

Iraq National PKI

Timestamping Authority Policy and Practice Statement

Document Control

Version	Date	Changes Description	Responsible
0.1	28/01/2023	Initial version.	Mustapha Touir
0.2	11/12/2023	Applying the Technology Source template document.	Mustapha Touir
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.	Mustapha Touir
1.1	05/10/2025	Annual review.	Technology Source
1.2	03/10/2026	Amendment to update Technology Source contact information.	Technology Source

Document Approval

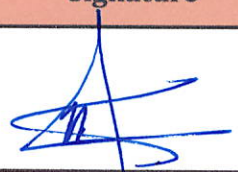
Version	Approver (Name/Title)	Signature
1.2	PKI GB Director Muhanad Ali Salim	 Date: 03/10/2026

Table of Contents

1 INTRODUCTION 4
1.1 OVERVIEW 4
1.2 SCOPE 6
2 REFERENCES 7
3 DEFINITION AND ABBREVIATIONS 8
3.1 DEFINITIONS 8
3.2 ABBREVIATIONS 9
4 GENERAL CONCEPTS 10
4.1 TIME-STAMPING SERVICES 10
4.2 TIME STAMPING AUTHORITY (TSA) 10
4.3 SUBSCRIBER 10
4.4 TIME-STAMP POLICY AND TSA PRACTICE STATEMENT 11
4.4.1 PURPOSE 11
5 TIMESTAMP POLICIES 11
5.1 OVERVIEW 11
5.2 IDENTIFICATION 11
5.3 USER COMMUNITY AND APPLICABILITY 12
6 POLICIES AND PRACTICES 12
6.1 RISK ASSESSMENT 12
6.2 TRUST SERVICE PRACTICE STATEMENT 12
6.3 TERMS AND CONDITIONS 13
6.3.1 TRUST SERVICE POLICY APPLIED 13
6.3.2 TIMESTAMP FORMAT 13
6.3.3 ACCURACY OF TIME 13
6.3.4 VERIFICATION OF THE TIMESTAMP 13
6.3.5 SERVICE AVAILABILITY 14
6.3.6 SUBSCRIBER OBLIGATIONS 14
6.3.7 RELYING PARTY OBLIGATIONS 14
6.3.8 LIMITATION OF USE OF SERVICE 14
6.3.9 RETENTION PERIOD 15
6.3.10 LIMITATION OF LIABILITY 15
6.3.11 APPLICABLE LEGAL SYSTEM, COMPLAINT, DISPUTE RESOLUTION 15
6.4 INFORMATION SECURITY POLICY 16
6.5 TSA OBLIGATIONS 16
6.5.1 GENERAL OBLIGATIONS 16

6.5.2 TSA Obligations toward Subscribers 16
6.6 Information for relying parties 16
7 TSA MANAGEMENT AND OPERATIONS 17
7.1 Internal Organization 17
7.2 Personnel Security 18
7.3 Asset Management 19
7.4 Access Control 20
7.5 Cryptographic Controls 20
7.5.1 TSA Key Generation 20
7.5.2 Private Key protection 20
7.5.3 Public Key Certificate 21
7.5.4 Rekeying TSU's Key 21
7.5.5 Life Cycle Management of Signing Cryptographic Hardware 21
7.5.6 End of TSU Key Life Cycle 21
7.6 Timestamping 22
7.6.1 Time-stamp Issuance 22
7.6.2 Clock Synchronization with UTC 22
8 PHYSICAL AND ENVIRONMENTAL SECURITY 23
8.1 Site Location and Construction 23
8.2 Physical Access 23
8.3 Power And Air Conditioning 23
8.4 Water Exposures 23
8.5 Fire Prevention and Protection 24
8.6 Media Storage 24
8.7 Waste Disposal 24
8.8 Off-Site Backup 24
8.9 Operation Security 24
8.10 Network Security 25
8.11 Incident Management 25
8.12 Collection of evidence 26
8.13 Business continuity management 26
8.14 TSA Termination and Termination Plans 27
8.15 Compliance 27
9 CONTACT INFORMATION 27

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 :

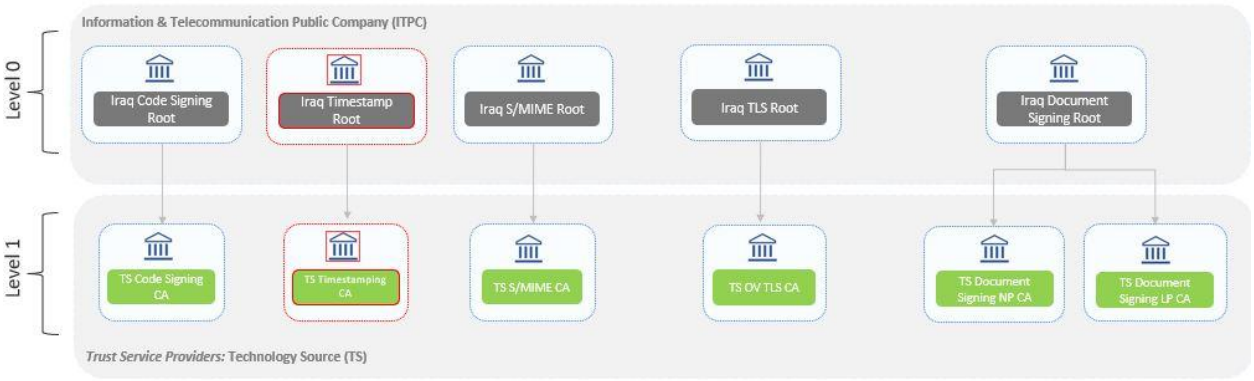


Figure 1 Iraq National PKI hierarchy

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"). This service provides secure timestamps that can support the integrity and evidentiary value of documents by proving their existence at a specific point in time.

The present document, titled "Timestamping Authority Policy and Practice Statement," describes the rules and operational procedures adopted by Tehnology Source, a Trust Service Provider (TSP) responsible for delivering the Timestamping Service in accordance with applicable regulatory and industry standards.

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 TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".
- 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).

This document is administered and approved by the TS PKI GB and should be read in conjunction with 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 leverages its public key infrastructure and trusted time sources to provide reliable, standards-based timestamps. These timestamps support electronic and eSeal signatures by establishing that specific data existed prior to a given point in time. t is important to note that a document may be signed without being timestamped, and conversely, it may be timestamped even in the absence of a signatory's signature—for instance, to establish the existence and integrity of the data at a specific point in time prior to any formal signing

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 (v1.2.1):** Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Timestamps.
- **ETSI EN 319 422(v 1.1.1):** Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.
- **ETSI EN 319 401 (v 3.1.1):** Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- **RFC 3161**: Internet X.509 Public Key Infrastructure Time-stamp Protocol (TSP).
- 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.

Re-Key: Certificate re-key refers to the issuance of a new certificate with a new subject public key for a subject to whom a certificate has previously been issued by the CA. Subject attributes and other certified attributes can be updated.

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 available at https://pki.techsource.iq 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.

6 Policies and Practices

6.1 Risk Assessment

Technology Source conducts an annual risk assessment covering all systems, processes, and assets related to its Timestamping Service. This assessment:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Time-Stamp Token data, Time-Stamp Unit (TSU) certificate data, or related certificate management processes,
2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Time-Stamp Token operations and TSU certificate management; and
3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that Technology Source has in place to counter such threats.

The remediation plan integrates administrative, organizational, technical, and physical controls that are appropriate to the sensitivity of the timestamping environment. In determining the suitable measures, consideration is given to the availability and cost of applicable technologies. The objective is to ensure that the implemented security controls are proportionate to the potential impact of a security breach and aligned with the criticality of the data and assets being protected.

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.

6.3 Terms and Conditions

This section outlines the Terms and Conditions applicable to the use of the Technology Source Timestamping Authority (TS-TSA) services. These provisions apply to all subscribers and relying parties who interact with or rely upon timestamps issued by TS-TSA.

6.3.1 Trust service policy applied

Technology Source issues the TSTs in accordance with ETSI EN 319 421 best practice for time-stamping policy (OID 0.4.0.2023.1.1).

6.3.2 Timestamp format

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

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

When submitting a timestamp request, the hash (message imprint) provided by the requester must also be generated using one of the supported algorithms listed above. Requests using unsupported hash functions will be rejected by the Time Stamping Authority (TSA).

6.3.3 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.

6.3.4 Verification of the Timestamp

6.3.4.1 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.

6.3.4.2 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.

6.3.5 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. Technology Source monitors the frequency and duration of service interruptions to ensure that the total annual unavailability remains within the defined SLA (99.6%). Each disruption event is recorded, and significant or repeated outages trigger incident escalation procedures.

6.3.6 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 6.3.4 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.

6.3.7 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 6.3.3 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.

6.3.8 Limitation of use of service

Technology Source provides timestamping services that may be used, without restriction, in connection with legal or other electronic transactions.

However, to the extent permitted under applicable laws of Iraq, Technology source shall not be held liable—except in cases of fraud or wilful misconduct—for:

- Loss of profits;
- Loss or corruption of data;
- Any indirect, incidental, consequential, or punitive damages arising from or related to the use, delivery, licensing, performance, or non-performance of timestamping services;
- Any other damages or losses not directly attributable to Technology Source.

Technology Source does not assume financial liability for timestamps that are misused or used in a manner inconsistent with the applicable policies or intended purpose of the service.

6.3.9 Retention Period

Technology Source retains all relevant records and data associated with the provision of its timestamping services for a minimum period as defined in their applicable CPS published at https://pki.techsource.iq . This includes timestamp requests, issued timestamps, and related audit logs necessary to demonstrate the integrity, authenticity, and compliance of the service.

Unless otherwise specified by applicable law or supervisory authority, the retention period shall not be less than 02 years from the date of issuance.

6.3.10 Limitation of liability

Technology Source operates the TS-TSA in accordance with the current applicable policy and practice statement and the relevant CPS, and the terms of conditions. All this documentation is published on the public PKI repository: https://pki.techsource.iq.

Technology Source shall not in any event be liable for any loss of profits, loss of sales or turnover, loss or damage to reputation, loss of contracts, loss of customers, loss of the use of any software or data, loss or use of any computer or other equipment save as may arise directly from breach of the TSA policy and practice statement, CPS, wasted management or other staff time, losses or liabilities under or in relation to any other contracts, indirect loss or damage, consequential loss or damage, special loss or damage, and for the purpose of this paragraph, the term “loss” means a partial loss or reduction in value as well as a complete or total loss.

6.3.11 Applicable Legal System, Complaint, Dispute Resolution

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.

6.4 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 6.3.7 for Relying Party Obligations.

7 TSA Management and Operations

7.1 Internal Organization

Technology Source has implemented a structured internal organization to ensure the effective, secure, and compliant operation of its Time Stamping Authority (TSA). This organizational model supports adherence to ETSI EN 319 421 and reflects sound operational and security principles widely adopted across the trust services industry.

Key elements of this internal framework include:

- **Role Definition and Responsibility Assignment:**

  TSA-related functions—such as system management, key operations, monitoring, and compliance—are distributed across clearly defined roles. These roles are formally assigned to ensure operational efficiency, security, and accountability.

- **Appointment of Trusted Personnel:**

  Only personnel meeting predefined criteria in terms of qualification, background, and training are permitted to perform sensitive TSA functions. Individuals in these roles operate under procedural safeguards to ensure the protection of critical systems and data.

- **Separation of Duties and Dual Authorization:**

  Controls are in place to ensure that no individual has unchecked access to critical systems or operations. Where necessary, dual authorization is enforced to protect against misuse or unauthorized actions in key processes such as cryptographic key lifecycle management and system configuration changes.

- **Governance and Oversight:**

  Technology Source maintains formal oversight mechanisms to regularly assess the performance, effectiveness, and compliance of TSA operations. TS PKI GB is responsible for supervising TSA activities and ensuring they align with established objectives, applicable technical standards, and internal policies.

- **Policy and Procedure Maintenance:**

  All security and operational procedures relevant to TSA functions are documented and maintained to reflect current requirements. These documents are reviewed periodically

and updated as needed to account for technical developments, emerging threats, or regulatory changes.

Technology Source maintains an active and structured security management program that supports the integrity and resilience of its entire PKI environment, including the TSA. This program is designed to document, implement, and continuously improve the organization's overall security posture. It covers key areas such as risk assessment and mitigation, access control, incident detection and response, operational continuity, and ongoing staff awareness.

This comprehensive internal framework enables Technology Source to provide trustworthy and reliable timestamping services, ensuring the integrity, authenticity, and availability of time-related data in accordance with the provisions of this document.

7.2 Personnel Security

TS-TSA operates as an integral component of Technology Source's Public Key Infrastructure (PKI). Technology Source maintains appropriate personnel security controls aligned with industry best practices and the requirements of applicable standards, such as ETSI EN 319 421 and ETSI EN 319 401.

Managerial and operational personnel assigned to TSA functions possess the necessary skills and knowledge in the fields of time stamping, digital signatures, trust services, and applicable information security procedures, including risk assessment and personnel security.

Technology Source defines Trusted Roles as positions with access to, or control over, cryptographic operations and other sensitive functions. These include, but are not limited to:

- Cryptographic business operations personnel.
- Security personnel.
- PKI, system, and network administration personnel.
- Compliance personnel.

For all individuals seeking to be assigned to Trusted Roles, Technology Source performs identity verification through established HR procedures. This includes checks of government-issued or well-recognized identification documents, and background screening consistent with Technology Source's internal policies and regulatory requirements.

Before any individual is granted Trusted Status, the following conditions must be met:

- Formal approval of the trusted role assignment by authorized management;
- Issuance of access devices and authorization to enter secure facilities;
- Provisioning of electronic credentials enabling access to TSA and related systems in line with assigned responsibilities.

Technology Source ensures that access to sensitive systems and cryptographic functions is strictly controlled, monitored, and restricted to personnel who have received proper authorization and training, thus maintaining the integrity and trustworthiness of its Time Stamping Services.

7.3 Asset Management

TS-TSA maintains a comprehensive and up-to-date inventory of all information assets relevant to its timestamping operations. These assets include information, hardware, software, systems, and applications that support or impact the TSA service.

Each asset is assigned a classification level based on its sensitivity and business value, consistent with the results of Technology Source's risk analysis. These classifications guide the application of appropriate protection and handling measures in accordance with security policies and applicable standards.

All changes to TSA-related applications, systems, or configurations are conducted in accordance with documented and approved change management procedures, ensuring proper review, testing, and authorization prior to implementation.

In cases where hardware components are replaced, the following security controls are enforced:

- Physical devices are delivered, transported, and installed in a controlled and monitored manner, ensuring traceability and integrity throughout the delivery process.
- Replacement procedures follow the same strict guidelines as the deployment of original devices.
- Only authorized, qualified, and trusted personnel are permitted to perform hardware replacements or installations.

These controls are in place to maintain the confidentiality, integrity, and availability of the TSA's assets and to ensure ongoing compliance with applicable security and operational standards such as ETSI EN 319 421 and ETSI EN 319 401.

7.4 Access Control

Technology Source's Time Stamping Authority (TS TSA) implements appropriate physical and logical access controls to protect facilities, systems, hardware, and information assets involved in the provision of timestamping services.

Access control measures applicable to the TS TSA are aligned with the overall access control practices applied across Technology Source's trusted services infrastructure. These controls are designed to ensure that only authorized individuals can access sensitive components or perform critical function.

User access rights are granted based on defined roles and responsibilities, following the principle of least privilege. Access is approved through formal procedures and is subject to periodic review to verify its continued relevance. Any access rights that are no longer required—due to role changes, termination, or other reasons—are promptly revoked to maintain system integrity and prevent unauthorized access.

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.

The TSU key generation algorithm, the resulting signing key length and signature algorithm used for signing Timestamps key are specified in the applicable CPS published at https://pki.techsource.iq

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

The operation period for TSU key pairs is defined by setting a private key usage period within the TSU's public key certificate. TSTs are signed with Technology Source's TSU certificates of three (03) years validity. Technology Source TSU certificates of three (03) years validity are only used to sign TST during a usage period of one (1) year. Technology Source TSU rekey procedure is executed upon expiry of the usage period (1 year) of the TSU certificate.

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.

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 Time-stamp Issuance

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.
- If the requester includes a nonce in the timestamp request, Technology Source will include the exact same nonce value in the TST response.

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, ETSI EN 319 422 and BR CS.

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

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.

8 Physical and Environmental Security

TS-TSA operates as an integral component of Technology Source's Public Key Infrastructure (PKI).

8.1 Site Location and Construction

All critical components of the Technology Source TSA infrastructure are hosted within a highly secure facility operated by Technology Source. Physical security controls are enforced so that access of unauthorized persons is prevented through four (04) layers tiers of physical security. When this layered access control is combined with the physical security protection mechanisms such as guards, intrusion sensors and CCTV, it provides robust protection against unauthorized access to the PKI systems.

The data centers hosting technology Source services are located in geographically distinct areas within the Republic of Iraq.

8.2 Physical Access

Technology Source data centers are protected by a minimum of 04 tiers of physical security, with access to a higher tier requiring prior access to the lower tier. Access to the highest tier requires the presence of two individuals in Trusted Roles. Unauthorized personnel, including untrusted third-party employees or visitors, are prohibited from entering without prior approval and must be escorted by an employee in a trusted role. Similar access restrictions apply to the Disaster Recovery site. A comprehensive log is maintained to record all entries into Technology Source's data centers.

8.3 Power And Air Conditioning

The facility hosting the TS-TSA infrastructure is designed to ensure uninterrupted operations, even in the event of a power failure. It is equipped with UPS units and backup generators capable of sustaining TSA system operations. These power backup solutions cover the entire facility. Additionally, a fully redundant air-conditioning system is installed in the areas housing the TSA systems, ensuring that the equipment operates consistently within the temperature and humidity ranges specified by the manufacturers.

8.4 Water Exposures

Technology Source has taken reasonable precautions to minimise the impact of water exposure to the information systems.

8.5 Fire Prevention and Protection

Technology Source has taken reasonable precautions to prevent and extinguish fires or other damaging exposure to flame or smoke. The fire prevention and protection measures of Technology Source have been designed to comply with local fire safety regulations.

8.6 Media Storage

Portable media, appliances and software may be removed from the premises of Technology Source pursuant to the established procedure. Data media containing sensitive information are stored exclusively in a designated fireproof safe and duplicated for secure storage at the disaster recovery location.

8.7 Waste Disposal

Media containing Sensitive Information are securely disposed of when no longer required. All wastepaper and storage media created within the secure facility shall be destroyed before discarding. Paper media shall be shredded using a crosshatch shredder, and magnetic media shall be wiped by de-magnetization, or physically destroyed. HSMs and related key management devices shall be physically destroyed or securely wiped (zeroized) prior to disposal. Authorization shall be granted for the destruction or disposable of any media.

8.8 Off-Site Backup

Technology Source performs routine backups of critical system data, audit log data, and other Sensitive Information. Technology Source has a disaster recovery location to ensure availability requirements. Databases in the disaster recovery location are synchronised in real time. Disaster recovery sites are in separate premises sufficiently distant from the primary location and benefit from equivalent security measures.

8.9 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.

8.10 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.

8.11 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.

8.12 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.

8.13 Business continuity management

If the TSU private key is compromised or suspected to be compromised, Technology Source shall inform Subscribers and Relying Parties and shall stop using the compromised key. In case of TSU certificate revocation, the necessary actions shall be performed in accordance with the business Continuty and Recovery Plan.

In case of clock synchronization loss, TS-TSA suspends its operations to prevent further damage. The business Continuty and Recovery Plan is activated to restore the synchronization and the service.

8.14 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 non expired TSU certificates.

8.15 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 Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates

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

9 Contact Information

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

Technology Source PKI Governance Board
Technology Source
Baghdad – Al Mansour – Hay Al Andalus – Nearby the Embassy of Algeria
Email: info@techsource.iq
Phone No.: (+964) 784 136 1693

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