

RAFFTECH

**Time- Stamping Authority (TSA)
Disclosure Statement**

Version 2.3

RFCA-RFDC-2400-TSDS-002

Effective Date: 30th March 2023

REVISION HISTORY

Date	Version	Description	Author
17 th May 2018	1.0	Time-Stamping Authority Disclosure Statement Version 1.0	Internal Audit Department
17 th July 2018	2.0	Time-Stamping Authority Disclosure Statement Version 2.0	Internal Audit Department
1 st August 2019	2.1	Time-Stamping Authority Disclosure Statement Version 2.0 - To include general complaint procedures.	Internal Audit Department
10 th November 2022	2.2	Time-Stamping Authority Disclosure Statement Version 2.2 - Update 3.0 Rafftech Contact Info	Business Compliance Department
30 th March 2023	2.3	Time-Stamping Authority Disclosure Statement Version 2.3 - Removed term stating this document is for internal use as this document is made available for public viewing. - Amended the definitions of “Relying Party”, “Subscriber”. - Updated Section 3.0 Rafftech TSA Contact Info to be into a table. - Updated Section 10.0 Applicable Agreements and Practice Statement. - Inserted the definition of “Force Majeure”. - Made global changes in order to be aligned with RAFFTECH TSAPPS and CP/CPS.	Business Compliance Department

TABLE OF CONTENTS**TABLE OF CONTENTS**

1.0	VITAL UNDERSTANDING OF THIS TIME-STAMPING AUTHORITY (TSA) DISCLOSURE STATEMENT	1
2.0	ENTIRE AGREEMENT	1
3.0	RAFFTECH TSA CONTACT INFO	2
4.0	TIME-STAMPING TOKEN AND USAGE.....	2
5.0	RELIANCE LIMITS	2
6.0	OBLIGATIONS OF SUBSCRIBERS	3
7.0	TIME-STAMPING UNIT PUBLIC KEY STATUS CHECKING OBLIGATIONS OF RELYING PARTIES	3
8.0	RETENTION OF EVENT LOGS	4
9.0	LIMITED WARRANTY AND DISCLAIMER	4
10.0	APPLICABLE AGREEMENTS AND PRACTICE STATEMENT	5
11.0	PRIVACY POLICY	5
12.0	REFUND POLICY	5
13.0	APPLICABLE LAW, COMPLAINTS AND DISPUTE SOLUTION	5
14.0	TSA AND REPOSITORY LICENCES, TRUST MARKS AND AUDIT	6

1.0 VITAL UNDERSTANDING OF THIS TIME-STAMPING AUTHORITY (TSA) DISCLOSURE STATEMENT

This document is the Time-Stamping Authority (“**TSA**”) Disclosure Statement (“**TSA Disclosure Statement**”) prepared by RAFFCOMM TECHNOLOGIES SDN. BHD. (“**RAFFTECH**”). This document does not substitute or replace the RAFFTECH Time-Stamping Authority Policy & Practice Statement (“**RAFFTECH TSAPPS**”) or the RAFFTECH Certificate Policy/ Certification Practice Statement (“**RAFFTECH CP/CPS**”). In order to ensure the provisions of an eligible electronic time-stamping, the recipient of the time-stamping service must read through the RAFFTECH TSAPPS and the CP/CPS documents which is published at RAFFTECH’s website at <https://www.rafftech.my/wp/knowledge/>.

This TSA Disclosure Statement consists of a set of statement regarding time-stamping policies and procedures related to the Subscriber and Relying Party. In this document, subscriber is referring to the subscriber of the time-stamping service (“**Subscriber(s)**”) and the Relying Party refers to any party who relies and benefits from the time-stamping service (“**Relying Party**”).

This TSA Disclosure Statement shall highlight on the contractual relationship between the Subscriber, the Relying Party and RAFFTECH. This segment emphasises on warranty, obligation and responsibility of the time-stamping services. This document also explains in detail the commitments and assurances towards the Relying Party. For contractual purposes, this TSA Disclosure Statement and any other commercial contractual terms and conditions shall apply together.

This document envisioned is for only the use of RAFFTECH and its business. This version of the TSA Disclosure Statement has been approved by the management and is subject to amendment and change in accordance with the policies and procedures adopted by the management.

2.0 ENTIRE AGREEMENT

This TSA Disclosure Statement provides detailed disclosures regarding RAFFTECH Time-Stamping Authority (“**RAFFTECH TSA**”). This document does not replace or override the decisiveness of RAFFTECH Certificate Policy and RAFFTECH Certificate Policy Statement which are available at <https://www.rafftech.my/wp/knowledge/>.

3.0 RAFFTECH TSA CONTACT INFO

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

4.0 TIME-STAMPING TOKEN AND USAGE

The provisions of the RAFFTECH TSA is aligned with the requirements of the Digital Signature Act 1997 and Digital Signature Regulations 1998. Time-stamping services by RAFFTECH can be subscribed by individuals, corporate or any entities within a specific group who might need proof of data existence. RAFFTECH time-stamp services may also apply to any application requiring proof of data existence before a particular time.

Acceptable Time-Stamp Request Hashes include all SHA2 family including SHA256. Supported signing algorithm is sha256withRSAEncryption (2048-bit key length). The RAFFTECH digital signature on the time-stamping token (“**TST**”) has a validity period of ten (10) years. The information on how to verify TST can be referred to Section 7.0 herein. RAFFTECH may charge fees for the time-stamping services provided by the RAFFTECH TSA.

The object-identifier (“**OID**”) of the RAFFTECH-TSAPPS is: 1.3.6.1.4.1.51215.6. This OID is included in each generated time-stamp. This indicates RAFFTECH claims conformance to RAFFTECH TSAPPS.

5.0 RELIANCE LIMITS

The accuracy of time for RAFFTECH TSA time-stamping service is \pm one (1) second with respect to the Malaysia Standard Time (“**MST**”). RAFFTECH TSA will not issue time-stamp if the MST trusted time source cannot be acquired. Records for RAFFTECH TSA activity will be securely retained for at least seven (7) years for legal evidence purposes.

6.0 OBLIGATIONS OF SUBSCRIBERS

The Subscribers must verify that the TST has been correctly signed and check the RAFFTECH Certificate Revocation List (“CRL”) to confirm that the validity of the private key used to sign the TST has not been compromised. The software used by the Subscribers to create the time-stamp must be an approved software by RAFFTECH. The Subscribers undertake not to exceed the quota of the purchased time-stamp without liaising with RAFFTECH. The Subscribers must inform RAFFTECH of all IP address to be used in the event that the Subscribers wish to use more than the purchased quota. Subscribers must inform its Relying Party to comply with RAFFTECH-TSAPPS and CP/CPS.

7.0 TIME-STAMPING UNIT PUBLIC KEY STATUS CHECKING OBLIGATIONS OF RELYING PARTIES

When relying on a time-stamp, the Relying Party must verify that the TST has been correctly signed and the related TSU certificate has not been revoked. If the TST is verified during the TSU certificate validity period, the validity of the signing key can be checked by making sure that the TSU certificate has not been revoked. RAFFTECH CA certificates, TSU certificates, CRL and Online Certificate Status Protocol (“OCSP”) are published <https://www.rafftech.my/wp/knowledge/>. In the event that the verification takes place beyond the end of the validity period of the certificate, the time-stamp verification may be impossible because certification authorities are not obliged to publish revocation data of expired certificates, including the revocation due to key compromise. However, the time-stamp can be verified even when the validity period of the certificate is expired provided that at the moment of verification it can be known that:

- the TSU private key has not been compromised at any time up to the time that a Relying Party verifies a time-stamp;
- the hash algorithms used in the TST exhibit no collisions at the time of verification;
- the signature algorithm and signature key size under which the time-stamp has been signed;
- is still beyond the reach of cryptographic attacks at the time of verification; and
- the verification of a time-stamp can still be performed beyond the end of the validity period of the certificate from the TSU.

8.0 RETENTION OF EVENT LOGS

TSA event logs are retained for at least seven (7) years in accordance with the archive record for audit logs as stipulate in the RAFFTECH CP/CPS.

9.0 LIMITED WARRANTY AND DISCLAIMER

Provision of RAFFTECH time-stamping service is in accordance to the Digital Signature Act 1997, Digital Signature Regulations 1998, RAFFTECH TSAPPS, CP/CPS and the terms agreed by the Subscriber.

RAFFTECH TSA bear full liability towards the Subscriber for any losses occasioned by it to Subscriber unless RAFFTECH TSA proves that RAFFTECH TSA was not at fault. Liability for minor negligence is excluded for RAFFTECH TSA.

RAFFTECH TSA shall not in any event be liable for any loss of profits, loss of sales or turnover, loss or damage reputation, loss of contracts, loss of customers, loss of opportunity, loss of the use of any software or data, loss or use of any computer or other equipment may arise directly from breach of RAFFTECH TSAPPS or CP/CPS, wasted management or other staff time, losses or liabilities under or in relation to any other contracts, indirect, consequential, special, incidental or punitive loss, damage or expenses. The term “**loss**” means a partial loss or reduction in value as well as complete or total loss.

The Subscriber shall fully indemnify RAFFTECH TSA from all third party claims resulting from breach of contract or unlawful or improper use of the time-stamping service. The indemnification shall also include the obligation to hold RAFFTECH TSA fully harmless against legal costs occurred (e.g. procedural costs and legal fees).

RAFFTECH shall not be liable to the Subscriber or Relying Party for any loss, cost, expense and/ or damages that is a result from any Force Majeure events for any period when RAFFTECH is prevented from performing all or parts of its obligations. The term “**Force Majeure**” shall mean any event or circumstance beyond RAFFTECH’s reasonable control, including but not limited to the acts of god, natural disasters, earthquakes, floods, fires, epidemic, pandemic, quarantine restrictions, riots, wars, acts of terrorism, shipwrecks, strikes, freight embargoes, lockouts and government regulations, which materially and adversely affect the performance of RAFFTECH.

10.0 APPLICABLE AGREEMENTS AND PRACTICE STATEMENT

The following documents shall be applicable for the Subscriber and the Relying Party (as amended, varied or revised from time to time):

- RAFFTECH Certificate Policy
- RAFFTECH Certification Practice Statement
- RAFFTECH Time-Stamping Authority Policy & Practice Statement
- RAFFTECH TSA Disclosure Statement
- RAFFTECH Subscriber Agreement
- RAFFTECH Relying Party Agreement
- Privacy Policy
- Privacy Notice
- Term of Use
- Anti-Bribery and Anti-Corruption Policy

The above documents are published at <https://www.rafftech.my/wp/knowledge/>

11.0 PRIVACY POLICY

RAFFTECH manages the Subscriber and the Relying Party data and other information in compliance with the applicable personal data protection law in Malaysia, including but not limited to the Personal Data Protection Act 2010 (“**PDPA**”). We are committed to ensuring the confidentiality, protection, security and accuracy of personal data made available to us. For further information, please refer to RAFFTECH Privacy Policy and RAFFTECH Privacy Notice published at <https://www.rafftech.my/wp/knowledge/>.

12.0 REFUND POLICY

RAFFTECH does not refund fees for time-stamping services.

13.0 APPLICABLE LAW, COMPLAINTS AND DISPUTE SOLUTION

The objective of RAFFTECH TSA is to ensure the provision of the time-stamping service to support qualified digital signatures according to specific laws and regulations.

For any general inquiries, comments or complaints relating to the time-stamping issues may be channeled to RAFFTECH's dedicated email at info@cyphersign.my.

However, any claims between the two or more participants in the RAFFTECH CA (for this purpose, RAFFTECH shall be deemed as "participant within the RAFFTECH CA") shall submit to the jurisdiction of the Malaysia court of law in the manner as set out in the RAFFTECH CP/CPS.

14.0 TSA AND REPOSITORY LICENCES, TRUST MARKS AND AUDIT

The RAFFTECH TSA is subject to periodic internal audit and external audit. The external audit is performed annually by an independent external auditor to assess the RAFFTECH TSA compliance with ETSI standard and WebTrust requirements.