TIME STAMPING POLICY (TSP)
AND
TIME STAMPING PRACTISE STATEMENT
(TSPS)

Table of Content

1. Introduction

1.1. Overview

TMCA, being both a Time-Stamping Authority (TSA) and a Time-Stamping Service Provider (TSSP), offers to its customers a Time-Stamping Service (TSS) complying notably with the qualification requirements of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates for a TSS.

The document herein is the TMCA Time-Stamping Policy (TSP). It describes the TMCA TSS and specifies the commitments of TMCA as a TSA towards this time stamping service. The present TSP also describes the obligations and requirements of Subscribers and Relying Parties.

A Time-Stamp Token (TST) generated by TMCA TSS provides evidence of the existence of a hash value at a given date and time. The TSTs are generated and digitally signed by the TSA through the use of Time-Stamping Units (TSUs).

This document aims at specifying TMCA commitments when, acting as TSA, it delivers and manages TSTs, as well as the obligations of other participants.

This document also includes and represents, the Time-Stamping Practice Statement (TSPS). TMCA TSPS presents the mechanisms and procedures implemented to reach the TSP security target and in particular the process to be followed by a TSU when generating TSTs and maintaining the accuracy of its clocks. TMCA acting as TSA may setup several TSUs in order to manage its TSS.

The Certification Authority (CA) delivering the certificates for the TSUs of the TSA also belongs to TMCA. Its specifications are described in the Certification Policy (CP) and Certificate Practice Statement (CPS) of TMCA.

This TSP/TSPS does not require any link between the hash to be time-stamped and the contents of the original electronic data. Only the Subscriber of the TSS is responsible for this match.

TMCA has also published the Terms of Use (ToU) for its subscribers of Time Stamping.

Within this TSP/TSPS, day and time of each TST are synchronized with the Coordinated Universal Time (UTC) with an accuracy of less than one second. This TSP applies the standard TST format specified in the [RFC 3161] document.

1.2. Principle of TMCA Time Stamping Service

Time-Stamping establishes evidence that a datum exists at a particular time. For this matter, it binds an unequivocal representation of a datum (i.e.: its hash value together with a hash algorithm identifier) to a particular time. A TST unequivocally performs this link; a TST is a signed structure including notably:

- the hash value and the hash algorithm of the time-stamped datum; date and universal time (UTC);
- the identifier of the TSU certificate that has generated the TST;

- the identifier of TMCA acting as TSA (within the time-stamp certificate);
- the identifier of the CA that has signed the private keys installed on the TSUs.

TMCA TSS benefits from the Public Key Infrastructure (PKI) that has been established by TMCA.

This certification service allows TMCA CA to issue the certificates of TMCA TSUs.

The clock synchronization system of the TSS allows TMCA to ensure the Subscriber the delivery of a TST with an accuracy of less than one second with respect to UTC.

TMCA TSA operates several TSUs. Each TSU signs TSTs on behalf of the TSA, using a dedicated private key, which matching public key has been previously certified by TMCA CA. Therefore, each TSU has its own time-stamping certificate.

1.3. Document Identification

This document is TMCA Time-Stamping Policy (TSP) and Time Stamping Practice Statement (TSPS). This TSP/TSPS is identified, within the documentation framework of TMCA trust architecture, by a unique identification number: 1.3.6.1.4.1.50977.1.0.2

This OID is built as follows:

OID	Description
1.3.6.1.4.1.50977	Telekom Malaysia CA branch
1.3.6.1.4.1.50977.1.0	Policies branch
1.3.6.1.4.1.50977.1.0.2	Time-Stamping Policies (TSP) branch

TSTs abiding by this policy refer to it by using this unique identifier (OID). Its value is included in the “Policy” field of the TSTs. Other more meaningful element (name, version number, date of update) can also identify it.

Default TST Policy OID: 1.3.6.1.4.1.50977.1.3.1
Custom TST Policy OID: 1.3.6.1.4.1.50977.1.3.X
(X indicates the sequential number for custom policy OIDs)

1.4. Time Stamping Service Participants

1.4.1. Certification Authorities

Within a TSS, the TSU certificates are supplied by a CA. These certificates allow Relying Parties to identify the TSA.

1.4.2. Time-Stamping Authorities

A Time-Stamping Authority and a Time-Stamping Service Provider are two notions that come naturally together.

Time-Stamping Service Provider (TSSP) is a person or an entity responsible to operate the Time Stamping Service (TSS), in order to manage / generate Time Stamp Tokens (TST), in order to manage the requests from the Subscribers, and meet the requirements of Relying Parties.

- The TSSP includes at least one TSA but could have several depending on its organization. Certificates of TSU will identify the TSSP, and the corresponding TSA.
- TMCA TSSP includes the TSA in-charge of the TSS, having one or more TSUs, with at least one Policy / Policy Identifier (OID).
- TSA is designated in the name of TSSP and shall function under the responsibility of the TSSP.

In the scope of this TSP/TSPS, the term TSA is used in the context of TSSP. It designates the TMCA TSA in charge of applying this TSP/TSPS, within the TMCA TSSP.

The TSA is managed by the TMCA Policy Authority. The Policy Authority consists of representatives from executive management, PKI operations and legal.

The Policy Authority approves the TSP and the documents regarding the TSS provided by TMCA. The Policy Authority has the final authority and responsibility for:

- specifying and approving the infrastructure and practices of the TMCA TSS;
- approving the TMCA TSP/TSPS;
- ensuring the persistent application of the TSP/TSPS stated by the TSA in the scope of functional, organizational and technical requirements;
- ensuring the persistent application of the compliance of the TSU implementation with the TSPS;
- publishing the TSP/TSPS and the ToU and their revisions to Subscribers and Relying Parties through the website.

1.4.3. Subscribers

A Subscriber is an entity requiring the services provided by TSA and which has agreed to its ToU.

1.4.4. Relying Parties

A Relying Party is an individual or entity that acts in reliance on a TST generated under this policy by the TMCA TSA. A Relying Party may, or may not also be a Subscriber.

1.4.5. Other Participants

Not applicable.

1.5. Policy administration

1.5.1. Organization administering the document

TMCA PKI Policy Authority
Telekom Applied Business Sdn Bhd
Menara TM One, No. 1,
Jalan Damansara, 60000
Kuala Lumpur, Malaysia
Phone: …
Email: …
Website: ..

1.5.2. Contact person

Questions concerning this TSP/TSPS should be sent to:

The Time-Stamping Policy Manager
Attn: Policy Director
Telekom Applied Business Sdn Bhd
Menara TM One, No. 1,
Jalan Damansara, 60000
Kuala Lumpur, Malaysia
Phone: …
Email: …
Website: ..

1.5.3. Person determining TSP/TSPS suitability for the policy

The TMCA PKI Policy Authority determines the suitability and applicability of this TSP/TSPS.

1.5.4. TSP/TSPS approval procedures

The approval of the conformance of the documented practices with the CP is pronounced by TMCA Policy Authority, in the light of the internal audits performed.

1.6. Definitions and Acronyms

Definitions
Auditor:
Person auditing the events of the TSS.

Certificate Revocation List (CRL):
The Certificate Revocation List is a list, digitally signed by the CA, and containing all the identifiers of the certificates that have been revoked prior to their expiration date.

Hash value:
Result of a hash function which characterizes a datum; it is a bit string with a fixed length for a specific hash function (for example 256 bits for SHA-256).

Hosting Provider:
Entity which hosts the technical platform of the service in a secure environment and in high availability network access.

Partners:
TMCA defines a partner as a person, a group, a community or an entity with which TMCA partners in order to provide its TSS to Subscribers and Relying Parties.

Time-Stamping Service (TSS):
Set of operations necessary to perform generation and management of TSTs.

Time-Stamping System:
Set consisting of all the TSUs together with the administration and supervision components used in order to provide the TSS.

Time-Stamp Token (TST):
Data object that binds a representation of a datum to a particular time, expressed in universal time (UTC), thus establishing evidence that the datum existed at that time.

Time-Stamping Unit (TSU):
Set of hardware and software used to create TSTs, characterized by an identifier of the Time-Stamping Unit certified by a CA, and which has a designated TST signing key

Acronyms	Description
CA	Certification Authority
CRL	Certificate Revocation List
NTP	Network Time Protocol
OID	Object Identifier
ToU	Terms of Use
TSA	Time-Stamping Authority
TSP	Time-Stamping Policy
TSPS	Time-Stamping Practice Statement
TSS	Time-Stamping Service
TSSP	Time-Stamping Service Provider
TST	Time-Stamp Token
TSU	Time-Stamping Unit

2. Publication and repository responsibilities

2.1. Repositories

TMCA, as a TSA, provides Relying Parties with this TSP/TSPS. This TSP/TSPS is available on Internet, on the TMCA website.

Repository URL: http://repository.TMCA.com

2.2. Publication of information

The published information's are the following:

- this TSP/TSPS;
- the corresponding ToU;
- the certificates of the TSUs.

2.3. Time or frequency of publication

A new TSP/TSPS will be published whenever there is a new major version approved.

The TSU certificates are published at most 24 hours after their generation and necessarily prior to their effective use.

2.4. Access controls on repositories

The published information's are published on the TMCA web site and can be freely read by anyone. The TSP and the ToU are freely readable by anyone wishing to access them on the TMCA website.

Additions, removal and modifications of these information are limited to authorized TMCA personnel, through access control.

3. General provisions

3.1. TSA obligations

- TMCA must comply with the requirements and the procedures defined in this TSP/TSPS.
- TMCA must comply with any additional obligations indicated in the TST either directly or incorporated by reference.
- TMCA must supply a TSS in accordance with its TSP/TSPS.
- TMCA must fulfill all its commitments in compliance with its ToU.
- TMCA must ensure the technical issuance of the TSTs.
- TMCA must ensure that its TSP/TSPS is applied and that the requirements specified in the present TSP/TSPS are satisfied.

3.2. Subscriber obligations

The Subscriber must accept and abide by the ToU of the TMCA TSS.

The Subscriber should also verify that the certificate of the TSU which delivers a TST is valid when the time-stamp request is performed.

3.3. Relying Party obligations

The Relying Party must verify that the TST have been correctly signed and that the corresponding TSU certificate is not revoked at the time of verification, by using the CRLs published by the TMCA CA.

The Relying Party must also verify that the TSTs requests are actually issued by an TMCA TSU. To do so, the Relying Party must verify that the TST includes a reference to an TMCA TSU.

Finally, the Relying Party should take into account the TST use limitations described in this TSP/TSPS and the related ToU.

3.4. Obligations for the CAs providing the TSU certificates

The TSU certificates must be issued by a CA which has been qualified according to the TMCA Certificate Policy. TSU certificates shall not be issued directly under the Root CA or an Intermediate that signs subordinate CAs.

3.5. Time Stamping Practice Statement (TSPS)

TMCA ensures that it has the reliability needed to provide a TSS and describes within this TSP/TSPS, how this TSS is implemented. This document warrants that:

1. TMCA carries out a risk assessment in order to evaluate business assets and threats to those assets in order to determine the necessary controls and operational procedures;

2. TMCA has a statement of the practices and procedures used to address all the requirements identified in the present TSP/TSPS;
3. The TSP/TSPS identifies the obligations and the implementation requirements to be complied with by the TSA, the Partners, the Subscribers and the Relying Party, in the scope of TMCA TSS;
4. TMCA provides Subscribers and Relying Parties with the public part of its TSP/TSPS (by including it in its ToU), so that they can assess conformance to this TSP/TSPS.
5. TMCA implements a relevant organization for the approval of its TSP/TSPS and the verification of conformity between this statement and this TSP/TSPS;
6. TSA ensures that the practices are properly implemented;
7. TMCA defines a periodic control procedure in order to verify that its practices comply with its TSP/TSPS;
8. TMCA aims at certification of compliance with the present TSP/TSPS delivered by an independent certification body.

Subsequently, any amendment initiated by TMCA and which could affect the compliance with its TSP/TSPS will again is submitted to the opinion of an independent certification body.

3.6. Terms of Use (ToU)

TMCA provides its ToU to its Subscribers. Subscribers must respect the clauses contained in these ToU.

These ToU are public and are published on TMCA website.

3.7. Conformance with legal requirements

3.7.1. Applicable law

The TSA under TMCA PKI shall be used by the subscribers and relying parties in accordance with the laws and regulations of the jurisdiction in which they are used or relied upon. The governing law for the purposes of this document shall be Malaysian Law, which shall supersede in case of contradictions.

3.7.2. Litigation settlement

In case of litigation between the parties resulting from the interpretation, the application and/or the execution of the contract, and in the absence of mutual agreement between the aforementioned parties, the only competent jurisdiction is India.

3.7.3. Intellectual property of TMCA infrastructures

Regarding intellectual property, the products operated to provide the TSS belong to TMCA.

The Subscribers or Relying Parties of these services have no intellectual property rights to these various elements. Any use or reproduction, total or partial, of these elements and/or information within, by any means, is strictly prohibited and is a forgery punishable under the Legislation relating to Intellectual Property, unless TMCA has previously given its written consent for such use or reproduction.

3.7.4. Personal data

The certificates issued under TMCA PKI shall be used by the subscribers and relying parties' only in accordance with the laws and regulations of the jurisdiction in which they are used or relied upon, subject to the definitions made in section 3.7.1 above. Subscribers are hereby informed that personal data they provide may be transferred and processed by TMCA and its partners involved in the given exchanges, in compliance with TMCA CP/CPS.

Subscribers are informed that they have the right to access, correct and delete the data regarding themselves by contacting TMCA.

They notably have no right to collect or to use in an inappropriate way the personal data they access, and generally speaking, to act in a way likely to be damaging to private life or to personal reputation.

TMCA is bound to keep the information provided by the Subscribers confidential, unless its disclosure is allowed by the Subscriber or demanded by regulation or adjudication.

3.8. Amendments

3.8.1. Procedure for amendment

TMCA is responsible, through its Policy Authority, for the creation, approval, maintenance, and modifications of the current TSP/TSPS.

When a new version of the TSP/TSPS is approved by the TMCA Policy Authority, it will be published on TMCA website and will replace the terms of the previous version.

3.8.2. Notification mechanisms and period

New version of the TSP/TSPS is notified through publication of it in the TMCA website for the information of all the Subscribers and Relying Parties of the TMCA TSS.

Unless otherwise stated, the new version of the TSP/TSPS will take immediate effect after its publication and will remain in effect until a further new version takes effect.

3.8.3. Circumstances under which OID must be changed

If the Policy Authority determines that an OID change is necessary, the new version will indicate the new OID.

The Policy Authority remains the only judge to determine if an OID change is necessary.

4. Operational requirements

4.1. Management of the TST requests

TMCA provides a service for the management of the TST requests. The specific conditions of this service are described in the ToU accepted by the subscribers.

4.2. Audit log

Unless otherwise mentioned, TMCA ensures that any appropriate information regarding the TSS operation is kept Seven (7) years after the corresponding TSU has been decommissioned, mainly in order to provide evidence in case of legal investigation.

Audit logs cover events relating to:

- generation of TST;
- administration of the TSS: context management, certificate import, service status;
- operation and synchronization of internal clock; TSU keys life cycle;
- TSU certificates life cycle;
- any kind of events which might impact the TSU operation.

Each audit record contains a precise date and time of the event.

The audit log confidentiality is ensured by appropriate management of the physical, system, and network access. The integrity is cryptographically ensured.

The management of these records complies with the management of TMCA classified information.

4.3. Private Key life cycle management

TMCA ensures that the private signing keys of the TSU are not used after the end of their life cycle.

The TSU destroys the private key when the usage period of the key is reached. TSU keys are not renewed.

TMCA ensures the number of TSUs in operation at any given time is sufficient to provide a reliable service.

4.4. Clock synchronization

TMCA ensures that its clocks are synchronized with the universal time (UTC) with the declared accuracy of one second.

More specifically:

1. the calibration of the TSU is maintained so that the clocks shall not be expected to drift outside the declared accuracy;

2. the TSU clocks are protected against threats related to their environment that could lead to a desynchronization with respect to UTC time outside the declared accuracy;
3. TMCA ensures that a TSU internal clock drift outside the bounds of the declared accuracy is detected.
4. if the clock of one of the TSU is detected as outside the declared accuracy, then TSTs will not be generated anymore until it is corrected;
5. TMCA ensures that clock synchronization is maintained when a leap second occurs as notified by the appropriate body. The change to take into account the leap second shall occur during the last minute of the day when the leap second is scheduled to occur. A record of the exact time (within the declared accuracy) is performed when this change occurs.

4.5. Time Stamp Token (TST)

TMCA ensures that the TSTs are generated securely and include the correct time.

4.5.1. Content of a TST

In the answer to a Subscriber request, TMCA provides a TST complying with the [RFC 3161], containing the fields as per TST profile provided in Section 7.2

4.5.2. TST signature

The signatures are based on the key algorithms (defined under Section 6.7).

All Signature Algorithms are used in conjunction with Digest Algorithm of SHA-256 or a hash algorithm that is equally or more resistant to a collision attack.

4.6. TSA compromise

In the case of events impacting the security of the TSS and which could impact the generated TSTs, TMCA ensures that appropriate information is provided to Subscribers and Relying Parties.

The TSA compromise could be caused by:

- the compromise of the TSU private keys;
- the compromise of the TMCA CA private key used to generate the TSU certificates;
- an operational problem.

TMCA has taken into account in its Disaster Recovery Plan the potential compromise of its TSS.

4.6.1. Disaster Recovery Plan

The Disaster Recovery Plan addresses the compromise of TSU private signing key, either actual or suspected, or the loss of calibration of a TSU clock, which might impact the issued TSTs.

TMCA ensures that all necessary measures have been taken in order to avoid operational incidents.

TMCA constantly updates its Disaster Recovery Plan in order to cover and to ensure the best possible service against the following threats:

- private key compromise; network failures;
- unavailability of qualified personnel;
- problems with clock calibration;
- failure of hardware components.

More generally, incidents on the TSS will be handled according to the incident management procedure in effect at TMCA.

4.6.2. Communication

In case of a compromise, real or suspected, or the loss of calibration of a TSU, that could impact generated TSTs, TMCA will notify the details through its website.

4.6.3. Interruption of TST generation

In case of a compromise, real or suspected, or the loss of calibration of a TSU, that could impact generated TSTs, TMCA takes all necessary measures to ensure that this TSU does not generate any further TSTs until steps are taken to restore the situation.

4.6.4. Information on TST validity

In case of a major compromise of TMCA operation or loss of calibration which might impact the issued TSTs, whenever possible, TMCA shall make available to all Subscribers and Relying Parties information which may be used to identify the TST which may have been impacted, unless this has breached the security of the TSS.

4.6.5. Alert

In case of a compromise, real or suspected, of its TSS, TMCA will notify directly and without delay to provided contact details with TMCA.

4.7. End of activity

Procedures to handle the end of an activity are defined by TMCA. Through these procedures, TMCA ensures that potential disruptions to Subscribers and Relying Parties are minimized should the TSS cease activity. In particular, TMCA ensures that all the information necessary to verify the correctness of TSTs will be provided, even after the termination of its TSS.

Prior to the termination of its TSS, the following procedures will be performed:

- TMCA will notify all its Subscribers and Relying Parties of the upcoming termination by publishing this information on its website;
- TMCA will terminate the authorization of all subcontractors to act on its behalf in carrying out any functions relating to the process of issuing TST;
- TMCA will transfer obligations to a “reliable body” _for maintaining event logs and audit archives necessary to demonstrate its correct operation for a reasonable period;

- TMCA will maintain its obligations to make available its public keys or certificates to relying parties for a reasonable period;
- the TSU private keys will be destroyed so that they cannot be retrieved, according to the procedure described in section 4.3.

TMCA takes all necessary measures to cover the costs to fulfil these minimum requirements in case it becomes bankrupt or for other reasons is unable to cover the costs by itself.

The provisions made for termination of service include:

- Notification to Subscribers and Relying Parties;
- Transfer of TMCA obligations to an identified reliable body, mentioned earlier.

5. Facility, management, and operational controls

5.1. Physical controls

5.1.1. Site location and construction

TMCA relies on secured premises to host its TSS. These premises feature locked rooms, cages and lockers.

5.1.2. Physical access

Access to TSS facilities is strictly restricted to authorized personnel listed on an access list. These authorizations are stated to the TMCA hosting provider and a logbook is updated each time maintenance is performed on the TSS equipment. This logbook records the following information:

- the date and time of the operation;
- the last name and first name of the persons present; the description of the maintenance operation;
- the date and time of the end of the operation; the signature of the persons present. Physical access is furthermore restricted by implementing mechanisms to control access into the high-security zones of the hosting provider. These mechanisms imply that authorized administrators own access cards.

The access security is strengthened by a biometric reader.
Access profiles to a zone are defined and maintained by the TSA and transferred to the hosting provider.

TMCA secured areas are audited on a regular basis to verify that the access control systems are always operational and running. Monitoring and logging systems are implemented in all sites for all secured areas.

Access controls apply to all secured zones.

5.1.3. Power and air conditioning

Emergency controls are operated by the hosting provider so that, the disruption of power supply or an air conditioning failure does not jeopardize TMCA commitments in terms of availability.

5.1.4. Water exposures

The specification of the security perimeter takes into account the risks related to water exposures. Protection controls are operated by the hosting provider in order to prevent from residual risks (pipe break for instance).

5.1.5. Fire prevention and protection

Secured areas benefit from appropriate prevention and protection against fire exposures.

5.1.6. Media storage

Media are stored securely. Backup media are securely stored in a separate location from the original media location.

All media storage areas are protected from fire, water exposure and damages.
Paper documents are kept by the TSS in secured locked premises and stored in a safe to which opening means are known only to the authorized TSA Officer and authorized personnel.

5.1.7. Waste disposal

Materials listed as confidentially sensitive are subject to destruction, or can be used again in a similar operational context at the same level of sensitivity.

5.1.8. Off-site backup

In order to ensure a recovery complying with its commitments after an incident, TMCA implements off-site backups of information and critical functions.

TMCA ensures that backups are exported out of the production site and are protected as regards confidentiality and integrity.

5.2. Procedural controls

5.2.1 Trusted roles

The following Trusted Roles are defined:

- TSA Security Officer: has responsibility for all security issues of the TSS
- TSA System Administrator: installs, configures and maintains the trustworthy systems of the TSS.
- TSA System Operator: responsible for operating the TSU on a day-to-day basis.
- TSA System Auditor: responsible for the day-to-day analysis of the audit logs.

Operations and supervisions are all performed by TMCA personnel.

5.2.2 Number of persons required per task

The TSA enforces procedures to ensure that multiple people in a Trusted Role are required to perform sensitive tasks.

5.2.3. Identification and authentication for each role

Identification and authentication controls are defined in order to support the implementations of the access control policy and the accountability of operations. The access control policy limits access to authorized personnel on a need to know basis.

Personnel in trusted roles are appointed by Policy Authority, with written notifications to the concerned person(s)

5.2.4. Roles requiring separation of duties

TMCA ensures that security procedures are separated from standard exploitation procedures and that they are always performed under the supervision of a personal in a trusted role.

5.2.5. Risks analysis

A risk analysis is carried out on the TSS in order to identify the threats on the TSU.

5.2.6. System access management

Identification and authentication:
Systems, applications and databases uniquely identify and authenticate operators and administrators. Any interaction between the system and an operator is possible only after successful identification and authentication. For any interaction, the system checks the identity of the operating personnel.

Authentication information is stored in a way they can only be accessed by authorized users.

Access control:
Profiles and access rights to the TSA equipment are specified and documented, as well as the registration/deregistration procedures of operating personnel.

Systems, applications and databases can distinguish and manage the access rights for each user on objects subject to rights management, at user level, at group level, or both. It is possible to:

- deny users or groups of users the access to an object;
- limit user access to an object to operations which do not modify this object;
- grant access rights to an object with the granularity level of the individual user

Someone who is not an authorized user cannot grant nor deny access rights to an object. Likewise, only authorized users are allowed to create new users, and to suppress or suspend existing users.

Someone who is not an authorized user cannot grant nor deny access rights to an object. Likewise, only authorized users are allowed to create new users, and to suppress or suspend existing users.

Administration and operation:
Usage of utility tools is restricted and controlled.

5.2.7. Operation management

System planning:
Systems load are monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available.

Protection against malicious codes:
Monitoring, detection and prevention are implemented on every component of the TSS so as to provide protection against malicious software.

Network security controls:
Implemented controls comply with the strategy of TMCA risks management for information systems. The TSS is implemented on a network protected firewall. These firewalls are configured to accept only connections which are strictly necessary.

The network communications transferring confidential information are protected against eavesdropping.

Security controls are implemented in order to protect the local components of the information system from non-authorized access.

Media handling and security:
All sensitive media of the TSS are subject to maintenance procedures in order to ensure the availability of functions and information.

End of life conditions (destruction and waste disposal) of equipment are documented in order to ensure the non-disclosure of sensitive information they may enclose.

Exchange of information:
Security controls are implemented in order to ensure the authentication of origin, the integrity and the confidentiality, when necessary, of exchanged data between parties involved in the process.

5.2.8. Trustworthy systems deployment and maintenance

The TSS use trustworthy components. In particular, the TSUs meet the regulatory requirements. The TSA Policy Authority is notified of any substantial change of the system.

Releases are subject to an update of the operational procedures. Controls of maintenance operations are implemented.

Proper performance of applications:
The development and test infrastructures are separated from the operational infrastructures of the TSS.

Criteria of acceptance and validation of new systems, upgrades and new versions are documented and appropriate tests are performed before acceptance and production step.

5.2.9. Incident reporting and response

Operation monitoring is possible through the audit logs.
Any TSU malfunction is immediately notified to the supervisor and operator of the TMCA platform. These notifications notably regard:

- Start /stop of services ;
- Desynchronization of the TSS clocks;
- TSS network problems.

Each event is stored in a database from which all service events, including incidents, can be traced. If an incident occurs, TMCA will act in an appropriate way in order to react rapidly, to limit the impact of security exposure and to restore the service in the best possible time.

5.3. Personnel controls

TMCA has documented information security for human resources. TMCA notably states that personnel in a Trusted Role of the TSS are carefully selected and clearly informed of operations and rules to be followed.

5.3.1. Qualifications, experience, and clearance requirements

Any person in a Trusted Role is subject to a clause of confidentiality, managed by TMCA. TMCA ensures that the professional skills of personnel in Trusted Roles comply with the requirements of their functions. TMCA management has appropriate expertise, and is familiar with security procedures. Any person in a Trusted Role is informed of his responsibility through its job description and/or procedures related to system security and personnel control.

Personnel working on the TMCA TSS possess appropriate knowledge of:

- time-stamping technology;
- digital signature technology;
- mechanisms for calibration or synchronization of the TSU clocks with UTC;
- security procedures, for personnel with security responsibilities;
- Information security and risk assessment.

5.3.2. Background check procedures

TMCA performs a background check prior to recruiting new personnel, in order to ensure the suitability with the open position.

5.3.3. Training requirements

Personnel are trained regarding software and hardware in use and regarding the application of internal procedures.

5.3.4. Retraining frequency and requirements

Each change of systems, procedures or organization results in information or training of the operating personnel when this change impacts the work of this category of personnel.

Operating personnel are trained regarding incident management and escalation.

5.3.5. Job rotation frequency and sequence

Not applicable.

5.3.6. Sanctions for unauthorized actions

Sanctions in case of unauthorized actions are listed in an IT charter and through the document regarding information security for human resources. All TMCA personnel are informed of these sanctions.

5.3.7. Independent contractor requirements

Requirements towards subcontractors are subject to contracts.

The commitments include contracts relating to service supply, non-disclosure agreements and IT charter.

5.3.8. Documentation supplied to personnel

Personnel are informed of the security rules related to their role as soon as they are appointed. Person in charge of an operational role in the TSS are provided with related procedures.

6. Technical security controls

6.1. Time accuracy

TSU clocks are managed and monitored through reference time servers. These servers are autonomous and are synchronized with UTC (k) reference servers. The mechanisms used allow the system to withstand attacks aiming at desynchronizing time sources, even major attacks against radio or satellite signals.

TMCA ensures that the TSTs generated by its TSS have an accuracy with respect to UTC time of less than one second.

6.2. Key generation

TMCA ensures that all cryptographic keys are generated in a controlled environment. Specifically, TSU signing keys are generated within a time-stamping module.

The generation of TSU cryptographic keys is performed within hardware security modules. TSU private keys are never exported outside of these modules.

The key generations are based on the supported key algorithms (defined under Section 6.7).

6.3. Certification of TSU keys

A TSU certificate request is transmitted to the TMCA CA, in accordance with the rules defined in the corresponding Certificate Policy.

The certificates delivered by the CA conform to the profile defined in the Certificate Policy.
The TSA abides by its obligations defined in the Certificate Policy of the CA.

The TSA verifies, when importing a certificate in a TSU that it comes from the TMCA CA.

6.4. Protection of TSU private keys

TMCA ensures that the TSU private keys are kept confidential and guarantees their integrity. Specifically, the TSU signing keys are kept and used within the time-stamping module.

6.5. Backup of TSU private keys

TMCA forbids the archival and backup of TSU private keys.

6.6. Destruction of TSU private keys

TMCA ensures that TSU private keys are destroyed at the end of their life cycle.

6.7. Mandatory algorithms

The TMCA TSA:

1. accepts hash values generated by Subscribers and using hash algorithms in compliance with regulatory requirements. The accepted hash algorithms are the following:

   SHA-1, SHA-256, SHA-384 and SHA-512

2. issues TSTs signed with algorithms and key lengths in compliance with regulatory requirements. TMCA ensures usage of minimum key length of 2,048-bit modulus certificates for RSA / DSA algorithms and minimum key length of 256bit for ECC algorithms. The signature algorithm uses a hash function belonging to the SHA-2 family.

6.8. TST verification

TMCA ensures that Relying Parties can obtain information needed to verify the digital signature of TSTs. TMCA notably ensures that the TSU certificates are available, either attached to the TSTs or from the TMCA website.

6.9. Validity period of TSU certificates

A TSU certificate is valid for maximum of 135 months. TMCA ensures that the algorithm and the key size are known to be adequate for this validity period.

6.10. Usage period of TSU private keys

The private key linked to the TSU certificate and which signs TSTs has a usage period of one year. However, Subscribers and Relying Parties can verify the validity of TSTs for at least till the TSU certificate expiry after their generation.

7. Certificate and TST profiles

7.1. Certificate profile

Base fields Version	V3
Serial Number	Unique Non-Sequential CSPRNG Number and is greater than zero.
Signature Algorithm	SHA-256, SHA-384 or SHA-512 with RSA _Encryption or ECDSA with SHA-256, SHA-384 or SHA-512
Issuer: CN	<Issuing CA Common Name>
Issuer: O	<Issuing CA Organization name>
Issuer: OU	<Issuing CA Organization unit>
Issuer: C	<Issuing CA Country>
Valid From	Start date expressed in UTC format
Valid To	Start date expressed in UTC format
Public Key	RSA 2048, 4096 (OR) ECC curves NIST P_-256, P-384, or P-521
Subject: CommonName	Common Name of TSA
Subject: OrganizationName	Legal Name of TSA Organization
Subject: OrganizationalUnitName	Variable Information representing TSU
Subject: CountryName	Country of TSA
Key Usage	Critical=TRUE digitalSignature
Enhanced Key Usage	id-kp-timeStamping
Certificate Policies	Critical=FALSE 1. Policy ID=1.3.6.1.4.1.50977.1.2.500 (User Notice, Time Stamping Certificate) 2. Policy ID=1.3.6.1.4.1.50977.1.0.1 (CPS), http://repository.TMCA.com
Subject Key Identifier	Critical=FALSE 160-bit hash (SHA-1)
Authority Key Identifier	Critical=FALSE 160-bit hash (SHA-1)
Basic Constraints	Critical=TRUE Subject Type=End Entity
CRL Distribution Points	Critical=FALSE CRL HTTP URL = http://crl.TMCA.com?<IssuerName>.crl

7.2. TST profile

Version	Version 1
policy	Policy OID as per Section 1.2 of this document.
messageImprint	OID of the hash algorithm and the hash value of the data to Timestamp.

	Note: this information is provided by the Subscriber in the request.
serialNumber	160-bit number uniquely identifying the TST
genTime	Time-stamp date in ASN.1 Generalized Time format
accuracy	Accuracy of 1 second
ordering	Flag set to FALSE
nonce	Value sent back identically if contained in the request
tsa	DN Details of the TSU Note: This field is the same as the “subject” of the certificate used to sign the TST.
extensions	Not used

8. Compliance audit and other assessments

8.1. Frequency or circumstances of assessment

TMCA shall comply to compliance audits as under:

- Minimum of one annual audit performed by a qualified auditor identified under Section 8.2.
- Minimum one audit, every 3 months, termed as. internal audit, performed by TMCA PKI, or a practitioner identified and/or approved by TMCA PKI.

TMCA shall also conduct suitable audit by its internal or external auditor for:

- Any qualification (new / renewal) by a regulator.
- Any major changes to this TSP/TSPS, as may be identified by TMCA Policy Authority.

8.2. Identity/qualifications of assessor

The assessor must act with rigour in order to ensure that policies, statements and services are properly implemented and to detect the non-compliance items which might jeopardize the security of the service.

The TSA commits to hire assessors with a high level of expertise in system security, particularly in the field of the audited component.

8.3. Assessor's relationship to assessed entity

The assessor is appointed by TMCA, and is allowed to audit the practices ruling the target component of the audit. Assessor may be part of TMCA but is independent from the TSA operations.

8.4. Topics covered by assessment

The assessor operates compliance audits of the specified component, covering totally or partly the implementation of:

- the TSP/TSPS;
- the TSS

Prior to every audit, the assessor will provide the TSA Policy Authority with a list of components and procedures they wish to audit, and will subsequently prepare the detailed audit program.

8.5. Actions taken as a result of deficiency

Following the compliance audit, the assessment team gives the TSA the result which can be "success", "failure" or "to be confirmed"

In case of failure, the assessment team delivers recommendations to the TSA. The TSA then decides which actions to perform.

In case of result to be confirmed, the assessment team identifies the non-compliances and prioritizes them. The TSA then schedules the correction of these non-compliances. A validation audit then checks for their effective corrections.

In case of success, the TSA confirms that the audited component complies with the requirements of the TSP/TSPS.

8.6. Communication of results

The audit results are made available to the Policy Authority of TMCA and to any other external organization for necessary qualification or other purposes (Example: Regulator, Application Provider, Trust Store Provider, etc.).