MCMC

MALAYSIAN COMMUNICATIONS AND MULTIMEDIA COMMISSION

REQUIREMENTS FOR CERTIFICATION AUTHORITY (CA) TO BE RECOGNISED AS A 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 principles and criteria for Certification Authorities (CAs) to be recognised as a Time Stamping Authority (TSA) that provide date time stamp services in Malaysia.

The principles and criteria are a set of requirements to enable trust and confidence in date-time stamping services based on the applicable requirements stated in the Digital Signature Act 1997 (Part VI, Section 70) and Digital Signature Regulations 1998 (Part IX, Regulation 58 – 70).

Time-stamping is gaining an increasing interest by the business sector and is becoming an important component of digital signatures. This is commonly based upon the Time-Stamp protocol from the RFC 3161 and the updates defined in RFC5816.

2. Scope

This document specifies the principle and criteria for the time stamping protocol, token profiles, policy and security requirements relating to the operation and management practices of CAs issuing time-stamps.

These principles and criteria are applicable to CAs issuing time-stamps. Such time-stamps can be used in support of digital signatures or for any application requiring to prove that a datum existed before a particular time.

These principles and criteria can also be used by independent bodies as the basis for confirming that a CA can be recognised for issuing time-stamps.

The present document does not specify:

- how the requirements identified herein can be assessed by registered auditor;
- requirements for information to be made available to such registered auditor;
- criteria for registered auditors.
- requirement for readiness assessment on controls designed at the Establishment Stage before moving into Operational Stage;
- requirement for Operational Effectiveness audit after three (3) to six (6) months in operations for Operational Stage;
- requirement for Annual compliance audit; and
- Timeline for recognition process

Above requirements will be defined under Certification Framework documents.

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

Coordinated Universal Time (UTC): time scale based on the second as defined in Recommendation ITU-R TF.460-6

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

time-stamp policy: named set of rules that indicates the applicability of a time-stamp to a particular community and/or class of application with common security requirements

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

trust service: electronic service that enhances trust and confidence in electronic transactions

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:

BIPM	Bureau International des Poids et Mesures
CA	Certification Authority
GMT	Greenwich Mean Time
IT	Information Technology
MCMC	Malaysian Communications and Multimedia Commission
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

4.1 General Policy Requirements Concepts

This document make references to Trust Service Principles and Criteria for Certification Authorities Version 2.0 (WebTrust for CA) for generic policy requirements common to all Certification Authorities.

These policy requirements are based upon the use of public key cryptography, public key certificates and reliable time sources.

Subscribers and relying parties are expected to consult the TSA's policy and practice statement to obtain further details of precisely how this time-stamp policy is implemented by the particular TSA (e.g. protocols used in providing this service).

4.2 Time-stamping Services

Timestamping services help organizations reduce the potential liability associated with time-sensitive transactions by providing a long term validation and non-repudiation of the time and date a transaction took place, using standards-based implementation that is easily recognizable and compatible.

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

- **Time-stamping provision:** This service component generates time-stamps.

- **Time-stamping management:** This service component monitors and controls the operation of the time-stamping services to ensure that the service provided is as specified by the TSA. This service component has responsibility for the installation and de-installation of the time-stamping provision service. For example, time-stamping management ensures that the clock used for time-stamping is correctly synchronized with Malaysia Standard Time (MST).

This subdivision of services is only for the purposes of clarifying the requirements specified in the present document and places no restrictions on any subdivision of an implementation of time-stamping services.

4.3 Time-Stamping Authority (TSA)

A licensed Certification Authority (CA) providing time-stamping services to the public, is called the Time-Stamping Authority (TSA). The TSA has overall responsibility for the provision of the time-stamping services identified in clause 5.4. The TSA has responsibility for the operation of one or more TSUs which creates and signs on behalf of the TSA. The TSA responsible for issuing a time-stamp is identifiable (see clause 5.5.2, g).

The TSA may make use of other parties to provide parts of the time-stamping services. However, the TSA always maintains overall responsibility (as per clause 5.4) and ensures that the policy requirements identified in the present document are met.

EXAMPLE: A TSA sub-contracts all the component services, including the services which generate timestamps using the TSU's keys. However, the private key or keys used to generate the time-stamps are identified as belonging to the TSA which maintains overall responsibility for meeting the requirements defined in the present document.

A TSA may operate several identifiable time-stamping units.

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 will have to apply as well 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 an organization is expected to suitably inform its end users.

When the subscriber is an end-user, the end-user will be held directly responsible if its obligations are not correctly fulfilled.

4.5 Time-stamp Policy and TSA Practice Statement

This clause explains the relative roles of time-stamp policy and TSA practice statement. It places no restriction on the form of a time-stamp policy or certificate practice statement specification.

The present document specifies a time-stamp policy to meet general requirements for trusted time-stamping services.

TSAs specify in TSA practice statements how these requirements are met.

4.5.1 Purpose

In general, the time-stamp policy states "what is to be adhered to", while a TSA practice statement states "how it is adhered to", i.e. the processes it will use in creating time-stamps and maintaining the accuracy of its clock. The relationship between the time-stamp policy and TSA practice statement is similar in nature to the relationship of other business policies which state the requirements of the business, while operational units define the practices and procedures of how these policies are to be carried out.

The present document specifies a time-stamp policy to meet general requirements for trusted time-stamping services. TSAs specify in TSA practice statements how these requirements are met.

4.5.2 Level of Specificity

A time-stamp policy is a less specific document than a TSA practice statement. A TSA practice statement is a more detailed description of the terms and conditions as well as business and operational practices of a TSA in issuing and otherwise managing time-stamping services. The TSA practice statement of a TSA enforces the rules established by a time-stamp policy. A TSA practice statement defines how a specific TSA meets the technical, organizational and procedural requirements identified in a time-stamp policy.

Even lower-level internal documentation may be appropriate for a TSA detailing the specific procedures necessary to complete the practices identified in the TSA practice statement.

4.5.3 Approach

The approach of a time-stamp policy is significantly different from a TSA practice statement. A time-stamp policy is defined independently of the specific details of the specific operating environment of a TSA, whereas a TSA practice statement is tailored to the organizational structure, operating procedures, facilities, and computing environment of a TSA. A time-stamp policy may be defined by the user of times-stamp services, whereas the practice statement is always defined by the TSA.

5. Requirements

5.1 Time-stamp Policies

5.1.1 Overview

The policy requirements are defined in the present document in terms of a time-stamp policy. A time-stamp policy is a "named set of rules that indicates the applicability of a time-stamp token to a particular community and/or class of application with common security requirements" (see clauses 3.1 and 4.4).

This document specifies one time-stamp policy for TSAs issuing time-stamps, supported by public key certificates, with an accuracy of 1 second or better.

A TSA may define its own policy which enhances a policy defined in the present document. Such a policy shall incorporate or further constrain the requirements identified in the present document.

If an accuracy of better than 1 second is provided by the TSA then the accuracy shall be indicated in the TSA's disclosure statement (see clause 5.3) and in each time-stamp issued to an accuracy of better than 1 second.

5.1.2 Identification

The object-identifier (OID) of the time-stamp policy specified shall be the Certificate of Recognition number.

TSA shall use its own identifier for the time-stamp policy.

A TSA shall include the identifier for the time-stamp policy being supported in the policy document, TSA practice statement, TSA disclosure Statement and made available to subscribers and relying parties to indicate its claim of conformance.

By including this object identifier in a time-stamp, the TSA claims conformance to the identified time-stamp policy.

5.1.3 User Community and Applicability

This policy is aimed at meeting the requirements of time-stamping qualified digital signatures (see Digital Signature Act 1997 and Digital Signature Regulations 1998) for long term validity but is generally applicable to any use which has a requirement for equivalent quality.

This policy may be used for public time-stamping services or time-stamping services used within a closed community.

5.1.4 Conformance

The TSA shall use the identifier for the time-stamp policy in time-stamp tokens as given in clause 5.1.2, or define its own time-stamp policy that incorporates or further constrains the requirements identified in the present document:

a) if the TSA claims conformance to the identified time-stamp policy and makes available to subscribers and relying parties on request the evidence to support the claim of conformance; or

b) if the TSA has been assessed to be conformant to the identified time-stamp policy by a qualified auditor.

A conformant TSA must demonstrate that:

c) it meets its obligations as defined in clause 5.4;

d) it has implemented controls which meet the requirements specified in clause 5.2.

5.2 TSA Practice Statement

The requirements identified in the WebTrust for CA Principle and Criteria clause 1.1, 2.2 and 2.3 shall apply.

The TSA shall ensure that it demonstrates the reliability necessary for providing time-stamping services.

In particular:

a) The TSA shall have a risk assessment carried out in order to evaluate business assets and threats to those assets in order to determine the necessary security controls and operational procedures.

b) The TSA shall have a statement of the practices and procedures used to address all the requirements identified in this time-stamp policy.

c) The TSA's practice statement shall identify the obligations of all external organizations supporting the TSA services including the applicable policies and practices.

d) The TSA shall make available to subscribers and relying parties its practice statement, and other relevant documentation, as necessary to assess conformance to the time-stamp policy.

e) The TSA shall disclose to all subscribers and potential relying parties the terms and conditions regarding use of its time-stamping services as specified in clause 5.3.

f) The TSA shall have a high level management body with final authority for approving the TSA practice statement.

g) The senior management of the TSA shall ensure that the practices are properly implemented.

h) The TSA shall define a review process for the practices including responsibilities for maintaining the TSA practice statement.

i) The TSA shall give due notice of changes it intends to make in its practice statement and shall, following approval as in (f) above, make the revised TSA practice statement immediately available as required under (d) above.

5.3 TSA disclosure Statement

Although security policy and practice statement documents are essential for describing and governing time-stamping policies and practices, many TSA users, especially consumers, may find these documents difficult to understand. Consequently, there is a need for a supplemental and simplified instrument that can assist TSA users in making informed trust decisions. Consequently, a TSA disclosure statement is not intended to replace a security policy or practice statement.

The TSA shall disclose to all subscribers and potential relying parties the terms and conditions regarding use of its time-stamping services.
This statement shall at least specify for each time-stamp policy supported by the TSA:

a) The TSA contact information.

b) The time-stamp policy being applied.

c) At least one hashing algorithm which may be used to represent the datum being time-stamped.

d) The expected life-time of the signature used to sign the time-stamp token (depends on the hashing algorithm being used, the signature algorithm being used and the private key length).

e) The accuracy of the time in the time-stamp tokens with respect to MST.

f) Any limitations on the use of the time-stamping service.

g) The subscriber's obligations as defined in clause 5.4.2, if any.

h) The relying party's obligations as defined in clause 5.4.4.

i) Information on how to verify the time-stamp token such that the relying party is considered to "reasonably rely" on the time-stamp token (see clause 5.4.4) and any possible limitations on the validity period.

j) The period of time during which TSA event logs (see clause 5.6.10) are retained.

k) The applicable legal system, including any claim to meet the requirements on time-stamping services under national law.

l) Limitations of liability.

m) Procedures for complaints and dispute settlement.

n) If the TSA has been assessed to be conformant with the identified time-stamp policy, and if so by which independent body.

The TSA should include in its time-stamping disclosure statement availability of its service. For example, the expected mean time between failure of the time-stamping service, expected mean time to recover following a failure and provisions made for disaster recovery including back-up services.

This information shall be available through a durable means of communication. This information shall be available in a readily understandable language. It may be transmitted electronically.

A model TSA disclosure statement which may be used as the basis of such a communication is given in annex B. Alternatively this may be provided as part of a subscriber / relying party agreement. These TSA disclosure statement may be included in a TSA practice statement provided that they are conspicuous to the reader.

The time stamp policy and TSA disclosure statement may be included in a TSA practice statement provided that it is conspicuous to the reader.

5.4 TSA Obligations

5.4.1 General

The TSA shall ensure that all requirements on TSA, as detailed in clause 5.2, are implemented as applicable to the selected trusted time-stamp policy.

The TSA shall ensure conformance with the procedures prescribed in this policy, even when the TSA functionality is undertaken by sub-contractors.

The TSA shall also ensure adherence to any additional obligations indicated in the time-stamp either directly or incorporated by reference.

The TSA shall provide all its time-stamping services consistent with its practice statement and disclosure statement.

5.4.2 TSA Obligations towards Subscribers

The present document places no specific obligations on the subscriber beyond any TSA specific requirements stated in the TSA's terms and conditions.

5.4.3 Subscriber Obligations

The present document places no specific obligations on the subscriber beyond any TSA specific requirements stated in the TSA's terms and condition.

NOTE: It is advisable that, when obtaining a time-stamp token, the subscriber verifies 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.

5.4.4 Relying Party Obligations

The terms and conditions made available to relying parties (see clause 5.2) shall include an obligation on the relying party that, when relying on a time-stamp token, it shall:

a) verify that the time-stamp token has been correctly signed and that the private key used to sign the time-stamp has not been compromised until the time of the verification;

NOTE: During the TSU's certificate validity period, the validity of the signing key can be checked using current revocation status for the TSU's certificate. If the time of verification exceeds the end of the validity period of the corresponding certificate, see annex D for guidance.

b) take into account any limitations on the usage of the time-stamp indicated by the time-stamp policy;

c) take into account any other precautions prescribed in agreements or elsewhere.

5.4.5 Liability

The present document does not specify any requirement on liability. In particular, it should be noticed that a TSA may disclaim or limit any liability unless otherwise stipulated by the applicable law.

5.5 TSA Management and Operation

5.5.1 TSU Key Management Life Cycle

Appropriate security controls shall be in place for the management of any cryptographic keys and any cryptographic devices throughout their lifecycle.

The requirements identified in WebTrust for CA Principle and Criteria clause 4 shall apply.

5.5.2 Time-stamp Issuance

Time-stamps shall conform to the time-stamp profile as defined in Annex A, Section 2.

The time-stamps shall be issued securely and shall include the correct time.

In particular:

a) The time-stamp token shall include an identifier for the time-stamp policy.

b) Each time-stamp token shall have a unique identifier.

c) The time values the TSU uses in the time-stamp shall be traceable to at least one of the real time values distributed by a NMIM laboratory.

d) The time included in the time-stamp shall be synchronized with MST within the accuracy defined in the policy and, if present, within the accuracy defined in the time-stamp itself.

e) If the time-stamp provider's clock is detected (see clause 5.5.3) as being out of the stated accuracy (see clause 5.3) then time-stamps shall not be issued.

f) The time-stamp token shall include a representation (e.g. hash value) of the datum being time-stamped as provided by the requestor.

g) The time-stamp shall be signed using a key generated exclusively for this purpose.

NOTE: A protocol for a time-stamp token is defined in RFC 3161 and profiled in Annex A.

h) The time-stamp token shall include:
- an identifier for the country in which the TSA is established;
- an identifier for the TSA;
- an identifier for the unit which issues the time-stamps.

i) The time-stamp generation system shall reject any attempt to issue time-stamps if the signing private key has expired.

5.5.3 Clock Synchronization with MST

The TSA clock shall be synchronized with MST within the declared accuracy with at least the following particular requirements:

a) The calibration of the TSU clocks shall be maintained such that the clocks do not drift outside the declared accuracy.

b) The declared accuracy shall be of 1 second or better.

c) The TSU clocks shall be protected against threats which could result in an undetected change to the clock that takes it outside its calibration.

NOTE 1: Threats can include tampering by unauthorized personnel, radio or electrical shocks.

d) The TSA shall detect if the time that would be indicated in a time-stamp drifts or jumps out of synchronization with MST.

NOTE 2: See clause 5.10.11 for notification requirements of such events to relying parties.

e) If it is detected that the time indicated in a time-stamp drifts or jumps out of synchronization with MST, the TSU shall stop time-stamp issuance.

f) The clock synchronization shall be maintained when a leap second occurs as notified by the appropriate body. The change to take account of the leap second shall occur during the last minute of the day when the leap second is scheduled to occur. A record shall be maintained of the exact time (within the declared accuracy) when this change occurred. See annex C for more details.

g) The TSA shall obtain written confirmation on annual basis from NMIM to verify that the TSU clocks are in synced with MST within the declared accuracy

5.5.4 TSA Termination and Termination Plans

The TSA shall ensure that potential disruptions to subscribers and relying parties are minimized as a result of the cessation of the TSA's time-stamping services, and in particular ensure continued maintenance of information required to verify the correctness of time-stamp tokens.

In particular:

a) The TSA shall have an up-to-date termination plan.

b) Before the TSA terminates its time-stamping services the following procedures shall be executed as a minimum:

- the TSA shall make available to all subscribers and relying parties information concerning its termination;

- TSA shall terminate authorization of all subcontractors to act on behalf of the TSA in carrying out any functions relating to the process of issuing time-stamp tokens;

- the TSA shall transfer obligations to a reliable party for maintaining event log and audit archives (see clause 5.6.10) necessary to demonstrate the correct operation of the TSA for a reasonable period;

- the TSA shall maintain or transfer to a reliable party its obligations to make available its public key or its certificates to relying parties for a reasonable period;

- TSU private keys, including backup copies, shall be destroyed in a manner such that the private keys cannot be retrieved.

c) The TSA shall have an arrangement to cover the costs to fulfil these minimum requirements in case the TSA becomes bankrupt or for other reasons is unable to cover the costs by itself.

d) The TSA shall state in its practices the provisions made for termination of service. This shall include:

- notification of affected entities;

- transferring the TSA obligations to other parties.

e) The TSA shall take steps to have the TSU's certificates revoked.

5.6 General Security and Controls

The TSA shall implement the following security controls requirements.

5.6.1 Security Management

The requirements identified in WebTrust for CA Principle and Criteria clause 3.1, shall apply.

5.6.2 Asset Classification and Management

The requirements identified in WebTrust for CA Principle and Criteria clause 3.2, shall apply.

5.6.3 Human Resource Security

The requirements identified in WebTrust for CA Principle and Criteria clause 3.3 shall apply.

5.6.4 Physical and Environmental Security

The requirements identified in WebTrust for CA Principle and Criteria clause 3.4 shall apply.

5.6.5 Operation Security

The requirements identified in WebTrust for CA Principle and Criteria clause 3.5 shall apply.

5.6.6 Incident Management

The requirements identified in WebTrust for CA Principle and Criteria clause 3.5 shall apply.

5.6.7 Access Control

The requirements identified in WebTrust for CA Principle and Criteria clause 3.6 shall apply.

5.6.8 System Development and Maintenance

The requirements identified in WebTrust for CA Principle and Criteria clause 3.7 shall apply.

5.6.9 Business Continuity Management

The requirements identified in WebTrust for CA Principle and Criteria clause 3.8 shall apply.

In addition the following particular requirements apply:

a) The TSA's disaster recovery plan shall address the compromise or suspected compromise of TSU's private signing keys or loss of calibration of a TSU clock, which may have affected time-stamps which have been issued.

b) In the case of a compromise, or suspected compromise or loss of calibration when issuing time-stamp the TSA shall make available to all subscribers and relying parties a description of compromise that occurred.

c) In the case of compromise to a TSU's operation (e.g. TSU key compromise), suspected compromise or loss of calibration the TSU shall not issue time-stamps until steps are taken to recover from the compromise.

d) In case of major compromise of the TSA's operation or loss of calibration, the TSA shall make available to all subscribers and relying parties information which can be used to identify the time-stamps which may have been affected, unless this breaches the privacy of the TSAs users or the security of the TSA services.

NOTE: In case the private key does become compromised, an audit trail of all time-stamps generated by the TSU can provide a means to discriminate between genuine and false backdated time-stamps. Two time-stamps from two different TSUs can be another way to address this issue.

5.6.10 Compliance

The requirements identified in WebTrust for CA Principle and Criteria clause 3.9 shall apply.

5.6.11 Collection of Evidence

The requirements identified in WebTrust for CA Principle and Criteria clause 3.10 (Audit Logging) shall apply.

In addition the following particular requirements apply:

TSU key management

a) Records concerning all events relating to the life-cycle of TSU keys shall be logged.

b) Records concerning all events relating to the life-cycle of TSU certificates (if appropriate) shall be logged.

Clock Synchronization

c) Records concerning all events relating to synchronization of a TSU's clock to MST shall be logged. This shall include information concerning normal re-calibration or synchronization of clocks used in time-stamping.

d) Records concerning all events relating to detection of loss of synchronization shall be logged.

Annex A (Normative) – Time-stamping protocol and time-stamp token profiles

A.1 Requirements for a time-stamping client

1.1 Profile for the format of the request

1.1.1 Core requirement

A time-stamping client shall support the time-stamping request as defined in IETF RFC 3161, clause 2.4.1 with the amendments defined in the following clauses.

1.1.2 Fields to be supported

The use of the following fields in the time-stamping request should be supported:

- the reqPolicy;
- the nonce; and
- the certReq.

1.1.3 Hash algorithms to be used

Hash algorithms used to hash the information to be time-stamped should be as specified in Annex A.4

1.2 Profile for the format of the response

1.2.1 Core requirement

A time-stamping client shall support the time-stamping response as defined in IETF RFC 3161, clause 2.4.2 with the amendments defined in the following clauses.

1.2.2 Fields to be supported

The following requirements apply:

- the `accuracy` field shall be supported; and
- the `nonce` field should be supported.

A TSU needs not support ordering hence clients should not depend on the ordering of time-stamps.
If the nonce field is present in the request, the nonce field shall be present in the response with the same value.

1.2.3 Algorithms to be supported

Time-stamp token signature algorithms to be supported should be as specified in Annex A.4

1.2.4 Key lengths to be supported

Signature algorithm key lengths for the selected signature algorithm should be supported as recommended in Annex A.4

A.2 Requirements for a time-stamping server

2.1 Profile for the format of the request

2.1.1 Core requirement

A time-stamping server shall support the time-stamping request as defined in IETF RFC 3161, clause 2.4.1 with the amendments defined in the following clauses.

2.1.2 Fields to be supported

The following requirements apply:

- `reqPolicy` field shall be supported;
- the `nonce` field shall be supported; and
- `certReq` field shall be supported.

2.1.3 Algorithms to be supported

Hash algorithms for the time-stamp data to be supported should be as specified in Annex A.4

2.2 Profile for the format of the response

2.2.1 Core requirement

A time-stamping server shall support the time-stamping response as defined in IETF RFC 3161, clause 2.4.2 with the amendments defined in the following clauses.

2.2.2 Fields to be supported

The requirements from IETF RFC 3161, clause 2.4.2 shall apply and the following requirements apply:

- the `policy` field shall be present as an identifier for the time-stamp policy and shall conform to annex A;
- a `genTime` field shall have a value representing time with a precision necessary to support the declared accuracy shall be supported;
- the `accuracy` field shall be present and a minimum accuracy of one second shall be supported;
- the `ordering` field shall not be present or shall be set to false; and
- no extension shall be marked as critical.

The following requirement applies to the content of the `SignedData` structure in which the `TSTInfo` structure is encapsulated:

- the certificate identifier of the TSU certificate (`ESSCertID` as in IETF RFC 3161 or `ESSCertIDv2` as in IETF RFC 5816) shall be included as a `signerInfo` attribute inside a `SigningCertificate` or a `SigningCertificateV2` attribute as specified in IETF RFC 5816, clause 2.2.1.

2.2.3 Algorithms to be used

Hash algorithms used to hash the information to be time-stamped and time-stamp token signature algorithms should be as specified in Annex A (1).

A.3 TSU certificate profile

The TSU certificate shall meet the following requirements

3.1 Subject name requirements

The countryName attribute shall specify the country in which the TSA is established (which is not necessarily the name of the country where the TSU is located).

For a TSA being a legal person or a natural person associated with a legal person the organizationName shall contain the full registered name of the TSA responsible for managing the TSU. That name should be an officially registered name of the TSA.

The commonName specifies an identifier for the TSU. Within the TSA, the attribute commonName uniquely identifies the TSU used.

For a TSA being a natural person, one instance of the attribute serialNumber should be included in the subject field.

3.2 Key lengths requirements

The key length for the selected signature algorithm of the TSU certificate should be as recommended in Annex A.4.

3.3 Key usage requirements

The TSU certificate extended key usage setting shall be as defined in IETF RFC 3161, clause 2.3.

The TSU certificate private key usage period extension should be used in order to limit the validity of the TSU's signing key.

3.4 Algorithm requirements

The TSU public key and the TSU certificate signature should use the algorithms as specified in Annex A.4

A.4 Algorithms for Time Stamping

4.1 Time Stamping Token (TST)

The following requirements apply to hash functions and TST signature algorithms.

Time Stamping Token	TST Requesters	TST Issuers	TST Verifiers
Hash Function	shall support SHA-256	shall support SHA-256	shall support SHA-256
TST Signature Algorithms	shall support RSA with SHA-256 or SHA-512	shall support RSA with SHA-256 or SHA-512 should support EC-DSA with SHA-256	shall support RSA with SHA-256 or SHA-512 should support EC-DSA with SHA-256

4.2 TSU Certificate

TSU Certificates	Issuers of TSU Certificates	Users of TSU Certificates
TSU Public Key	should support RSA with SHA-256 or SHA-512 should support EC-DSA with SHA-256	shall support RSA with SHA-256 or SHA-512 should support EC-DSA with SHA-256
Issuer CA Public Key	shall support RSA with SHA-256 or SHA-512 should support EC-DSA with SHA-256	shall support RSA with SHA-256 or SHA-512 should support EC-DSA with SHA-256

Annex B (informative): Model TSA disclosure statement

B.1 Introduction

The proposed model TSA disclosure statement in table B.1 is designed for use by a CA issuing time-stamps as a supplemental instrument of disclosure and notice. A TSA disclosure statement can assist a TSA to respond to regulatory requirements and concerns, particularly those related to consumer deployment. Further, the aim of the model TSA disclosure statement is to foster industry "self-regulation" and build consensus on those elements of a security policy and/or practice statement that require emphasis and disclosure.

Although security policy and practice statement documents are essential for describing and governing time-stamp policies and practices, many TSA users, especially consumers, can find these documents difficult to understand.

Consequently, there is a need for a supplemental and simplified instrument that can assist TSA users in making informed trust decisions. Consequently, a TSA disclosure statement is not intended to replace a security policy or practice statement.

This annex provides an example of the structure for a TSA disclosure statement, illustrating the harmonized set of statement types (categories) that would be contained in a deployed time-stamping service.

B.2 TSA disclosure statement structure

The TSA disclosure statement contains a section for each defined statement type. Each section of a TSA disclosure statement contains a descriptive statement, which may include hyperlinks to the relevant certificate policy/certification practice statement sections.

Table B.1: Model of TSA disclosure statement structure

Statement Types	Statement Description	Specific Requirements
Entire agreement	A statement indicating that the disclosure statement is not the entire agreement, but only a part of it.	-
TSA contact info	The name, location and relevant contact information for the TSA.	-
Electronic time-stamp types and usage	A description of each class/type of electronic time-stamps issued by the TSA (in accordance with each time-stamp policy) and any restrictions on time-stamp usage.	Indication of the policy being applied (i.e. BTSP), including the contexts for which the time-stamp can be used (e.g. only for use with electronic signatures), the hashing algorithms, the expected life time of the timestamp signature, any limitations on the use of the timestamp and information on how to verify the time-stamp.
Reliance limits	The reliance limits, if any.	Indication of the accuracy of the time in the time-stamp, and the period of time for which TSA

		event logs are maintained (and hence are available to provide supporting evidence).
Obligations of subscribers	The description of, or reference to, the critical subscriber obligations.	No specific requirements identified in the present document. Where applicable the TSA may specify additional obligations.
TSU public key certificate status checking obligations of relying parties	The extent to which relying parties are obligated to check the TSU public key certificate status, and references to further explanation.	Information on how to validate the TSU public key certificate status, including requirements to check the revocation status of TSU public key certificate, such that the relying party is considered to "reasonably rely" on the time-stamp (see clause 5.4.4).
Limited warranty and disclaimer/Limitation of liability	Summary of the warranty, disclaimers, limitations of liability and any applicable warranty or insurance programs.	Limitations of liability (see clause 5.4.5)
Applicable agreements and practice statement	Identification and references to applicable agreements, practice statement, time-stamp policy and other relevant documents.	-
Privacy policy	A description of and reference to the applicable privacy policy.	-
Refund policy	A description of and reference to the applicable refund policy	-
Applicable law, complaints and dispute resolution	Statement of the choice of law, complaints procedure and dispute resolution mechanisms.	The procedures for complaints and dispute settlements. The applicable legal system.
TSA and repository licenses, trust marks, and audit	Summary of any governmental licenses, seal programs; and a description of the audit process and if applicable the audit firm.	If the TSA has been assessed to be conformant with the identified time-stamp policy, and if so through which independent party.

Annex C (informative): Malaysia Standard Time (MST)

C.1. Malaysia Standard Time (MST)

The Malaysia local time or officially named as the Malaysia Standard Time (MST) is decided by the Time and Frequency Laboratory of the National Metrology Institute of Malaysia (NMIM), the appointed national timekeeper (refer to Cabinet Note H 226/92), from the caesium atomic clocks that it maintained.

The time is determined or decided by the practice adopted as practiced by other developed or developing countries, where the clocks data are submitted daily to the International of Weights and Measures (BIPM). Being a member of the BIPM helps a lot, since the performance, accuracy and stability of Malaysia Standard Time is computed from the International Atomic Timescale (TAI), aggregated and based, on all the atomic clocks belonging to other timing laboratories and the derived Universal Coordinated Time (UTC).

BIPM monthly publication of Circular-T provides the details of the computation for each laboratory and is used to evaluate the performance of the time dissemination services. NMIM provides time dissemination services such as Network Time Protocol (NTP) service, Precise Time Protocol (PTP) service and Malaysia Standard Time display through the website, http://mst.sirim.my.

NMIM has also developed a Malaysian Standard Time Clock with millisecond accuracy which is a network time protocol based clock that periodically synchronized to NMIM’s network time protocol servers (ntp1.sirim.my, and ntp2.sirim.my) via internet.

C.2. Coordinated Universal Time (UTC)

Coordinated Universal Time (UTC) is the international time standard that became effective on January 1, 1972. UTC has superseded Greenwich Mean Time (GMT), but in practice they are never more than 1 second different. Hence many people continue to refer to GMT when in fact they operate to UTC.

UTC is the time-scale maintained by the BIPM, with assistance from the IERS, which forms the basis of a coordinated dissemination of standard frequencies and time signals. It corresponds exactly in rate with TAI but differs from it by an integer number of seconds.

Zero (0) hours UTC is midnight in Greenwich, England, which lies on the zero longitudinal meridian. Universal time is based on a 24 hour clock, therefore, afternoon hours such as 4 pm UTC are expressed as 16:00 UTC (sixteen hours, zero minutes).

The full definition of UTC is contained in Recommendation ITU-R TF.460-6.

Annex D (informative): Long term verification of time-stamps

Usually, a time-stamp becomes unverifiable beyond the end of the validity period of the certificate from the TSU, because the CA that has issued the certificate does not usually warrant any more providing revocation status information for expired certificates.

If at the time of verification:

- the TSU private key has not been compromised at any time up to the time that a relying part verifies a timestamp;

- the hash algorithms used in the time-stamp exhibits no collisions at the time of verification; and

- 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;

then verification of a time-stamp can still be performed beyond the end of the validity period of the certificate from the TSU.

The validity may be maintained by applying an additional time-stamp to protect the integrity of the previous one. Alternatively the time-stamped data may be placed in secure storage.

The present document does not specify the details of how such protection can be obtained. For the time being, and until some enhancements are defined to support these features, the information may be obtained using-out-of bands means or alternatively in the context of closed environments. As an example, should a CA guarantee to make the revocation status information of TSU certificates available after the end of its validity period, this would fulfill verification that the TSU private key has not been compromised.

Annex E (informative): Possible implementation architectures - time-stamping service

E.1 Managed time-stamping service

Some organizations will be willing to host one or more Time-Stamping Units in order to take advantage of both the proximity and the quality of the time-stamping service, without being responsible for the installation, operation and management of these Time-Stamping Units.

This can be achieved by using units that are installed in the premises from the hosting organization and then remotely managed by a Time-Stamping Authority that takes the overall responsibility of the quality of the service delivered to the hosting organization.

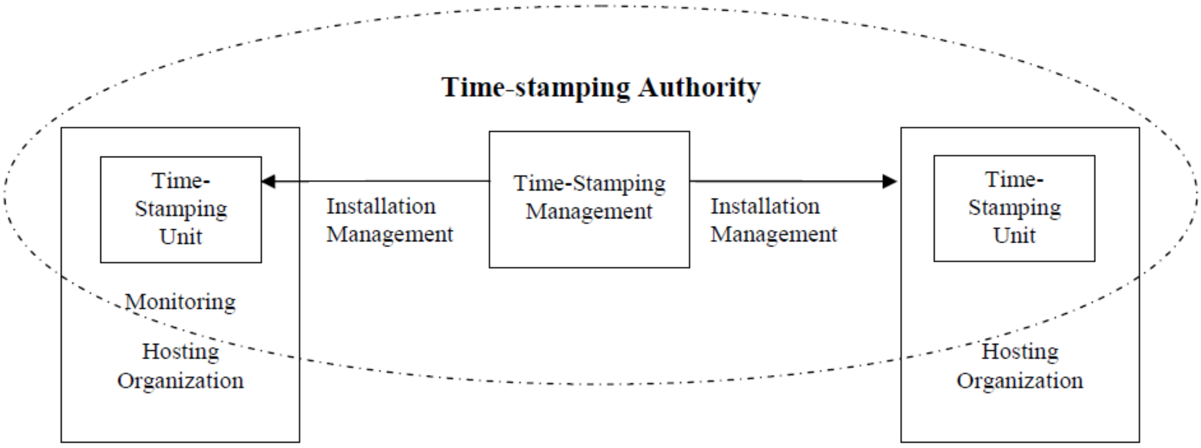

Figure E.1: Managed time-stamping service

The requirements for time-stamping services described in the present document include requirements on both the timestamping management and for the operation of the unit which issues the time-stamps. The TSA, as identified in the time-stamp, has the responsibility to ensure that these requirements are met (for example through contractual obligations).

The hosting organization will generally want to be able to monitor the use of the service and, at a minimum, know whether the service is working or not and even be able to measure the performances of the service, e.g. the number of time-stamps generated during some period of time. Such monitoring can be considered to be outside of TSA's timestamping service.

Therefore the description of the management operation described in the main body of the present document is not limitative. Monitoring operations, if performed directly on the unit, can be permitted by the Time-Stamping Authority.

E.2 Selective alternative quality

Some relying parties will be willing to take advantage of particular characteristics from a time-stamp such as a specific signature algorithm and/or key length or a specific accuracy for the time contained in the time-stamp.

These parameters can be considered as specifying a "quality" for the time-stamp.

Time-stamps with various qualities can be issued by different time-stamping units operated by the same or different TSAs.

A particular time-stamping unit will only provide one combination of algorithm and key length (since a time-stamping unit is a set of hardware and software which is managed as a unit and has a single time-stamp signing key). In order to obtain different combinations of algorithm and key length, different time-stamping units need to be used.

A particular time-stamping unit can provide a fixed accuracy for the time contained in the time-stamp or different accuracy if instructed to do so either by using a specific mode of access (e.g. e-mail or http) or by using specific parameters in the request.

Annex F (informative): References

F.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] Trust Service Principles and Criteria for Certification Authorities Version 2.0 (WebTrust for CA)

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

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

F.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 v1.1.1: "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-stamps".

[2] ETSI TS 102 023 v1.2.2: "Electronic Signatures and Infrastructures (ESI); Policy requirements for timestamping authorities".

[3] ETSI EN 319 422 v1.1.0: "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp profiles".

F.3 Table of References

No.	Section in Framework	Mapped Section in Reference
1.	1. Introduction	ETSI EN 319 421
2.	2. Scope	ETSI TS 102 023 (Item 1)
3.	3. Terms and Definitions	ETSI 102 023 (Item 3)
4.	3.1 Definitions	ETSI 102 023 (Item 3.1)
5.	3.2 Abbreviations	ETSI 102 023 (Item 3.2)
6.	3.3 Modal Verbs Terminology	RFC 2119
7.	4. General Concepts	ETSI EN 319 421 (Item 4)
8.	4.1 General Policy Requirements Concepts	ETSI EN 319 421 (Item 4.1)
9.	4.2 Time-Stamping Services	ETSI EN 319 421 (Item 4.2)
10.	4.3 Time-Stamping Authority (TSA)	ETSI EN 319 421 (Item 4.2)
11.	4.4 Subscriber	ETSI EN 319 421 (Item 4.3)
12.	4.5 Time-Stamp Policy and TSA Practice Statement	ETSI EN 319 421 (Item 4.5)
13.	4.5.1 Purpose	ETSI TS 102 023 (Item 4.4.1)
14.	4.5.2 Level Of Specificity	ETSI TS 102 023 (Item 4.4.2)
15.	4.5.3 Approach	ETSI TS 102 023 (Item 4.4.3)
16.	5. Principles and Criteria	ETSI TS 102 023 (Item 5)
17.	5.1 Time-Stamp Policies	ETSI TS 102 023 (Item 5)
18.	5.1.1 Overview	ETSI TS 102 023 (Item 5.1)
19.	5.1.2 Identification	ETSI TS 102 023 (Item 5.2)
20.	5.1.3 User Community and Applicability	ETSI TS 102 023 (Item 5.3)
21.	5.1.4 Conformance	ETSI TS 102 023 (Item 5.4)
22.	5.2 TSA Practice Statement	ETSI TS 102 023 (Item 7.1.1)
23.	5.3 TSA Disclosure Statement	ETSI TS 102 023 (Item 7.1.2)
24.	5.4 TSA Obligations	ETSI TS 102 023 (Item 6.1)
25.	5.4.1 General	ETSI TS 102 023 (Item 6.1.1)
26.	5.4.2 TSA Obligations towards Subscribers	ETSI TS 102 023 (Item 6.1.2)
27.	5.4.3 Subscriber Obligations	ETSI TS 102 023 (Item 6.2)
28.	5.4.4 Relying Party Obligations	ETSI TS 102 023 (Item 6.3)
29.	5.4.5 Liability	ETSI TS 102 023 (Item 6.4)
30.	5.5.2 TSA Key Generation	ETSI TS 102 023 (Item 7.2.1)
31.	5.5.3 TSU Private Key Protection	ETSI TS 102 023 (Item 7.2.2)
32.	5.5.4 TSU Public Key Distribution	ETSI TS 102 023 (Item 7.2.3)
33.	5.5.5 Rekeying TSU's Key	ETSI TS 102 023 (Item 7.2.4)
34.	5.5.6 End of TSU Key Life Cycle	ETSI TS 102 023 (Item 7.2.5)
35.	5.5.7 Life cycle management of Cryptographic Module Used to Sign Time-Stamps	ETSI TS 102 023 (Item 7.2.6)
36.	5.5.8 Time-Stamp Issuance	ETSI TS 102 023 (Item 7.3.1)
37.	5.5.9 Clock synchronization with MST	ETSI EN 319 421 (Item 7.7.2)
38.	5.5.10 TSA termination and Termination Plans	ETSI EN 319 401 (Item 7.12) ETSI TS 102 023 (Item 7.4.9)
39.	5.6 General Security and Controls	ETSI TS 102 023 (Item 7.4)
40.	5.6.9 Business Continuity Management	ETSI EN 319 401 (Item 7.11) and ETSI EN 391 421 (Item 7.13)
41.	5.6.11 Collection of Evidence	ETSI EN 319 401 (Item 7.10) & ETSI EN 319 421 (Item 7.12)
42.	Annex A (Normative) – Time-Stamping Protocol and Time-Stamp Token Profiles	ETSI EN 319 422 (Items 4, 5, and 6)
43.	Annex B (informative): Model TSA Disclosure Statement	ETSI EN 319 421 (Annex B)
44.	Annex C (informative): Malaysia Standard Time (MST)	ETSI TS 102 023 (Annex C)

45.	Annex D (informative): Long Term Verification of Time-Stamps	ETSI EN 319 421 (Annex D)
46.	Annex E (informative): Possible Implementation Architectures - Time-Stamping Service ()	ETSI EN 319 421 (Annex F)
47.	Annex F (informative): References	ETSI EN 319 421 (Item 2)