applications, CRL records.

5.5.2. Retention Period for Archive

i. RAFFTECH SHALL retain audit logs for not less than ten (10) years from the date of the last entry or the date of issue, as stipulated in DSR 1998.

5.5.3. Protection of Archive

i. Archives are created in such a way that they cannot be deleted or destroyed (except for transfer to long term media) within the period for which they are required to be held. Archive protection ensures that only trusted roles can perform operations without modifying integrity, authenticity, and confidentiality of the data. If the original media cannot retain the data for the required period, a mechanism to periodically transfer archived data to new media SHALL be defined.

5.5.4. Archive Backup Procedures

i. Backups are replicated daily and stored at RAFFTECH DR site, in a location which is different from the original online system. One backup SHALL be stored in a fire rated media safe. An offline backup is taken at the end of any key ceremony (with the exception of any encrypted material which is stored separately in line with key ceremony procedures).

5.5.5. Requirements for Time-Stamping of Records

i. All electronic archives shall be recorded with system time as they are created. Manual archives have a manually entered date and time. Irrespective of timestamping methods, RAFFTECH SHALL ENSURE all logs MUST indicate the time at which the event occurred

5.5.6. Archive Collection System (Internal or External)

i. RAFFTECH archival system is operated internally by authorized trusted personnel.

5.5.7. Procedures to Obtain and Verify Archive Information

i. Only authorized CA personnel SHALL have access to primary and backup archives. RAFFTECH MAY, at its own discretion, release specific archived information, following a formal request from a Subscriber, a Relying Party, or an authorized agent thereof.

5.6. KEY CHANGEOVER

i. RAFFTECH CA Certificate contains a validity period that is at least as long as that of any Certificate being issued under that Certificate. When RAFFTECH-CA changes keys, it SHALL follow the procedures described in RFC 6489.

ii. The period of maximum validity of RAFFTECH Certificates mentioned below unless otherwise mentioned in this CPS:

- Root CA Certificate are valid for **Twenty-Five (25) years**;
- Intermediate and/or Issuing CA Certificates are valid for **Ten (10) years**; and

5.7. COMPROMISE AND DISASTER RECOVERY

i. RAFFTECH-PKI is operated from redundant production sites. Should a disaster causes an outage at one site, RAFFTECH-PKI operations can be provided from an alternate location.

5.7.1. INCIDENT AND COMPROMISE HANDLING PROCEDURES

i. In the event that RAFFTECH-PKI computing resources, software, and/or data are corrupted or otherwise damaged, RAFFTECH SHALL assess the situation, including its impact on CA integrity and security, and take appropriate action. CA operations may be suspended until mitigation is complete. Subscribers may be notified if corruption or damage has a material impact on the service provided to them.

ii. RAFFTECH SHALL maintain an Incident Response Plan and a Disaster Recovery Plan, which set out the procedures necessary to ensure business continuity, to notify affected stakeholders, and to reasonably protect Application Software Suppliers, Subscribers, and Relying Parties in the event of a disaster, security compromise, or business failure. RAFFTECH annually tests, reviews, and updates its business continuity plan and its security plans and makes them available to its auditors upon request.

5.7.2. COMPUTING RESOURCES, SOFTWARE, AND/OR DATA ARE CORRUPTED

i. RAFFTECH establishes the necessary measures to ensure full recovery of the service, in an appropriate time frame depending on the type of disruption, in case of a disaster, corrupted servers, software or data.

5.7.3. ENTITY PRIVATE KEY COMPROMISE PROCEDURES

i. In the event RAFFTECH Private Keys is compromised or suspected of being compromised, RAFFTECH will:

- Immediately cease using the compromised key material;
- Revoke all Certificates signed with the compromised key;
- Take commercially reasonable steps to notify all Subscribers of the Revocation; and

ii. Once the compromised key material has been replaced and a secure operation of the CA in question has been established, RAFFTECH-CA may re-issue the revoked Certificates following the procedure for initially providing the Certificates.

5.7.4. BUSINESS CONTINUITY CAPABILITIES AFTER A DISASTER

i. Should RAFFTECH primary operation site security is affected due to natural or other disaster, RAFFTECH shall invoke business continuity/disaster recovery procedure and execute the procedure activating its alternate facility.

ii. The disaster recovery plan deals with the business continuity as described in Section 5.7.1. Certificate status information systems should be deployed so as to provide 24 hours per day, 365 days per year availability.

5.8. CA OR RA TERMINATION

i. In the event that it is necessary to terminate the operation of Certificate Authorities (CA), RAFFTECH SHALL notify Malaysian Communications and Multimedia Commission (MCMC) and announce to the public at least 3 months in advance. RAFFTECH will plan and coordinate the termination process with its Subscribers and Relying Parties, such that the impact of the termination is minimized. RAFFTECH will make commercially reasonable effort to provide prior notice to Subscribers and Relying Parties and preserve relevant records for a period of time deemed fit for functional and legal purposes.

6. TECHNICAL SECURITY CONTROLS

6.1. KEY PAIR GENERATION AND INSTALLATION

i. RAFFTECH SHALL have effective practices and controls in place to reasonably assure that the generation of Root, Intermediate and/or Issuing CA key pairs are performed in a physically secured environment, using cryptographic modules that meet the requirements of Section 6.2, by multiple Trusted Role personnel, following a prepare generated script, and either witnessed in-person or validated from a recorded video of the ceremony by a Qualified Auditor.

6.1.1. KEY PAIR GENERATION

i. RAFFTECH generates Key Pairs pursuant to formal key generation procedures and inside of a FIPS 140-2 Level 3 certified Hardware Security Module from where the private key cannot be extracted in plaintext.

ii. The Key Pairs created/generated that are used as Root CA Key Pairs, RAFFTECH SHALL:

- ensure only personnel in trusted roles under the principles of multiple person control and split knowledge;
- generate the CA keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in RAFFTECH Certificate Policy and/or Certification Practice Statement;
- Ensure key generation activities are logged; and
- Maintain effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in its Certificate Policy and/or Certification Practice Statement and (if applicable) its Key Generation Script.

6.1.2 PRIVATE KEY DELIVERY TO SUBSCRIBER

i. RAFFTECH, upon generating a key pair using a hardware cryptographic module for the subscriber, SHALL ensure that:

- it uses a secure protocol that incorporates adequate safeguards and security features for the distribution or transmission of the private key to the subscriber.
- no copy of the subscriber's private key is retained or otherwise kept by the licensed certification authority.
- alternative out-of-band communication method shall be identified to deliver password for the private key.

6.1.3 PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER

i. No Stipulation.

6.1.4 CA PUBLIC KEY DELIVERY TO RELYING PARTIES

i. RAFFTECH CA public keys are made available from the online Repository at https://www.rafftech.my/repository. Additionally, the public keys of RAFFTECH root CAs are delivered through their inclusion into the root programs of software such as ADOBE AATL.

6.1.5 KEY SIZES

i. To prevent cryptanalytic attacks, all RAFFTECH CAs use key sizes and cryptographic protocols which adhere to NIST recommendations and to the applicable provisions of this CPS.

ii. Certificates issued under RAFFTECH-CA hierarchy SHALL meet the following minimum requirements:

KEY ALGORITHM	VALUES
Digest Algorithm	SHA-256, SHA-384, SHA-512
Minimum RSA Modulus Size (bits)	2048
ECC Curve	NIST P-256, P-384, OR P-512
Figure 6.1.5.a	Digital Signature Algorithm (DSA) key lengths (L and N) are described in the Digital Signature Standard, FIPS 186-4 (http://csrc.nist.gov/publications/pubsfips.html).

6.1.6 PUBLIC KEY PARAMETERS GENERATION AND QUALITY CHECKING

i. RAFFTECH-CA SHALL generate Private Keys using secure algorithms and parameters based on current research and industry standards.

ii. Quality checks for both RSA and ECC algorithms are performed on generated CA keys.

iii. RAFFTECH performs cryptographic functions within a HSM device that conforms to FIPS 186-2 and provides random number generation and on-board generation of up to 4096 bit RSA Public Keys and a wide range of ECC curves.

6.1.7 KEY USAGE PURPOSES (AS PER X.509 V3 KEY USAGE FIELD)

i. RAFFTECH includes Key Usage and Extended Key Usage fields in Certificates as defined in the Certificate profile.

ii. Private Keys corresponding to Root Certificates SHALL NOT be used to sign Certificates except in the following cases:

- Self-signed Certificates to represent the Root CA itself;
- Certificates for Intermediate and/or Issuing CAs and Cross Certification;
- Certificates for infrastructure purposes (i.e. internal CA operational device Certificates); and
- Certificates for OCSP Response verification.

6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

i. RAFFTECH implements physical and logical security controls to prevent the unauthorized issuance of a Certificate. The CA Private Key MUST be protected outside of the validated system or device specified above, using physical security, encryption, or a combination of both, and be implemented in a manner that prevents its disclosure. RAFFTECH SHALL encrypt the Private Key with an algorithm and key-length that 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

i. RAFFTECH-CA protects all generated Private Keys in cryptographic modules that meet at least one of the following:

- Certified to FIPS 140-1 or 140-2, Level 3 (or higher)
- Certified to ISO/IEC 19790, Level 3 (or higher)
- Certified to EAL4 (or higher) of the CWA 14169 or EN 14169 Protection Profile under the Common Criteria (ISO/IEC-15408) framework

ii. CA key pairs are generated and protected by validated FIPS 140-2 level 3 hardware cryptographic modules that meet industry standards for random and prime number generation.

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

i. RAFFTECH authentication mechanisms are protected securely when not in use and may only be accessed by actions of multiple trusted persons.

ii. Backups of CA Private Keys are securely stored in a fireproof safe. The activation of a backed-up CA Private Key (unwrapping) requires the same security and multi person control as when performing other sensitive CA Private Key operations.

6.2.3. Private Key Escrow

i. RAFFTECH does not escrow its signature keys and does not provide Subscriber key escrow.

6.2.4. Private Key Backup

i. Backup copies of CA Private Keys SHALL be backed up by multiple persons in Trusted Role positions and only be stored in encrypted form on cryptographic modules that meet the requirements specified in Section 6.2.1. and stored into a fireproof safe box.

6.2.5. Private Key Archival

i. RAFFTECH does not provide keys archiving.

6.2.6. Private Key Transfer Into or From a Cryptographic Module

i. All keys SHALL be generated by and in a cryptographic module. Private Keys are exported from the cryptographic module only for backup purposes. The private keys will never leave the module except in encrypted form for backup and/or transfer to a new module.

6.2.7. Private Key Storage on Cryptographic Module

i. RAFFTECH Private Keys are generated and stored inside cryptographic modules which meet the requirements of Section 6.2.1.

6.2.8. Method of Activating Private Key

i. Cryptographic modules used for CA Private Key protection utilize a smart card-based activation mechanism by multiple Trusted Role personnel using multi-factor authentication.

6.2.9. Method of Deactivating Private Key

i. No Stipulation.

6.2.10. Method of Destroying Private Key

i. CA Private Keys SHALL be destroyed when they are no longer needed or when the Certificates, to which they correspond, expire or are revoked. The destruction process shall be performed by multiple Trust Role personnel and documented using verifiable methods.

6.2.11. Cryptographic Module Rating

i. Refer to Section 6.2.1.

6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1. PUBLIC KEY ARCHIVAL

i. Copies of CA and Subscriber Certificates and Public Keys SHALL be archived in accordance with Section 5.5.

6.3.2. CERTIFICATE OPERATIONAL PERIODS AND KEY PAIR USAGE PERIODS

i. For Certificates issued after the publication of this CPS, the following operational periods SHALL be deployed.

RAFFTECH CERTIFICATES	CERTIFICATE VALIDITY
Root CA Certificates	25 years
Intermediate / Issuing CA Certificates	10 years
CRL and OCSP responder signing Certificates	02 years
Time Stamping Authority Certificates	10 years

FIGURE 6.3.2.a

6.4. ACTIVATION DATA

i. Activation data (secret shares) used to protect the tokens containing RAFFTECH Root CA, Intermediate and/or Issuing CA Private Key are generated in accordance to Section 6.2.2.

6.4.1. ACTIVATION DATA GENERATION AND INSTALLATION

i. RAFFTECH-CA SHALL protect activation data from compromise or disclosure. Appropriate cryptographic and physical access controls shall be implemented to prevent unauthorized use of any CA Private Key activation data.

6.4.2. ACTIVATION DATA PROTECTION

i. RAFFTECH Issuing CA activation data is protected from disclosure through a combination of cryptographic and physical access control mechanisms. RAFFTECH activation data is stored on smart cards.

6.4.3. OTHER ASPECTS OF ACTIVATION DATA

i. RAFFTECH activation data may only be held by RAFFTECH personnel in trusted roles.

6.5. COMPUTER SECURITY CONTROLS

6.5.1. SPECIFIC COMPUTER SECURITY TECHNICAL REQUIREMENTS

i. RAFFTECH-PKI systems SHALL be secured from unauthorized access using multi-layer security controls such as follows:

- Provide discretionary access control with least privilege and authenticate the identity of users before permitting access to the system or applications;
- Generate and archive audit records for all transactions;
- Require use of cryptography for session communication;
- Provide means to maintain software and firmware integrity;
- Enforce domain isolation for security critical processes and support recovery from system failure.

6.5.2. COMPUTER SECURITY RATING

i. No Stipulation

6.6. LIFECYCLE TECHNICAL CONTROLS

6.6.1. SYSTEM DEVELOPMENT CONTROLS

i. RAFFTECH system development controls are as follows:

- Commercial off-the shell software that was designed and developed under a formal and documented development methodology.
- Hardware SHALL be inspected during commissioning process to ensure conformity to supply, and no evidence of tampering found. Hardware and software procured are purchased in a fashion to reduce the likelihood that any particular component was tampered.
- Hardware and software are dedicated to performing CA activities. Ensure there are no other applications, hardware devices, network connections, or component software installed which are not part of the CA operation.
- Hardware and software updates are purchased or developed in the same manner as original equipment and are installed by trusted and approved personnel in a defined manner.

6.6.2. SECURITY MANAGEMENT CONTROLS

i. The configuration of RAFFTECH-PKI systems as well as any modifications and upgrades are documented and controlled by RAFFTECH Security Team. There is a mechanism for detecting unauthorized modification to RAFFTECH-PKI software or configuration. A formal configuration management methodology is used for installation and on-going maintenance of RAFFTECH systems. RAFFTECH software, when first loaded, is checked as being that supplied from the vendor, with no modifications, and is the version intended for use.

6.6.3. LIFE CYCLE SECURITY CONTROLS

i. RAFFTECH maintains a maintenance scheme to ensure the level of trust of software and hardware that are evaluated and certified.

6.7. NETWORK SECURITY CONTROLS

i. CA systems SHALL reside in highly segmented networks constrained from both the Internet and corporate networks via multiple levels of firewalls. Interaction with outside entities shall only be performed with servers located in a demilitarized zone (DMZ). All networks associated with CA operations SHALL be monitored by a network intrusion detection system. All systems associated with CA activities shall be hardened with services restricted to only those necessary for CA operations. Changes SHALL be documented and approved via a change management system. Logical and physical access to CA systems security cage requires two trusted and qualified RAFFTECH employees.

6.8. TIME-STAMPING

i. Certificates, CRLs, and other revocation database entries SHALL contain time and date information. RAFFTECH-PKI components are regularly synchronized with a reliable MALAYSIAN time service (SIRIM) to establish the correct time for:

- initial validity time of a CA Certificate.
- revocation of a CA Certificate.
- posting of CRL updates; and
- issuance of Subscriber end entity Certificates.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1. CERTIFICATE PROFILE

7.1.1. VERSION NUMBER(S)

i. RAFFTECH SHALL issue Certificates that are compliant with X.509 Version 3.

7.1.2. CERTIFICATE EXTENSIONS

i. RAFFTECH X.509 v3 Certificates provide methods for associating additional attributes with users or Public Keys and for managing the certification hierarchy. Each extension in a Certificate is designated as either critical or non-critical.

ii. Certificate extensions, their criticality, and cryptographic algorithm object identifiers, are provisioned according to the IETF RFC 5280 standards and/or comply with WebTrust guidelines.

7.1.2.1 RAFFTECH ROOT CA CERTIFICATE

i. Root CAs SHALL ensure that the content of the Certificate Issuer Distinguished Name field matches the Subject DN of the Issuing CA to support Name chaining, as specified in RFC 5280.

7.1.2.2 RAFFTECH INTERMEDIATE AND/OR ISSUING CA AND SUBSCRIBER CERTIFICATE

i. RAFFTECH Intermediate and/or Issuing CA and Subscriber Certificates MAY include extensions and values that are pertinent for their intended use, in accordance with this CPS and RFC 5280, and the WebTrust guideline.

7.1.3. ALGORITHM OBJECT IDENTIFIERS

i. RAFFTECH Algorithm OIDs conforms to RFC 3279 and RFC 3280. The following algorithm applies to RAFFTECH Certificates.

ALGORITHM NAME	OID
SHA256WithRSAEncryption	1.2.840.113549.1.1.112
SHA384WithRSAEncryption	1.2.840.113549.1.1.122
SHA512WithRSAEncryption	1.2.840.113549.1.1.132
ECDSA-With-SHA1	1.2.840.10045.4.12
ECDSA-With-SHA256	1.2.840.10045.4.3.22
ECDSA-With-SHA384	1.2.840.10045.4.3.32
ECDSA-With-SHA512	1.2.840.10045.4.3.42

Figure 7.1.3.a

7.1.4. NAME FORMS

i. RAFFTECH SHALL issue Certificates with Name Forms in accordance with RFC 5280 and Section 3.1.1 of this CPS.

7.1.5. NAME CONSTRAINTS

i. RAFFTECH reserve the right to issue Certificates with Name Constraints and mark them as critical, where necessary. Unless otherwise documented in this CPS the use of Name Constraints SHALL conform to the X.509 V3 standard RFC 5280 and the WebTrust Principles and Criteria for Certification Authorities guideline.

7.1.6. CERTIFICATE POLICY OBJECT IDENTIFIER

i. RAFFTECH SHALL issue Certificate with policy Object Identifier (OID) in accordance with RFC 3039 as set forth in Section 1.2 herein of this CPS.

7.1.7. USAGE OF POLICY CONSTRAINTS EXTENSION

i. RAFFTECH certificates Policy constraints should be supported as per RFC 3280.

7.1.8. POLICY QUALIFIERS SYNTAX AND SEMANTICS

i. RAFFTECH MAY populate X.509 Version 3 Certificates with a policy qualifier within the Certificate Policies extension. Generally, such Certificates contain a CPS pointer qualifier that points to the applicable Relying Party Agreement or the RAFFTECH CPS. In addition, some Certificates may contain a User Notice Qualifier that points to the applicable Relying Party Agreement.

7.1.9. PROCESSING SEMANTICS FOR THE CRITICAL CERTIFICATE POLICIES EXTENSION

i. No stipulation.

7.2. CRL PROFILE

7.2.1. VERSION NUMBER(S)

i. RAFFTECH SHALL issue CRL Certificates that are compliant with X.509 V2 Certificate Revocation List (CRL). The version number of Certificate revocation list in accordance with the RFC 5280 will be specified the value of version to be 2.

7.2.2. CRL AND CRL ENTRY EXTENSIONS

i. RAFFTECH supports and uses the following CRL and CRL entry extensions:

- CRL Number: monotonically increasing sequence number for each CRL issued by the CA; and
- X509v3 CRL Reason Code: non-critical extension, carrying the revocation reason code as specified in RFC 3647.

7.3. OCSP PROFILE

7.3.1. VERSION NUMBER(S)

i. OCSP version indicates the version of the protocol. The version number of OCSP in accordance with IETF RFC 6960 “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP” will be specified the value of version to be 1.

7.3.2. OCSP EXTENSIONS

i. RAFFTECH OCSP profile SHALL support CRL extensions defined in IETF RFC 6960 “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP”.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

i. RAFFTECH SHALL at all times:

- Be licensed as a CA in each jurisdiction of operation, where required, for the issuance of Certificates.
- Operate its PKI and issue Certificates in accordance with all applicable laws and guidelines in every jurisdiction of operation.
- Comply with the audit requirements set forth in this Section.
- Comply with these requirements

8.1. FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

i. On an annual basis, RAFFTECH retains an independent auditor listed by the Office of the Controller who assesses the CA's operations complies to the stated requirements and practices of this CPS, the CP as required by Section 20 of the DSA 1997 and the WebTrust for CA guidelines.

8.2. IDENTITY/QUALIFICATIONS OF ASSESSOR

i. The annual performance audit will be performed by the qualified auditors registered with the Office of the Controller. Please refer to www.skmm.gov.my for further details.

8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

i. The entity that performs the annual audit SHALL be completely independent of RAFFTECH and shall not have any kind of relationship that could derive in any conflict of interest.

8.4. TOPICS COVERED BY ASSESSMENT

i. Each audit shall include, but is not limited to, compliance with RAFFTECH's CP and WebTrust standards for Certification Authorities. The operational practices of RAFFTECH-CA and its RA functions is audited to ensure compliance with the DSA and DSR. These requirements may vary as audit schemes are updated.

8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY

i. Based on the information gathered in the audit, the qualified auditor shall categorise RAFFTECH's compliance as one of the following:

a) full compliance, if RAFFTECH complies with, amongst others, all the requirements of the DSA, DSR and the WebTrust standards for Certification Authorities;

b) substantial compliance, if RAFFTECH appears to comply generally with the requirements of the DSA, DSR and the WebTrust standards for Certification Authorities;

c) partial compliance, if RAFFTECH appears to comply with some of the requirements of the DSA, DSR and the WebTrust standards for Certification Authorities but was not found to have complied with or not to be able to demonstrate with one or more important safeguards; or

d) Non-compliance, if RAFFTECH: i. complies with a few or none of the requirements of the DSA, DSR and the WebTrust standards for Certification Authorities ii. fails to keep adequate records to demonstrate compliance with more than a few requirements; or iii. refuses to submit to an audit.

ii. If an audit reports a material non-compliance with the applicable law, this CPS, or any other contractual obligations related to RAFFTECH's services, then:

- The auditor will document the discrepancy;
- The auditor will promptly notify RAFFTECH; and
- RAFFTECH will develop a plan to cure the noncompliance.

iii. RAFFTECH will submit the plan to the management for approval and to any third party that RAFFTECH is legally obligated to satisfy. RAFFTECH may require additional action if necessary to rectify any significant issues created by noncompliance, including requiring suspension of Certificate issuance to the Subscriber.

8.6. COMMUNICATION OF RESULTS

i. As per Regulation 43 of the DSR 1998, the results of the annual audit shall be reported to the Office of the Controller by the qualified auditor within (14) four-teen days from the completion of a compliance audit. All information not considered public domain by RAFFTECH is to be kept confidential.

8.7. SELF-AUDITS

i. RAFFTECH MAY perform self-audits of its PKI business practices, in accordance with its CPS, the RAFFTECH-PKI Services CP, and the respective WebTrust Principles and Criteria for Certification Authorities.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. FEES

ii. As per the licence condition, the cost of RAFFTECH digital certificate is according to specific classes and is subjected to be approved by MCMC. In general, the fees levied are as shown below:

SERVICES	FEES LEVIED
Class 1	Not more than RM50
Class 2	Not more than RM120
Class 3	Not more than RM3400

The final cost of using the digital signature may vary depending on application requirements, the type of class used, the type of services offered, as well as the hardware and software that may be involved.

9.1.1. CERTIFICATE ISSUANCE OR RENEWAL FEES

i. RAFFTECH reserves the right to charge Subscribers fees for Certificate issuance and renewals of Certificates. The fees and any associated terms and conditions shall be made clear to the end-users or Subscribers by RAFFTECH when an application is made.

9.1.2. CERTIFICATE ACCESS FEES

i. RAFFTECH does not charge for making a Certificate available in its repository.

9.1.3. REVOCATION OR STATUS INFORMATION ACCESS FEES

I. RAFFTECH does not charge a fee to Relying Parties for access to revocation or status information in accordance with Section 2.

ii. RAFFTECH PKI Services reserves the right to charge a fee for providing customized CRLs or other value-added revocation and status information services.

9.1.4. Fees for Other Services

i. RAFFTECH does not charge a fee for accessing this CPS. However, any use of the CPS for purposes other than viewing the document, including reproduction, redistribution, modification, or creation of derivative works, MAY subject to a license agreement with the entity holding the copyright to the document.

9.1.5. Refund Policy

i. RAFFTECH does not practice refunds. However, if a Certificate contains information different than that on the application due to causes by RAFFTECH or the RA, a new Certificate shall be issued free of charge.

9.2. FINANCIAL RESPONSIBILITY

9.2.1. Insurance Coverage

i. RAFFTECH maintains insurance or self-insures in accordance to Office of the Controller DSA-Licensing-Guidebook and other applicable regulatory requirements.

ii. RAFFTECH shall only be liable for the issued Certificates not exceeding the amount as per the reliance limit in this CPS Section 9.8.

9.2.2. Other Assets

i. No stipulation

9.2.3. Insurance or Warranty Coverage for End-Entities

i. No stipulation

9.3. CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1. Scope of Confidential Information

i. Sensitive RAFFTECH PKI Services information shall remain confidential to RAFFTECH PKI Services. The following information is considered confidential to RAFFTECH PKI Services and may not be disclosed:

- RAFFTECH PKI Services policies, procedures and technical documentation supporting this CPS;
- Subscriber registration records, including: Certificate applications, whether approved or rejected, proof of identification documentation and details;
- Certificate information collected as part of the registration records, beyond that which is required to be included in Subscriber Certificates;
- Audit trail records;
- Any Private Key within the RAFFTECH PKI Services CA hierarchy; and
- Compliance audit results except for WebTrust for CAs audit reports which may be published at the discretion of Office of the Controller.

ii. All information above shall not be released unless required by law as per Section 9.4.6 of this CPS.

9.3.2. Information Not Within the Scope of Confidential Information

i. Information and documents not expressly deemed confidential under Section 9.3.1 shall be considered neither confidential nor private. Certificates, CRLs and customer guides related to user Certificate life cycle, CP and CPS are deemed public documents. This section is subject to applicable privacy laws.

ii. This CPS, Certificates and CRLs issued by RAFFTECH-CA and any information that has explicitly authorized to disclose are not considered confidential.

9.3.3. Responsibility to Protect Confidential Information

i. RAFFTECH shall be responsible to protect all confidential information and no person or third party other than the authorised personnel of RAFFTECH is allowed to access any of the Confidential Information.

ii. RAFFTECH-PKI participants receiving private information shall secure it from compromise and disclosure to third parties.

9.4. PRIVACY OF PERSONAL INFORMATION

9.4.1. Privacy Plan

i. RAFFTECH shall adhere to its privacy policy which is made available at: https://www.rafftech.my

9.4.2. Information Treated as Private

i. 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 a reasonable degree of care and appropriate safeguards.

9.4.3. Information Not Deemed Private

i. Information about Subscribers that is publicly available through the content of the issued Certificate and CRLs is deemed not private, subject to applicable laws.

9.4.4. Responsibility to Protect Private Information

i. RAFFTECH shall handle private information in strict confidence and meet the requirements of the applicable laws in Malaysia. All private information is securely stored and protected against accidental disclosure.

9.4.5. Notice and Consent to Use Private Information

i. Unless otherwise stated in this CPS, the applicable Privacy Policy or private information will not be used without the consent of the party to whom that information applies. This section is subject to applicable privacy laws.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

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

9.4.7. Other Information Disclosure Circumstances

i. No stipulation.

9.5. INTELLECTUAL PROPERTY RIGHTS

i. The following are the property of RAFFTECH:

- This CPS;
- Policies and procedures supporting the operation of RAFFTECH-PKI Services;
- Certificates and CRLs issued by RAFFTECH-PKI Services managed CAs;
- Distinguished Names (DNs) represent entities within the RAFFTECH-PKI Services CA hierarchy; and
- CA infrastructure and Subscriber key pairs.

ii. RAFFTECH retains all 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.

iii. RAFFTECH-PKI participants acknowledge that RAFFTECH retains all Intellectual Property Rights in and to this CPS.

9.6. REPRESENTATIONS AND WARRANTIES

i. RAFFTECH warrants and promises to provide certification authority services substantially in compliance with this CPS and the relevant RAFFTECH Certificate Policies. RAFFTECH makes no other warranties or promises and has no further obligations to Subscribers or Relying Parties, except as set forth under this CPS.

9.6.1. CA REPRESENTATIONS AND WARRANTIES

i. 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 CPS and its CP.

ii. RAFFTECH-CA warrants that:

1. Each digital signature created using the private key corresponding to the public key listed in the Certificate is the digital signature of the Subscriber and the Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created;
2. Their private key is protected, and that no unauthorized person has ever access to the Subscriber's private key;
3. All representations made by the Subscriber in the Certificate Application the Subscriber submitted are true;
4. All information supplied by the Subscriber and contained in the Certificate is true;
5. The Certificate is being used exclusively for authorized and legal purposes, consistent with this CPS; and
6. The Subscriber is an end-user Subscriber and not a CA and is not using the private key corresponding to any public key listed in the Certificate for purposes of digitally signing any Certificate (or any other format of certified public key) or CRL, as a CA or otherwise.

* Subscriber Agreements may include additional representations and warranties.

9.6.2. RA REPRESENTATIONS AND WARRANTIES

i. 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.

ii. RAs warrant that:

1. There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate;
2. There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application as a result of a failure to exercise reasonable care in managing the Certificate Application;
3. Their Certificates meet all material requirements of this CPS; and
4. Revocation services (when applicable) and use of a repository conform to the applicable CPS in all material aspects.

* Subscriber Agreements may include additional representations and warranties.

9.6.3. SUBSCRIBER REPRESENTATIONS AND WARRANTIES

i. 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 fulfil all obligations stipulated under this CPS and its CP.

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

iii. Subscribers warrants that:

1. Each digital signature created using the private key corresponding to the public key listed in the Certificate is the digital signature of the Subscriber and the Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created;
2. Their private key is protected, and that no unauthorized person has ever had access to the Subscriber's private key;
3. All representations made by the Subscriber in the Certificate Application submitted are true;
4. All information supplied by the Subscriber and contained in the Certificate is true,
5. The Certificate is being used exclusively for authorized and legal purposes, consistent with this CPS; and
6. The Subscriber is an end-user Subscriber and not a CA and is not using the private key corresponding to any public key listed in the Certificate for purposes of digitally signing any Certificate (or any other format of certified public key) or CRL, as a CA or otherwise.

* Subscriber Agreements may include additional representations and warranties.

9.6.4. RELYING PARTY REPRESENTATIONS AND WARRANTIES

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

ii. Relying Party Agreements require Relying Parties to acknowledge that they have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in a Certificate, that they are solely responsible for deciding whether or not to rely on such information, and that they shall bear the legal consequences of their failure to perform the Relying Party obligations in terms of this CPS.

* Relying Party Agreements may include additional representations and warranties.

9.6.5. REPRESENTATIONS AND WARRANTIES OF OTHER PARTICIPANTS

i. No stipulation.

9.7. DISCLAIMERS OF WARRANTIES

i. Except as expressly stated herein or to the extent permitted by law, RAFFTECH disclaims all other warranties and obligations, express and implied with respect to this CPS and its CP.

9.8. LIMITATIONS OF LIABILITY

9.8.1. CA LIABILITY

i. To the extent that RAFFTECH has issued and managed the Certificate(s) in compliance with the CP and CPS, RAFFTECH shall have no liability to the Subscriber, Relying Party and/or any third party for any damages or losses suffered as a result of the use or reliance on such Certificate(s) except where expressly provides for it. RAFFTECH shall only be liable for the issued Certificates to an amount not exceeding the following:

CERTIFICATE CLASS	RELIANCE LIMIT/LIABILITY CAP
Class 1 Individual	**RM2,000.00**
Class 2 Individual	**RM25,000.00**
Class 2 Organisation	**RM50,000.00**
Class 3 Individual	**RM50,000.00**
Class 3 Organisation	**RM100,000.00**

Figure 9.8.1.a

9.8.2. RA LIABILITY

i. RAs shall be subjected to the same liabilities as applicable to RAFFTECH as stipulated in Section 9.8.1. Or as set out in any of the agreements between the authorised RAs and RAFFTECH.

9.8.3. SUBSCRIBER'S LIABILITY

i. Subscriber's liability shall be as set forth in the applicable Subscriber Agreements.

9.9. INDEMNITIES

i. Indemnification of RAFFTECH by subscriber

- By accepting a Certificate, a subscriber undertakes to indemnify RAFFTECH for any loss or damage caused by issuance or publication of the Certificate in reliance on (i) a false and material representation of fact by the subscriber; or (ii) the failure by the subscriber to disclose a material fact.
- Where RAFFTECH issued the Certificate at the request of one or more agents of the subscriber, the agent or agents personally undertake to indemnify RAFFTECH, as if they were accepting subscribers in their own right.

9.10. TERM AND TERMINATION

9.10.1. TERM

i. This version of CPS is valid and will remain in effect upon publication in our repository until replaced by a newer version and is published thereafter.

9.10.2. TERMINATION

i. This version of CPS is valid and will remain in effect upon publication in our repository until replaced by a newer version and is published thereafter.

9.10.3. Effect of Termination and Survival

i. Upon termination of this CPS, the effect of termination of this CPS or any of its newer versions will be communicated via publication on RAFFTECH's repository.

9.11. INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

i. Any notice, demand, or request pertaining to this CPS shall be communicated either using digitally signed messages consistent with this CPS, or in writing. RAFFTECH accepts notices related to this CPS at the locations specified in Section 2.2 Notices are deemed effective after the sender receives a valid and digitally signed acknowledgment of receipt from RAFFTECH. If an acknowledgement of receipt is not received within five days, the sender must resend the notice in paper form to the street address specified in Section 2.2 using either a courier service that confirms delivery or via certified or registered mail with postage prepaid and return receipt requested. RAFFTECH may allow other forms of notice in its Subscriber Agreements.

9.12. AMENDMENTS

9.12.1. Procedure for Amendment

i. RAFFTECH reserves the right to amend this CPS at any time. Any amendments made to the CPS will be published as a new version and all amendments made therein shall be recorded in the version history published in RAFFTECH's repository. The updates will supersede any designated or conflicting provisions of the referenced version of the CPS.

9.12.2. Notification Mechanism and Period

i. In the event that there are any changes or amendments to this CPS, these updates will be posted at RAFFTECH's repository at URL https://www.rafftech.my/repository under the CPS section. These amendments will become enforceable automatically upon publication to the website unless RAFFTECH explicitly states otherwise or issues a notice of withdrawal.

9.12.3. Circumstances Under Which OID Must Be Changed

i. Should RAFFTECH deem that the amendments to the specifications could affect the acceptability of the Certificates for specific purposes, the amendments will be notified to the users of the Certificates by updating the CPS.

9.13. DISPUTE RESOLUTION PROVISIONS

i. To the extent permitted by applicable law, Subscriber Agreement and the Relying Party Agreement, the parties are required to notify RAFFTECH and attempt to resolve disputes directly before resorting to any dispute mechanism. Every party, including RAFFTECH partners, the Subscribers and relying parties, shall submit to the jurisdiction of the Malaysian court of law.

9.14. GOVERNING LAW

i. This CPS complies with the Malaysian Law, i.e. Digital Signature Act 1997 (Act 562) and the Digital Signature Regulations 1998. Compliance with applicable law

9.15. COMPLIANCE WITH APPLICABLE LAW

i. RAFFTECH is responsible for ensuring compliance with the applicable legislation stated in Section 9.14 of this CPS.

9.16. MISCELLANEOUS PROVISIONS

9.16.1. ENTIRE AGREEMENT

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

9.16.2. ASSIGNMENT

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

9.16.3. SEVERABILITY

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

9.16.4. ENFORCEMENT (ATTORNEY'S FEE AND WAIVER OF RIGHTS)

i. RAFFTECH may seek indemnification and attorney’s fees from a party for damages, loses and expenses related to that party’s conduct. RAFFTECH’s failure to enforce a provision of this CPS does waive its right to enforce the same provision later or right to enforce any other provision of this CPS.

9.16.5. FORCE MAJEURE

i. RAFFTECH shall not be liable for failure to perform any obligation under this CPS to the extent such failure is caused by a force majeure event (including acts of God, natural disasters, war, civil disturbance, action by governmental entity, strike and other causes beyond the party’s reasonable control). The party affected by the force majeure event will provide notice to the other party within a reasonable time and will use reasonable efforts to resume performance as soon as practicable. Obligations not performed due to a force majeure event, will be performed as soon as reasonably possible when the force majeure event ceases.

9.17. OTHER PROVISION

9.17.1. PERSONAL DATA

i. RAFFTECH are subjected to the PDPA Act 2010 (Act 709) and registered and party with the Jabatan Perlindungan Data Peribadi (JPDP). All the obligations stipulated in the act are deemed to be accepted by all parties as final and will not be subjected to any other obligations. The personal data involved shall be protected under the law.

9.17.2. RIGHT TO AUDIT

i. RAFFTECH has been deemed been audited by its independent external auditor qualified under MCMC and shall not be subjected to any other audit requirements as stipulated by any other written law as it will be conflicting with the jurisdiction among government agencies i.e., MCMC and any other Commissions and legislations.

APPENDIX 1: TERMS DESCRIPTION

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	A set of rules that indicates the applicability of named certificate and PKI requirement wit common security requirements.
Certificate Revocation List (CRL)	A periodically issued list, digital signed by Certification Authority of identified certificate that has been revoked prior to its expiry dates.
Certification Authority	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	A document from a Certification Authority which describes its practice for issuing and managing certificates through its lifecycle.
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	An online database contained publicly disclosed PKI governance documents and certificates status information either in form or CRL or OCSP response.
Root CA	The top-level CA whose root certificate is distributed and issue Intermediate and/or Issuing CA certificate.
Intermediate and/or Issuing CA	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.
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. They are used to manage identity and security in internet communications and computer networking.

APPENDIX 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
RAFFTECH-CA	RAFFTECH Certification Authority
RAFFTECH-PKI	RAFFTECH Public Key Infrastructure
RAFFTECH-RA	RAFFTECH Registration Authority
RFC	Request for Comment (document published by IETF for guidelines)
TSA	Time Stamping Authority