Agence Nationale de Certification Electronique

TunStamp Authority
Timestamp Policy / Timestamp Practice Statement

Review

Version	Date	Comment	Section/Page
00	15/02/2017	1st Writing	Whole document
01	17/03/2017	2nd revision	Add section 5.5 Review section 7.2.1 and 7.3.2
02	24/04/2017	3rd revision	Review of section 6.2 and section 7.2.2
03	28/09/2018	4th revision	Whole document
04	12/09/2019	5th revision	Sections 1, 7.2.2, 8.3, 8.6.3, 8.7, 8.10, 8.12, 8.14, 8.15 and 9.1
04.1	16/11/2022	6th revision	Sections 1, 2, 3, 4.1, 4.2, 5.1, 5.2, 6.1, 6.3, 6.4, 7.1, 7.2.1, 7.2.2, 7.3, 7.6, 8.2, 8.6, 8.6.1, 8.6.3, 8.6.6, 8.7.1, 8.7.2, 8.8, 8.9, 8.10, 8.11, 8.13 and 8.14

Approval of the document

	Wrote by	Validated by	Approved by
Function :	TunTrust	TunTrust Board of Directors	TunTrust Board of Directors
Date :	09/11/2022	16/11/2022	16/11/2022

Contents

1 Introduction

The Agence Nationale de Certification Electronique (TunTrust) was founded in accordance with Law no. 2000-83 of 9 August 2000 governing electronic exchanges and commerce in Tunisia. The Agence Nationale de Certification Electronique is a government-owned Certificate Authority (CA) and will be referred to in the remainder of this document with its trademark name "TunTrust".

This document entitled TimeStamp Policy / TimeStamp Practice Statement of the TunStamp Authority (to be referred to as “TP/TPS” hereafter) has been prepared for the purpose of explaining the technical and legal requirements met by the Tunisian TimeStamp Authority (to be referred to as “TunStamp”).

The present document specifies policy and security requirements relating to the operation and management practices of the TunStamp Authority 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.

This TP/TPS is applicable to all persons, including, without limitation, all requesters, Subscribers, Relying Parties, registration authorities and any other persons, that have a relationship with TunTrust with respect to timestamps issued by the TunStamp Authority.

This TP/TPS also provides statements of the rights and obligations of TunStamp Authority, authorized registration authorities, Applicants, Subscribers and Relying Parties that use or rely on timestamps issued by the TunStamp Authority.
The present document can be used by independent bodies as the basis for confirming that TunStamp can be trusted for issuing time-stamps according to international standards.

The structure and contents of this TP/TPS are laid out in accordance with ETSI EN 319 421" Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps". In the event of any inconsistency between this TP/TPS document and the ETSI EN 319 421, the requirements set out in the ETSI EN 319 421 document take precedence over this one.

2 Scope

TunTrust 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 TunStamp authority such that Subscribers and Relying Parties may evaluate their trust in the operation of the time-stamping services.
TunTrust aims to deliver time-stamping services used in support of qualified electronic signatures, as well as under applicable Tunisian law and regulations. However, TunTrust time-

stamps may be equally applied to any application requiring proof that a datum existed before a particular time.

The present document does not specify:

- Protocols used to access the TSUs;
- How the requirements identified herein can be assessed by an independent body;
- Requirements for information to be made available to such independent bodies;
- Requirements on such independent bodies.

3 References

This TP/TPS describes the practices used to comply with the current versions of the following policies, guidelines, and requirements:

1. Recommendation ITU-R TF.460-6 (2002): "Standard-frequency and time-signal emissions".
2. ISO/IEC 19790:2012: "Information technology -- Security techniques -- Security requirements for cryptographic modules".
3. ISO/IEC 15408 (parts 1 to 3): "Information technology -- Security techniques -- Evaluation criteria for IT security".
4. ETSI EN 319 421: Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
5. ETSI EN 319 422: Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles
6. ETSI EN 319 401 : Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
7. ETSI TS 101 861 : Electronic Signatures and Infrastructures (ESI); Time stamping profile
8. RFC 3628: Policy Requirements for Time-Stamping Authorities
9. RFC 3161, Internet X.509 Public Key Infrastructure Time-stamp Protocol (TSP)
10. FIPS PUB 140-2 (2001): "Security Requirements for Cryptographic Modules".

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

Time-Stamping Authority (TSA) : TSP which issues time-stamps using one or more time-stamping units
Time-stamping service: trust service for issuing time-stamps.

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 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

Trust Service Provider (TSP): entity which provides one or more trust services

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

UTC(k): time scale realized by the laboratory "k" and kept in close agreement with UTC, with the goal to reach ±100 ns.

4.2 Abbreviations

BIPM	Bureau International des Poids et Mesures
BTSP	Best practices Time-Stamp Policy
CA	Certification Authority
GMT	Greenwich Mean Time
IERS	International Earth Rotation and Reference System Service
IT	Information Technology
TAI	International Atomic Time
TP	TimeStamp Policy
TPS	TimeStamp Practice Statement
TSA	Time-Stamping Authority

TSP	Trust Service Providers
TST	TimeStamp Token
TSU	Time-Stamping Unit
UTC	Coordinated Universal Time

5 General Concepts

5.1 Time-Stamping Services

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 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.

5.2 Time-Stamping Authority (TSA)

TunTrust is the Tunisian timestamp provider responsible of provisioning time-stamps services to the public. It has the responsibility for the operation of the one or more time-stamp units that are creating and signing on behalf of the TunStamp Authority.

TunStamp Authority operates time-stamping units.

This authority is trusted by Subscribers and Relying Parties for the issued time-stamp Tokens.

Although providing time-stamp services could be outsourced, TunTrust has the ultimate responsibility of ensuring that the requirements of the time-stamp policy herein are met.

TunStamp Authority is :

- compliant with this TP/TPS,
- providing trustworthy time-stamps,
- providing UTC time accuracy of ± 1 second,
- delivering time-stamping services based on minimum 99,9% availability,
- performing internal and external audits to assure compliance to this TP/TPS,
- ensuring that all requirements and procedures detailed in this TP/TPS are implemented,
- authenticating requests for time countermarks using electronic certificates or by Remote address authentication.

5.3 Subscribers

Subscribers are either Legal Entities or natural persons that have agreed to the TunStamp Subscriber Agreement.

- When the Subscriber is an individual, he / she will be held directly responsible if his / her obligations are not correctly fulfilled.

- When the Subscriber is an organization, 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 the organization is expected to suitably inform its end-users.

5.4 Relying parties

Relying parties are individuals or organizations that use timestamps of the TunStamp Authority to verify the timestamp. Relying parties are allowed to use such timestamps only in accordance with the terms and conditions set forth in this TP/TPS. It is in their sole responsibility to verify legal validity and applicable policies.

The terms and conditions set for Relying Parties include an obligation on the Relying Party that, when relying on a time-stamp token, the Relying Party shall:

a) verify that the time-stamp token has been correctly signed and that the private key used to sign the timestamp has not been compromised until the time of the verification. TunStamp publishes an online tool for validating a signed digital signature and time stamp, publicly available at the following url: https://www.tuntrust.tn/content/utiliser-gratuitement-la-solution-de-signature

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

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

After expiry of the time-stamp certificate, the Relying Party should:

– verify that the TSU private key is not revoked, and

– verify that the cryptographic hash function and the signing algorithm used in the timestamp token are still considered secure.

5.5 Time-Stamp Policy and TSA Practice Statement

5.5.1 Purpose

The TunTrust Time-Stamp Policy (“what is adhered to”) and the TunTrust Timestamp Practice Statement (“how it is adhered to”) have been merged into one document, the TunStamp-TP/TPS. This document specifies a time-stamp policy and practice statement to meet general requirements for trusted time-stamping services as defined by the standards in section 2 (References) of this document.

5.5.2 Level of Specificity

This TunStamp TP/TPS extends the CP/CPS of the Tunisian National PKI which regulates the operation of the Tunisian National PKI and associated non-repudiation services. Both of the documents are public documents and may be downloaded at https://www.tuntrust.tn/repository.

5.5.3 Approach

The TunStamp TP/TPS establishes the general rules concerning the operation of the Tunstamp TSA. Additional internal documents define how TunTrust meets the technical, organizational, and procedural requirements identified in the TunStamp TP/TPS. These documents may be provided only under strictly controlled conditions.

6 Time-Stamp Policies

6.1 Overview

This TunStamp TP/TPS is a set of rules that indicates the applicability of a 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 and RFC 3628.
- The TunStamp TSA holds private keys used in signing time-stamps.
- TSTs are issued with the accuracy of ± 1 second, as indicated in Section 5.2 (Timestamping Authority).
- Means used in requesting for time-stamps include the Transfer Control Protocol (TCP) and Hypertext Transfer Protocol (HTTP).

6.2 Document Name and Identification

The object identifier (OID) for the TunStamp TP/TPS is : 2.16.788.1.2.6.1.11
Through the conclusion of this object identified in the issued tokens for electronic timestamp, TunTrust confirms compliance with this policy.
The object identifier described above is in compliance with ETSI BRSP (Best Practices Policy for Time-Stamps) OID=0.4.0.2023.1.1, in accordance with the standard ETSI EN 319 421.

6.3 User Community and Applicability

The TunStamp TSA's User Community is composed of Subscribers and Relying Parties. Accordingly, Subscribers are also regarded as Relying Parties.

This TunStamp TP/TPS aims to meet the requirements of time-stamping qualified digital signatures 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 time-stamps issued.

6.4 Conformance

To show conformance with this document, the TunStamp TSA uses the identifier for the time-stamp policy established in Section 6.2 (Document Name and Identification) of this document in its issued TSTs.

The TunStamp TSA is subject to periodic independent internal and external audits. The TunStamp TSA guarantees conformance of its implemented controls and ensures that it meets its obligations specified in Section 5.2 (TimeStamping Authority) of this document.

7 Policies and practices

7.1 Risk Assessment

TunTrust carries out a risk assessment to evaluate business risks and determine the necessary security requirements and operational procedures. This risk analysis performed with the full support and collaboration of all component services providers and is regularly reviewed and revised if necessary. This risk analysis is available as an internal document.
TunTrust performs annual risk assessments that:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Process;
2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that TunTrust has in place to counter such threats.

7.2 Trust Service Practice Statement

Based on the Risk Assessment, TunTrust develops, implements, and maintains a security plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to manage and control the risks identified during the Risk Assessment. The security plan includes administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the Timestamping Data. The security plan also considers then-available technology and the cost of implementing the specific measures, and implements a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

Additionally to be compliant to ETSI EN 319 421, the following measures have been applied in order to guarantee the quality, performance and operation of the time-stamping service:

7.2.1 The Timestamp request format

The timestamp client must support the Timestamp request in accordance with the IETF RFC 3161 section 2.4.1 Standard. In particular, it is recommended to use the following fields:

- nonce
- hash algorithm SHA256 or greater.

7.2.2 The Timestamp response format

TunStamp supports the timestamp response in accordance with the IETF RFC 3161 Chapter 2.4.2 Standard, with the following additional requirements:

- It is mandatory to use the "accuracy" field;
- Use of the "nonce" field is recommended. In the case of using the "nonce" field in the timestamp request, the response timestamp must contain the same value as the request.
- hash algorithm SHA256 or greater.

TunStamp uses policies related to cryptographic algorithms and the length of the signature keys of the Timestamp conforms to what is specified in ETSI TS 119 312 .

7.2.3 Accuracy of the time

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

7.2.4 Limitations of the service

Every TSU certificate is issued at least once a year with a validity period of 03 years each.
Thereby, the TunStamp digital signature on the Time-Stamp Token (TST) has a validity period of two years. So, the expected validity period of every TST is two years.
The timestamp service can only be provided to authorized TunStamp Subscribers holding a valid electronic certificate in order to authenticate to the TunStamp server or having an authorized public IP address.

7.3 Terms and conditions

Within the “Terms and conditions for timestamp Subscribers”, which is publicly available at https://www.tuntrust.tn/repository, information about e.g. limitation of the service, Subscribers obligations, information for Relying Parties or limitations of liability can be found. Additionally, the following information apply:

7.3.1 Trust service policy being applied

The present document represents the applied trust service policy, see chapter 6 for further information.

7.3.2 Period of time during which TSP event logs are retained.

TunTrust retains any audit logs generated for at least seven years. TunTrust makes these audit logs available to its Qualified Auditor upon request.

TunTrust retains all documentation relating to timestamp requests and the verification thereof, and all timestamps and revocation thereof, for at least 20 years after any timestamp based on that documentation ceases to be valid.

7.4 Information Security Policy

TunTrust Board of Directors is responsible for defining the information security policy and ensuring publication and communication of the policy to all personnel who are impacted by the policy.

This information security policy is implemented with the full support and collaboration of all component services providers and is regularly reviewed and revised if necessary. Appropriate systems, infrastructures and measures for quality and information security management are implemented and maintained at all times. Any changes that would impact on the level of security provided must be approved by TunTrust through its TunTrust Board of Directors. The TunTrust information security policy as well as documentation on security controls and operating procedures is available as separate and internal documents.

7.5 TimeStamp policy and TSA practice statement

As specified in ETSI EN 319 401, a Time-Stamp Policy is a form of Trust Service Policy. However, TSA Practice Statement is a form of Trust Service Practice Statement. Both are applicable to trust service providers issuing time-stamps. TunTrust makes the choice to combine them in a unique policy specifying the general requirements for trusted time-stamping services and how those last are met.

The policy herein states that TunTrust :

- Provides a trustworthy service for all Subscribers and Relying Parties,
- Is issuing TimeStamp Tokens in compliance with the RFC 3161,
- Ensures that the private keys of the TimeStamp Services are protected at all time,
- Is compliant with Tunisian law and regulations,
- Ensures that audits are performed by an independent body.

7.6 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.

7.7 Information for relying parties

When relying on a time-stamp, relying parties have to:

a) verify that the time-stamp 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;

b) consider any limitations on the usage of the time-stamp indicated by the time-stamp policy; and
c) consider any other precautions prescribed in agreements or elsewhere.

8 TSA Management and Operation

8.1 Introduction

TunTrust 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

TunTrust, which is a legal entity according to Tunisian national law, ensures that :

- Trust service practices under which TunStamp operates are non-discriminatory.

- Trust services are accessible to all applicants whose activities fall within its declared field of operation and that agree to abide by their obligations as specified in sections 5.3 & 5.4 of the present policy.

- TunTrust has documented agreements and contractual relationships in place where the provisioning of services involves subcontracting, outsourcing or other third-party arrangements.

- TunTrust has implemented an information security management system to maintain the security of the trust service provided.

- TunTrust employs sufficient number of personnel having the necessary education, training, technical knowledge and experience relating to the type, range and volume of work necessary to provide time-stamping services. In order to satisfy this adequacy, periodic improvement of the required skills and competencies in addition to providing interims are applied.

8.3 Personnel Security Controls

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

The requirements governing the qualifications, selection and oversight of individuals who operate, manage, oversee, and audit the CA are set forth in the CP/CPS.

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 TunTrust are formally assigned by the senior management. TunTrust has ensured the definition of critical roles such as:

Validation Specialist	Employees responsible for routine certification services such as customer services, document control, processes relating to Subscriber Certificate registration, generation and revocation. They are also responsible for interacting with Applicants and Subscribers, managing the Certificate request queue and completing the Certificate approval checklist as identity vetting items are successfully completed. A person to whom this role is assigned can be a shareholder of CA private keys activation data.
System Administrator	The System Administrator is responsible for the installation and configuration of PKI components (CA, RA, ...). This administrator is also responsible for keeping PKI systems updated with software patches and other maintenance needed for system stability and recoverability. A person to whom this role is assigned can be a shareholder of CA private keys activation data.
System Operator	The System Operator is responsible for the installation and configuration of the system hardware, including servers and different components of the Front End / Internal Support System. The System Administrator is also responsible for keeping systems updated with software patches and other maintenance needed for system stability and recoverability. A person to whom this role is assigned can be a shareholder of CA private keys activation data.
Application Administrator	The Application Administrator is is responsible for the installation, configuration and operations of the applications related to TunTrust.
Physical and Logical Security Officer	The Physical and Logical Security Officer is responsible for the installation and configuration of the physical security platforms (access control, video surveillance, IDS, ...) and the logical security platforms (firewalls, WAF, routers, network configuration). A person to whom this role is assigned can be a shareholder of CA private keys activation data.

Auditor	The Auditor is authorized to view archives and audit logs. The auditor is also responsible for overseeing internal compliance to determine if TunTrust is operating in accordance with this CP/CPS. This includes acting as internal auditor in TunTrust key ceremonies. A person to whom this role is assigned cannot be a shareholder of CA private keys activation data.
Key/Ceremony Manager	The Key/Ceremony Manager is responsible of conducting the key ceremonies.
Shareholders	Holders of secret shares needed to operate TunTrust CA private keys.

8.4 Asset management

TunTrust has ensured an appropriate level of protection of its assets including information assets.

TunTrust has maintained an inventory of all information assets and has assigned a classification consistent with the risk assessment.

All media are handled securely in accordance with requirements of the information classification scheme.

Media containing sensitive data is securely disposed of when no longer required.

8.5 Access control

TunTrust time-stamping system access is restricted to authorized individuals.

In particular:
a) Multiple Firewalls technologies are implemented to protect TunTrust 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) TunTrust personnel is identified and authenticated before using critical applications related to the service. TunTrust personnel is accountable for their activities.

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

8.6 Cryptographic control

TunTrust key pair generation creates a verifiable audit trail that the security requirements procedures were followed. Only TSA authorized personnel are allowed to create new key-pairs. Private keys and TSA certificates are not used after the end of its life cycle. A private key is destroyed after its end-of-life.

8.6.1 TSU Key generation

For the generation of the TSU's signing keys, TunTrust performs the following controls:

1. generates the keys in a physically secured environment as described in this TP/TPS;
2. generates the TSU keys using personnel in trusted roles under the principles of multiple person control and split knowledge;
3. generates the TSU keys within cryptographic modules which are trustworthy systems, assured by FIPS 140-2 Level 3 and meeting the applicable technical and business requirements as disclosed in this TP/TPS;
4. The TSU key generation algorithm, the resulting signing key length and signature algorithm used for signing time-stamps key should be as specified in ETSI TS 119 312,
5. A TSU's signing key should not be imported into different cryptographic modules;
6. A TSU shall have a single time-stamp signing key active at a time.
7. logs its TSU key generation activities; and
8. maintains effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in this TP/TPS and (if applicable) its Key Generation Script.

8.6.2 TSU private key protection

TunStamp private keys are protected within a hardware security module (HSM) meeting FIPS 140-2 Level 3.

Copying, storing or recovering operations carried out on the TSU's backed up signing keys are undertaken in a physically secured environment by personnel in trusted roles under dual control. The personnel authorized to carry out those actions is limited to those required to do so under TunStamp's practices.

8.6.3 TSU public key certificate

TunTrust ensures the integrity and authenticity of its signature keys when made available to Relying Parties.

The electronic certificates are published on TunTrust website: https://www.tuntrust.tn/repository

The minimum length of key used for electronic signing/marking of issued timestamps is 2048 bits.

TunTrust CAs certificate profiles description is available as in the naming and profile document (published in the repository https://www.tuntrust.tn/repository).

8.6.4 Rekeying TSU's key

In standard situations (expiry of the term of a certificate of the relevant TSU), the replacement of data for the verification of electronic signatures/marks in issued timestamps shall be sufficiently in advance prior to the expiry of the term of the certificate performed in the form of issuance of a new certificate of the relevant TSU.

In the event of non-standard situations (for example in the event of a development of cryptanalytic methods that may endanger the security of the process of creation of electronic signatures/marks, i.e. a change in encryption algorithms, key length, etc.), the replacement shall be performed at the adequate time.

Both in the event of standard and non-standard situations, the replacement of data for the verification of electronic signatures/marks in a certificate of the relevant TSU shall be notified to the general public in advance (if possible) and in an appropriate manner.

8.6.5 Certificate Revocation and Suspension

TunTrust does not provide the service of certificate suspension.

TunTrust will revoke the TSA Certificate if one or more of the following occurs:

a) TunTrust obtains evidence that the TSA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise;
b) TunTrust obtains evidence that the Certificate was misused;
c) TunTrust is made aware that the Certificate was not issued in accordance with or that the TSA has not complied with the applicable TP/TPS;
d) TunTrust determines that any of the information appearing in the TSU Certificate is inaccurate or misleading;
e) TunTrust or the TSA ceases operations for any reason;
f) TunTrust or TSA's right to issue timestamps under these Requirements expires or is revoked or terminated;
g) Revocation is required by TunTrust TP/TPS; or
h) The technical content or format of the TSU Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties.

8.6.6 Life cycle management of signing cryptographic hardware

TunTrust ensures that :

- The time-stamp signing cryptographic hardware won't be tampered with during shipment or when and while stored. In the process of receipt of the HSM, the correctness and integrity of the seals of the manufacturer's shipping container are inspected. The HSM is stored in a safe place with a controlled access, and the basic installation including tests, synchronization and inspection follow. Each of the above activities shall be recorded in writing.
- The installation, initialization, inspection and synchronization of the TSU is performed by persons in trusted roles and in the presence of witnesses. In the event of having the TSU hardware repaired or in the event of termination of the provision of certification

services or in the event of termination of the activities of TunTrust, the data for the creation of electronic signatures/marks of generated timestamps shall be destroyed as recommended by the manufacturer. Specific procedures of the TSU administration are described in the relevant internal documents of TunTrust.

- Activation and duplication of TunStamp's signing keys in cryptographic hardware is done only by personnel in trusted roles using dual control in a physically secured environment.
- TunStamp private signing keys stored on TSU cryptographic module will be erased upon device retirement in a way that it is practically impossible to recover them.

8.6.7 End of TSU key life cycle

TunTrust defines an expiration date for TSU's keys which is not to be longer than the end of validity of the associate public key certificate. However, in order to be able to verify during a sufficient lapse of time the validity of the time-stamps, the validity of the TunStamp's signing key will be reduced.

The expiration date for TunStamp's keys is to be defined when the TSU cryptographic module is initialized or by setting a private key usage period within the TSU's public key certificate.

TunTrust ensures that its private signing keys will not be used beyond the end of their life cycle :

- Operational or technical procedures will be in place to ensure that a new key is put in place when TunStamp's key expires.

- TunStamp private signing keys including any copies will be destroyed such that the private keys cannot be retrieved.

The life cycle of a certificate ends in the following cases :

- Expiration of the timestamp certificate or
- Revocation of the timestamp certificate.

8.7 Time-stamping

8.7.1 Time-stamp issuance

TunStamp employs time-stamping on all security related transactions using a trusted time source.

TunStamp uses a key generated exclusively for time-stamp signing.

The time-stamp generation system of TunStamp automatically rejects any attempt to issue time-stamps if the signing private key has expired.

TunTrust makes available for Subscribers and Relying Parties a tool that tests a timestamp issued by TunStamp as an input and displays information about this specific timestamp. The tool is available online at https://www.tuntrust.tn/content/utiliser-gratuitement-la-solution-de-signature .

8.7.2 Clock Synchronization

The TunStamp 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.
- TunTrust has protected its TSU clocks against threats which could take it outside its calibration.
- TunTrust ensures that time-stamp 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. A record shall be maintained of the exact time (within the declared accuracy) when this change occurred.

8.8 Physical and environment Security

Entry to TunTrust Data Centers containing the TSUs certificate manufacturing facility is achieved only through a limited number of access points controlled by security personnel on duty full time (24 hours per day, 365 days per year). Intruder detection systems including infrared walls are installed and regularly tested to cover all external doors of the data centers housing the TSUs operational facilities. All critical TSUs operations take place within a physically secure facility with at least four layers of security to access sensitive hardware or software.

Such systems are physically separated from the organization’s other systems so that only authorized employees of TunTrust can access them. The secure parts of TunTrust hosting facilities are protected using physical access controls with biometric scanners or card access systems making them accessible only to appropriately authorized individuals.

TSUs operational facilities are physically locked and alarmed when unoccupied. All personnel and visitors entering and leaving TSUs operational facilities are logged. Entry, exit, and activities within TSUs facilities are under constant video surveillance. Third party support services personnel are granted restricted access to secure TSUs operational facilities only when required and such access is authorized and accompanied. Access rights to TSUs facilities are regularly reviewed and updated.

Physical and environmental security controls are implemented to protect the facility that houses system resources, the system resources themselves, and the facilities used to support their operation. The TSA's physical and environmental security policy for systems related to time-stamping management addresses as a minimum the physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking and entering, and disaster recovery.

All media containing production software and data, audit, archive, or backup information are stored within TunTrust facilities with appropriate physical and logical access controls designed to limit access to authorized personnel and protect such media from accidental damage such as water, fire, and electromagnetic.

TunTrust performs routine backups of critical system data, and other sensitive information. The backed-up data are stored in a physically secured offsite locations.

8.9 Operation security

TunTrust 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 management procedures are applied for releases, modifications and emergency software fixes of any operational software.

d) The integrity of TunTrust systems and information are protected against viruses, malicious and unauthorized software through the use of antivirus systems and integrity check systems.

e) Media used within time-stamping systems is securely handled to protect it from damage, theft, unauthorized access and obsolescence.

f) TunTrust has implemented several procedures for all trusted and administrative roles that impact on the provision of services.

g) TunTrust performs periodic monitoring for new security patches and vulnerabilities that should be applied within a reasonable time after being tested.

8.10 Network security controls

TunTrust’s CA system is connected to an internal network and is protected by firewalls, a Demilitarized Zone (DMZ) and Network Address Translation for all internal IP addresses. TunTrust 's customer support and vetting workstations are also protected by firewall(s) and only use 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 TSA services by such systems. It is TunTrust's security policy to block all ports and protocols and open only necessary ports to enable TSA functions. All TSA equipment are 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 change management procedures.

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

8.11 Incident Management

TunTrust TSA acts in a timely and coordinated manner to respond quickly to incidents and to limit the impact of security breaches.
TunTrust TSA has a defined and approved information security incident management process covering incident identification, categorization and response, among others.
Audit logs of the timestamping service are monitored and reviewed regularly to identify any evidence of potential security incidents.
TunTrust TSA monitoring activities cover various parameters including access to IT systems, usage of systems, availability of the service, among others. Taking into account the sensitivity of the information collected or analyzed from the TSA logs, appropriate access restrictions are implemented for all monitoring activities.
TunTrust TSA will notify, without undue delay, any affected Subscribers of any breach of security that may adversely impact them.

8.12 Collection of evidence

In the event of detecting a potential hacking attempt or other form of compromise, TunTrust refers to its incident management procedure and disaster recovery plan, and eventually performs an investigation in order to determine the nature and the degree of damage :

TSU key management

a) Records concerning all events related to the life-cycle of TSU keys will be logged.
b) Records concerning all events related to the life-cycle of TSU certificates will be logged.

Clock Synchronization

c) Records concerning all events related to synchronization of a TSU's clock to UTC will be logged. This includes 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 will be logged.

The confidentiality and integrity of current and archived records concerning operation of services shall be maintained. They will be completely and confidentially archived in accordance with disclosed business practices.
Those records will be made available if required for the purposes of providing evidence of the correct operation of the services for the purpose of legal proceedings.
Those events will be securely saved in a way that they cannot be deleted easily or destroyed for a period of 20 years.

8.13 Business Continuity Management

TunTrust documents a business continuity procedure and disaster recovery plan designed to notify and reasonably protect Application Software Suppliers, Subscribers, and Relying Parties in the event of a disaster, security compromise, or business failure.
TunTrust does not disclose business continuity plans to Subscribers, Relying Parties, or to Application Software Suppliers, but will provide business continuity procedure and the risk treatment plan to TunTrust auditors upon request.
TunTrust annually tests, reviews, and updates these procedures. The business continuity procedure includes:

- The conditions for activating the plan,
- Emergency procedures,
- Fallback procedures,
- Resumption procedures,
- A maintenance schedule for the plan;
- Awareness and education requirements;
- The responsibilities of the individuals;
- Recovery time objective (RTO);
- Regular testing of contingency plans.
- TunTrust's plan to maintain or restore the CA's business operations in a timely manner following interruption to or failure of critical business processes ;
- A requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location;
- What constitutes an acceptable system outage and recovery time ;
- How frequently backup copies of essential business information and software are taken;
- The distance of recovery facilities to the CA's main site; and
- Procedures for securing its facility to the extent possible during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site.

8.14 TSA termination

In case of termination of TSA operations for any reason whatsoever, TunTrust will provide timely notice and transfer of responsibilities to succeeding entities, maintenance of records, and

remedies. Before terminating its own TSA activities, TunTrust will where possible take the following steps:

- Continued maintenance of information required to verify the correctness of trust services, for a reasonable period, will be provided.
- Giving Notice period without seeking Subscriber's consent.
- Make reasonable arrangements to preserve its records according to the applicable TP/TPS.
- Reserve its right to provide succession arrangements for the re-issuance of certificates by a successor TSA that has all relevant permissions to do so and complies with all necessary rules, while its operation is at least as secure as TunTrust is.

The requirements of this article may be varied by contract, to the extent that such modifications affect only the contracting part.

8.15 Compliance

TunTrust operates at all times in compliance to the following:

A. the applicable laws;

B. the requirements of this TP/TPS; and

C. the requirements of the then-current ETSI EN 319 401 and ETSI EN 319 421 (latest relevant version).

9 Other Business and Legal Matters

9.1 Dispute resolution provisions

In case of litigation or dispute, any party must notify TunTrust by registered letter with acknowledgment of receipt. TunTrust undertakes to process these notifications and to provide a response within thirty (30) days.

The requests are addressed directly or through a lawyer to the TunTrust 's CEO, by registered letter with acknowledgment of receipt.
The request must contain the following information :

- The name, the legal form, the registered office of the applicant and, where applicable, the registration number in the trade register,
- The name and registered office of the defendant;
- A detailed statement of the subject matter of the dispute and requests.

The application must be accompanied by all documents, correspondence and preliminary evidence.
The office of the agency is responsible for registering the request according to its number and date, in the business register.

The dispute can be settled amicably. In case of failure of the conciliation attempt, the courts of Ariana in Tunisia are competent.

9.2 Governing law

The laws and regulations in force in Tunisia are applied.

9.3 Compliance with applicable law

This TP/TPS is subject to the laws and regulations applicable in Tunisia.