National Digital Certification Agency

Timestamp Policy / Timestamp Practice Statement of the TunStamp Authority

Update

Rev	**Date**	**Revision Type**	**Page**
Rev 00	15/02/2017	1st Writing	Whole document
Rev 01	17/03/2017	1st revision	Add section 5.5 Review section 7.2.1 and 7.3.2

	Wrote by	**Validated by**	**Approved by**
Function :	NDCA	Board Commitee	CEO
Date :	14/03/2017	16/03/2017	17/03/2017

Contents

1 Introduction

This document titled 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 policy describes the obligations that the Tunisian TimeStamp authority should respect while generating, handling or delivering time-stamps. It is also intended to inform subscribers and relying parties about their obligations towards the time-stamps usage.

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/TSP 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 addition, the present document is aiming to meet the general requirements of the international community to provide trust and confidence in electronic transactions including, amongst others, applicable requirements from Regulation (EU) No 910/2014.

2 Scope

The TunStamp Authority 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 confidence in the operation of the time-stamping services.
The TunStamp aims to deliver time-stamping services used in support of qualified electronic signatures, as well as under applicable Tunisia law and regulations. However, TunStamp time-stamps may be equally applied to any application requiring proof that a datum existed before a particular time.

3 References

1. ETSI EN 319 421: Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
2. ETSI EN 319 422: Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles

3. ETSI EN 319 401 : Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
4. ETSI TS 101 861 : Electronic Signatures and Infrastructures (ESI); Time stamping profile
5. RFC 3628: Policy Requirements for Time-Stamping Authorities
6. RFC 3161, Internet X.509 Public Key Infrastructure Time-stamp Protocol (TSP)

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

NDCA	National Digital Certification Agency
BIPM	Bureau International des Poids et Mesures
BTSP	Best practices Time-Stamp Policy
CA	Certification Authority
GMT	Greenwich Mean Time
IT	Information Technology
TAI	International Atomic Time
TSA	Time-Stamping Authority
TSP	Trust Service Providers
TSU	Time-Stamping Unit
UTC	Coordinated Universal Time

5 General Concepts

5.1 TimeStamp Authority

TunStamp 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 unit that are creating and signing on behalf of the TunStamp Authority.

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

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

5.2 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 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.

5.3 TimeStamp Authority Obligations

TunStamp Authority is :

- Compliant with the NDCA's TunStamp policy,
- Providing trustworthy time-stamp,
- 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 policy
- Ensuring that all requirements and procedures detailed in this TSP are implemented,
- Authenticating requests for time countermarks using electronic certificates.

5.4 Subscribers

The subscriber refers to either an individual or an organization 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.

5.5 Relying parties

The terms and conditions made available to relying parties shall 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;

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.

5.6 Time-Stamp Policy and TSA Practice Statement

5.5.1 Purpose

The Tunstamp Time-Stamp Policy (“what is adhered to”) and the TunStamp Stamp 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 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 http://www.certification.tn.

5.4.3 Approach

The TunStamp TP/TPS establishes the general rules concerning the operation of the Tunstamp TSA. Additional internal documents define how NDCA 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 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 5.3 (Timestamp Authority Obligations).
- 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 : 2.16.788.1.2.6.1.10

By including this object identifier in a time-stamp, the TunStamp Authority 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 TunStamp TSA's User Community is composed of subscribers and relying parties. Accordingly, subscribers are also regarded as relying parties.

This TunStamp TP/TPS is aimed at meeting 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 5.3 (TimeStamp Authority Obligations) of this document.

7 Policies and practices

7.1 Risk Assessment

TunStamp Authority 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 TunStamp management approve the risk assessment and accept the residual risk identified.

7.2 Trust Service Practice Statement

Additionally to be compliant to ETSI TS 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. Time-stamp format

The issued time-stamp token by TunStamp are compliant to RFC 3161 time-stamps. The service issues RSA2048 encrypted time-stamps that accept one of the following hash algorithm:

- SHA256

7.2.2. Accuracy of the time

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

7.2.3. Limitations of the service

The timestamp service can only be provided to authorized TunStamp subscribers holding a valid electronic certificate in order to authenticate to the TunStamp timestamp server.

7.3 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. 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.

Event logs are retained for at least three month. Timestamp protocols, meaning every issued timestamp, are kept for at least 20 years.

7.4 Information Security Policy

TunStamp Authority 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.

7.5 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. TunStamp make 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 TunStamp :

- 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,
- Is compliant with Tunisian law and regulations,
- Ensure that audits are performed by an independent body,

8 TunStamp Management and Operation

8.1 Introduction

TunStamp 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

TunStamp, which is a legal entity according to Tunisian national law, ensure 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 section [6.3] of the present policy.

- TunStamp has a documented agreement and contractual relationship in place where the provisioning of services involves subcontracting, outsourcing or other third party arrangements.

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

- TunStamp employ 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 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 TunStamp are formally assigned by the senior management. Tunstamp 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 TSP trustworthy systems for service management.
- System Auditors: Authorized to view archives and audit logs of the TSP trustworthy systems.

8.4 Asset management

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

TunStamp 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

The TunStamp time-stamping system access is restricted to authorized individuals.

In particular:

a) Multiple Firewalls technologies are implemented to protect TunStamp 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) TunStamp personnel is identified and authenticated before using critical applications related to the service. TunStamp 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 Private Key Life-cycle Management

TunStamp key pair generation must create 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 shall not be used after end of its life cycle. A private key shall be destroyed after its end-of-life.

8.6.1 TSU Key generation

The generation of the TSU's signing keys are undertaken in a physically secured environment by personnel in trusted roles under dual control. The personnel authorized to carry out this function is limited to those required to do so under TunStamp's practices.

Access to the HSM within the TSA environment is restricted by the use of smartcard and biometric device. The HSM is always stored in a physically secure environment and subject to security controls throughout its lifecycle.

The TSU key generation algorithm, the resulting signing key length and signature algorithm used for signing time-stamps key are (recognized by the NACS: National Agency for Computer Security and) in accordance with the highest existing applicable standards.

Generation within the HSMs are manually logged in the Key-Ceremony Document.

8.6.2 TSU private key protection

TunStamp private keys are protected within a hardware security module (HSM) meeting Level 3 of the Federal Information Processing Standard 140 (FIPS 140).

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

TunStamp ensures the integrity and authenticity of its signature keys when made available to relying parties.

The electronic certificates are published on the NDCA's website: www.certification.tn, www.ance.tn

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

<u>TSU Certificate Basic field</u>

Field	Content
Version	V3
serialNumber	Unique serial number of issued certificate
SignatureAlgorithm	Identifier of the algorithm used for the electronic signature of the issued certificate to the particular TSU (sha256WithRSAEncryption)
Issuer	Identification of the issuer of the certificate
Validity NotBefore NotAfter	 Beginning of the term of the issued certificate (UTC) End of the term of the issued certificate (UTC)
Subject	Identification of the subscriber
SubjectPublicKeyInfo Algorithm SubjectPublicKey	 Identifier of the algorithm used by the public key indicated in the issued certificate Public key in the issued certificate (2048 bits)
Extensions	Certificate extensions

<u>Issuer</u>

Field	Content

Organization (O)	National Digital Certification Agency
Organization Unit (OU)	-
CommonName (CN)	TnTrust Gov CA
Country (C)	TN

Subject

Field	Content
Organization (O)	National Digital Certification Agency
Organization Unit (OU)	-
CommonName (CN)	ts* TnTrust Government Time Stamping
Country (C)	TN

Note: * - TunStamp has 3 instances of time stamping services (ts1, ts2 and ts3).

TSU Certificate Extensions

Field	Content	Critical
AuthorityKeyIdentifier	Hash of public key of certificate issuer	NO
SubjectKeyIdentifier	Hash of public key of issued certificate	NO
CRL Distribution Points	http://crl.certification.tn/tntrustgovca.crl	NO
KeyUsage	Digital Signature	YES
ExtendedKeyUsage	Id-kp-timeStamping	YES

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

NDCA does not provide the service of certificate suspension.

a) Certificate Revocation List
The profile of a certificate revocation list shall be in accordance with the internationally recognized standards and regulations.

b) Circumstances for Revocation
A TSU certificate may be revoked only under the following circumstances:

- the data for the creation of electronic signatures/marks used to sign/mark qualified certificates, qualified system certificates and certificate revocation lists have been compromised or there is a reasonable suspicion that the data have been compromised,

- the data for the creation of electronic signatures/marks of this particular TSU have been compromised or there is a reasonable suspicion that the data have been compromised NDCA shall revoke the certificate of particular TSU on the initiative of:
  - entities defined by applicable legislation,
  - CEO of NDCA.

8.6.6 Life cycle management of signing cryptographic hardware

TunStamp ensure 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 shall be inspected. The TSU shall be stored in a safe place with a controlled access, and the basic installation including tests, synchronization and inspection shall follow. Each of the above activities shall be recorded in writing.
- The installation, initialization, inspection and synchronization of the TSU shall be performed by persons in credible 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 NDCA, 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 NDCA.

- 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

TunStamp shall define an expiration date for TSU's keys which is not 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 be defined when the TSU cryptographic module is initialized or by setting a private key usage period within the TSU's public key certificate.

TunStamp ensure 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

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

- The time values the TSU uses in the time-stamp is traceable to at least one of the real time values distributed by a UTC(k) laboratory.

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

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

8.8 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.

- TunStamp has protected its TSU clocks against threats which could takes it outside its calibration.

- TunStamp ensure 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.

8.9 Physical Security Controls

All TunStamp equipments, including cryptographic modules, are running with a redundant installation. Backups are stored at an off-site location in order to grant disaster recovery and business continuity. They are protected from unauthorized access at all times.

Physical security controls have been applied to all TunStamp Authority 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 3 HSM.

The big lines related to TunStamp physical security controls are given below:

Physical access

The TunStamp equipments are protected from unauthorized access. The following physical access control requirements applies

- 3 different security zones exist with enforced new authorization for each level
- Card number and user name 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

Media storage

The following controls apply to media handling :

- Confidential media are stored in the archive room
- Dual control and two factor authentication applies to the archive room
- Media should be stored in a safe when not in the archive room
- Passwords and HSM cards are stored in safe

Off-site Backup

- All TunStamp systems are running with a redundant installation. Backups are stored at an off-site location in order to grant disaster recovery and business continuity.

TunStamp 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

8.10 Operation security

TunStamp 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.

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

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

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

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

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

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

8.11 Network security controls

TunStamp 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. TunStamp'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 time stamping services by such systems. It is the NDCA's security policy to block all ports and protocols and open only necessary ports to enable Time stamping functions. The TunStamp 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.

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

8.12 Incident Management

- TunStamp 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.

- TunStamp 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.

- TunStamp 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.

8.13 Collection of evidence

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

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

Clock Synchronization
c) Records concerning all events relating to synchronization of a TSU's clock to UTC will be logged. This include information concerning normal re-calibration or synchronization of clocks used in time-stamping.
d) Records concerning all events relating to detection of loss of synchronization 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 easily deleted or destroyed for a period of 20 years.

8.14 Business Continuity Management

In the case of a compromise, or suspected compromise or loss of calibration when issuing time-stamp, TunStamp will make available to all subscribers and relying parties the following :

- A description of compromise that occurred.
- Will not issue time-stamps until steps are taken to recover from the compromise.
- Information which can be used to identify the time-stamps which may have been affected,

unless this breaches the privacy of the TSAs users or the security of the TSA services

The HSM in question would be isolated from the network immediately and corrective measures will be taken.

TunStamp will activate its Business Continuity Plan, Backup and Restoration Plan.

8.15 TSA termination

In the event the TunStamp Authority terminates its operations for any reason whatsoever, NDCA will carry out those actions :

- A timely notice will be provided for all all subscribers and other entities with which the TunStamp has agreements or other form of established relations, among which relying parties, in order to minimize any disruptions that are caused because of the termination of the services.
- Continued maintenance of information required to verify the correctness of trust services, for a reasonable period, will be provided.
- TunStamp will terminate authorization of all its subscribers;
- TunStamp's private keys, including backup copies, will be destroyed, or withdrawn from use, in a manner such that the private keys cannot be retrieved;
- Transferring the TSP obligations (provision of trust services for its existing customers to other parties.

8.16 Compliance

TunStamp is convinced that compliance is a key factor for business success. In order to achieve this, TunStamp Authority will ensure compliance with applicable law and international standards at all times.

Specifically, the TSA will be compliant to the references given in section [6.4] of the present document.

9 Other Business and Legal Matters

9.1 Dispute resolution provisions

In case of litigation or dispute, any party must notify NDCA by registered letter with acknowledgment of receipt. NDCA 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 NDCA 's General Manager, by registered letter with acknowledgment of receipt.

The request must contain the following informations :

- 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 are competent.

9.2 Governing law

The laws and regulations in force in Tunisia are applied.

9.3 Compliance with applicable law

This TunStamp policy is subject to the laws and regulations applicable in Tunisia.