WIPO
WORLD
INTELLECTUAL PROPERTY
ORGANIZATION

WIPO | PROOF

Timestamping Policy and Practice Statement

Version: 2.0

CONTENTS

Document Maintenance **2**

Revision History **3**

1 Scope **4**

2 References **4**

3 Definitions and abbreviations **5**

3.1 Abbreviations 5

3.2 Definitions 5

4 GeneralConcepts **6**

4.1 Concepts and general requirements 6

4.2 Timestamping services 6

4.3 Timestamping services parties 6

4.3.1 Time Stamping Authority (TSA) 7

4.3.2 Subscriber 6

4.3.3 TSA relying party 7

5 Timestamp policies **7**

5.1 General 7

5.2 Identification 7

5.3 User community and applicability 7

6 Policies and Practices **7**

6.1 Risk assessment 7

6.2 Trust service practice statement 7

6.2.1 Timestamp format 7

6.2.2 Time accuracy 7

6.2.3 Limitations of the service 7

6.2.4 Obligations of the subscribers 8

6.2.5 Obligations of relying parties 8

6.2.6 Timestamp verification 8

6.2.7 Applicable law 8

6.2.8 Service availability 8

6.2.9 Practice statement approval procedures 8

6.3 terms and conditions 9

6.4 Information security policy 9

6.5 TSA Obligations 8

6.5.1 TSA obligations towards subscribers 8

6.6 Information for relying parties 9

7 TSA Management and Operations **9**

7.1 Introduction 9
7.2 Internal organization 9
7.3 Trusted personnel 9
7.4 Asset management 10
7.5 Access control 11
7.6 Cryptographic controls 11
7.6.1 TSU's key generation 11
7.6.2 TSU's private key protection 11
7.6.3 TSU Public key certificate 12
7.6.4 TSU's key renewal 13
7.6.5 Life cycle management of cryptographic hardware 13
7.7 Timestamping 13
7.7.1 Timestamp issuance 13
7.7.2 Clock synchronization with UTC 13
7.8 Physical and environmental security 13
7.9 Security of TSA operations 14
7.10 Network security 14
7.11 Incident management 15
7.12 Collection of evidence 15
7.13 Business continuity management 15
7.14 TSA termination plan 16
7.15 Compliance 16

DOCUMENT MAINTENANCE

This document is valid from the day of its publication on WIPO'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 Changes
April 17 2020	1.0	Initial issue
July 10 2020	2.0	- Separation between document approval workflow and revision history -Clarification on role of Certsign (4.3 Timestamp services parties) -Addressing inconsistency in the name of the TSA (3.1 –Definitions) -Updates to trusted roles by replacing system operator with HSM administrator role and tweaks to HSM operator and system administrator roles (7.3 Trusted personnel) -Including links to published certificate information (6.2- Timestamp verification, 6.6 – Information for relying parties) -Updates to clarify WIPO TSA compliance approach (7.15 Compliance)

DOCUMENT APPROVAL WORKFLOW

Role	Responsible
Initial draft, internal review and updates	WIPO PROOF team
Review and endorsement	WIPO Timestamping Policies and Procedures Board
Review and approval	WIPO PROOF Project Board

1 SCOPE

This document is the World Intellectual Property Organization (WIPO) Timestamping Service (known as WIPO PROOF) Policy and Practice Statement. Users of WIPO PROOF are advised to read the document before using the services.

This document lays out the specific security policies, practices and controls relating to the operation and management of WIPO PROOF as a Timestamping Authority. This is in accordance with the ETSI EN 319 421 standard "Policy and Security Requirements for Trust Service Providers issuing Timestamps".

The document is authored and updated by the WIPO PROOF team, reviewed and endorsed by the WIPO Timestamping Policies and Procedures Board and approved by the WIPO Timestamping Service governing body. It is subject to amendment and change, when the need arises, conforming to section 6.2.9.

2 REFERENCES OF STANDARDS AND REGULATIONS

1. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
2. IETF RFC 3161 "Internet X.509 Public Key Infrastructure Timestamp Protocol"
3. ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers"
4. ETSI EN 319 421: "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Timestamps"
5. ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Timestamping protocol and timestamp token profiles"
6. ISO/IEC 19790:2012: "Information technology – Security techniques – Security requirements for cryptographic modules"
7. ISO/IEC 15408 (parts 1 to 3): "Information technology – Security techniques – Evaluation criteria for IT security"
8. FIPS PUB 140-2 (2001): "Security Requirements for Cryptographic Module"

3 DEFINITIONS AND ABBREVIATIONS

3.1 Abbreviations

CA	Certification Authority
IT	Information Technology
OID	Object Identifier
TSA	Time Stamping Authority
TSP	Trust Service Provider
TSPS	Timestamping Policy and Practice Statement
TST	Times tamp Token
TSU	Timestamping Unit
UTC	Coordinated Universal Time
WIPO	World Intellectual Property Organization

3.2 Definitions

- **Coordinated Universal Time (UTC):** Time scale based on the second as defined in Recommendation ITU-R TF.460-6. UTC is the principal standard of the hour by which the world regulates clocks and the time.
- **NTP:** "Network Time Protocol (NTP) is a networking protocol for clock synchronization of computer systems over network packet routing with variable latency.
- **OID:** Unique number of the object identifier
- **Relying party:** The recipient of a timestamp who relies on that timestamp.
- **Time Stamping Authority (TSA):** It is the TSP providing timestamping services using one or more timestamping units.
- **Subscriber:** Legal or natural person to whom a timestamp is issued.
- **Timestamp:** Data in electronic form which binds other electronic data to a time, providing evidence that these data existed at such time.
- **Timestamping policy:** A set of rules that indicate the applicability of a timestamp to a community and/or class of application of the common security requirements. This is a specific type of trust service policy as defined in ETSI EN 319 421.
- **Timestamping service:** trust service for issuing timestamps.
- **Timestamping Unit (TSU):** The set of hardware and software which is managed as a unit and has a single timestamp signing key active at a time.
- **Trust Service Provider (TSP):** industry standard compliant entity which provides one or more trust services.
- **TSA practice statement:** statement of the practices that a TSA employs in issuing timestamps.
- **TSA system:** Set of IT products and components employed to provide support to the provision of timestamping services.
- **WIPO PROOF:** Brand name for the digital timestamping service designed, developed, and maintained by the World Intellectual Property Organization.
- **WIPO TSA:** represents "World Intellectual Property Organization" as a Time Stamping Authority functioning in accordance with the ETSI EN 319 421 "Policy and Security Requirements for Trust Service Providers issuing Timestamps"

4 GENERAL CONCEPTS

4.1 Concepts and general requirements

The TSPS is a detailed description of the security policies, practices and controls that the WIPO TSA applies in the provision of timestamping services.

4.2 Timestamping services

The provision of timestamping services is broken down, in the present document, into the following component services for the purposes of classifying requirements:

- Timestamping provision: This service component generates TSTs.
- Timestamping management: The service component that monitors and controls the operation of timestamping services to ensure that the service provided is as specified in the TSPS.

WIPO TSA adheres to the standards and regulations specified in section 2 of this document to keep trustworthiness of the timestamping services for subscribers and relying parties.

4.3 Timestamping services parties

4.3.1 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 4.2. The TSA has responsibility for the operation of the timestamping service in line with the requirements specified in this document.

WIPO TSA hereby confirms that it is audited at least every 24 months by an accredited conformity assessment body. If the conformity assessment body requires the TSA to remediate any gaps in order to fulfil the conformity requirements, WIPO as TSA shall act accordingly and in a timely manner.

WIPO TSA may make use of other parties to provide parts of the timestamping services. However, the TSA always maintains overall responsibility (as per clause 6.5) and ensures that the policy requirements identified in the present document are met. Currently, WIPO uses certSIGN SA as a technical implementation and integration partner. Furthermore, WIPO TSA certificate has been signed by certSIGN Qualified CA which is listed on European Trusted List as Qualified Electronic Seal Certificate issuer.

Contact Information:
World Intellectual Property Organization
Address: 34 Chemin des Colombettes,
1211 Geneva 20,
Switzerland
Phone: +41 22 338 9111
Fax: +41 22 733 5428
Web: www.wipo.int
Contact Us: https://www3.wipo.int/contact/en/area.jsp?area=wipoproof

4.3.2 Subscriber

When the subscriber is an end-user, the end-user is directly responsible for fulfilling User obligations as indicated in the Terms of Use & Privacy policy.

When the subscriber is an organization, this entity will be directly responsible for fulfilling User obligations as indicated in the Terms of Use & Privacy policy.

4.3.3 TSA relying party

A relying party is an individual or entity that acts in reliance on a TST generated under WIPO's TSA policy [ETSI EN 319 421]. A Relying Party may be a subscriber or any other user.

5 TIMESTAMP POLICIES

5.1 General

WIPO TSA issues the TSTs in accordance with this TSPS which is aligned with the ETSI EN 319 421 standard's requirements. The TSTs are issued with an accuracy of 1 second of UTC or better.

5.2 Identification

The object identifier of the timestamp policy specified in the present document is OID: **1.3.6.1.4.1.48669.2.1.1**

{iso (1) identified-organization (3) dod (6) internet (1) private (4) enterprise (1) WIPO (48669) timestamp-policy
(2) policy-identifiers (1) timestamp-unit-policy (1)}

By including this object identifier in the generated timestamps, WIPO claims conformance with this timestamp policy. The timestamps also include the OID **0.4.0.2023.1.1**, if this is specified in the timestamp request content.

5.3 User community and applicability

WIPO TSA's User Community is composed of subscribers and relying parties.

This TSPS may be used for public timestamping services or for timestamping services used within a closed community.

WIPO TSA does not impose restrictions on the applicability of timestamps, with the exception of cases referred to in this document and in the Terms of Use & Privacy policy.

6 POLICIES AND PRACTICES

6.1 Risk assessment

WIPO TSA performs risk assessments on a regular basis to ensure the confidentiality, integrity and availability of the timestamping services. The security controls related to the timestamping services are regularly reviewed by the TSA, in line with the WIPO internal risk management framework. These assessments are periodically validated by independent auditors.

Regular reporting on identified risks related to timestamping services is done to WIPO management and any risk acceptance decisions taken in line with WIPO's risk management framework.

6.2 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 ETSI EN 319 421 requirements.

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

6.2.1 Timestamp format

The Timestamp Tokens (TSTs) issued by WIPO TSA 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.

6.2.2 Time accuracy

The TSTs are issued with an accuracy of 1 second of UTC or better.

6.2.3 Limitations of the service

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

6.2.4 Obligations of the subscribers

For detailed information, please see the "Terms of Use & Privacy Policy".

6.2.5 Obligations of relying parties

For detailed information, please see the "Terms of Use & Privacy Policy".

6.2.6 Timestamp verification

Verification of the timestamp issuer

The issuer is the WIPO TSA, which uses an appropriate private key and a digital certificate for issuing the timestamp. The public key included in the TSU certificate and CA certificates are used to perform the verification that the timestamp has been correctly signed by the TSA.

Verification of the timestamp integrity

The cryptographic integrity of the timestamp is in the responsibility of the Relying Party. WIPO TSA provides a service on its web portal for verifying the integrity of the Timestamp Token (this can be done using the "verify token" option). This can also be verified independently.

6.2.7 Applicable law

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

6.2.8 Service availability

WIPO TSA has implemented the following measures to ensure availability of the service:

- Redundant setup of IT Systems to avoid single points of failure.
- Redundant high-speed internet connections to avoid loss of service.
- Use of uninterruptable power supply and power supply redundancies.

Although these measures ensure service availability of the WIPO TSA, an annual availability of 100% cannot be guaranteed. WIPO TSA aims to provide an availability of the service of 99.99% per year.

6.2.9 Practice statement approval procedures

The WIPO Timestamping Service governing body is responsible for the approval of the TSPS as well as any subsequent changes to it, following the review and endorsement by WIPO's Timestamping Policies and Procedures Board.

The TSPS shall be reviewed at least once every two years.

The only changes that the WIPO TSA may make to these TSPS specifications without notification are minor changes that do not affect the assurance level of this TSPS, e.g. editorial or typographical corrections, or changes to the contact details.

Any changes to the TSPS shall be approved by the WIPO Timestamping Service governing body and announced to WIPO TSA customers through a publication on the timestamping service website. Subjects/Subscribers shall comply only with the currently applicable TSPS.

6.3 Terms and conditions

The published document "Terms of Use & Privacy Policy" contains further information about limitations of the service, subscriber's obligations, information for relying parties or limitations of liability, among others.

6.4 Information security policy

WIPO has implemented an information security policy framework throughout the organization and its employees are required to adhere to the requirements stated therein. The information security policy framework is reviewed periodically and updated as the need arises. WIPO management approves all changes to this policy framework.

6.5 TSA Obligations

6.5.1 TSA obligations towards subscribers

WIPO TSA ensures conformance with the procedures stated in the present document. An independent auditor verifies the efficiency of procedures on a regular basis.

6.6 Information for relying parties

Before acquiring a timestamp, Relying Parties shall verify that it has been correctly signed and that the corresponding TSU certificate has not been revoked or isn't expired at the time of verification. This can be done by checking the Certificate Revocation List.

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

The Relying Party is expected to always take into account the usage limitations of the service, as described in the Terms of Use & Privacy policy.

7 TSA MANAGEMENT OPERATIONS

7.1 Introduction

WIPO TSA has implemented an Information Security Management System comprised of policies, procedures, technical and operational practices required to meet its Information security objectives. These are further described below;

7.2 Internal organization

WIPO's organizational structure, policies, procedures and controls are applicable to WIPO TSA.

7.3 Trusted personnel

WIPO TSA ensures that the personnel assigned trusted roles and job responsibilities:

- Are qualified and possess the required skillset to meet the minimum requirements for the assigned role;
- Have signed a contract that describes their roles and responsibilities as well as their obligations to protection of sensitive information;
- Have undertaken a mandatory information security training on protection of sensitive information;
- Do not fulfill tasks that could generate conflicts of interest.

The following are the trusted roles defined for the WIPO TSA:

- **System administrator**

- Initiates and is authorized to carry out installation, configuration and management of WIPO TSA's software applications;
- In consultation with the relevant authorities, initiates and suspends the services provided by WIPO TSA;
- Coordinates and supervises the HSM and System operators;
- Initiates and oversees the key generation process and the generation of shared secrets;
- Manages the Hardware Security Module and creates operator cards with participation of HSM Administrator;
- Is responsible for the daily operation of the TSA systems and applications;
- Authorized to execute back-up and system restart operations.

- **HSM administrator**

- Collaborates with system administrator to ensure that HSM reconfiguration changes are implemented
- Collaborates with system administrator in creation of operator cards

- **HSM operator**

- Participates in the key generation process;
- Participates in service restart process.

- **Information Security Officer**

- Has the overall responsibility for enforcing security policies and procedures;
- Approves user access rights and privileges;

- Authorized to access the archives and audit logs of the TSA's systems;
- Supervises internal and external audits;
- Receives and responds to audit reports;
- Supervises the remediation of deficiencies found after the audit.

- **System auditor**
- Responsible for conducting audits to confirm the TSA's compliance with applicable best practices and standards;
- Validates the TSA compliance with the Timestamping Policy and Practice Statement.

The number of people required to perform a task

The following critical operations of the TSU are performed in a physically secured environment and in the presence of at least two of the trusted roles:

- TSU key generation process;
- Loading the cryptographic key in the Hardware Security Module;
- Activating the private key;
- Restarting the Timestamping service.

Any other operation or role, described in this TSPS can be performed by a single, specifically designated person.

Identification and authentication for each role

WIPO personnel are subject to identification and authentication controls whenever they access the data center, TSA computer systems or applications. One of the following methods or a combination of different methods is used for identification and authentication:

- User ID and password;
- Electronically stored private key and PIN;
- Hardware private key stored (on a cryptographic device) and PIN;
- Access card;
- Biometrics.

Each assigned TSA user account is required to meet the following criteria:

- Must be unique and directly assigned to a specific individual user;
- Should not be shared with any other user;
- Shall be access restricted to the role or profile assigned to the respective user.

Personnel training requirements

All Personnel performing tasks as a result of assuming a role in the TSA are made aware of, and adequately trained on the following key aspects:

- Responsibilities arising from roles and tasks performed as part of the TSA;
- Acceptable and secure usage of the TSA software applications;
- Polices, practices and security controls implemented by the TSA.

Response to unauthorized actions

In case of discovery or suspicion of unauthorized actions or policy violations by trusted roles or other users, the system administrator may suspend the suspected account's access to the service. The incident(s) shall be investigated in line with the existing WIPO incident management/investigation procedures. Disciplinary measures, where required may be enforced in line with the applicable WIPO policies.

7.4 Asset management

WIPO TSA 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 WIPO's Information Security Classification and Handling Policy and standard.

All changes made on the TSA applications are done in line with the documented and approved WIPO change management processes and procedures. In line with change management best practices, the TSA development, test and production environments are completely segregated.

7.5 Access control

In line with WIPO's Access Control policy and standard, TSA profiles and access rights are granted through a controlled process involving formal access requests and approval by the relevant managers before assignment by system administrators.

The principles of least privilege, need to know and the segregation of duties principle are respected.

Access rights of users involved in TSA operations are promptly modified in case of change of roles or revoked in case the users leave the organization.

Periodic review of user access is conducted to validate the continuing appropriateness of user access rights and confirm the revocation of rights that are no longer required.

Relationships with service providers

WIPO TSA ensures that any contracted third-party service providers meet WIPO's security requirements (based on WIPO's Service Provider Security Policy) before any access to TSA systems can be authorized. Risk assessments are conducted to confirm the extent to which the service provider meets WIPO's requirements and identify any residual risks. The approved third parties are also contractually bound to continuing compliance with these security requirements.

Monitoring

The TSA systems and services are constantly monitored to ensure timely identification of and response to any security events.

7.6 Cryptographic controls

7.6.1 TSU's key generation

The TSU key pair is generated by dual control, in WIPO's location, in the presence of a group of trusted roles (according to the matrix of roles for the WIPO TSA). The private key is permanently kept in encrypted format on this device and never leaves the device in unencrypted format.

Actions taken when the key pair is generated are recorded, dated and signed by each person present during the key pair generation. Records are kept for audit reasons or for regular system checks.

The key is generated and exists throughout its entire lifetime in a physically and logically secured environment.

After the key pair for timestamp signing is generated and the private key is activated in the hardware security module, it can be used in cryptographic operations until its validity period expires or until it is compromised.

The TSU uses a RSA key pair with a length of 2048-bit. This key pair is used only for signing TSTs.

7.6.2 TSU's private key protection

WIPO TSA private keys are protected with a Hardware Security Module (HSM) compliant with the FIPS 140-2 level 3, or ISO 15408 Common Criteria EAL 4+ standards.

The digital signature is created using the RSA algorithm in combination with the SHA-256 cryptographic summary.

The dual-control access is achieved through the distribution of shared secrets to licensed operators. The secrets are stored on cryptographic cards or tokens, protected by a PIN and transferred to their respective authenticated owners. For operations such as initiating the hardware cryptographic module and transferring the private key, an access threshold scheme (type k of n) is implemented through shared secrets distribution.

The shared secret transfer procedure involves the presence of the secret holder throughout the key generation process and during its distribution process, accepting the given secret and the responsibilities arising from keeping it.

Before receiving their part of the secret, each holder of the shared secret must be present, in person, when the secret is shared, to verify the correctness of the created secret and its distribution. Each part of the shared secret must be transferred to the holder on a cryptographic card protected by a PIN chosen and known solely by the holder.

The creation and the receipt of the shared secret are confirmed by a handwritten signature on a form, a copy of which is preserved by the TSA.

The shared secret holders are prohibited from disclosing, copying and sharing their part of the secret with any other users in an unauthorized manner. They are also required to immediately notify the secret issuer in case of theft, loss, unauthorized disclosure or any other security compromise of the secret.

WIPO TSA creates a backup copy of the private keys used for timestamp signing. The copies are used during the implementation of the emergency key recovery procedures (e.g. in case of disaster recovery). The copies of the private keys are protected by the shared secret created during the generation of the original keys.

The operation of introducing a private key in a cryptographic module applies in the following cases:

- Occasionally, when creating backups of the private key stored in a cryptographic module (e.g. in case of module failure or if the module is compromised), the introduction of a key pair into a different security module may be required;
- When the transfer of a private key from the operational module used for standard operations to another module is required; the situation may occur when invoking the Disaster Recovery plan or if the operational mode needs to be destroyed.

The introduction of a private key in a security module is a critical operation and shall be protected against unauthorized disclosure and alteration through the implementation of the following measures and procedures;

- The introduction of a private key in the TSU's HSM requires the restoration of the key from cards in the presence of an adequate number of shared secret holders;
- During import, generation or restoration, the private key of a TSU is deactivated. The key activates when the service is turned on. Once activated, a key can be used as long as the service is running. When the service shuts down, the key shall be deactivated;
- The activation of private keys is always preceded by operator authentication. The authentication is performed based on a cryptographic card held by the operator after inserting the card into the cryptographic module and using a PIN code;
- The hardware protection of the private key means that it is never available in clear text, not even in the memory of the application;
- In WIPO's case, the deactivation of a private key is performed by people with trusted roles, but only in cases when the service is stopped for updates, maintenance or for other reasons.

7.6.3 TSU Public key certificate

The TSA guarantees the integrity and authenticity of the TSU signature verification (public) keys as follows:

a) TSU signature verification (public keys) are available to relying parties that trust in a public key certificate. The certificates are published in the following link: https://wipoproof.wipo.int/wdts/globally-trusted.xhtml. The TSU does not issue a timestamp before its signature verification (public key). When the certificate is loaded in the TSU, the TSA verifies that the certificate was duly signed (including verification of the certificate chain of a trusted certification authority).

b) Only one TSU certificate with its private key is issued.

c) TSU certificates are not renewed.

d) Validity information regarding the TSU certificates is updated periodically and the CRLs or OCSP services are available with the references located in the certificates.

The electronic timestamps issued by WIPO are aligned with and meet the eIDAS requirements (EU No 910/2014) and the service will be periodically audited by accredited auditors to certify this conformity.

7.6.4 TSU's key renewal

The lifetime of the TSU certificate corresponds to the period of the chosen algorithm and to the key length. The keys of the TSU shall have a maximum operating life of 3 years. The keys shall be renewed before expiry of the validity period.

7.6.5 Life cycle management of cryptographic hardware

WIPO TSA assures that:

a) The integrity of the cryptographic security modules was not tampered with during transportation from the manufacturer.

b) The integrity of the cryptographic security modules was not affected during their storage, prior to their installation.

c) They are installed, managed and operated by trusted personnel /roles using, at least, dual control in a physically secured environment.

d) The cryptographic security modules work correctly.

e) The private signing keys stored on the cryptographic security modules are destroyed the moment it is taken out of production.

After private keys expiration, the private keys within the cryptographic module are destroyed in a way that they can no longer be retrieved.

7.7 Timestamping

7.7.1 Timestamp issuance

WIPO TSA issues timestamping services complaint with using RFC 3161 "Timestamp Protocol ".

Each TST contains the Timestamping Policy identifier, a unique serial number and a certificate containing the identification information of the WIPO TSA's TSU.

The TSU, in the timestamp requests, accepts SHA256 hash algorithms and uses the SHA-256 cryptographic hash function to sign the TST.

The TSU keys are 2048-bit RSA keys. The key is used only for signing TSTs.

TSA logs all issued TSTs. The TSTs are logged for an indefinite period. WIPO TSA can prove the existence of a TST at the request of a relying party. WIPO TSA can request the relying party to cover the costs of such service.

The TSU does not issue any TST when the end of the validity of the TSU private key has been reached.

7.7.2 Clock synchronization with UTC

The WIPO TSA 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 or better, using the NTP protocol.
- WIPO TSA ensures protection of its TSU clocks against threats, which could take it outside its calibration.
- WIPO TSA ensures that timestamp issuance will be stopped in case of drifts 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.

7.8 Physical and environmental security

WIPO TSA equipment are protected from unauthorized access and potential damage with the following physical and environmental security controls.

WIPO provides a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of information assets.

Physical access to WIPO's premises is controlled through multiple layers including, but not limited to the following;

- Physical security controls around the WIPO perimeter.
- All users, including visitors are provided proportionate access to WIPO premises in line with the identified and approved business needs. Physical locations that are deemed sensitive are reinforced with additional access controls and require additional access rights.
- Controls supporting early detection of and response to unauthorized access attempts have been implemented by the TSA.
- Robust fire prevention, detection and extinguishing procedures and controls are deployed to mitigate fire related risks.
- WIPO premises are equipped with heating/ventilation/air conditioning systems to control temperature and humidity to approved levels.
- Power supply controls including backup power systems are implemented to ensure continuous, uninterrupted access to electric power in case of disruptions.
- Controls and procedures to address the potential risk of water and flooding are implemented.

Storage of information storage media

All media containing TSA information are stored within WIPO facilities or in the case of backups, in a secure off-site storage facility, with appropriate physical and logical access controls designed to limit access to authorized personnel and protect such media from accidental damage (e.g., water, fire, and electromagnetic, etc.).

Information Disposal

All sensitive documents and storage media are securely and irreversibly destroyed in line with the requirements of WIPO's Information Security Classification and Handling Policy and standard.

Off-site backup

To ensure business continuity and disaster recovery, WIPO performs routine backups of critical TSA information and ensures that the backups are securely stored at an off-site location.

7.9 Security of TSA operations

WIPO TSA uses trustworthy systems and products that are protected against unauthorized modification and access through the following operational security controls.

- Identification and analysis of security requirements is carried out at the design and requirements specification stage of WIPO TSA systems;
- Capacity and scalability management requirements and tests are planned to ensure that future operational needs of the TSA are met;
- Change control procedures are applied for releases, modifications and emergency software fixes of any operational TSA systems/ applications;
- Anti-malware software and other relevant controls are implemented to ensure the integrity of TSA systems and that its information is protected against malware, unauthorized software and any other threats to integrity;
- Media used within timestamping systems are securely handled and protected from damage, theft, unauthorized access and obsolescence;
- Vulnerability management procedures to ensure timely identification and remediation of any security vulnerabilities.

WIPO TSA has implemented operational procedures for all trusted and administrative roles that are involved in management of TSA services.

7.10 Network security

WIPO has implemented risk-based controls and follows best practices required to protect its network and systems against malicious attacks.

- Firewalls and boundary control devices are deployed and configured to allow access only by the addresses, ports, protocols and commands required for the trustworthy provision of timestamping services.
- All firewall configurations and related changes go through a documented approval process before implementation.
- WIPO TSA traffic is encrypted to protect against risks such as eavesdropping and man in the middle attacks.
- WIPO ensures that all accounts, applications, services, protocols, and ports that are not required and deemed unnecessary for the TSA operations are disabled.
- WIPO TSA network controls are routinely subjected to audits, vulnerability scans and penetration tests by qualified, authorized and independent third parties. Any identified vulnerabilities are remediated by WIPO within the shortest possible intervals.
- Network monitoring is implemented to facilitate timely identification and response to network security events and/ or incidents.
- Access controls are implemented in order to protect the WIPO TSA hardware and software components from unauthorized access.

7.11 Incident management

- WIPO TSA acts in a timely and coordinated manner to respond quickly to incidents and to limit the impact of security breaches.
- WIPO TSA has a defined and approved information security incident management process covering incident identification, categorization and response, among others. This also includes reporting and a notification procedures.
- Audit logs of the timestamping service are monitored and reviewed regularly to identify any evidence of potential security incidents.
- WIPO 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.
- WIPO TSA will notify, without undue delay, any affected subscribers of any breach of security that may adversely impact them.

7.12 Collection of evidence

The TSA records shall be kept accessible for an appropriate period, including after the activities of the TSA have ceased.

All the relevant TSA 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 synchronization of a TSU's clock to UTC are logged. This includes information concerning normal re-calibration or synchronization of clocks used in timestamping.

Records concerning all events relating to detection of loss of synchronization are logged.

The events are logged in a way that they cannot be deleted or destroyed for a period of 10 years.

7.13 Business continuity management

To mitigate effects of natural or man-made disasters, WIPO TSA has developed, implemented, tested and maintained up to date Business Continuity and Disaster Recovery Procedures for its information assets including those used for the timestamping service.

- A secure Disaster Recovery site has been set up at an off-site location from WIPO’s primary premises.
- Generally, any disruptions are handled in line with WIPO’s Business Continuity and Disaster Recovery Plans and procedures.
- In the event of a natural or man-made disaster resulting in disruption of TSA operations, the Business Continuity/ Disaster Recovery procedures shall be initiated in line with the approved protocols to restore and recover essential TSA operations.

- To facilitate this, WIPO TSA has implemented additional controls such as synchronization of production databases and maintenance of up to date backups at the recovery site.

In the case of compromise, or suspected compromise or loss of calibration when issuing timestamps, WIPO TSA 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 TSA may partially or fully suspend issuing of timestamps until steps have been taken to recover from the compromise.
- The affected systems may be isolated from the network to allow implementation of corrective measures.

7.14 TSA termination plan

In the event of termination of its operations for any reason whatsoever, WIPO TSA 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.
- Ensure that the TSA private keys, including backup copies, shall be destroyed, or withdrawn from use, in a way that the private keys can no longer be retrieved.
- Take the necessary steps to have the TSU certificates revoked.

7.15 Compliance

WIPO TSA ensures alignment with best practices, standards and regulations at all times. Specifically, it is aligned with:

a) EU Regulation 910/2014
b) ETSI TS 319 401
c) ETSI TS 319 421
d) IETF (RFC 3161)

This alignment is validated by competent, accredited auditors through periodic conformity assessment audits.

WIPO TSA’s conformity assessment audit results shall not be submitted to any supervisory body in order to be granted the “Qualified” status because as an international organization and specialized agency of the United Nations, WIPO operates on a multi-lateral framework and does not subject itself to such bilateral arrangements. However, WIPO TSA shall ensure that the services are trusted and fully meet the technical requirements of the above listed best practices, standards and regulations.