Crowe FST Audit Kft.
Member of Crowe Global

H-1124 Budapest
Jagelló út 14.
Hungary
Tel: +36 1 225-3490
Fax: +36 1 225-3491
www.crowe.hu

INDEPENDENT ASSURANCE REPORT

To the management of Electronic Certification Accreditation Council
Certification Authority ("ECAC")

Scope

We have been engaged, in a reasonable assurance engagement, to report on ECAC Certification Authority management's assertion that for its Certification Authority (CA) operations at Islamabad and Lahore, Pakistan, throughout the period 2024-08-01 to 2025-02-28 for its CAs as enumerated in **Annex A**, ECAC has:

(1) disclosed SSL certificate lifecycle management business practices in its:

- Pakistan National PKI, Certificate Policy (CP) for Trust Services Providers (TSPs), v2.1,
- Pakistan National PKI, Certificate Policy (CP) for Trust Services Providers (TSPs), v2.0,
- Pakistan National PKI, ECAC TLS Subordinate CAs Certificate Practice Statement, v2.0,
- Pakistan National PKI, ECAC TLS Subordinate CAs Certificate Practice Statement, v2.1,
- Pakistan National PKI, ECAC TLS Subordinate CAs Certificate Practice Statement, v2.2,

including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the ECAC website, and provided such services in accordance with its disclosed practices;

(2) maintained effective controls to provide reasonable assurance that:

- the integrity of keys and SSL certificates it manages is established and protected throughout their lifecycles;
- SSL subscriber information is properly authenticated (for the registration activities performed by ECAC);

(3) maintained effective controls to provide reasonable assurance that:

- logical and physical access to CA systems and data is restricted to authorized individuals;
- the continuity of key and certificate management operations is maintained; and
- CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity;

in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline – Version 2.8.

ECAC does not escrow its CA keys, does not provide subscriber key generation and end entity certificate issuance services, and does not provide certificate renewal and suspension services. Accordingly, our procedures did not extend to controls that would address those criteria.

ECAC has renewed its Root CA and subordinate CA infrastructure in the audit period. The go live process was finished on 2025-02-28, and the new TLS CA services are in place since 2025-02-28.

Certification authority's responsibilities

ECAC's management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline – Version 2.8.

Crowe FST Audit Kft. is a member of Crowe Global, a Swiss verein. Each member firm of Crowe Global is a separate and independent legal entity. Crowe FST Audit Kft. and its affiliates are not responsible or liable for any acts or omissions of Crowe Global or any other member of Crowe Global. Crowe Global does not render any professional services and does not have an ownership or partnership interest in Crowe FST Audit Kft.

Our independence and quality management

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior.

The firm applies International Standard on Quality Management (ISQM) 1, Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.]

Practitioner's responsibilities

Our responsibility is to express an opinion on management's assertion based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information,* issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion is fairly stated, and, accordingly, included:

(1) obtaining an understanding of ECAC's SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal;

(2) selectively testing transactions executed in accordance with disclosed SSL certificate lifecycle management practices;

(3) testing and evaluating the operating effectiveness of the controls; and

(4) performing such other procedures as we considered necessary in the circumstances.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

The Audit Team consisted of 6 people including Audit Quality Reviewers. The team qualifications included CPA, PhD, CISA, CISM, CISSP and was led by Péter Máté Erdősi PhD CISA. The average years of auditing experience – auditing trust services or similar information systems – are 13 years in the audit team.

All team members have knowledge of

(1) audit principles, practices and techniques,

(2) the issues related to various areas of public key infrastructure of CAs information security including risk assessment/management, network security and physical security;

(3) the applicable standards, publicly available specifications and regulatory requirements for CAs and other relevant publicly available specifications including standards for IT product evaluation; and

(4) the WebTrust Audit processes.

Additional qualification and personal experience of the Lead Auditor, the Lead Auditor

(1) has acted as auditor more than 40 complete trust service provider audits including 17 WebTrust audits since 2000,

(2) has adequate knowledge and attributes to manage the audit process, and

(3) has the competence to communicate effectively, both orally and in writing.

The relative effectiveness and significance of specific controls at ECAC and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Inherent limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. For example, because of their nature, controls may not prevent, or detect unauthorised access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection to the future of any conclusions based on our findings is subject to the risk that controls may become ineffective.

Opinion

In our opinion, throughout the period 2024-08-01 to 2025-02-28, ECAC management’s assertion, as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline – Version 2.8.

This report does not include any representation as to the quality of ECAC’s services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline – Version 2.8, nor the suitability of any of ECAC’s services for any customer's intended purpose.

Use of the WebTrust seal

ECAC’s use of the WebTrust for Certification Authorities – SSL Baseline Seal constitutes a symbolic representation of the contents of this report, and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

Crowe FST Audit Ltd.
Budapest, Hungary

2025-03-19

Kőszegi Anna

Anna Kőszegi
Partner

Péter Máté Erdősi PhD CISA
Director

Annex A

New PKI Hierarchy

Root CA

ECAC TLS Root CA G1	
Subject	CN=ECAC TLS Root CA G1,O=Electronic Certification Accreditation Council,C=PK
Issuer	CN=ECAC TLS Root CA G1,O=Electronic Certification Accreditation Council,C=PK
Serial	4DA71C129CAE6AD72318CD7E43FF218D
Key Algorithm	RSA
Key Size	4096
Digest Algorithm	SHA256
Not Before	2025-01-08 12:02:47 UTC+00:00
Not After	2040-01-08 12:02:47 UTC+00:00
SKI	A8ADEAB139265E8E2F5986FF77891BA2261826E1
SHA256 Fingerprint	1601DC334704BD853062D6DEBFEECAB38D496F515E186DA56175D9CA6F27256C

Subordinate CA

ECAC OV TLS CA G1	
Subject	CN=ECAC OV TLS CA G1,O=Electronic Certification Accreditation Council,C=PK
Issuer	CN=ECAC TLS Root CA G1,O=Electronic Certification Accreditation Council,C=PK
Serial	788B6ECD9DE1FD5C144CD3306CC35CE4
Key Algorithm	RSA
Key Size	4096
Digest Algorithm	SHA256
Not Before	2025-01-09 11:42:31 UTC+00:00
Not After	2031-01-09 11:42:31 UTC+00:00
SKI	22051A9D7B31E41851FAE8AB683A8951FE9E0237
Key Usage	Certificate Sign, CRL Sign
Extended Key Usage	TLS Web Client Authentication, TLS Web Server Authentication
SHA256 Fingerprint	1C26939AD9A91D707FD040E5A3800E4D010F9E36886F50CDE69B8CF10BAD49DC

Old PKI Hierarchy

Root CA

Root CA	
Subject	CN=ECAC Root CA G1,O=Electronic Certification Accreditation Council,C=PK
Issuer	CN=ECAC Root CA G1,O=Electronic Certification Accreditation Council,C=PK
Serial	75F3520C33E0E4D4F3F36799B7DB1CF15F20B265
Key Algorithm	RSA
Key Size	4096 bit
Digest Algorithm	SHA256
Not Before	2023-01-16 11:57:11 GMT
Not After	2048-01-16 11:57:11 GMT
SKI	3907EEE66F43BA389288B93173B690D671F7EDDE
SHA256 Fingerprint	4EC7B0E3257F710D2F2D90D3CF9E0C87ECF3D2CE59D724F9DDAE1C2485611324

Subordinate CAs

ECAC Commercial TLS CA G1	
Subject	CN=ECAC Commercial TLS CA G1,O=Electronic Certification Accreditation Council,C=PK
Issuer	CN=ECAC Root CA G1,O=Electronic Certification Accreditation Council,C=PK
Serial	2C54F22077FA7E28191234F38DE01799DA79346C
Key Algorithm	RSA
Key Size	4096 bit
Digest Algorithm	SHA256
Not Before	2023-01-16 13:24:23 GMT
Not After	2040-01-16 13:24:23 GMT
SKI	9E0A1D5E38A20DC7AC34C9E022082D5DB5CE21EE
SHA256 Fingerprint	8992E142128A9C22BCE74FC48F6BFB46FBBF5CC0604C7DC213323036AFAAC502

ECAC Government TLS CA G1	
Subject	CN=ECAC Government TLS CA G1,O=Electronic Certification Accreditation Council,C=PK
Issuer	CN=ECAC Root CA G1,O=Electronic Certification Accreditation Council,C=PK
Serial	55763E2DCF7C02DD776C551D79DC8F1BE0047E8F
Key Algorithm	RSA
Key Size	4096 bit

ECAC Government TLS CA G1	
Digest Algorithm	SHA256
Not Before	2023-01-16 132934 GMT
Not After	2040-01-16 132934 GMT
SKI	FF52146C41472EA47326FDDFEF26444A42832B95
SHA256 Fingerprint	8B32E9E5F919BD7449099E439F149829ABB1830C88E079E8AD26D11BB0D0DAD0

ELECTRONIC CERTIFICATION ACCREDITATION COUNCIL
MINISTRY OF INFORMATION TECHNOLOGY &
TELECOMMUNICATION
NTC HQs Building, G-5/2, Islamabad

A GATEWAY TO DIGITAL PAKISTAN

Electronic Certification Accreditation Council
MANAGEMENT'S ASSERTION

Electronic Certification Accreditation Council Certification Authority ("ECAC") operates the Certification Authority (CA) services known as list of Root and Subordinate CAs in scope (see **Appendix A**) and provides SSL CA services.

The management of ECAC is responsible for establishing and maintaining effective controls over its SSL CA operations, including its SSL CA business practices disclosure on its website, SSL key lifecycle management controls, and SSL certificate lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, even effective controls can only provide reasonable assurance with respect to ECAC Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

ECAC management has assessed its disclosures of its certificate practices and controls over its SSL CA services. Based on that assessment, in providing its SSL CA services at Islamabad and Lahore, Pakistan, throughout the period 2024-08-01 to 2025-02-28, ECAC has

(1) disclosed its SSL certificate lifecycle management business practices in its

- Pakistan National PKI, Certificate Policy (CP) for Trust Services Providers (TSPs), v2.1,
- Pakistan National PKI, Certificate Policy (CP) for Trust Services Providers (TSPs), v2.0,
- Pakistan National PKI, ECAC TLS Subordinate CAs Certificate Practice Statement, v2.0,
- Pakistan National PKI, ECAC TLS Subordinate CAs Certificate Practice Statement, v2.1,
- Pakistan National PKI, ECAC TLS Subordinate CAs Certificate Practice Statement, v2.2,

including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the ECAC website, and provided such services in accordance with its disclosed practices,

(2) maintained effective controls to provide reasonable assurance that

- the integrity of keys and SSL certificates it manages is established and protected throughout their lifecycles; and
- SSL subscriber information is properly authenticated (for the registration activities performed by ECAC),

(3) maintained effective controls to provide reasonable assurance that

- logical and physical access to CA systems and data is restricted to authorized individuals;
- the continuity of key and certificate management operations is maintained; and
- CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline, Version 2.8.

ECAC does not escrow its CA private keys and any subscriber private keys, does not provide subscriber key generation, certificate renewal and suspension services. Accordingly, our assertion does not extend to controls that would address those criteria.

ECAC has renewed its Root CA and subordinate CA infrastructure in the audit period. The go live process was finished on 2025-02-28, and the new TLS CA services are in place since 2025-02-28.

Abdul Wahid Khan

ECAC PMA Head

March 19, 2025

Appendix A

Root CA

ECAC TLS Root CA G1	
Subject	CN=ECAC TLS Root CA G1,O=Electronic Certification Accreditation Council,C=PK
Issuer	CN=ECAC TLS Root CA G1,O=Electronic Certification Accreditation Council,C=PK
Serial	4DA71C129CAE6AD72318CD7E43FF218D
SHA256 Fingerprint	1601DC334704BD853062D6DEBFEECAB38D496F515E186DA56175D9CA6F27256C

Subordinate CA

ECAC OV TLS CA G1	
Subject	CN=ECAC OV TLS CA G1,O=Electronic Certification Accreditation Council,C=PK
Issuer	CN=ECAC TLS Root CA G1,O=Electronic Certification Accreditation Council,C=PK
Serial	788B6ECD9DE1FD5C144CD3306CC35CE4
SHA256 Fingerprint	1C26939AD9A91D707FD040E5A3800E4D010F9E36886F50CDE69B8CF10BAD49DC