MALAYSIAN COMMUNICATIONS AND MULTIMEDIA COMMISSION

RECOGNITION FRAMEWORK FOR TIME STAMPING AUTHORITY (TSA)

(Effective 1st February 2018)

Table of Contents

1. Introduction

This document has been issued by the Malaysian Communications and Multimedia Commission ("MCMC") detailing the framework to recognise a Time Stamping Authority (TSA) that provides date time stamp services in Malaysia.

2. Scope

This document specifies the requirements for readiness assessment, operational effectiveness audit and annual compliance to be conducted by a registered auditor at establishment stage and operational stage for TSA to obtain and maintain the certificate of recognition.

The present document does not specify:

- The requirements for the time stamping protocol, token profiles, policy and security requirements relating to the operation and management practices of the TSA issuing time-stamps.

3. Terms and Definitions

3.1 Definitions

For the purposes of the present document, the following terms and definitions the following apply:

Certification Authority (CA): means a person who issues certificate

qualified auditor means a certified public accountant or an accredited computer security professional registered as a qualified auditor under, Regulation 41 of the Digital Signature Regulations 1998;

relying party: recipient of a time-stamp who relies on that time-stamp

subscriber: legal or natural person to whom a time-stamp is issued and who is bound to any subscriber obligations

time-stamp: data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time

"certified public accountant": public accountant registered under the Accountants Act 1967 [Act 94];

Time-Stamping Authority (TSA): License CA which issues time-stamps using one or more time-stamping units

Time-Stamping Unit (TSU): 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 CA that particularly require emphasis or disclosure to subscribers and relying parties, for example to meet regulatory requirements

TSA practice statement: statement of the practices that a TSA employs in issuing time-stamp

TSA system: composition of IT products and components organized to support the provision of time-stamping services

3.2 Abbreviations

For the purposes of the present document, the following abbreviation apply:

CA	Certification Authority
GMT	Greenwich Mean Time
IT	Information Technology
MCMC	Malaysian Communications and Multimedia Commissions
MST	Malaysia Standard Time
NMIM	National Metrology Institute of Malaysia
TAI	International Atomic Time
TSA	Time-Stamping Authority
TSU	Time-Stamping Unit
UTC	Coordinated Universal Time

3.3 Modal verbs terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described below:.

1. MUST This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.

2. MUST NOT This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.

3. SHOULD This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

4. SHOULD NOT This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.

5. MAY This word, or the adjective "OPTIONAL", mean that an item is truly optional.

4. General concepts

The overall aim of the recognition framework is to give confidence to all interested parties that the time stamping services provided by a Time Stamping Authority (TSA) fulfils the specified requirements set by MCMC.

Parties that have an interest in the recognition framework include, but are not limited to:

a) the TSA;

b) the subscribers of the time stamping services;

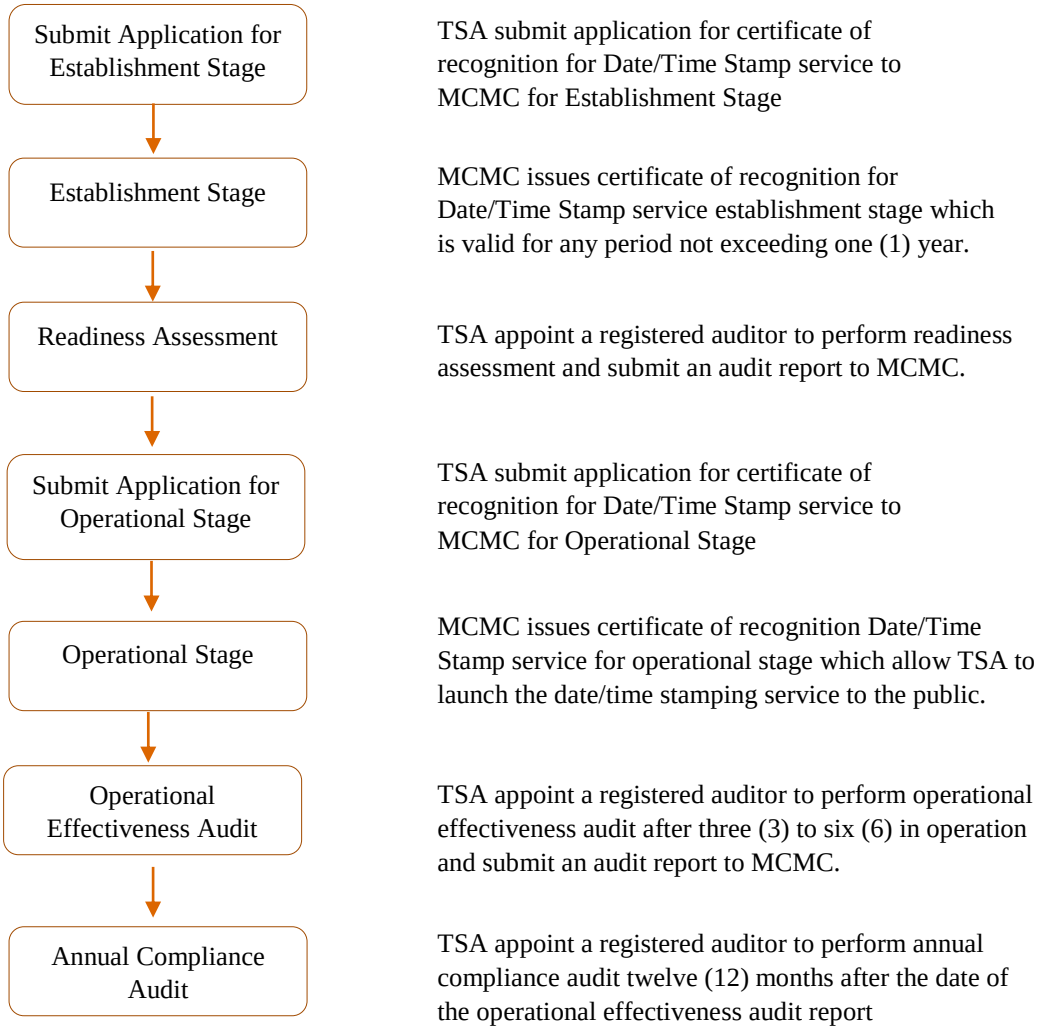
c) MCMC;

d) consumers and other members of the public.

Certificate of recognition is a means of providing assurance that the TSA comply with specified requirements for Certification Authorities (CA) to be recognised as a Time Stamping Authority (TSA).

5. Recognition Process Flow

The diagram below depicts the process for recognition of a Time Stamping Authority (TSA):



6. Application for Certificate of Recognition

TSA shall apply to MCMC for a certificate of recognition for date/time stamp service to establish a recognised TSA. An application to establish a recognise TSA shall be accompanied by the following information required under Digital Signature Regulations 65:

i) the particulars of the applicant;

ii) the anticipated operational costs and proposed financing;

iii) details of the personnel to be employed and their qualifications, if available;

iv) the proposed technology and operating procedure;

v) the services to be provided and the fees and charges to be imposed therefor; and

vi) such other information or document as MCMC may require.

7. Guidelines for Readiness Assessment

Prior the issuance of certificate of recognition for an operational stage, an independent readiness assessment shall be conducted by a Registered Auditor based on Requirements to be recognised as a Time Stamping Authority (TSA) for the purpose of ascertaining effectiveness of the control design of its security and trustworthiness.

The readiness assessment shall focus on the following areas:

i) the software,

ii) the hardware,

iii) technical components,

iv) algorithms,

v) standards

vi) other pertinent parameters

vii) other equipment to be used by the TSA

viii) Time Stamp Policies

ix) TSA Practise Statement

x) TSA Disclosure Statements

xi) TSA Obligation

xii) TSA Management and Operation

xiii) General Security and Controls

8. Guidelines for Operational Effectiveness Audit

After three (3) to six (6) months of the issuance of certificate of recognition for an operational stage, an operational effective audit shall be conducted by a Registered Auditor based on Principles and Criteria (Requirements) to be recognised as a Time Stamping Authority (TSA) for the purpose of ascertaining compliance to its security and trustworthiness.

9. Guidelines for Annual compliance audit

The operations of a recognised TSA shall be audited a least once a year to evaluate its compliance with the Principles and Criteria (Requirements) to be recognised as a Time Stamping Authority (TSA).

The following requirements defined in the Digital Signature Regulations 42. Procedure for annual compliance audit shall apply:

(1) The qualified auditor shall give the licensed certification authority at least seven days written notice before the qualified auditor carries out the annual compliance audit.
(2) The licensed certification authority shall make available any information, document or personnel as may be required by the qualified auditor.
(3) Based on the information gathered in the audit, the qualified auditor shall categorise the licensed certification authority's compliance as one of the following:
- *(a) full compliance, if the licensed certification authority appears to comply with all the requirements of the Act and these Regulations;*
- *(b) substantial compliance, if the licensed certification authority appears generally to comply with the requirements of the Act and these Regulations but one or more instances of non-compliance or of inability to demonstrate compliance were found in the audited sample, that were likely to be inconsequential;*
- *(c) partial compliance, if the licensed certification authority appears to comply with some of the requirements of the Act and these Regulations but was found not to have complied with or not to be able to demonstrate compliance with one or more important safeguards; or*
- *(d) non-compliance, if the licensed certification authority*
  - *(i) complies with few or none of the requirements of the Act or these Regulations;*
  - *(ii) fails to keep adequate records to demonstrate compliance with more than a few requirements; or*
  - *(iii) refused to submit to an audit.*

MCMC shall publish in the TSA disclosure record that it maintains for the recognised TSA concerned the date and result of the audit.

10. Criteria for Registered Auditors

The following requirements defined in the Digital Signature Regulations 41. Qualification and registration of auditors shall apply:

(1) A certified public accountant or an accredited computer security professional intending to act as a compliance auditor under section 20 of the Act shall satisfy the following requirements:
- *(a) holds such accreditation or qualification as the Controller may determine;*
- *(b) has at least two years experience in trusted computer information systems, trusted telecommunications networking environments and professional audit techniques;*
- *(c) has at least two years experience in digital signature technology, standards and practices; and*
- *(d) demonstrates knowledge of the requirements of the Act and these Regulations that satisfies the Controller.*

(2) A certified public accountant or an accredited computer security professional intending to act as a compliance auditor under section 20 of the Act shall apply in writing to the Controller to be registered as a qualified auditor.
(3) If the Controller is satisfied that the requirements under subregulation (1) have been complied with, the Controller may register the applicant as a qualified auditor.
(4) A qualified auditor registered with the Controller under these Regulations shall not operate as or in any way participate in the operation of or be concerned in a certification authority, a repository or a date/time stamp service.
(5) The Controller shall keep and maintain a Register of Qualified Auditors in such form as he thinks fit.
(6) A person may inspect the Register of Qualified Auditors and make copies of or take extracts from the Register.

11. Report format.

Audit Report is a report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the requirements to be recognised as a Time Stamping Authority (TSA) and the mandatory provisions of the Digital Signature Regulations 1998.

The qualified auditor shall within fourteen days from the completion of a compliance audit under regulation 43 submit a written report to the MCMC.

The auditor's report shall contain -

(*a*) the date of the audit;
(*b*) a list of the information or documents studied or of the personnel interviewed;
(*c*) the extent of compliance with the Act and these Regulations;
(*d*) the results of the audit;
(*e*) the categorisation of the licensed certification authority; and
(*f*) such other information as the qualified auditor thinks fit.

Annex A (Informative): References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

The following referenced documents are necessary for the application of the present document. Not applicable.

[1] Digital Signature Act 1997

[2] Digital Signature Regulations 1998

[3] Requirements for Certification Authorities (CA) to be Recognised as a Time Stamping Authority (TSA)

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[1] ETSI EN 319 421: "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-stamps".

[2] ETSI TS 102 023: "Electronic Signatures and Infrastructures (ESI); Policy requirements for timestamping authorities".

[3] ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp profiles".

[4] Trust Service Principles and Criteria for Certification Authorities Version 2.0 (WebTrust for CA)

[5] IETF RFC 3161 (2001): "Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP)".

[6] IETF RFC 5816: "ESSCertIDV2 update to RFC 3161".