

## 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 2 intermediate CAs in scope (as enumerated in the **Annex**), ECAC has:

(1) disclosed its extended validation SSL (“EV SSL”) certificate lifecycle management business 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](#),

including its commitment to provide EV SSL certificates in conformity with the CA/Browser Forum Guidelines 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 EV SSL certificates managed by the licensed TSPs is established and protected throughout their lifecycles; and
- EV SSL subscriber information is properly authenticated (for the registration activities performed by the licensed TSPs);

in accordance with the [WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL – Version 1.8](#).

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.

### 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 – Extended Validation SSL – Version 1.8](#).

### 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 Historical Financial Information, and Other Assurance and Related Services*”, 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 EV SSL certificate lifecycle management business practices including its relevant controls over the issuance and revocation of EV SSL certificates;
- (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

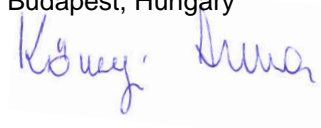
In our opinion, throughout the period 2023-08-01 to 2024-07-31, ECAC management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with the [WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL – Version 1.8](#).

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 – Extended Validation SSL – Version 1.8](#), 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 – Extended Validation SSL 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



Anna Kőszegi  
Partner



Péter Máté Erdősi PhD CISA  
Director

October 30, 2024

**Annex**

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

**Technically constrained CAs**

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

<b>ECAC Government TLS CA G1</b>	
<b>Subject</b>	CN=ECAC Government TLS CA G1,O=Electronic Certification Accreditation Council,C=PK
<b>Issuer</b>	CN=ECAC Root CA G1,O=Electronic Certification Accreditation Council,C=PK
<b>Serial</b>	55763E2DCF7C02DD776C551D79DC8F1BE0047E8F
<b>Key Algorithm</b>	RSA
<b>Key Size</b>	4096 bit
<b>Digest Algorithm</b>	SHA256
<b>Not Before</b>	2023-01-16 132934 GMT

<b>ECAC Government TLS CA G1</b>	
<b>Not After</b>	2040-01-16 132934 GMT
<b>SKI</b>	FF52146C41472EA47326FDDFEF26444A42832B95
<b>SHA256 Fingerprint</b>	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 Extended Validation SSL ("EV SSL") CA services.

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

(1) disclosed its extended validation SSL ("EV SSL") certificate lifecycle management business 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](#),

including its commitment to provide EV SSL certificates in conformity with the CA/Browser Forum Guidelines [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 EV SSL certificates managed by the licensed TSPs is established and protected throughout their lifecycles;
- EV SSL subscriber information is properly authenticated (for the registration activities performed by the licensed TSPs);

in accordance with the [WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL – Version 1.8](#).



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



**A GATEWAY TO DIGITAL PAKISTAN**

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



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



**A GATEWAY TO DIGITAL PAKISTAN**

**Appendix A**

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

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

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