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 Authority (CA) operations at Islamabad and Lahore, Pakistan, throughout the period 11 January 2023 to 31 July 2023 for its CAs as enumerated in Appendix A(i), ECAC has:

- Disclosed its 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 SSL certificates in conformity with the CA/Browser Forum Requirement 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 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)

- Maintained effective controls to provide reasonable assurance that:
  - Logical and physical access to CA systems and data is restricted to authorised to individuals;
  - The continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorised and performed to maintain CA systems integrity

And for its CAs as enumerated in Appendix A(ii):

- Maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.7.

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 with Network Security v2.7.

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 SSL certificate lifecycle management business practices, including its relevant control over the issuance, rekey and revocation of SSL certificates, and obtaining an understanding of ECAC's network and certificate system security to meet the requirements set forth by the CA/Browser Forum;
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 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 - SSL Baseline with Network Security v2.7.

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 with Network Security v2.7, 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 with Network Security Seal constitutes of 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(i) – List of SSL 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 A(ii) – List of SSL and Non-SSL 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 Client Authentication CA G1	3FD0E0EA61B72BDD2599163127015ADD0E0C37B6	33F5587821962FEE27D17A10FBD133C12A895374ECF565925F63633442DB71D2
3	ECAC Government TLS CA G1	55763E2DCF7C02DD776C551D79DC8F1BE0047E8F	8B32E9E5F919BD7449099E439F149829ABB1830C88E079E8AD26D11BB0D0DAD0
4	ECAC Government Code Signing CA G1	3D7958777463C7486C818F88F370553CD5716998	29F0E39869B6DDBC269623EDCC453F764E026559A0B238A0BADC5F27743D1931
5	ECAC Government Timestamping CA G1	30ACF22688DDB7ACB4290F27DF5A41EDFB2BC02F	1CBF424FFABEB601E8210B12A7BDB9C211DB96B798FE879945F57EE704D291A1
6	ECAC Government SMIME CA G1	50716918A1FFB95858E090D039BE0A5C33A9E62E	2371A3686D2A1BAEC08E560755DB7BE9424408023DD5BB995C0211E0059818DE
Intermediate Commercial CA			
7	ECAC Commercial Client Authentication CA G1	49333F5787900990DF0C4C1545B8515EF13AB224	094C6668F247B148AAC26DEF75ECBB351A08BACA2156401B08FCF62D49EDAFC6
8	ECAC Commercial TLS CA G1	2C54F22077FA7E28191234F38DE01799DA79346C	8992E142128A9C22BCE74FC48F6BFB46FBBF5CC0604C7DC213323036AFAAC502
9	ECAC Commercial Code Signing CA G1	5AC2DA6E334A70FFDDEC6A24C857F95E9F939482	304475CD3886E9F89FA4ACCDFA721FF3A46380164E06D6B30BC780848D677825
10	ECAC Commercial Timestamping CA G1	59992794C79053A9E7FA788767A42E7B5B71B005	8D2FEC8E06B5F85D00ACE69E3A45BB2B9F52C58B3922C34749660E71D374ED24

11	ECAC Commercial SMIME CA G1	2A1FA8CC3E6BDEB25D4743425EEC04C5945B3726	153A825CDCFBF89157AE6DF13FC1045D405E7257C8979F35A612322B2232D6B1

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	-

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

A GATEWAY TO DIGITAL PAKISTAN

Dated: 18th September 2023

ECAC MANAGEMENT'S ASSERTION

Electronic Certification Accreditation Council ("ECAC") operates the Certification Authority (CA) services known as enumerated in Appendix A(i), root and intermediate CAs in scope for SSL Baseline Requirements and provides SSL CA services.

ECAC operates the CA services known as enumerated in Appendix A(ii) for root and intermediate CAs in scope for the Network Security Requirements and provides SSL and non-SSL CA services.

The management of ECAC is responsible for establishing and maintaining effective controls over its SSL and non-SSL CA operations, including its network and certificate security system controls, its SSL CA business practices disclosure on its website, SSL key lifecycle management controls, and SSL certificate lifecycle management controls. These controls contain monitoring mechanism, 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 disclosure of its certificate practices and controls over its CA services. Based on that assessment, in providing its SSL and non-SSL CA services at Islamabad and Lahore, Pakistan throughout the period 11 January 2023 to 31 July 2023, ECAC has:

- Disclosed its SSL certificate lifecycle management business practices in applicable versions of its Certification Practice Statement as enumerated in Appendix B including its commitment to provide SSL certificate in conformity with the CA/Browser Forum Requirement 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 SSL certificate it manages is established and protected throughout their lifecycles; and
  - SSL subscriber information is properly authenticated (for the registration activities performed by ECAC).
- 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.
- Maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by CA/Browser Forum.

in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.7.

Miraj Gul
ECAC PMA Head

Appendix A(i) – List of SSL 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 A(ii) – List of SSL and Non-SSL 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 Client Authentication CA G1	3FD0E0EA61B72BDD2599163127015ADD0E0C37B6	33F5587821962FEE27D17A10FBD133C12A895374ECF565925F63633442DB71D2
3	ECAC Government TLS CA G1	55763E2DCF7C02DD776C551D79DC8F1BE0047E8F	8B32E9E5F919BD7449099E439F149829ABB1830C88E079E8AD26D11BB0D0DAD0
4	ECAC Government Code Signing CA G1	3D7958777463C7486C818F88F370553CD5716998	29F0E39869B6DDBC269623EDCC453F764E026559A0B238A0BADC5F27743D1931
5	ECAC Government Timestamping CA G1	30ACF22688DDB7ACB4290F27DF5A41EDFB2BC02F	1CBF424FFABEB601E8210B12A7BDB9C211DB96B798FE879945F57EE704D291A1
6	ECAC Government SMIME CA G1	50716918A1FFB95858E090D039BE0A5C33A9E62E	2371A3686D2A1BAEC08E560755DB7BE9424408023DD5BB995C0211E0059818DE
Intermediate Commercial CA			
7	ECAC Commercial Client Authentication CA G1	49333F5787900990DF0C4C1545B8515EF13AB224	094C6668F247B148AAC26DEF75ECBB351A08BACA2156401B08FCF62D49EDAFC6
8	ECAC Commercial TLS CA G1	2C54F22077FA7E28191234F38DE01799DA79346C	8992E142128A9C22BCE74FC48F6BFB46FBBF5CC0604C7DC213323036AFAAC502
9	ECAC Commercial Code Signing CA G1	5AC2DA6E334A70FFDDEC6A24C857F95E9F939482	304475CD3886E9F89FA4ACCDFA721FF3A46380164E06D6B30BC780848D677825
10	ECAC Commercial Timestamping CA G1	59992794C79053A9E7FA788767A42E7B5B71B005	8D2FEC8E06B5F85D00ACE69E3A45BB2B9F52C58B3922C34749660E71D374ED24
11	ECAC Commercial SMIME CA G1	2A1FA8CC3E6BDEB25D4743425EEC04C5945B3726	153A825CDCFBF89157AE6DF13FC1045D405E7257C8979F35A612322B2232D6B1

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	-