

## 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](#), ECAC has:

- Disclosed its code signing (“CS”) certificate lifecycle management business practices in applicable versions of its Certification Practice Statement (CPS) as enumerated in [Appendix B](#), including its commitment to provide CS certificate in conformity with the CA/Browser Forum Requirements on the ECAC website, and provided such services in accordance with its disclosed practices
- Maintained effective controls to provide reasonable assurance that:
  - CS subscriber information is properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified; and
  - The integrity of keys and CS certificates it manages is established and protected throughout their lifecycles.
- Maintained effective controls to provide reasonable assurance that:
  - EV CS subscriber information is properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified; and
  - The integrity of keys and EV CS certificates it manages is established and protected throughout their lifecycles.

in accordance with the [WebTrust Principles and Criteria for Certification Authorities - Code Signing Baseline Requirements v3.2](#).

### 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, based on the WebTrust Principles and Criteria for Certification Authorities - Code Signing Baseline Requirements v3.2.



## **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 CS and EV CS certificate lifecycle management business practices, including its relevant controls over the issuance, rekey, and revocation of CS and EV CS certificates;
2. Selectively testing transactions executed in accordance with disclosed CS and EV CS 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 - Code Signing Baseline Requirements v3.2.

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 - Code Signing Baseline Requirements v3.2, nor the suitability of any of ECAC's services for any customer's intended purposes.

## Use of the WebTrust seal

ECAC's use of the WebTrust for Certification Authorities - Code Signing 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
<b>Root CA</b>			
1	ECAC Root CA G1	75F3520C33E0E4D4F3F36 799B7DB1CF15F20B265	4EC7B0E3257F710D2F2D90 D3CF9E0C87ECF3D2CE59D7 24F9DDAE1C2485611324
<b>Intermediate Government CA</b>			
2	ECAC Government Code Signing CA G1	3D7958777463C7486C818 F88F370553CD5716998	29F0E39869B6DDBC269623 EDCC453F764E026559A0B2 38A0BADC5F27743D1931
3	ECAC Government Timestamping CA G1	30ACF22688DDB7ACB429 0F27DF5A41EDFB2BC02F	1CBF424FFABEB601E8210B 12A7BDB9C211DB96B798FE 879945F57EE704D291A1
<b>Intermediate Commercial CA</b>			
4	ECAC Commercial Code Signing CA G1	5AC2DA6E334A70FFDDEC 6A24C857F95E9F939482	304475CD3886E9F89FA4AC CDFA721FF3A46380164E06 D6B30BC780848D677825
5	ECAC Commercial Timestamping CA G1	59992794C79053A9E7FA7 88767A42E7B5B71B005	8D2FEC8E06B5F85D00ACE6 9E3A45BB2B9F52C58B3922 C34749660E71D374ED24

## Appendix B - Certification Practice Statements in Scope

Certification Practice Statement	Begin Effective Date	End Effective Date
<a href="#">Version 1.2</a>	28 December 2022	21 February 2023
<a href="#">Version 1.3</a>	22 February 2023	16 July 2023
<a href="#">Version 1.4</a>	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: 14<sup>th</sup> November, 2023

### ECAC MANAGEMENT'S ASSERTION

Electronic Certification Accreditation Council ("ECAC") operates the Certification Authority (CA) services for the root and intermediate CAs in scope enumerated in [Appendix A](#), and provide code signing (CS) CA services.

The management of ECAC is responsible for establishing and maintaining effective controls over its code signing services, including its code signing business practices disclosure on its [website](#), code signing key lifecycle management controls, and certificate lifecycle management controls. These controls contain monitoring mechanisms, and action 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 CS CA services. Based on that assessment, in ECAC management's opinion, in providing its CS CA services at Islamabad and Lahore, Pakistan, throughout the period 11 January 2023 to 31 July 2023, ECAC has:

- Disclosed its CS certificate lifecycle management business practices in applicable versions of its Certification Practice Statement (CPS) as enumerated in [Appendix B](#), including its commitment to provide CS certificate in conformity with the CA/Browser Forum Requirements on the ECAC website, and provided such services in accordance with its disclosed practices;
- Maintained effective controls to provide reasonable assurance that:
  - CS subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified;
  - The integrity of keys and CS certificates it manages is established and protected throughout their lifecycles
- Maintained effective controls to provide reasonable assurance that:
  - EV CS subscriber information was properly collected, authenticated (for the registration activities performed by the CA, RA and subcontractor) and verified;
  - The integrity of keys and EV CS certificates it manages is established and protected throughout their life cycles

in accordance with the [WebTrust Principles and Criteria for Certification Authorities – Code Signing Baseline Requirements v3.2](#).

  
Miraj Gul  
ECAC PMA Head

### Appendix A - List of CS Root and Intermediate CAs in Scope

No.	Common Name	Certificate Serial No.	SHA-256 Fingerprint
<b>Root CA</b>			
1	ECAC Root CA G1	75F3520C33E0E4D4F3F3 6799B7DB1CF15F20B265	4EC7B0E3257F710D2F2D90 D3CF9E0C87ECF3D2CE59 D724F9DDAE1C248561132 4
<b>Intermediate Government CA</b>			
2	ECAC Government Code Signing CA G1	3D7958777463C7486C818 F88F370553CD5716998	29F0E39869B6DDBC269623 EDCC453F764E026559A0B 238A0BAD5F27743D1931
3	ECAC Government Timestamping CA G1	30ACF22688DDB7ACB4 290F27DF5A41EDFB2BC 02F	1CBF424FFABEB601E8210 B12A7BDB9C211DB96B798 FE879945F57EE704D291A1
<b>Intermediate Commercial CA</b>			
4	ECAC Commercial Code Signing CA G1	5AC2DA6E334A70FFDD EC6A24C857F95E9F9394 82	304475CD3886E9F89FA4A CCDFA721FF3A46380164E 06D6B30BC780848D677825
5	ECAC Commercial Timestamping CA G1	59992794C79053A9E7FA 788767A42E7B5B71B005	8D2FEC8E06B5F85D00AC E69E3A45BB2B9F52C58B3 922C34749660E71D374ED2 4

### Appendix B - Certification Practice Statements in Scope

Certification Practice Statement	Begin Effective Date	End Effective Date
<a href="#">Version 1.2</a>	28 December 2022	21 February 2023
<a href="#">Version 1.3</a>	22 February 2023	16 July 2023
<a href="#">Version 1.4</a>	17 July 2023	-