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 2023-08-01 to 2024-07-31 for its Root CA with CN=ECAC Root CA G1, O=Electronic Certification Accreditation Council, C=PK, and 10 intermediate CAs in the scope (see in the **Annex**), ECAC has:

(1) disclosed its business, key lifecycle management, certificate lifecycle management, and CA environment control practices in its:

- ECAC Certification Authorities CP/CPS v1.4,
- ECAC Certification Authorities CP/CPS v1.5 and
- Certificate Policy (CP) for Trust Services Providers (TSPs) v1.3,

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

- ECAC provides its services in accordance with its Pakistan National PKI ECAC Certification Authorities CP/CPS,

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

- the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
- it is enforced that subscriber information is properly authenticated (for the registration activities performed by the TSPs); and
- subordinate CA certificate requests are accurate, authenticated, and approved

(4) 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 v2.2.2.

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.

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 v2.2.2.

Our independence and quality control

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 Control 1 "Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance and 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.

Auditor'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 key and certificate lifecycle management business practices and its controls over key and certificate integrity, over the authenticity and confidentiality of subscriber and relying party information, over the continuity of key and certificate lifecycle management operations and over development, maintenance and operation of systems integrity;

(2) selectively testing transactions executed in accordance with disclosed key and certificate lifecycle management business 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 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 2023-08-01 to 2024-07-31, 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 v2.2.2.

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 v2.2.2, 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 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.

Anna Kőszegi
Partner

Péter Máté Erdősi PhD CISA
Director

October 30, 2024

Annex

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

Technically constrained CAs

ECAC Commercial Client Authentication CA G1	
Subject	CN=ECAC Commercial Client Authentication CA G1,O=Electronic Certification Accreditation Council,C=PK
Issuer	CN=ECAC Root CA G1,O=Electronic Certification Accreditation Council,C=PK
Serial	49333F5787900990DF0C4C1545B8515EF13AB224
Key Algorithm	RSA
Key Size	4096 bit
Digest Algorithm	SHA256
Not Before	2023-01-16 13:18:19 GMT
Not After	2040-01-16 13:18:19 GMT
SKI	A80C6E808FEFF71D83FBDF0C26592B24AEF67311
SHA256 Fingerprint	094C6668F247B148AAC26DEF75ECBB351A08BACA2156401B08FCF62D49EDAFC6

ECAC Commercial Code Signing CA G1	
Subject	CN=ECAC Commercial Code Signing CA G1,O=Electronic Certification Accreditation Council,C=PK
Issuer	CN=ECAC Root CA G1,O=Electronic Certification Accreditation Council,C=PK
Serial	5AC2DA6E334A70FFDDEC6A24C857F95E9F939482
Key Algorithm	RSA
Key Size	4096 bit
Digest Algorithm	SHA256
Not Before	2023-01-16 13:29:34 GMT

ECAC Commercial Code Signing CA G1	
Not After	2040-01-16 13:29:34 GMT
SKI	F09FB73D45E4951CB950E2F2A3FB9348A7605E9B
SHA256 Fingerprint	304475CD3886E9F89FA4ACCDFA721FF3A46380164E06D6B30BC780848D677825

ECAC Commercial SMIME CA G1	
Subject	CN=ECAC Commercial SMIME CA G1,O=Electronic Certification Accreditation Council,C=PK
Issuer	CN=ECAC Root CA G1,O=Electronic Certification Accreditation Council,C=PK
Serial	2A1FA8CC3E6BDEB25D4743425EEC04C5945B3726
Key Algorithm	RSA
Key Size	4096 bit
Digest Algorithm	SHA256
Not Before	2023-01-16 13:31:38 GMT
Not After	2040-01-16 13:31:38 GMT
SKI	A2C0795DD151AA2EA56B5F3E79D900241E38A469
SHA256 Fingerprint	153A825CDCFBF89157AE6DF13FC1045D405E7257C8979F35A612322B2232D6B1

ECAC Commercial Timestamping CA G1	
Subject	CN=ECAC Commercial Timestamping CA G1,O=Electronic Certification Accreditation Council,C=PK
Issuer	CN=ECAC Root CA G1,O=Electronic Certification Accreditation Council,C=PK
Serial	59992794C79053A9E7FA788767A42E7B5B71B005
Key Algorithm	RSA
Key Size	4096 bit
Digest Algorithm	SHA256
Not Before	2023-01-16 13:27:07 GMT
Not After	2040-01-16 13:27:07 GMT
SKI	F36BCDFB5E5E2193A51903C8E3EAF396DA942304
SHA256 Fingerprint	8D2FEC8E06B5F85D00ACE69E3A45BB2B9F52C58B3922C34749660E71D374ED24

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 Client Authentication CA G1	
Subject	CN=ECAC Government Client Authentication CA G1,O=Electronic Certification Accreditation Council,C=PK
Issuer	CN=ECAC Root CA G1,O=Electronic Certification Accreditation Council,C=PK
Serial	3FD0E0EA61B72BDD2599163127015ADD0E0C37B6
Key Algorithm	RSA
Key Size	4096 bit
Digest Algorithm	SHA256
Not Before	2023-01-16 13:13:52 GMT
Not After	2040-01-16 13:13:52 GMT
SKI	5E655DBCD819671660511E3BEFCDCA1895F90D57
SHA256 Fingerprint	33F5587821962FEE27D17A10FBD133C12A895374ECF565925F63633442DB71D2

ECAC Government Code Signing CA G1	
Subject	CN=ECAC Government Code Signing CA G1,O=Electronic Certification Accreditation Council,C=PK
Issuer	CN=ECAC Root CA G1,O=Electronic Certification Accreditation Council,C=PK
Serial	3D7958777463C7486C818F88F370553CD5716998
Key Algorithm	RSA
Key Size	4096 bit
Digest Algorithm	SHA256
Not Before	2023-01-16 13:28:56 GMT
Not After	2040-01-16 13:28:56 GMT
SKI	F9DB1C60182DD16DAA25B919D8E3CE41BB4DCB1C
SHA256 Fingerprint	29F0E39869B6DDBC269623EDCC453F764E026559A0B238A0BADC5F27743D1931

ECAC Government SMIME CA G1	
Subject	CN=ECAC Government SMIME CA G1,O=Electronic Certification Accreditation Council,C=PK
Issuer	CN=ECAC Root CA G1,O=Electronic Certification Accreditation Council,C=PK
Serial	50716918A1FFB95858E090D039BE0A5C33A9E62E
Key Algorithm	RSA
Key Size	4096 bit
Digest Algorithm	SHA256
Not Before	2023-01-16 132934 GMT
Not After	2040-01-16 132934 GMT
SKI	07ED94DD1A3667CDC73D32B687C1F991128CC73D
SHA256 Fingerprint	2371A3686D2A1BAEC08E560755DB7BE9424408023DD5BB995C0211E0059818DE

ECAC Government Timestamping CA G1	
Subject	CN=ECAC Government Timestamping CA G1,O=Electronic Certification Accreditation Council,C=PK
Issuer	CN=ECAC Root CA G1,O=Electronic Certification Accreditation Council,C=PK
Serial	30ACF22688DDB7ACB4290F27DF5A41EDFB2BC02F
Key Algorithm	RSA
Key Size	4096 bit
Digest Algorithm	SHA256
Not Before	2023-01-16 13:26:16 GMT
Not After	2040-01-16 13:26:16GMT
SKI	F4436E13DB3BA44CA25E4D45134EC878B11D5A12
SHA256 Fingerprint	1CBF424FFABEB601E8210B12A7BDB9C211DB96B798FE879945F57EE704D291A1

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
Digest Algorithm	SHA256

ECAC Government TLS CA G1	
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") is operated by Electronic Certification Accreditation Council, Pakistan known as list of Root and Subordinate CAs in scope (see **Appendix A**), and provides the following CA services

- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation
- Subordinate CA certification

The management of ECAC is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure on its website, CA business practices management, CA environmental controls, CA key lifecycle management controls, certificate lifecycle management controls, and subordinate CA 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 CA services. Based on that assessment, in providing its Certification Authority (CA) services at Islamabad and Lahore, Pakistan, throughout the period 2023-08-01 to 2024-07-31, ECAC has

(1) disclosed its business, key lifecycle management, certificate lifecycle management, and CA environment control practices in the following documents

- ECAC Certification Authorities CP/CPS v1.4,
- ECAC Certification Authorities CP/CPS v1.5 and
- Certificate Policy (CP) for Trust Services Providers (TSPs) v1.3,

(2) maintained effective controls to provide reasonable assurance that

- ECAC provides its services in accordance with its Pakistan National PKI ECAC Certification Authorities CP/CPS,

(3) maintained effective controls to provide reasonable assurance that

- the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
- it is enforced that subscriber information is properly authenticated (for the registration activities performed by the TSPs); and
- subordinate CA certificate requests are accurate, authenticated, and approved

(4) 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 v2.2.2, including the following

CA Business Practices Disclosure

- combined Certificate Policy (CP) / Certification Practice Statement (CPS)

CA Business Practices Management

- combined Certificate Policy (CP) / Certification Practice Statement (CPS) Management

CA Environmental Controls

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical & Environmental Security
- Operations Management
- System Access Management
- System Development and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Audit Logging

CA Key Lifecycle Management Controls

- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Archival and Destruction
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management

Enforcing Subscriber Key Lifecycle Management Controls

- Requirements for Subscriber Key Management (via Certificate Policy (CP) for Trust Services Providers (TSPs))

Certificate Lifecycle Management Controls

- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

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

A GATEWAY TO DIGITAL PAKISTAN

Subordinate CA Certificate Lifecycle Management Controls

- Subordinate CA Certificate Lifecycle Management

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.

Abdul Wahid Khan
ECAC PMA Head
October 26, 2024

Appendix A

Root CA	
Subject	CN=ECAC Root CA G1,O=Electronic Certification Accreditation Council,C=PK
Serial	75F3520C33E0E4D4F3F36799B7DB1CF15F20B265
SHA256 Fingerprint	4EC7B0E3257F710D2F2D90D3CF9E0C87ECF3D2CE59D724F9DDAE1C2485611324

ECAC Commercial Client Authentication CA G1	
Subject	CN=ECAC Commercial Client Authentication CA G1,O=Electronic Certification Accreditation Council,C=PK
Serial	49333F5787900990DF0C4C1545B8515EF13AB224
SHA256 Fingerprint	094C6668F247B148AAC26DEF75ECBB351A08BACA2156401B08FCF62D49EDAFC6

ECAC Commercial Code Signing CA G1	
Subject	CN=ECAC Commercial Code Signing CA G1,O=Electronic Certification Accreditation Council,C=PK
Serial	5AC2DA6E334A70FFDDEC6A24C857F95E9F939482
SHA256 Fingerprint	304475CD3886E9F89FA4ACCDFA721FF3A46380164E06D6B30BC780848D677825

ECAC Commercial SMIME CA G1	
Subject	CN=ECAC Commercial SMIME CA G1,O=Electronic Certification Accreditation Council,C=PK
Serial	2A1FA8CC3E6BDEB25D4743425EEC04C5945B3726
SHA256 Fingerprint	153A825CDCFBF89157AE6DF13FC1045D405E7257C8979F35A612322B2232D6B1

ECAC Commercial Timestamping CA G1	
Subject	CN=ECAC Commercial Timestamping CA G1,O=Electronic Certification Accreditation Council,C=PK
Serial	59992794C79053A9E7FA788767A42E7B5B71B005
SHA256 Fingerprint	8D2FEC8E06B5F85D00ACE69E3A45BB2B9F52C58B3922C34749660E71D374ED24

ECAC Commercial TLS CA G1	
Subject	CN=ECAC Commercial TLS CA G1,O=Electronic Certification Accreditation Council,C=PK
Serial	2C54F22077FA7E28191234F38DE01799DA79346C
SHA256 Fingerprint	8992E142128A9C22BCE74FC48F6BFB46FBBF5CC0604C7DC213323036AFAAC502

ECAC Government Client Authentication CA G1	
Subject	CN=ECAC Government Client Authentication CA G1,O=Electronic Certification Accreditation Council,C=PK
Serial	3FD0E0EA61B72BDD2599163127015ADD0E0C37B6
SHA256 Fingerprint	33F5587821962FEE27D17A10FBD133C12A895374ECF565925F63633442DB71D2

ECAC Government Code Signing CA G1	
Subject	CN=ECAC Government Code Signing CA G1,O=Electronic Certification Accreditation Council,C=PK
Serial	3D7958777463C7486C818F88F370553CD5716998
SHA256 Fingerprint	29F0E39869B6DDBC269623EDCC453F764E026559A0B238A0BADC5F27743D1931

ECAC Government SMIME CA G1	
Subject	CN=ECAC Government SMIME CA G1,O=Electronic Certification Accreditation Council,C=PK
Serial	50716918A1FFB95858E090D039BE0A5C33A9E62E
SHA256 Fingerprint	2371A3686D2A1BAEC08E560755DB7BE9424408023DD5BB995C0211E0059818DE

ECAC Government Timestamping CA G1	
Subject	CN=ECAC Government Timestamping CA G1,O=Electronic Certification Accreditation Council,C=PK
Serial	30ACF22688DDB7ACB4290F27DF5A41EDFB2BC02F
SHA256 Fingerprint	1CBF424FFABEB601E8210B12A7BDB9C211DB96B798FE879945F57EE704D291A1

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

A GATEWAY TO DIGITAL PAKISTAN

ECAC Government TLS CA G1	
Subject	CN=ECAC Government TLS CA G1,O=Electronic Certification Accreditation Council,C=PK
Serial	55763E2DCF7C02DD776C551D79DC8F1BE0047E8F
SHA256 Fingerprint	8B32E9E5F919BD7449099E439F149829ABB1830C88E079E8AD26D11BB0D0DAD0