Timestamping
Disclosure Statement

Document Control

Prepared / Updated By	Reviewed By	Approved By	Owner	Version	Date of Approval
			Tech Source	0,10.21.0	

Change History

Sr. No	Version	Changes Description	
0,1	18/12/2023	Initial version	Touir Mustapha
0.2	15/03/2024	Reviewed and updated	Yasir Khan

Document Approval

VerSr. No	Approver (Name/Title)	Signatures
0.21	Governance BoardPKI GB Director	
		Date:

Table of Contents

Formatted: Default Paragraph Font, Check spelling and grammar

Formatted: Default Paragraph Font, Check spelling and grammar

Formatted: Default Paragraph Font, Check spelling and grammar

Formatted: Default Paragraph Font, Check spelling and grammar

Formatted: Default Paragraph Font, Check spelling and grammar

Formatted: Default Paragraph Font, Check spelling and grammar

Formatted: Default Paragraph Font, Check spelling and grammar

Formatted: Default Paragraph Font, Check spelling and grammar

Formatted: Default Paragraph Font, Check spelling and grammar

Formatted: Default Paragraph Font, Check spelling and grammar

Formatted: Default Paragraph Font, Check spelling and grammar

Formatted: Default Paragraph Font, Check spelling and grammar

Formatted: Default Paragraph Font, Check spelling and grammar

Formatted: Default Paragraph Font, Check spelling and grammar

Formatted: Default Paragraph Font, Check spelling and grammar

Formatted: Default Paragraph Font, Check spelling and grammar

Formatted: Default Paragraph Font, Check spelling and grammar

Formatted: Default Paragraph Font, Check spelling and grammar

Formatted: Default Paragraph Font, Check spelling and grammar

Formatted: Default Paragraph Font, Check spelling and grammar

Formatted: Default Paragraph Font, Check spelling and grammar

Formatted: Default Paragraph Font, Check spelling and grammar

Formatted: Default Paragraph Font, Check spelling and grammar

Formatted: Default Paragraph Font, Check spelling and grammar

Formatted: Default Paragraph Font, Check spelling and grammar

Formatted: Default Paragraph Font, Check spelling and grammar

1 Entire Agreement

This TSA Disclosure Statement provides high level disclosures regarding the Technology Source Time-stamp 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.:

- Acceptable Time Stamp Request Hashes: SHA-256, SHA-384 and SHA-512.

- Supported signing algorithms is SHA384 with ECDSA.

Commented [MT1]: @Yasir Khan writing this way mean that we need to amend the certificate policy extension in the TSU certificate profile. Refer to section 7.6.1.

Formatted Table

Formatted: Centered

Formatted: Normal, No bullets or numbering

The TS TSA ~~TS~~ digital signature on the Time~~s-S~~tamp Token (TST) has a validity period of ~~Five~~ Three (~~5~~3) years. The signatures are generated within a high-quality and ~~high-security~~high security ~~HSM (~~Hardware Security Module~~)~~ (HSM) with FIPS 140-2 Level 3 certification.

~~The object-identifier (OID) of the TS Time-stamping Policy for Document Signing is: 2.16.368.1.2.1.6.1. This OID is referenced in all the tTimestamps issued by TS TSA for Document Signing TSA requests. This Timestamping Policy is based on the ETSI BTSP best practices policy for Timestamps (OID 0.4.0.2023.1.1).~~

~~The object-identifier (OID) of the TS Timestamping Policy for Code Signing is: 2.16.368.1.2.1.6.2. This OID is referenced in all the timestamps issued by TS TSA for Code Signing TSA requests.~~

Formatted: Normal

~~Technology Source has responsibility for the operation of one or more 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://twokeyok.iq for a complete list of Technology Source TSUs.~~

Formatted: Hyperlink

Formatted: Hyperlink

~~6~~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.

~~6.1~~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 policy and certificate practice statement.

~~7~~5 Obligations of Subscribers

Obligations of subscribers can be found in the TSA Practice Statement, published on the public PKI repository: https://pki.techsource.iq ~~https://twokeyok.iq~~

~~8~~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. ~~https://twokeyok.iq~~.

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

~~9~~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~~https://twokeyok.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 ~~TSP~~ 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.

~~11~~8 Applicable agreements and practice statement

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

~~12~~9 Privacy policy

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

~~13~~10 Refund policy

Technology Source does not refund fees for timestamp services.

1411 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.

1512 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 https://twokeyok.iq for Technology Source audits and accreditations.