TECHNOLOGY SOURCE

SMART.SPEED.SOLUTIONS

Timestamping Authority Policy and Practice Statement

Document Control

Prepared / Updated By	Reviewed By	Approved By	Owner	Version	Date of Approval
			Tech Source	1.0	

Change History

Sr. No	Version	Changes Description	
0.1	28.01.2023	Initial version	Touir Mustapha
02	11.12.2023	Applying the Tech Source template document	Touir Mustapha
0.3	15/03/2024	Reviewed and updated	Yasir Khan
1.0	15/07/2024	Updates based on auditor's recommendations following the Point-In-Time audit.	Touir Mustapha

Document Approval

Ver. No	Approver (Name/Title)	Signatures	
1.0	PKI GB Director		
			Date:

Table of Contents

1 Introduction

1.1 Overview

The Iraq National PKI is established under Information & Telecommunication Public Company (ITPC) with multiple root CAs representing national root PKI program. With this National PKI, the Iraqi Government aims to provide a framework to facilitate the establishment of Trust Service Providers (TSP) offering digital certification and trust services to government and non-government entities. The Iraq PKI hierarchy has two levels described as following:

Level 0:

The below five (5) Roots Certification Authorities (CA) are established for the different type of certificates to be issued. The Information & Telecommunication Public Company (ITPC) is responsible for this Root CA layer. As the national PKI governance body, the ITPC is mandated to operate the Policy Management Authority (PMA). ITPC Root CAs are:

- **Iraq Code Signing Root CA**: certifies/signs Code Signing Subordinate CAs
- **Iraq S/MIME Root CA:** certifies/signs email protection Subordinate CAs
- **Iraq TLS Root CA:** certifies/signs SSL/TLS Subordinate CAs
- **Iraq Document Signing Root CA**: certifies/signs natural & legal persons document signing Subordinate CAs
- **Iraq Timestamp Root CA**: certifies/signs Timestamping Subordinate CA.

Level 1: The TS's Subordinate CAs falls at this level within the National PKI hierarchy as shown in the below figure :

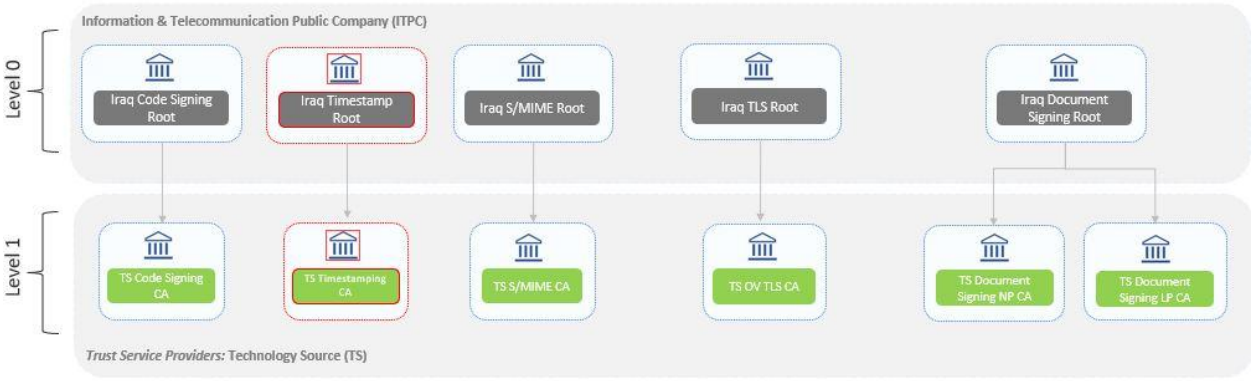

Figure 1 Iraq National PKI hierarchy

Technology Source is the organization to operate the Subordinate CAs and offer related trust services to the government and non-government domains. As such the Technology Source operates as a Trust Services Provider (TSP) offering its services through a hierarchy of Subordinate CAs, implemented under the ITPC Root CAs. ITPC Root CAs certified TSP Subordinate CAs for Technology Source as follows:

- **Technology Source Code Signing CA**: Subordinate CA that issues certificates to sign the software libraries, .jar files, .exe file, .msi files etc.
- **Technology Source S/MIME CA:** Subordinate CA that will issue certificates for email signing and encryption.
- **Technology Source SSL/TLS CA:** Subordinate CA that will issue web server SSL/TLS organization validation (OV) certificates.
- **Technology Source Document Signing NP CA:** Subordinate CA that will issue document signing certificates to natural persons (citizens and employees).
- **Technology Source Document Signing LP CA:** Subordinate CA that will issue document signing certificates to legal persons (Non government and government entities).
- **Technology Source Timestamping CA:** Subordinate CA that will issue TSA certificates involved in document signing and code signing.

The above use cases are key enablers of digital transformation as they represent the corner stone of securing electronic transactions. Supporting these use cases under a unified trust model with government assurance, facilitates adoption, enables interoperability, and enhances user trust.

As part of the certification services provided, Technology Source also offers a timestamping service named “Technology Source Timestamping Authority Services” (further referred to as “TS TSA Services”) to support both documents signing and code signing.

The present document named “Timestamping Authority Policy and Practice Statement” is intended to describe the rules and operational procedures adopted by Technology Source who is a Trusted Service Provider (TSP) for the provision of the Timestamping Services.

The timestamp services have been implemented to satisfy the following requirements, where applicable:

- CA/Browser Forum Network and Certificate System Security Requirements
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates.

- ETSI EN 319 421: “Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.”
- ETSI EN 319 422: “Time-stamping protocol and time-stamp token profiles.”
- ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers”.
- ETSI TS 119 312: “Electronic Signatures and Infrastructures (ESI); Cryptographic Suites”.
- IETF RFC 3628: “Policy Requirements for Time-Stamping Authorities (TSAs)”
- IETF RFC 3161 “Internet X.509 Public Key Infrastructure Time-stamp Protocol”

The structure and contents of this document are laid out in accordance with ETSI EN 319 421 (Policy and Security Requirements for Trust Service Providers issuing Electronic Timestamps). In the event of any inconsistency between this document and the ETSI EN 319 421, the requirements set out in the ETSI EN 319 421 document take precedence over this one.

This document is administered and approved by the TS PKI GB and should be read in conjunction with the TSP CP and the Timestamping CA CPS. Both documents can be downloaded from https://pki.techsource.iq

1.2 Scope

The present document specifies policy and security requirements relating to the operation and management practices of Technology Source TSA for issuing electronic time-stamps, as well as establish the conditions of use, obligations and responsibilities of the different entities involved.

Technology Source uses its public key infrastructure and trusted time sources to provide reliable, standards-based time-stamps used in support of electronic/eSeal signatures or for any application requiring to prove that a datum existed before a particular time.

This document can be used by independent entities as the basis for confirming that Technology Source TSA is a trusted entity of the issuance of electronic time stamps in accordance with the Iraqi regulation.

This document does not specify:

- protocols used to access the TS TSA;
- how the requirements identified herein can be assessed by an independent entity;
- the requirements for making the information available to such independent entities (Assessors);
- the requirements that must be met by such independent entities (Assessors).

This document extends the applicable practices of Timestamping CPS.

2 References

- **ETSI EN 319 421:** Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Timestamps.
- **ETSI EN 319 422:** Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.
- **ETSI EN 319 401:** Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- **RFC 3161**: Internet X.509 Public Key Infrastructure Time-stamp Protocol (TSP).
- **FIPS PUB 140-2 (2001):** "Security Requirements for Cryptographic Modules."
- **ETSI EN 319 411-1:** "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements".
- **ETSI EN 319 411-2**: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates".
- CA/Browser Forum Network and Certificate System Security Requirements.
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates

3 Definition and abbreviations

3.1 Definitions

Coordinated Universal Time (UTC): time scale based on the second as defined in Recommendation ITU-RTF.460-6.

Relying party: recipient of a time-stamp who relies on that time-stamp.

Subscriber: legal or natural person to whom a time-stamp is issued and who is bound 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 token: data object defined in IETF RFC 3161 [1], representing a time-stamp

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 providing time-stamping services 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 that enhances trust and confidence in electronic transactions.

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

3.2 Abbreviations

For the purpose of the present document, the following abbreviations apply:

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

TST Time Stamp Token

UTC Coordinated Universal Time

The reader may refer to Technology Source CPS's for additional abbreviations.

4 General Concepts

4.1 Time-stamping services

TS TSA Services consists of the management of the infrastructure for, and the provisioning of Time Stamp Tokens. These services are provided by the Technology Source Time Stamping Authority (TSA) to the Subscribers and are an integral part of the Technology Source Public Key Infrastructure (PKI).

Technology Source offers time-stamping services using RFC 3161 Time Stamp Protocol over HTTP transport. Each TST contains Time-Stamping Policy identifier, unique serial number and TSU certificate containing TSA identification information.

Technology Source does not rely on third-party collaborating entities for the provision of time stamping services, it maintains general responsibility and ensures that the performance requirements mentioned in this document are met.

The offered service assures use of a reliable time source and proper management of all system components.

4.2 Time Stamping Authority (TSA)

Technology Source Time Stamping Authority (TSA) is responsible for provisioning of Time Stamping Services as described in this document.

It has the responsibility for the operation of the relevant Time Stamping Units (TSUs) which creates and signs on behalf of the TSA. The legal entity responsible for the TSA is Technology Source acting as timestamping service provider (TSSP).

The Timestamp Authority synchronizes its timestamp server at least every 24 hours with a UTC(k) time source.

4.3 Subscriber

The Subscriber is the applicant, natural or legal person, to whom the time stamp is provided and who is contracted with Technology Source.

The Subscriber may be an organization comprising several end-users or an individual end-user. 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 such an organization shall duly notify its end-users.

When the Subscriber is an end-user, the end-user will be held directly responsible if its obligations are not correctly fulfilled.

4.4 Time-stamp policy and TSA practice statement

4.4.1 Purpose

This document specifies the policy and practices statement for the timestamp service provided by Technology Source, in order to meet the safety and reliability requirements described in section 2 of this document.

This policy has been crafted to the general level, without describing any technical details about the IT system and communications, organizational structure and operating and protection procedures. These details can be found in the Timestamping CPS of Technology Source.

5 Timestamp Policies

5.1 Overview

This policy defines a set of rules adhered to by Technology Source when issuing Timestamps.

TS TSA signs timestamps using private keys that are specifically reserved for this purpose. The timestamps signature private keys (i.e., TSUs private keys) are stored in a cryptographic device (HSM).

Each TST (Time Stamp Token) shall contain an identifier to the applicable policy and the TSTs shall be issued with an accuracy of ± 1 second of UTC.

The time-stamps shall be requested through Hypertext Transfer Protocol (HTTP), as described by the RFC 3161.

The URL for **TS TSA Service is:** https://tsa.techsource.iq.

5.2 Identification

The object identifier of the TS Timestamp Policy and Practices statement is: **2.16.368.1.2.1.6.** This policy is accessible to all subscribers and relying parties.

Moreover, the TS TSA includes the following additional OID to distinguish between timestamps in support of document signing and code signing:

	OID	
Code Signing	2.16.368.1.2.1.6.2	timestamps issued by TS TSA in support of code signing signature.

	2.23.140.1.4.2	to assert compliance with timestamp certificates requirements defined in the CAB/forum CS BR
Document Signing	2.16.368.1.2.1.6.1	timestamps issued by TS TSA in support of document signing signature.

5.3 User Community and Applicability

The community of users of TS TSA Services includes subscribers and relying parties. Accordingly, Subscribers are also regarded as Relying Parties.

This policy is aimed at meeting the requirements of Timestamps for long term validity (e.g. as defined in ETSI EN 319 122) but is generally applicable to any use which has a requirement for equivalent quality.

The TS TSA does not impose restrictions on the applicability of timestamps, except for the cases referred to in the TS Timestamping CA CPS (Section 1.4.2 Prohibited Certificate Uses).

6 Policies and Practices

6.1 Risk Assessment

Technology Source conduct an annual Risk Assessment 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 Processes,
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 TS has in place to counter such threats.

Based on the risk assessment results (which coincides with the annual external vulnerability and penetration testing exercise), the Technology Source higher PKI operational management will develop and present a security plan to the TS PKI GB seeking the necessary approvals to proceed with the remediation implementation. Additional details may be found in Section 5.4.8 (Vulnerability Assessment) of the TS Timestamping CA CPS.

6.2 Trust Service Practice Statement

Technology source shall ensure the quality, performance, and operation of the timestamping service through the implementation of various security policies and controls. The security policies and controls are reviewed regularly by an independent auditor, whilst trained trustworthy personnel check the adherence of the security controls to the policies (to ensure that the practices are properly implemented).

The TS PKI GB has the responsibility for maintaining and approving all PKI policies and practices according to the terms of Section 1.5 (Policy Administration) of the TS Timestamping CPS.

The present document, the TS Timestamping CPS, and other public documents are publicly disclosed at https://pki.techsource.iq

Internal documents may only be supplied under strictly controlled conditions. Notice will be given regarding any changes to this present Policy.

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

6.2.1 Timestamp format

The service issues Timestamps signed using one of the following digest algorithms:

- SHA-256
- SHA-384
- SHA-512

6.2.2 Accuracy of Time

Timestamping services time signal is provided from GPS-NTP. The time-stamping service uses this time signal as time sources. With that setup the time-stamping services reaches an accuracy of the time of +/-1s or better with respect to UTC.

6.2.3 Limitation of Service

No stipulation

6.2.4 Subscriber Obligations

When obtaining a TST, the Subscriber shall verify that the TST has been correctly signed and that the private key used to sign it has not been compromised. Refer to section 6.2.6 of this document for more details on the timestamp verification.

Timestamps shall be requested through HTTP, as described by RFC 3161.

Subscribers must use a method or software toolkit approved by Technology Source to request timestamps, unless otherwise specifically authorized in writing by Technology Source.

6.2.5 Relying Party Obligations

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:

1) Verify that the time-stamp token (TST) has been correctly signed and that the private key used to sign the timestamp has not been compromised until the time of the verification (refer to 6.2.6 for more details on the timestamp verification and section 9.6.4 of the Timestamping CA CPS);

2) Consider any limitations on the usage of the timestamp indicated by this policy.

3) Consider any other precautions prescribed in agreements or elsewhere.

4) In case the verification takes place after expiry of the time-stamp certificate, the relying party should consider the following (taken from guidance denoted in Annex D of ETSI EN 319 421):

a. Verify that the TSU private key is not revoked, and
b. Verify that the cryptographic hash function and the signing algorithm used in the timestamp token are still considered secure.

6.2.6 Verification of the Timestamp

6.2.6.1 Verification of timestamp Issuer

TSU and TS TSA certificates are published to allow Relying Parties to verify that Timestamps are issued by a TSU operated by Technology Source on https://pki.techsource.iq

The public key included in the TSU certificates and CA certificates are used to perform the verification that the timestamp has been correctly signed by the TSA.

6.2.6.2 Verification of timestamp revocation status

During and after the TSU Certificate validity period, the status of the private key can be checked using the Certificate Revocation List (CRL) and/or Online Certificate Status Protocol (OCSP) referenced in CRL Distribution Point (CDP) and the Authority Information Access (AIA) extensions of the TST signing certificate respectively.

6.2.7 Applicable law

The laws of the Republic of Iraq shall govern the enforceability, construction, interpretation, and validity of the present document. All disputes associated with this document will be in all cases resolved according to the laws of the Republic of Iraq.

6.2.8 Service Availability

Technology Source 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, an annual availability of 100% cannot be guaranteed. TS TSA aims to provide an availability of the service of 99.99% per year.

6.3 Terms and Conditions

For Subscriber refer to section 6.2.4.

For Relaying Party refer to section 6.2.5.

This document represents the applied trust service policy.

6.4 Information Security Policy

Technology Source implements an information security policy that is applicable to the PKI employees, suppliers, and contractors. The information security policy is maintained and reviewed regularly (annually) and whenever significant changes occur.

6.5 TSA Obligations

6.5.1 General Obligations

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

6.5.2 TSA Obligations toward Subscribers

The TS TSA assumes the following obligations towards the subscribers of the timestamp service:

1. Its timestamp activity is based on certified equipment and software.

2. To operate in accordance with this Time-stamping Policy, and the other relevant operational policies and procedures.

3. It ensures that the timestamps maintain an accuracy of at least one (1) second relative to UTC.

4. To maintain a competent and experienced team that can ensure the continuity of the Time Stamp Service.

5. To undergo internal and external reviews to assure compliance with relevant legislation and adopted TS internal policies and procedures.

6. To monitor and control the Time Stamp Service and the whole TSA infrastructure, to prevent or limit any disturbance or unavailability of the service except in the case of planned technical interruptions and loss of time synchronization.

6.6 Information for relying parties

Refer to section 6.2.5 for Relying Party Obligations.

7 TSA Management and Operations

7.1 Internal Organization

Technology Source has an active security management program designed to document, implement, and maintain adequate security provisions for TS PKI according to the best practice and the requirements of relevant standards.

Additional information is provided in Section 5 (Management, Operational and Physical Controls) and Section 6 (Technical Security Controls) of the TS Timestamping CA CPS.

7.2 Personnel Security

TS TSA is operated as part of TS PKI infrastructure, the provisions in Section 5 (Management, Operational and Physical Controls) and Section 6 (Technical Security Controls) of the TS Timestamping CA CPS apply.

7.3 Asset Management

TS TSA maintains an accurate and up to date inventory of information assets, including systems and applications s and assign a classification for the protection requirements to those assets consistent with the risk analysis. All changes made on the TSA applications are done in line with the documented and approved change management processes and procedure.

Additional information is provided in Section 6.6 (Life Cycle Technical Controls) of the TS Timestamping CA CPS.

7.4 Access Control

TS TSA maintain appropriate physical and logical access controls for affected facilities, hardware, systems and information.

The systems' access management controls for the TS TSA are incorporated within the overall PKI systems access management controls. 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.

Additional information is provided in Section 5 (Management, Operational and Physical Controls) and Section 6 (Technical Security Controls) of the TS Timestamping CA CPS.

7.5 Cryptographic Controls

7.5.1 TSA Key Generation

The generation of the TSU's signing key(s) is undertaken in a physically secured environment by personnel in trusted roles under at least dual control. The personnel authorized to carry out this function is limited to those required to do so under TS TSA practices.

The generation of the TSU's signing key(s) is carried out within a cryptographic module which is conformant to FIPS PUB 140-2 level 3.

The TSU key generation algorithm, the resulting signing key length and signature algorithm used for signing Timestamps key are specified in the TS Timestamping CA CPS.

Additional information is provided in the section 6 of the TS Timestamping CA CPS.

7.5.2 Private Key protection

TS TSA ensure that TSU private keys remain confidential and maintain their integrity. These include use of Hardware Security Modules (HSMs) certified to FIPS 140-2 Level 3 to hold and sign with the keys.

When TSU private keys are backed up, they shall be copied, stored, and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment.

The personnel authorized to carry out this function shall be limited to those requiring doing so under TS TSA practices.

7.5.3 Public Key Certificate

TS TSA ensures the integrity and authenticity of its signature keys when made available to relying parties. Digital Certificates used in the TSU are issued by the TS Timestamping CA.

The TSU electronic certificates are published on Technology Source website: https://pki.techsource.iq

Additional information is provided in Section 6.1 (Key Generation and Installation) of the TS Timestamping CA CPS.

7.5.4 Rekeying TSU's Key

TSU private signing keys shall be replaced before the end of their validity period. If an algorithm becomes compromised or is not suitable anymore, Technology Source will rekey any affected private keys.

Additional information is provided in Section 4.7 (Certificate Re-key) of the TS Timestamping CA CPS.

7.5.5 Life Cycle Management of Signing Cryptographic Hardware

The TS TSA assures that:

- The integrity of the cryptographic security modules was not tampered with during transportation from the manufacturer.
- The integrity of the cryptographic security modules was not affected during their storage, prior to their installation.
- They are installed, managed, and operated by trusted personnel /roles using, at least, dual control in a physically secured environment.
- The cryptographic security modules work correctly.
- The private signing keys stored on the cryptographic security modules are destroyed the moment it is taken out of production.

Additional information is provided in Section 6.6 (Life Cycle Technical Controls) of the TS Timestamping CA CPS.

7.5.6 End of TSU Key Life Cycle

The validity of TSU private keys never exceeds the validity of the associated public key certificate. After expiration of the private keys, the TSA shall reject any attempt to issue timestamps.

After expiry the private keys within the cryptographic hardware are destroyed in a manner such that the private keys cannot be retrieved or used anymore. Operational or technical procedures shall be in place to ensure that a new key is put in place when a TSU's key expires.

7.6 Timestamping

7.6.1 Timestamping

Technology Source has technical prescriptions in place to ensure that TSTs are issued securely and include the correct time. In line with the protocols referenced in Section 3 of this document, each TST includes:

- A representation (e.g., hash value) of the datum being time-stamped as provided by the requestor.
- A unique serial number that can be used to identify specific TST.
- An identifier for the Time-stamp Policy.
- The time calibrated to within 1 second of UTC, traceable to a UTC(k) source.
- An electronic signature generated using a key used exclusively for timestamping.
- An identifier for the TSA and the TSU.

Technology Source maintains audit logs for all calibrations against the UTC (k) references.

The following types of timestamps are provided:

- DS timestamps: tokens issued in compliance with RFC 3161 and ETSI EN 319 422.
- CS-timestamps: tokens issued in compliance with RFC 3161 and BR CS.

7.6.2 Clock Synchronization with UTC

TS TSA provides time with plus or minus 1 second of UTC by calibration with an NTP server. TS TSA have technical measures in place to ensure that the time of its TSU is synchronized with UTC within the declared accuracy. TS TSA ensure that clock synchronization is maintained when a leap second occurs as notified by the appropriate body.

The operated TSU shall also monitor time drift outside present boundaries and request additional recalibrations as needed. In case where the TSU clock drifts out of accuracy, no Timestamp will be issued until re-synchronization of the clock.

Audit and calibration records are maintained by the TSUs operated by Technology Source.

7.7 Physical and Environmental Security

Since TS TSA is operated as part of TS PKI infrastructure, the provisions in Section 5 (Management, Operational and Physical Controls) and Section 6 (Technical Security Controls) of the TS Timestamping CA CPS apply.

7.8 Operation Security

TS TSA implements a set of system and security controls to ensure service quality and availability:

- An analysis of security requirements is carried out at the design and requirements specification stage of timestamping systems.
- Change control procedures are applied for releases, modifications, and emergency software fixes of any operational software.
- The integrity of timestamping systems and information shall be protected against viruses, malicious and unauthorized software.
- Procedures are established and implemented for all trusted and administrative roles that impact on the provision of timestamping services.
- 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.

Additional provisions in Section 5 (Management, Operational and Physical Controls) of the TS Timestamping CA CPS.

7.9 Network Security

TS TSA implemented strong network security, including managed firewalls and intrusion detection systems.

The network is segmented into several zones, based on their functional, logical, and physical relationship. Network boundaries is applied to limit the communication between systems (within zones) and communication between zones, with rules that support only the services, protocols, ports, and communications that the CA has identified as necessary to its operations, disabling all accounts, applications, services, protocols, and ports that are not used in the TSA's operations.

TS TSA's system is protected within a highly Secure network Zone. It is to highlight that the production platform is separated from other environments not concerned with live operations.

In addition, the TS TSA performs regular vulnerability assessment and penetration testing covering all assets related to certificate issuance, products, and services. Assessments focus on internal and external threats that could result in unauthorized access, tampering, modification, alteration, or destruction of the certificate issuance process. Refer to Section 6 (Technical Security Controls) of the Timestamping CPS for more details.

7.10 Incident Management

TS TSA maintains an incident management process that enables timely, prompt and coordinated actions to incidents to limit the impact of security breaches. TSA will:

- Ensure a regularly review and approve of the information security incident management process covering incident identification, categorization, and response, among others. This also includes reporting and a notification procedure.
- Ensure the monitoring and regularly review the timestamping service audit logs to identify any evidence of potential security incidents. Monitoring activities cover various parameters including access to IT systems, usage of systems, and availability of the service, among others. Dedicated personnel in trusted role with appropriate access restrictions are involved in monitoring activities seen the sensitivity of the information collected or analysed from the TSA logs.

TSA will notify, without undue delay, any affected subscribers of any breach of security that may adversely impact them.

Refer to Section 5 (Management, Operational and Physical Controls) of the TS Timestamping CA CPS for additional details regarding events to records.

7.11 Collection of evidence

TS TSA records and keeps accessible for an appropriate period, including after the activities of the TS TSA have ceased, all relevant information concerning data issued and received by TS TSA, in particular, for providing evidence in legal proceedings and for the purpose of ensuring continuity of the service.

In particular:

- The confidentiality and integrity of current and archived records concerning operation of services is maintained.
- Records concerning the operation of services are completely and confidentially archived in accordance with disclosed business practices.
- Records concerning the operation of services are made available if required for the purposes of providing evidence of the correct operation of the services for the purpose of legal proceedings.
- The precise time of significant TSP's environmental, key management and clock synchronization events shall be recorded.
- The time used to record events as required in the audit log shall be synchronized with UTC ceaselessly.

Records concerning the operation of time-stamping services are held for a period after the expiration of the validity of the signing keys for providing necessary legal evidence if required by court order or another legal requirement.

TS TSA maintain records, including precise time of:

- Time-stamp requests and created timestamps.
- Events related to TSA administration (including certificate management, key management, and lock synchronization)
- Events relating to the life cycle of TSA keys and certificates.

Refer to Section 5 (Management, Operational and Physical Controls) of the TS Timestamping CA CPS for additional details regarding events and frequency to records.

7.12 Business continuity management

In the event of compromise of a TSA private key, TS shall follow the procedures outlined in Section 5.7 (Compromise and Disaster Recovery) of the TS Timestamping CA CPS. This includes revoking the relevant certificate and adding it to trust services CA CRL. The TSA will not issue timestamps if its private key is not valid. The TSA will not issue timestamps if its clock is outside the declared accuracy from reference UTC, until steps are taken to restore calibration of time.

7.13 TSA Termination and Termination Plans

To minimize potential disruptions to subscriber and relaying parties following the cessation of TS TSA services, TS TSA maintains an up-to-date termination plan by which its ensure before terminates its services:

1. Inform the following of the termination: all subscribers and other entities with which the Technology Source has agreements or other form of established relations, and other relying parties;
2. Terminate authorization of all subcontractors to acting on its behalf in carrying out any functions relating to the process of issuing trust service tokens.
3. If deemed appropriate, transfer obligations (provision of timestamping services) to an identified reliable third party.
4. Ensure that the TSA private keys, including backup copies, are destroyed, or withdrawn from use, in a way that the private keys can no longer be retrieved.
5. Revoking all TSU certificates.

Additional information is provided in Section 5.8 (CA or RA Termination) of the TS Timestamping CA CPS.

7.14 Compliance

TS TSA ensures compliance with Iraqi applicable law and alignment with best practices, standards, and regulations at all times. Specifically and where applicable, it is aligned with:

a) ETSI TS 319 422
b) IETF (RFC 3161)
c) CA/Browser Forum Network and Certificate System Security Requirements
d) CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates

This alignment is validated by independent internal and external reviews (audits).

8 Contact Information

Requests for information related to this practice statement should be addressed to:

Technology Source PKI Governance Board
Technology Source,
Baghdad-Four streets- nearby AL-maamon high school
Email: muhanad.ali@techsource.iq
Phone no.: +9647726695600 / +9647842002124

The TS PKI GB accepts comments regarding this policy only when they are addressed to the contact above.