RAFFTECH

Time- Stamping Authority Policy/ Practice Statement

Version 1.3

RFCA-RFDC-2300-TSAPPS

Effective Date: 18th April 2023

REVISION HISTORY

Date	Version	Description	Author
29 January 2019	1.0	Time-Stamping Policy/ Practice Statement ver 1.0	Internal Audit Department
1 August 2019	1.1	Time-Stamping Policy/ Practice Statement ver 1.1 - To include TSA termination plan	Internal Audit Department
10 November 2022	1.2	Time-Stamping Policy/ Practice Statement - Update Business Address	Business Compliance Department
18 April 2023	1.3	Time-Stamping Authority Policy/ Practice Statement Version 1.3 - To refine the document format. - Removed term that stating this document is for internal use as this document is made available for the public viewing. - Made global changes in order to be aligned with RAFFTECH CP/CPS and the information in RAFFTECH's website. - Updated Section 3.1 – Definition. - Updated Section 4.1 – to include MCMC Requirements for CA To be Recognised As A TSA document. - Updated Section 6.2, 6.3.1, 7.1.1 and 7.1.2 where the Subscriber Agreement and the Relying Party Agreement are as published in https://www.rafftech.my/wp/knowledge/ - Updated Section 7.1.2 RAFFTECH TSA Contact Information to be into a table.	Business Compliance Department

TABLE OF CONTENTS

1. INTRODUCTION

RAFFCOMM TECHNOLOGIES SDN. BHD. ("**RAFFTECH**") operates as a digital certificate services provision pursuant to the Digital Signature Act 1997 ("**DSA**") and Digital Signature Regulation 1998 ("**DSR**").

This document is the Time-Stamping Authority Policy/Practice Statement ("**TSAPPS**") prepared by RAFFTECH to describe the policies and rules to be followed in the course of activities of RAFFTECH's time stamping services. This policy ensures RAFFTECH as the Time Stamping Authority ("**TSA**") is conforming to the guidelines and principles established by Malaysian Communications and Multimedia Commission ("**MCMC**") to enable trust and confidence towards the date-time stamping services based on the applicable requirements stated in the **DSA (Part VI, Section 70)** and **DSR (Part IX, Regulation 58 – 70)**. This document is also based on the time-stamping protocol in RFC 5816 (update for RFC 3161).

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

This document specifies the policy and security requirements relating to the operation and management practices of RAFFTECH as the TSA in issuing qualified electronic time stamps. The requirement herein supports electronic signatures or for any application required to prove that a datum existed before a specific time.

The present document can be used by independent entities as the basis to confirm that RAFFTECH's TSA is a trusted entity for the issuance of qualified electronic time stamps in accordance with the DSA and the DSR.

The version number and date of this RAFFTECH TSAPPS document is provided herein on the cover page.

3. IDENTIFICATION AND AUTHENTICATION

This section contains a list of definitions for the defined terms and acronyms used within this document. Any additional definitions and abbreviations are provided under RAFFTECH CPS.

3.1 DEFINITIONS

Certificate Practice Statement ("CPS")	A statement of the practices, which a certificate authority applied in issuing and managing digital certificate, or for the provision of certificate applicability related to the digital signatures.
Coordinated Universal Time ("UTC")	Time scale based on the second as defined in recommendation by ITU-R TF.460-6. For all practical purposes, UTC is equivalent to the solar time average in the prime meridian (0°). More specifically, UTC is a compromise between the highly stable atomic time (Temps Atomic International - TAI) and the solar time derived from the irregular earth rotation. The UTC is the principal standard of the hour by which the world regulates clocks and the time.
Malaysia Standard Time ("MST")	Malaysia Standard Time (MST) is a standard time established and maintained by national metrology institute of Malaysia, which is eight (8) hours ahead of Greenwich Mean Time and Coordinated Universal Time.
Network Time Protocol ("NTP")	Network Time Protocol (NTP) is a networking protocol for clock synchronization of computer systems over network packet routing with variable latency. The standard for reference is the IETF RFC 1305 (Network Time Protocol (NTP v3).
Relying Party	The recipient of a time-stamp who relies and benefits from the time-stamping services.
Subscriber	The subscriber of the time-stamping service.
Time Stamp	A digitally signed notation append and/ or attach to a certificate, digital signature or message in proving the date, time and identify of person existed at the particular time.
Time-Stamping Authority ("TSA")	A Trust Service Provider (TSP) providing time-stamping services using one (1) or more time-stamping units.
Time-Stamping Unit ("TSU")	The set of hardware and software which is managed as a unit and has a single time-stamp signing key active at a time.

TSA Disclosure Statement	Set of statements about the policies and practices of a TSA which particularly require emphasis in the disclosure to the Subscribers and the Relying Parties, for example to meet regulatory requirements.
TSA System	Set of information technology products and components employed to provide support to the provision of time-stamping services.
x.509	The ITU- T standard for certificates and their corresponding authentication framework.

3.2 ABBREVIATIONS

CPS	Certificate Practice Statement
DRC	Disaster Recovery Center
DSA	Digital Signature Act 1997
DSR	Digital Signature Regulation 1998
GMT	Greenwich Mean Time
HSM	Hardware Security Module
MCMC	Malaysian Communications And Multimedia Commission
MST	Malaysia Standard Time
PKI	Public Key Infrastructure
RFC	Request For Comment (Document Published By IETF For Guidelines)
TAI	International Atomic Time
TSA	Time Stamping Authority
TSP	Trust Service Provider

TSAPPS	Time Stamping Authority Policy/ Practice Statement
TST	Time Stamping Token
TSU	Time Stamping Unit
UTC	Universal Time Clock

4. GENERAL CONCEPTS

4.1 CONCEPT AND GENERAL REQUIREMENTS

It follows the requirements established in the MCMC Requirements For Certification Authority (CA) To Be Recognised As A Time Stamping Authority (TSA) document and RAFFTECH's CPS which follows the Principles and Criteria for Certification Authorities Version 2.2.2 (Web Trust for CA) for generic policy requirements common to all Certification Authorities.

4.2 TIME-STAMPING SERVICES

The provision of time-stamping services is broken down in this document into the following component services for the purposes of classifying requirements:

- **Time-stamping provision**: This service component generates time-stamping token.
- **Time-stamping management**: The service component that monitors and controls the operation of the time-stamping services to ensure that the service provided is as specified in the CPS and this RAFFTECH TSAPPS document.

The RAFFTECH TSA adheres to the standards and regulations established in **Section 1** of this RAFFTECH TSAPPS document to keep trustworthiness of the time-stamping services for the Subscribers and the Relying Parties.

4.3 TIME-STAMPING AUTHORITY

The TSA has the overall responsibility for the provision of the time-stamping services identified in **Section 4.2** in this document. The TSA has responsibility over the operation of one (1) or more

TSUs which creates and signs on behalf of the TSA. The TSA responsible for issuing a time stamp that is identifiable.

RAFFTECH TSA hereby confirms that the TSA is audited at least every twelve (12) months by a conformity assessment body and deliver the assessment report as soon as it is received by the TSA. When the regulatory body requires the TSA to remedy any breach of the requirements, the TSA shall act accordingly in due course. The regulatory body shall be informed of any changes to the TSA provision.

RAFFTECH TSA may make use of other parties to provide parts of the time-stamping services. However, the TSA shall always maintain overall responsibility (as per **Section 4.2**) and ensures that the policy requirements identified in the present document are met.

RAFFTECH TSA may operate several identifiable time-stamping units.

RAFFTECH TSA issues time-stamps to the users of time-stamping services (i.e. the Subscribers as well as the Relying Parties). RAFFTECH TSA is identified in the TSU certificate(s) used for signing TST.

4.4 SUBSCRIBER

When the Subscriber is an organization, it comprises several end users or an individual end user and some of the obligations that apply to that organization must be applied to the end users. In any case, the organization will be held responsible if the obligations from the end users are not correctly fulfilled and therefore such organization is expected to suitably inform its end users.

When the Subscriber is an end user, the end user will be fully responsible if its obligations are not correctly fulfilled.

4.5 RELYING PARTY

A Relying Party is an individual or entity that acts in reliance of a TST generated under RAFFTECH TSA. A Relying Party may, or may not be a Subscriber of RAFFTECH TSA.

4.6 TIME-STAMPING POLICY AND TSA PRACTICE STATEMENT

4.6.1 PURPOSE

This RAFFTECH TSAPPS document is to be used in conjunction/ to be read together with the RAFFTECH CP/CPS.

This RAFFTECH TSAPPS document specifies a Time-Stamping Policy to meet general requirements for trusted time stamping services. The RAFFTECH CP/CPS specifies what and how these requirements are met (including personnel management, personnel selection, physical security, etc.).

4.6.2 LEVEL OF SPECIFICITY

This RAFFTECH TSAPPS document describes only general rules of issuing and managing TST. Detailed descriptions of the infrastructure and related operational procedures are described in additional documents that are not made publicly available.

These additional documents are only available to the authorized RAFFTECH personnel and, on a needs basis, to auditors of the TSA.

4.6.3 APPROACH

This RAFFTECH TSAPPS document defined independently the specific details of the specific operating environment of the RAFFTECH TSA, whereas RAFFTECH CP/CPS is tailored to the organizational structure, operating procedures, facilities, and computing environment of the RAFFTECH TSA.

5. TIME-STAMPING POLICIES

5.1 OVERVIEW

This RAFFTECH TSAPPS document is a set of rules used during issuing TST and regulating security level for the RAFFTECH TSA according to the MCMC requirement and guidelines for TSA.

TST's are issued with an accuracy of one (1) second or better.

The RAFFTECH time-stamping service signs the TST using private keys that are dedicated for that purpose. The profiles of the public key certificates used by the RAFFTECH TSA comply with the RFC 3161.

The RAFFTECH TSA benefits from the Public Key Infrastructure (PKI) that has been established and operated by RAFFTECH CA, including the certification service which allows RAFFTECH CA to issue the certificates of RAFFTECH TSA.

5.2 IDENTIFICATION

The object-identifier of the current policy is defined as follows:

Policy Identifier (OID)
1.3.6.1.4.1.51215.6

The OID is specified in every time-stamp issued by the TSA.

5.3 USER COMMUNITY AND APPLICABILITY

The current policy does not define any limitations on users or applicability of the services delivered. The RAFFTECH TSA can provide time-stamping services for electronic data to any user, including to the closed community.

5.4 CONFORMANCE

The RAFFTECH TSA uses the identifier for the current policy in TST as given in **Section 5.2 Identification**.

The RAFFTECH TSA ensures compliance of provided services with the regulations as specified in **Section 6.1 TSA Obligations** and ensures reliability of control mechanisms as described in **Section 7 Requirements on TSA practices**.

6. OBLIGATION AND LIABILITY

6.1 TSA OBLIGATIONS

6.1.1 GENERAL

This chapter includes all the obligations, liabilities, guarantees and responsibilities of the RAFFTECH TSA, its Subscribers and the Relying Parties. This obligations and responsibilities are described in the RAFFTECH Subscriber Agreement and RAFFTECH Relying Party Agreement published under https://www.rafftech.my/wp/knowledge/.

RAFFTECH guarantees that all the requirements of the RAFFTECH TSA, including procedures and practices related to the issuance of TST, review of system and security audit are in accordance with regulations described in **Section 7 Requirements on TSA Practices**.

6.1.2 TSA OBLIGATIONS TOWARDS SUBSCRIBERS

The Subscribers and the Relying Parties can access the time-stamping system on a twenty-four (24) hours a day and seven (7) days a week basis. Notwithstanding what is mentioned before, access to the time-stamping system could be disrupted due to maintenance windows, for each calendar month, the total time of unavailability of the time-stamping service, measured in minutes, cumulated over the whole month should not be more than 0.5% of the total number of minutes of that calendar month.

Moreover, RAFFTECH warrants that:

- It complies with this this RAFFTECH TSAPPS document and its amendments as published under https://www.rafftech.my/wp/knowledge/;
- It archives logging data of time-stamp issuance for a duration as legally required or in case no legal requirement would apply for at least seven (7) years starting from the time mentioned in the TST;
- The TSU maintain a minimum MST time accuracy of one (1) second or better;
- Its commercial activity is provided on the basis of reliable equipment and software;
- The activities and services provided are legal, in particular, they do not violate intellectual property, license and other related rights;
- Services delivered are conforming to generally accepted norms;

- High availability access to the time-stamping system is maintained except in case of planned maintenance or loss of time synchronization;
- Issued TST do not contain any false data and/ or mistakes;
- It will deliver, upon subscriber request, all elements that permit attestation of the reliability of date and time contained in the TST;
- That it will maintain a competent and experienced team that can ensure the continuity of the TSA;
- It will ensure continuous the physical and logical security, as well as the integrity of materials, software and databases required for the correct functioning of the TSA as described in the RAFFTECH CP/CPS;
- It will monitor and control the whole TSA infrastructure, in order to prevent or limit any disturbance or unavailability of the TSA resulting from deliberate attacks, as described in this RAFFTECH TSAPPS document and the RAFFTECH CP/CPS;
- It will take all measures required according to generally accepted norms to secure its services, in order to prevent outages of the TSA; and
- It will make available a back-up infrastructure that can be used in case of service interruption of the main infrastructure.

6.2 SUBSCRIBER OBLIGATIONS

The Subscribers retrieving TST, should verify the digital signatures posed by the RAFFTECH TSA on the TST.

Such verification comprises:

- Verification whether the signature on the TST is correct;
- Verification of the TSA certificate;
- Verification of the trusted path up to the trusted root certificate, and for each of the certificates in the chain (including the TSA certificate itself):

- Verification whether the certificate is not expired at the moment of signature; and
- Verification whether the certificate was not revoked or suspended at the moment of signature; and

- Additional Subscriber obligations are described in the RAFFTECH Subscriber Agreement published under https://www.rafftech.my/wp/knowledge/.

6.3 RELYING PARTY OBLIGATIONS

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

6.3.1 NEED FOR NAMES TO BE MEANINGFUL

Parties relying on TST, should verify the electronic signatures posed by the RAFFTECH TSA on the TST.

Such verification comprises:

- Verification whether the signature on the TST is correct;
- Verification of the TSA certificate;
- Verification of the trusted path up to the trusted root certificate, and for each of the certificates in the chain (including the TSA certificate itself); and
- Verification whether the certificate was not revoked or suspended at the moment of signature.

In case the Relying Party intends to rely on a TST where the TSA certificate has expired, he should only do so when a non-repudiation proof exists (e.g. another TST, or notary record) that guarantees that the TST did exist before expiry of the certificate and has not been changed since. This is specifically importance when the cryptographic functions or the TSA certificate key length of the TST are not considered secure anymore at the time the party intends to rely on the TST.

Additional Relying Party obligations are described in the RAFFTECH Relying Party Agreement published under https://www.rafftech.my/wp/knowledge/.

6.4 LIABILITY

RAFFTECH is only liable for damages to Subscribers or Relying Parties that result from RAFFTECH's failure to comply with the DSA and DSR. The RAFFTECH TSA must supply evidence that they have adhered to applicable laws, rules, and regulations.

RAFFTECH shall in no event be liable, for any loss of profits, indirect and consequential damages, or loss of data, to the extent permitted by applicable law. The RAFFTECH TSA shall not be liable for any damages resulting from infringements by the Subscriber or the Relying Party on the applicable terms and conditions, including the exceeding of the transaction limit.

RAFFTECH shall under no circumstances be liable for damages that result from force majeure events as detailed in **Section 7.6** of this RAFFTECH TSAPPS document and in **Section 9.16.5** of RAFFTECH CP/CPS. RAFFTECH shall take commercially reasonable measures to mitigate the effects of force majeure in due time. Any damages resulting from any delay caused by force majeure will not be covered by the RAFFTECH TSA.

7. REQUIREMENT OF TSA PRACTICES

RAFFTECH TSA shall operate its services in accordance with the rules established in this RAFFTECH TSAPPS document, RAFFTECH CP/CPS, and relevant internal document defining technical, operational and procedural requirements.

7.1 PRACTICE AND DISCLOSURE STATEMENTS

7.1.1 TSA PRACTICE STATEMENT

- Risk Assessment: The provision of the RAFFTECH TSA services is laid down in a more general context of the provision of trust (certification) services as ruled in the RAFFTECH CP/CPS. A risk assessment has been and is carried out in order to evaluate business assets and threats to those assets in order to determine the necessary security controls and operational procedures that have been taken in place.

- Procedures, control mechanisms and technical infrastructure described in **Section 7** of this RAFFTECH TSAPPS document are the basis of the RAFFTECH TSA function. Other controls are further described in the RAFFTECH CP/CPS.

- This RAFFTECH TSAPPS document and the RAFFTECH CP/CPS are available to the public and published on the RAFFTECH website https://www.rafftech.my/wp/knowledge/. This RAFFTECH TSAPPS document and the associated internal documents laid down the rules for the RAFFTECH TSA services operation.

- The terms and conditions regarding the use of the RAFFTECH TSA services are disclosed and made available to all subscribers and Relying Parties as specified in **Section 7.1.2** of this RAFFTECH TSAPPS document.

- Final authority and management of the RAFFTECH TSA services and its practices are ensured by RAFFTECH. Management committee of RAFFTECH shall ensure that the practices are properly implemented.

- The RAFFTECH TSA will give due notice of changes it intends to make in this RAFFTECH TSAPPS document. Any such changes will be subject to revision and approval by the management committee. The RAFFTECH TSA shall make the revised version immediately available.

7.1.2 TSA DISCLOSURE STATEMENT

THE RAFFTECH TSA shall disclose to all the Subscribers and the Relying Party regarding the terms and conditions of the use of its time-stamping services. The TSA Disclosure Statement from the RAFFTECH TSA is compliant with requirement from ETSI TS 102 023 and is included in the Subscriber Agreement and the Relying Party Agreement as published in https://www.rafftech.my/wp/knowledge/.

The RAFFTECH TSA contact information is:

Corporate Office	**Raffcomm Technologies Sdn. Bhd.**

	Company No.: 201001015711 (1000449-W) Lot 32.02, Level 32, Sunway Putra Tower No. 100, Jalan Putra, 50350 Kuala Lumpur Wilayah Persekutuan Kuala Lumpur, Malaysia
Website	https://www.rafftech.my/
General Line	+603 4040 0195
E-mail	hello@rafftech.my

Every TST issued by the RAFFTECH TSA includes the policy identifier, defined in **Section 5.2** of this RAFFTECH TSAPPS document. Cryptographic hash functions, used in the time-stamping process are in accordance with normative requirements. The expected validity of a TST is for a period of ten (10) years. Accuracy of the time, which is provided in a TST is regulated in **Section 6.1.2** of this RAFFTECH TSAPPS document. Limitations related with the TSA system have been defined in **Section 6.1.2** of this RAFFTECH TSAPPS document.

The Subscriber's obligations are described in **Section 6.2** of this RAFFTECH TSAPPS document. TST verification should be performed with the usage of appropriate software.

All TST will be archived for duration for at least seven (7) years, starting from the time stated in the TST. Liabilities are defined in **Section 6.4** of this RAFFTECH TSAPPS document.

Complaints, suggestions and remarks on THE RAFFTECH TSA services should be addressed to the RAFFTECH hotline using contact information in the table above.

Provision of the RAFFTECH TSA services are ruled by the Malaysian court of law.

7.2 KEY MANAGEMENT LIFECYCLE

7.2.1 TSA KEY GENERATION

The RAFFTECH TSA ensures that any cryptographic keys are generated under controlled circumstances and in accordance with general key pair generation and installation practices as described in **Section 6.1** of RAFFTECH CP/CPS.

The RAFFTECH TSA keys are generated within a Hardware Security Module (HSM) complying with FIPS 140-1 Level 3 in a physically secured environment, by personnel in trusted role in accordance with the RAFFTECH CP/CPS. The TSA key generation algorithm is described in **Section 4.0** of RAFFTECH TSA.

7.2.2 TSU PRIVATE KEY PROTECTION

The RAFFTECH TSA ensures that TSU private keys remain its confidentiality and integrity. The RAFFTECH TSA keys are generated, held and used within Hardware Security Module (HSM), complying with the FIPS 140-1 Level 3 in a physically secured environment, which can only be accessed by personnel in trusted roles in accordance with the RAFFTECH CP/CPS.

In case of a disaster, failure of the system or system conservation, the TSA key back-up and key recovery are to ensure it is in accordance with the procedurals of RAFFTECH CP/CPS.

7.2.3 TSU PUBLIC KEY DISTRIBUTION

The RAFFTECH TSA ensures that the integrity and the authenticity of the TSU signature verification (public) keys and any associated parameters are maintained during its distribution towards Relying Party. The RAFFTECH TSA certificates are published in the RAFFTECH website. RAFFTECH TSU certificates are issued by the RAFFTECH CA in accordance with the RAFFTECH CP/CPS.

7.2.4 REKEYING TSU KEYS

The lifetime of the RAFFTECH TSU certificates are not longer than the period of time of the chosen algorithm and the key length which are recognized as being fit for the purpose.

The RAFFTECH TSA rekey procedure is executed upon expiry of validity period of the certificate of the TSA in accordance with the RAFFTECH CP/CPS. Public keys are

archived for a minimum period of seven (7) years. Private key protection is in accordance with the RAFFTECH CP/CPS.

7.2.5 END OF TSU KEY LIFE CYCLE

The RAFFTECH TSA ensures that TSU private signing keys are not used beyond the end of their life cycle. In particular, operational and technical procedures are in place to ensure that a new key is put in place when a TSU's key expires, TSU private keys or any part, including any copies shall be destroyed such that the private key cannot be retrieved as in accordance with the RAFFTECH CP/CPS. TST generation system shall reject any attempt to issue a TST if the signing private key is expired.

7.2.6 LIFE CYCLE MANAGEMENT OF CRYPTOGRAPHIC MODULE TO SIGN TIME-STAMPS

The RAFFTECH TSA ensures the security of the HSM throughout its lifecycle. Procedure and controls are in place in accordance with the RAFFTECH CP/CPS, to ensure that TST signing cryptographic hardware (HSM) are not tampered with during shipment, while it is stored, that installation, activation and duplication of TSU's signing keys in HSM's shall be done only by personnel in trusted roles, in a physically secure environment, TST HSM's are functioning correctly, and that TSU private signing keys stored on TSU HSM's are erased upon device retirement.

7.3 TIME-STAMPING

7.3.1 TIME-STAMP TOKEN

The RAFFTECH TSA ensures that TST are issued securely and include the correct time. Every TST issued by the RAFFTECH TSA, shall include a unique identifier of the policy as described in **Section 5.2** of this RAFFTECH TSAPPS document. TST issued by The RAFFTECH TSA include date and time value traceable to the real MST time value. Accuracy of the time is defined in **Section 6.1.2** of this RAFFTECH TSAPPS document.

Each TST has a unique identifier and is signed using a key generated exclusively for the purpose. The TST shall include the policy ID of the TSU that created the timestamp and the TSA name (equal to the DN of the TSU Certificate).

7.3.2 CLOCK SYNCHRONIZATION WITH MST

The RAFFTECH TSA ensures that its clock is synchronized with MST within the declared accuracy. The RAFFTECH TSA incorporates the time in the TST with the accuracy described in **Section 6.1.2** of this RAFFTECH TSAPPS document.

The RAFFTECH TSA ensures and able to detect that if the time that would be indicated in a TST drifts or jumps out of synchronization with MST.

RAFFTECH has security controls in place to prevent unauthorized operation, aimed at calibration of the clock out of order, any manipulation or physical damage to the clock.

7.4 TSA MANAGEMENT AND OPERATION

7.4.1 SECURITY MANAGEMENT

The RAFFTECH TSA ensures that administrative and management procedures are applied adequately and parallel with recognized best practices. All requirements and subjects related to security management are implemented as described in the RAFFTECH CP/CPS.

7.4.2 ASSET CLASSIFICATION AND MANAGEMENT

The RAFFTECH TSA ensures that its information and other assets receive an appropriate level of protection. The description of methods and measures undertaken for affirmation of continuity and stability of TSA system operation is described in the RAFFTECH CP/CPS.

7.4.3 PERSONNEL SECURITY

The RAFFTECH TSA ensures that the personnel and the hiring practice enhance and support the trustworthiness of the TSA operations. Description of the personnel security

rules as well as the trusted roles used in the TSA services environment is provided in the RAFFTECH CP/CPS. Managerial and operational personnel possess the appropriate skills and knowledge of time-stamping, digital signatures and trust services as well as security procedures for personnel with security responsibilities, information security and risk assessment.

7.4.4 PHYSICAL AND ENVIRONMENTAL SECURITY

The RAFFTECH TSA ensures that physical access to critical services is controlled and physical risks to its assets minimized. The implementation of the physical environmental security is in accordance with the rules described in the RAFFTECH CP/CPS.

7.4.5 OPERATIONS MANAGEMENT

The RAFFTECH TSA ensures that the TSA system components are secured and correctly operated with minimal risk of failure.

The RAFTECH TSA possesses the procedures, processes and infrastructure ensure it is comply with the operational management and procedural security requirements as defined in the ETSI TS 102 023. The information of procedures, processes and infrastructure is classify as internal company documentation and will disclosed periodically to the TSA auditors only when it is requested.

7.4.6 SYSTEM ACCESS MANAGEMENT

The RAFFTECH TSA ensures that the TSA system access is limited to authorized individuals in accordance with RAFFTECH CP/CPS.

7.4.7 TRUSTWORTHY SYSTEM DEPLOYMENT AND MAINTENANCE

The RAFFTECH TSA ensures that it uses trustworthy systems and products that are protected against modifications in accordance with the RAFFTECH CP/CPS. Analysis of security requirements shall be carried out at the design and requirement specifications stage of any systems development project undertaken by the TSA or on behalf of the TSA to ensure that security is built into IT systems. Change control procedures shall be applied for releases, modifications and emergency software fixes of any operational software.

7.4.8 COMPROMISE AND DISASTER RECOVERY OF TSA SERVICES

The RAFFTECH TSA ensures that in the case of events which affects the security of the TSA services, including compromise of TSU private signing keys or detected loss of calibration, that relevant information is made available to subscribers and Relying Parties in accordance with the RAFFTECH CP/CPS.

7.4.9 TSA TERMINATION

The RAFFTECH TSA ensures that potential disruptions to Subscribers and Relying Parties are minimized as a result of the cessation of the TSA time-stamping services, and in particular ensures that continuous maintenance of information required to verify the correctness of time-stamp tokens.

In the event of termination, RAFFTECH shall notify the local TSA regulatory body and announce to the public at least three (3) months in advance. The RAFFTECH TSA shall not be issuing and deliver time-stamp tokens but shall destroy all the TSU private keys prior to the termination. RAFFTECH shall ensure the archive record are transferred to the appropriate TSA upon approval from local TSA regulatory body.

7.4.10 COMPLIANCE WITH LEGAL REQUIREMENT

The RAFFTECH TSA ensures compliance with appropriate legal requirements and is acting under the Malaysian law, regulations, and in particular the DSA and the DSR.

7.4.11 RECORDING OF INFORMATION CONCERNING OPERATION OF TIME-STAMPING SERVICE

The RAFFTECH TSA ensures that all relevant information concerning the operations of the RAFFTECH TSA time-stamping services is recorded for a defined period of time, in particular for the purpose of providing evidence for the purposes of legal proceedings, in accordance with the RAFFTECH CP/CPS.

7.5 ORGANIZATIONAL

The organization that maintains the RAFFTECH TSA is the same with that maintains RAFFTECH CA. The organizational, technical and security personnel are defined in the RAFTTECH CP/CPS and in accordance with relevant law and regulations as defined in this RAFFTECH TSAPPS document.

7.6 FORCE MAJEURE

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

7.7 DISPUTE RESOLUTION PROVISIONS

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