Timestamp Policy / Timestamp Practice statement

Thailand Post e-Timestamp

Version 1.0

Contents

DOCUMENT MAINTENANCE

This document is valid from the day of its publication on Thailand Post's website (marked in the revision history table below) and until a new published version of the document is made available.

Revision History

Date	Version	Summary of change
October 2021	1.0	Initial issue

1. Introduction

This document titled TimeStamp Policy / TimeStamp Practice Statement Thailand Post e-Timestamp (to be referred to as “TP/TPS” hereafter) has been prepared for the purpose of explaining the technical and legal requirements met by the Thailand Post e-Timestamp.

The present document specifies policy and security requirements relating to the operation and management practices of the Thailand Post e-Timestamp proceeding time-stamps. Such time-stamps can be used for preventing document modification , supporting digital signatures or for any application requiring to prove that a datum existed before a particular time.

This policy describes the obligations that the Thailand Post e-Timestamp should respect while proceeding, handling or delivering time-stamps. It is also intended to inform subscribers and relying parties about their obligations towards the time-stamps usage.

2. Scope

The Thailand Post e-Timestamp uses its public key infrastructure and trusted time sources to provide reliable, standards-based time-stamps. This Time-stamp Policy/Practice Statement defines the operational and management practices of the Thailand Post such that Subscribers and Relying Parties may evaluate their confidence in the operation of the time-stamping services. The Thailand Post e-Timestamp aims to deliver time-stamping services used in support of qualified electronic document, as well as under applicable Thailand electronic transaction law and regulations. However, Thailand Post e-Timestamp may be equally applied to any application requiring proof that a datum existed before a particular time.

3. Reference of standard and regulation

ETSI TS 101 861 : Time stamp Authority Policy Requirement

ETSI TS-102-023 : Time Stamping Profile

RFC 3161 : Time-stamp Protocol (TSP)

IETF RFC 5544: Syntax for Binding Documents with Time-Stamps

FIPS 140-2 Level 2 and 3 : "Security Requirements for Cryptographic Module”

4. Definitions and Abbreviations

4.1 Definitions

- **Coordinated Universal Time (UTC) :** time scale based on the second as defined in Recommendation ITU-R TF.460-6
- **Relying party** : natural or legal person that relies upon an electronic identification or a trust service Subscriber : legal or natural person bound by agreement with a trust service provider 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
- **Trust service :** electronic service which enhances trust and confidence in electronic transactions Time-stamp token : data object defined in IETF RFC 3161, representing a time-stamp
- **Trust service policy :** set of rules that indicates the applicability of a trust service to a particular community and/or class of application with common security requirements
- **Trust service practice statement :** statement of the practices that a TSP employs in providing a trust service
- **Trust service provider :** entity which provides one or more trust services
- **Time-Stamping Authority (TSA) :** TSP which issues time-stamps using one or more time-stamping units
- **Time-Stamping Unit (TSU) :** set of hardware and software which is managed as a unit and has a single time-stamp signing key active at a time
- **TSA Disclosure statement :** set of statements about the policies and practices of a TSA 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

4.2 Abbreviations

CA	Certification Authority
GMT	Greenwich Mean Time
IT	Information Technology
TSA	Time-Stamping Authority
TSP	Trust Service Providers
TSU	Time-Stamping Unit
TST	Time-Stamp Token
UTC	Coordinated Universal Time

5. General Concepts

5.1 Time-Stamping Services & Usage

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

- Time-stamping provision : This service component generates time-stamps compliant with the RFC 3161.
- Time-stamping management : This service component monitors 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.

5.2 Timestamping services parties

5.2.1. Time Stamping Authority (TSA)

An industry standard compliant Trust Service Provider (TSP) providing timestamping services to the public is called the Time Stamping Authority (TSA). The TSA has the overall responsibility for the provision of the timestamping services identified in clause 5.1.

Thailand Post e-Timestamp service working with a certificate Timestamp Authority known as “uanataca”. Uanataca is a Trust Service Provider (TSP) and source of Trust obtain from European Union Trusted Lists (EUTL).

5.2.2. Subscriber

Currently, the Thailand Post e-Timestamp service available to an organization subscriber, this entity will be directly responsible for fulfilling User obligations as indicated in the Terms of Use & Privacy policy.

6. Timestamp Policies

6.1 Overview

This Thailand Post e-Timestamp TP/TPS is set of rules that indicates the applicability of a Time-Stamp Token (TST) to a particular community or class of application with common security requirements, which include:

- The TSU, private keys, and profiles of public key certificates are in compliance with technical specifications of the RFC 3161
- The Thailand Post e-Timestamp TSA holds private keys used in signing timestamps.
- Delivering timestamping services based on 99.5 % availability.
- Authenticating requests for e-Timestamping process.
- Providing trustworthy time-stamp
- Time synchronization with Thailand post GPS and National Institute of Metrology (Thailand) NTP server.
- Means used in requesting for timestamps include the Transfer Control Protocol (TCP)

6.2 Document Name and Identification

The object identifier (OID) for the Thailand Post e-Timestamp TP/TPS is 2.16.764.1.4.1.3.2.1

By including this object identifier in a timestamp, the Thailand Post e-Timestamp claims conformance to the identified time-stamp policy and so the ETSI time-stamping identifier is being supported.

6.3 User Community and Applicability

The Thailand Post e-Timestamp User Community is composed of subscribers and relying parties. Accordingly, subscribers are also regarded as relying parties.

This Thailand Post e-Timestamp TP/TPS is aimed at meeting the requirements of timestamping qualified for long term validity, but is generally applicable to any requirement for an equivalent quality.

This policy does not define restrictions on the applicability of the timestamps issued.

6.4 Conformance

To show conformance with this document, the Thailand Post e-Timestamp uses the identifier for the timestamp policy established in Section 6.2 (Document Name and Identification) of this document in its issued TSTs.

The Thailand Post e-Timestamp is subject to periodic independent internal audits. The Thailand Post e-Timestamp guarantees conformance of its implemented controls and ensures that it meets common security requirements

7. Policies and practices

7.1 Risk Assessment

Thailand Post e-Timestamp performs risk assessments on a regular basis to ensure the quality and reliability of the time-stamping services. The security controls related to the time-stamping services are regularly reviewed and revised by an independent body, trained trustworthy personal check the adherence of the security controls.

The Thailand Post management approve the risk assessment and accept the residual risk identified.

7.2 Trust service practice statement

Security controls for the timestamping service are fully documented and regularly reviewed by an independent auditor to ensure alignment with the ISO/IEC 27001 requirements.

Additionally, the following measures have been applied to ensure the quality, performance and operation of the timestamping service for the following services.

7.3 Timestamp format

The Timestamp Tokens (TSTs) issued by Thailand Post e-Timestamp are compliant to RFC 3161 requirements.

The service issues timestamps with an RSA algorithm and a key length of 2048, which accepts the SHA256 hash algorithm.

7.4 Accuracy of the time

The time signal is provided via GPS-NTP in 1st priority. The time-stamping service uses this time signal and a set of ntp servers as time sources. With that setup the timestamping service reaches an accuracy of the time of +/-100ms or better with respect to UTC.

7.5 Limitations of the service

For detailed information, please see “Terms of Use & Privacy Policy”.

7.6 Terms and conditions

Within the published document “Terms and conditions for timestamp customers” information about e.g. limitation of the service, subscribers obligations, information for relying parties or limitations of liability can be found.

7.7 Information Security Policy

Thailand Post e-Timestamp has implemented an information systems security policy throughout the company. All employees must adhere to the regulations stipulated in that policy and derived security concepts.

7.8 TimeStamp policy

As specified in ISO/IEC 27001, a Time-Stamp Policy is a form of Trust Service Policy. This is applicable to trust service providers issuing timestamps.

The policy herein states that Thailand Post e-Timestamp :

- Provide a trustworthy service for all Subscribers and Relying Parties,
- Is issuing of TimeStamp Tokens in compliance with the RFC 3161,
- Ensure that the private keys of the TimeStamp Services are protected at all time
- Ensure that audits are performed in every year,

8. Thailand Post e-Timestamp Management and Operation

8.1 Introduction

Thailand Post e-Timestamp has implemented a corporate information security framework (a set of policies, processes, organizational culture, technical and operational practices, etc) in order to meet its strategic objectives related to IT security.

8.2 Internal organization

Thailand Post’s organizational structure, policies, procedures and controls are applicable to Thailand Post e-Timestamp.

8.3 Personal Security Controls

All persons filling timestamping operations are selected on the basis of skills, loyalty, trustworthiness, and integrity. Persons should at the minimum have no criminal record.

Appropriate disciplinary sanctions are applied to personnel violating TSP policies or procedures.

Both permanent and temporary employees have their job descriptions taking into account segregation of duties and least privilege.

Trusted roles in Thailand Post e-Timestamp are formally assigned by the senior management. Thailand Post e-Timestamp has ensured the definition of critical roles such as :

- Security Officers: Overall responsibility for administering the implementation of the security practices.
- System Administrators: Authorized to install, configure and maintain the Thailand Post e-Timestamp service trustworthy systems for service management.
- System Auditors: Authorized to view archives and audit logs of the Thailand Post e-Timestamp service trustworthy systems.

8.4 Asset management

Thailand Post e-Timestamp ensures proportionate and risk-based levels of protection for its information assets and maintains an accurate and up to date inventory of these assets, including systems and applications.

All media are securely handled and disposed of when no longer required, in accordance with Thailand Post's Information Security Classification and Handling Policy and standard.

All changes made on the Thailand Post e-Timestamp system, applications and appliances are done in line with the documented and approved Thailand post's change management processes and procedures. In line with change management best practices, the Thailand Post e-Timestamp system development, test and production environments are completely segregated.

8.5 Access Control

The Thailand Post e-Timestamp system access is restricted to authorized individuals. In particular:

a) Multiple Firewalls technologies are implemented to protect Thailand Post e-Timestamp internal network and to prevent all protocols and accesses not required for its operations.
b) User account management and timely modification or removal of access are deployed.
c) Computer security controls are activated for the separation of trusted roles, including the separation of security administration and operation functions.
d) Thailand Post e-Timestamp is identified and authenticated before using service. Thailand Post e-Timestamp personnel is accountable for their activities.

e) All sensitive data is protected against disclosure through re-used storage objects being accessible to unauthorized users.

f) The Thailand Post e-Timestamp systems and services are constantly monitored to ensure timely identification of and response to any security events.

g) All activities Logs are kept in the centralize log system

8.6 Timestamping

- Thailand Post e-Timestamp employs timestamping on all security related transactions using trusted time source.
- The time values, the TSU uses in the timestamp is traceable to at least one of the real time values distributed by a UTC(k) laboratory.
- Thailand Post e-Timestamp requires an authentication, the validly account shall process e-timestamp
- The timestamp generation system of Thailand Post e-Timestamp automatically reject any attempt to issue timestamps if the authentication failed.

8.7 Clock Synchronization

The Thailand Post e-Timestamp clock is synchronized with UTC Time within the declared accuracy with the following particular requirements:

- The calibration of the TSU clocks is maintained such that the clocks do not drift outside the declared accuracy.
- The declared accuracy shall be of 1 second.
- Thailand Post e-Timestamp has protected its TSU clocks against threats which could takes it outside its calibration.
- Thailand Post e-Timestamp ensure that timestamp issuance will be stopped in case of drifts or jumps out of synchronization with UTC.
- The clock synchronization shall be maintained when a leap second occurs. 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.

8.8 Physical Security Controls

All Thailand Post e-Timestamp equipments, including all system and application, are protected from unauthorized access at all times.

Physical security controls have been applied to all Thailand Post e-Timestamp and any remote workstations used to administer the trust system, except where specifically noted.

The time-stamping service itself is located in a physical secured environment that minimizes the risk of natural disasters.

The private keys of the TSU are securely stored in a FIPS 140-2 Level 2 and 3 certification HSM.

The big lines related to Thailand Post e-Timestamp physical security controls are given below:

Physical access

The Thailand Post e-Timestamp equipments are protected from unauthorized access. The following physical access control requirements applies

- security zones exist with enforced new authorization for each level
- Card number and username are will occur in the log for Physical Access to the secure premises.
- Two-factor authentication are needed for the secure area access
- Visitors are required to provide identification for the secure area in a manual log-book
- CCTV cameras monitors all personnel within the secure area

Thailand Post e-Timestamp has setted multiple physical security controls, the following topics are covered:

- Power and air conditioning
- Water exposures
- Fire prevention and protection
- Physical Intrusion detection system
- Uninterrupted Power supply systems
- CCTV cameras

8.9 Operation security

Thailand Post e-Timestamp uses trustworthy systems and products that are protected against modification. In order to ensure the technical security and reliability of the processes supported by them, the following steps were taken :

a) An analysis of security requirements is carried out at the design and requirements specification stage of any systems.

b) Capacity requirements and scalability testing are planned to ensure the future required capacities of the timestamp service,

c) Change control procedures are applied for releases, modifications and emergency software fixes of any operational software.

d) The integrity of Thailand Post e-Timestamp systems and information are protected against viruses, malicious and unauthorized software through the use of antivirus systems and integrity check systems.

e) No media as electronic document keeps in Thailand Post e-Timestamp storage.

f) Thailand Post e-Timestamp has implemented several procedures for all trusted and administrative roles that impact on the provision of services.

g) Thailand Post e-Timestamp security officers perform periodic monitoring for new security patches and vulnerabilities that should be applied within a reasonable time after being tested.

8.10 Network security controls

Thailand Post e-Timestamp system is connected to one internal network and is protected by firewalls, a Demilitarized Zone (DMZ) and Network Address Translation for all internal IP addresses.

Firewalls and boundary control devices are configured to allow access only by the addresses, ports, protocols and commands required for the trustworthy provision of time stamping services by such systems. It is the Thailand Post's security policy to block all ports and protocols and open only necessary ports to enable Time stamping functions. The Thailand Post e-Timestamp equipment is configured with a minimum number of services and all unused network ports and services are disabled. All firewall configurations and changes thereto are documented, authorized and implemented in accordance with the relevant interval procedure.

Thailand Post's network configuration is available for review on-site by its auditors and consultants under an appropriate non-disclosure agreement.

8.11 Incident Management

- Thailand Post e-Timestamp monitoring activities includes access to IT systems, user of IT systems, and service requests . Sensitivity of any information collected or analyzed is taken into account.
- Thailand Post e-Timestamp has defined an incident management procedure which includes a reporting and a notification process in order to respond efficiently to those problems by appropriate parties.

- Deep analysis are accurately conducted to avoid a new happening of an incident. Audit logs shall be monitored or reviewed regularly to identify evidence of malicious activity.
- Thailand Post e-Timestamp will notify, without undue delay, any natural or legal person to whom the trusted service has been provided, about a breach of security or loss of integrity in case if this is likely to adversely affect him.

8.12 Collection of evidence

The Thailand Post e-Timestamp system records shall be kept accessible for an appropriate period, including after the activities of the Thailand Post e-Timestamp system have ceased.

All the relevant Thailand Post e-Timestamp system records shall be securely stored in case of future need to provide evidence in legal proceedings and to ensure continuity of the service.

The confidentiality and integrity of current and archived records concerning operation of services is maintained.

- Records concerning all events relating to all activity with The Thailand Post e-Timestamp system
- Records concerning all events relating to incident detection of The Thailand Post e-Timestamp system
- The events are logged in a way that cannot be deleted or destroyed for a period of 90 days.

8.13 Business continuity management

In the case of compromise, or suspected compromise or loss of calibration when issuing timestamps, Thailand Post e-Timestamp system will take the following steps;

- Make available to all affected subscribers and relying parties a description of the incident that has occurred and actions taken to mitigate the impact.
- The Thailand Post e-Timestamp system may partially or fully suspend issuing of timestamps until steps have been taken to recover from the compromise.

8.14 Thailand Post e-Timestamp termination plan

In the event of termination of its operations for any reason whatsoever, Thailand Post e-Timestamp shall;

- Notify the subscribers, relying parties and other affected entities. To minimize disruptions from the termination of services, the notification shall be done prior to termination.

- Implement the necessary measures that ensure retention of all the relevant archived records prior to the service termination.
- Terminate authorization of any subcontractors to act on its behalf in carrying out any functions relating to the timestamping service.
- If deemed appropriate, transfer obligations (provision of timestamping services) to an identified reliable third party.

8.15 Compliance

Thailand Post e-Timestamp is convinced that compliance is a key factor for business success. In order to achieve this, Thailand Post e-Timestamp will ensure compliance with applicable Thailand's law and standards about electronics transaction. Specifically, it is aligned with:

- ETSI TS 101 861 : Time stamp Authority Policy Requirement
- ETSI TS-102-023 : Time Stamping Profile
- RFC 3161 : Time-stamp Protocol (TSP)
- IETF RFC 5544: Syntax for Binding Documents with Time-Stamps