Tel: +603 2616 2888
Fax: +603 2616 2829
www.bdo.my

Level 8
BDO @ Menara CenTARa
360 Jalan Tuanku Abdul Rahman
50100 Kuala Lumpur
Malaysia

INDEPENDENT ASSURANCE REPORT

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

Scope

We have been engaged, in a reasonable assurance engagement, to report on ECAC management's assertion that for its Certification Authorities (CA) operations at Islamabad and Lahore, Pakistan, throughout the period 11 January 2023 and 31 July 2023 for its CA as enumerated in Appendix A, ECAC has:

- Disclosed its extended validation SSL ("EV SSL") certificate lifecycle management business practices in applicable versions of its Certification Practice Statement (CPS) as enumerated in Appendix B, 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

- Maintained effective controls to provide reasonable assurance that:
  - The integrity of keys and EV SSL certificates it manages is established and protected throughout their lifecycles; and
  - EV SSL subscriber information is properly authenticated (for the registration activities performed by ECAC)

in accordance with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.8.

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 v1.8.

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 behaviour.

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 EV SSL certificate lifecycle management business practices, including its relevant controls over the issuance, rekey, and revocation of EV SSL certificates;
2. Selectively testing transactions executed in accordance with disclosed EV 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 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 11 January 2023 to 31 July 2023, 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 v1.8.

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 v1.8, 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.

BDO Consulting Sdn. Bhd.
BDO Consulting Sdn. Bhd.
Kuala Lumpur, Malaysia
14 November 2023

Appendix A - List of Root and Intermediate CAs in Scope

No.	Common Name	Certificate Serial No.	SHA-256 Fingerprint
Root CA			
1	ECAC Root CA G1	75F3520C33E0E4D4F3F36799B7DB1CF15F20B265	4EC7B0E3257F710D2F2D90D3CF9E0C87ECF3D2CE59D724F9DDAE1C2485611324
Intermediate Government CA			
2	ECAC Government TLS CA G1	55763E2DCF7C02DD776C551D79DC8F1BE0047E8F	8B32E9E5F919BD7449099E439F149829ABB1830C88E079E8AD26D11BB0D0DAD0
Intermediate Commercial CA			
3	ECAC Commercial TLS CA G1	2C54F22077FA7E28191234F38DE01799DA79346C	8992E142128A9C22BCE74FC48F6BFB46FBBF5CC0604C7DC213323036AFAAC502

Appendix B - Certification Practice Statements in Scope

Certification Practice Statement	Begin Effective Date	End Effective Date
Version 1.2	28 December 2023	21 February 2023
Version 1.3	22 February 2023	16 July 2023
Version 1.4	17 July 2023	-

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

A GATEWAY TO DIGITAL PAKISTAN

Dated: 14th November, 2023

ECAC MANAGEMENT'S ASSERTION

Electronic Certification Accreditation Council ("ECAC") operates the Certification Authority (CA) services known as enumerated in 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's CA 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 CA services at Islamabad and Lahore, Pakistan, throughout the period 11 January 2023 to 31 July 2023, ECAC has:

- Disclosed its EV SSL certificate lifecycle management business practices in applicable versions of its Certification Practice Statement as enumerated in Appendix B including its commitment to provide EV SSL certificates in conformity with the CA/Browser Forum Guidelines on the ECAC website, and provide such services in accordance with its disclosed practices;

- Maintained effective controls to provide reasonable assurance that:
  - The integrity of keys and EV SSL certificates it manages is established and protected throughout their lifecycles; and
  - EV SSL subscriber information is properly authenticated (for the registration activities performed by ECAC).

in accordance with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.8.

Miraj Gul
ECAC PMA Head

Appendix A – List of Root and Intermediate CAs in Scope

No.	Common Name	Certificate Serial No.	SHA-256 Fingerprint
Root CA			
1	ECAC Root CA G1	75F3520C33E0E4D4F3F36799B7DB1CF15F20B265	4EC7B0E3257F710D2F2D90D3CF9E0C87ECF3D2CE59D724F9DDAE1C2485611324
Intermediate Government CA			
2	ECAC Government TLS CA G1	55763E2DCF7C02DD776C551D79DC8F1BE0047E8F	8B32E9E5F919BD7449099E439F149829ABB1830C88E079E8AD26D11BB0D0DAD0
Intermediate Commercial CA			
3	ECAC Commercial TLS CA G1	2C54F22077FA7E28191234F38DE01799DA79346C	8992E142128A9C22BCE74FC48F6BFB46FBBF5CC0604C7DC213323036AFAAC502

Appendix B – Certification Practice Statements in Scope

Certification Practice Statement	Begin Effective Date	End Effective Date
Version 1.2	28 December 2022	21 February 2023
Version 1.3	22 February 2023	16 July 2023
Version 1.4	17 July 2023	-