Timestamping Disclosure Statement

Document Control

Approved By	Owner	Version	Date of Approval
PMA	ECAC	2.0	10/12/2024
PMA	ECAC	2.1	17/10/2025

Change History

Version	Date	Changes Description	Approved By
2.0	10/12/2024	Final version released	PMA
2.1	17/10/2025	Annual review. No changes applied.	PMA

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 4

8 APPLICABLE AGREEMENTS AND PRACTICE STATEMENT 5

9 PRIVACY POLICY 5

10 REFUND POLICY 5

11 APPLICABLE LAW, COMPLAINTS, AND DISPUTE RESOLUTION 5

12 TSA AND REPOSITORY LICENSES, TRUST MARKS, AND AUDIT 5

1 Entire Agreement

This TSA Disclosure Statement provides high level disclosures regarding the Electronic Certification Accreditation Council (ECAC) Timestamp Authority (ECAC-TSA). It does not replace or override the definitive ECAC policy and practice documents which are available at https://ecac.pki.gov.pk.

2 TSA Contact Information

The TSA is operated by the Electronic Certification Accreditation Council (ECAC) that can be contacted through the following address:

Policy Management Authority
Electronic Certification Accreditation Council (ECAC),
5th Floor NTC HQ Building, G-5/2,
Islamabad, Pakistan
Tel: +92 51 9245739
Email: ecac.certification.info@pki.gov.pk

3 Electronic Timestamp Types and Usage

ECAC 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 "ECAC TSA PC/PS" published on https://ecac.pki.gov.pk for more details.

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

	OID	
Code Signing	1.3.6.1.4.1.59337.3.3.3	timestamps issued by ECAC-TSA in support of code signing signature.
Document Signing	1.3.6.1.4.1.59337.3.3.4	timestamps issued by ECAC-TSA in support of document signing signature.

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

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

The ECAC-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 policy and certificate practice statement.

5 Obligations of Subscribers

Obligations of subscribers can be found in the TSA Practice Statement, published on the public PKI repository: https://ecac.pki.gov.pk

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 ECAC TSA PC/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.

ECAC Timestamp CA and TSU Certificates are published at https://ecac.pki.gov.pk.

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

7 Limited Warranty and Disclaimer/Limitation Of Liability

ECAC operates the TSA in accordance with the applicable "ECAC-TSA PC/PS" and the relevant CPS, and the terms of agreements. All this documentation is published on the public PKI repository: https://ecac.pki.gov.pk.

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

ECAC 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 ECAC-TSA PC/PS, the ECAC's 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://ecac.pki.gov.pk.

9 Privacy policy

Refer to the public PKI repository: https://ecac.pki.gov.pk.

10 Refund policy

ECAC does not refund fees for timestamp services.

11 Applicable law, complaints, and dispute resolution

The laws of the Islamic Republic of Pakistan 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 Islamic Republic of Pakistan.

12 TSA and repository licenses, trust marks, and audit

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

Refer to https://ecac.pki.gov.pk for ECAC audits and accreditations.