

Timestamping Disclosure Statement

Document Control

Sr. No	Version	Changes Description	
0.1	18/12/2023	Initial version	Touir Mustapha
0.2	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
1.1	30/07/2025	Amended to align with TSA policy and practice statement	Technology Source

Document Approval

Ver. No	Approver (Name/Title)	Signatures
1.1	PKI GB Director	Date[1]: 30/07/2025

[1] In light of the last review activity conducted after the Point-in-Time (PIT) date, this review is exceptionally being submitted for Governance Board approval beyond the one-year period, in order to address all auditor comments collected during the Period-of-Time audit conducted in August 2025

Table of Contents

1 ENTIRE AGREEMENT....3

2 TSA CONTACT INFORMATION....3

3 ELECTRONIC TIMESTAMP TYPES AND USAGE....3

4 RELIANCE LIMITS....4

4.1 RETENTION OF EVENT LOGS....4

5 OBLIGATIONS OF SUBSCRIBERS....4

6 OBLIGATIONS OF RELYING PARTIES....4

7 LIMITED WARRANTY AND DISCLAIMER/LIMITATION OF LIABILITY....5

8 APPLICABLE AGREEMENTS AND PRACTICE STATEMENT....5

9 PRIVACY POLICY....5

10 REFUND POLICY....6

11 APPLICABLE LAW, COMPLAINTS, AND DISPUTE RESOLUTION....6

12 TSA AND REPOSITORY LICENSES, TRUST MARKS, AND AUDIT....6

1 Entire Agreement

This TSA Disclosure Statement provides high level disclosures regarding the Technology Source Timestamp Authority (TS TSA). It does not replace or override the definitive Technology Source policy and practice documents which are available at https://pki.techsource.iq.

2 TSA Contact Information

The TSA is operated by Technology Source that can be contacted through the following address:

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

3 Electronic Timestamp Types and Usage

Technology Source has responsibility for the operation of two Time-stamping Units (TSU) which create and sign Timestamps on behalf of the TSA. Each TSU has a different key. Refer to the "TS TSA TSP/PS" published on https://pki.techsource.iq _for more details.

Technology Source distinguishes between timestamps in support of document signing and code signing using the following OID:

	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.

The above OIDs is referenced in all the timestamps issued by TS TSA.

The cryptographic algorithms and key lengths used by the TS TSA comply with ETSI EN 319 422 & BR CS.

The TS TSA digital signature on the Timestamp Token (TST) has a validity period of Three (3) years. The signatures are generated within a high-quality and high security Hardware Security Module (HSM) with FIPS 140-2 Level 3 certification.

4 Reliance limits

The accuracy of the time reference included in time-stamp tokens is ± 1 second, with reference to UTC (Universal Time Coordinated). If a trusted UTC time source cannot be acquired the time stamp will not be issued.

4.1 Retention of Event Logs

TSA event logs are retained in accordance with the retention period for audit logs as described in the applicable certificate practice statement published at https://pki.techsource.iq.

5 Obligations of Subscribers

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 the TSA policy and practice statement document published at https://pki.techsource.iq 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 Obligations of Relying Parties

Before placing any reliance on a Timestamp, Relying Parties must verify that the Timestamp has been correctly signed and that the Private Key used to sign the Timestamp has not been revoked. The Relying Party should consider any limitations on usage of the Timestamp indicated by this TS TSA TSP/PS and any other reasonable precautions. During the TSU Certificate validity period, the status of the Private Key can be checked using the relevant CRL.

Technology Source Timestamp CA and TSU Certificates are published at https://pki.techsource.iq.

Note that Technology Source operates multiple TSUs. See Section 3 (Electronic Timestamp Types and Usage) of this document.

7 Limited Warranty and Disclaimer/Limitation Of Liability

Technology Source operates the TS TSA in accordance with the applicable "TS TSA TSP/PS" and the relevant CPS, and the terms of agreements. All this documentation is published on the public PKI repository: https://pki.techsource.iq.

Technology Source makes no express or implied representations or warranties relating to the availability or accuracy of the time-stamping service.

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 TS TSA TSP/PS, the Technology Source 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.

8 Applicable agreements and practice statement

Refer to the public PKI repository: https://pki.techsource.iq.

9 Privacy policy

Technology Source is committed to protecting the confidentiality and privacy of all non-public and sensitive information it handles. Access to such private information is strictly limited to trusted personnel authorized to perform tasks related to certificate lifecycle management.

Technology Source will not disclose private information without the explicit consent of the legitimate data owner, unless required by a valid court order or legal obligation. In any such case, Technology Source will take all reasonable measures to ensure that the disclosed information is used solely for its intended and authorized purpose.

Any party granted access to private data is obligated to safeguard it from unauthorized use, disclosure, or compromise. These parties must comply with applicable personal data protection laws and regulations in the Republic of Iraq, and are contractually bound to uphold privacy and confidentiality requirements.

Technology Source will not disclose private information to subscribers, except for data pertaining to themselves and only as permitted by the contractual agreement in place between Technology Source and the subscriber.

In all data handling activities—including the collection, use, storage, and disclosure of non-public information— Technology Source adheres to relevant privacy and data protection laws, trade secret regulations (where applicable), and its privacy policy.

10 Refund policy

Technology Source does not refund fees for timestamp services.

11 Applicable law, complaints, and 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.

12 TSA and repository licenses, trust marks, and audit

Technology Source PKI is subject to compliance to the AICPA/CPA Canada Principles and Criteria for Certification Authorities ("WebTrust for CA").

Refer to https://pki.techsource.iq for Technology Source audits and accreditations.