Tel: +603 2616 2888
Fax: +603 2616 3190 / 2616 3191
www.bdo.my

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

INDEPENDENT ASSURANCE REPORT

To the management of Sri Lanka CERT (Private) Limited ("Sri Lanka CERT"):

Scope

We have been engaged, in a reasonable assurance engagement, to report on Sri Lanka CERT management's assertion that for its Certification Authority (CA) operations at Colombo, Sri Lanka, throughout the period 15 May 2025 to 31 August 2025 for its CA as enumerated in Appendix A, Sri Lanka CERT has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its Certification Practice Statement (CPS) as enumerated in Appendix B

- maintained effective controls to provide reasonable assurance that it provides services in accordance with its CPS

- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
  - subordinate CA certificate requests are accurate, authenticated, and approved

- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorised 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

in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.2.2.

Sri Lanka CERT does not escrow its CA key and does not provide subscriber key lifecycle management services as it only issues subordinate CA certificates. Sri Lanka CERT 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

Sri Lanka CERT'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 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 Sri Lanka CERT's key and certificate lifecycle management business practices and its control 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 relative effectiveness and significance of specific controls at Sri Lanka CERT 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 15 May 2025 to 31 August 2025, Sri Lanka CERT 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 Sri Lanka CERT's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities v2.2.2, nor the suitability of any of Sri Lanka CERT's services for any customer's intended purpose.

Use of the WebTrust seal

Sri Lanka CERT'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.

BDO PLT

BDO PLT
Kuala Lumpur, Malaysia
5 March 2026

Appendix A - List of Root CAs in Scope

Common Name	Certificate Serial No.	Subject Key Identifier	SHA-256 Fingerprint
National Certification Authority of Sri Lanka DS Root CA – G1	4F22ED33AA74F0A4297D02EF7F24611DA9E2AD72	30677294CEC789CCF0BC39904930688F9EAC2F4F	2072C50689F0771DD5087273641168 54A5D54D0991B9F75906BB2A94D4C628D3
National Certification Authority of Sri Lanka TLS Root CA – G1	169E55B09DB9F912E4EBA9C8CCCEC11E1CE6D667	1957B482F2F6A53833C1F5A32486E33CC167EDDC	173CF0179612EF44B4491127DF9CD24EA68B745388903569164 3B26C4E511F37

Appendix B - Certificate Policy and Certification Practice Statement in Scope

CP/CPS	Begin Effective Date	End Effective Date
National Certification Authority of Sri Lanka Certificate Policy / Certification Practice Statement version 1.0	7 May 2025	-

ශ්‍රී ලංකා පරිගණක හදිසි ප්‍රතිචාර සංසදය
இலங்கை கணினி அவசர தயார்நிலை அணி
Sri Lanka Computer Emergency Readiness Team

කාමර අංක. 4-112, බී.එම්.අයි.සි.එච්, බෞද්ධාලෝක මාවත, කොළඹ 07.
அறை இல. 4-112, பி.எம்.ஐ.சி.எச், பௌத்தாலோக மாவத்தை, கொழும்பு 07.
Room No. 4-112, BMICH, Bauddhaloka Mawatha, Colombo 07.

Sri Lanka CERT MANAGEMENT'S ASSERTION

Sri Lanka CERT (Private) Limited ("Sri Lanka CERT") operates the Certification Authority ("CA") services known as enumerated in Appendix A and provides the following CA services:

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

The management of Sri Lanka CERT 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 Sri Lanka CERT's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

Sri Lanka CERT management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in Sri Lanka CERT management's opinion, in providing its Certification Authority (CA) services at Colombo, Sri Lanka, throughout the period 15 May 2025 to 31 August 2025, Sri Lanka CERT has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its Certification Practice Statement (CPS) as enumerated in Appendix B

- maintained effective controls to provide reasonable assurance that it provides services in accordance with its CPS as enumerated in Appendix B

- maintained effective controls to provide reasonable assurance that:
    - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
    - subordinate CA certificate requests are accurate, authenticated, and approved

- maintained effective controls to provide reasonable assurance that:
    - logical and physical access to CA systems and data is restricted to authorised 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

in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.2.2, including the following:

CA Business Practices Disclosure

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

CA Business Practices Management

- CP/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
- CA Key Destruction
- CA Key Compromise

- CA Cryptographic Hardware Lifecycle Management
- CA Key Transportation
- CA Key Migration

Certificate Lifecycle Management Controls

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

Subordinate CA Certificate Lifecyle Management Controls

- Subordinate CA Certificate Lifecycle Management

Sri Lanka CERT does not escrow its CA key and does not provide subscriber key lifecycle management services as it only issues subordinate CA certificates. Sri Lanka CERT does not provide certificate renewal and suspension services. Accordingly, our assertion does not extend to controls that would address those criteria.

Dr. Kanishka Karunasena
Chief Executive Officer (Actg.)
5th March 2026
Sri Lanka CERT (Private) Limited

Appendix A - List of Root CAs in Scope

Common Name	Certificate Serial No.	Subject Key Identifier	SHA-256 Fingerprint
National Certification Authority of Sri Lanka DS Root CA - G1	4F22ED33AA74F0A4297D02EF7F24611DA9E2AD72	30677294CEC789CCF0BC39904930688F9EAC2F4F	2072C50689F0771DD5087273641168 54A5D54D0991B9F75906BB2A94D4C628D3
National Certification Authority of Sri Lanka TLS Root CA - G1	169E55B09DB9F912E4EBA9C8CCCEC11E1CE6D667	1957B482F2F6A53833C1F5A32486E33CC167EDDC	173CF0179612EF44B4491127DF9CD24EA68B745388903569164 3B26C4E511F37

Appendix B - Certificate Policy and Certification Practice Statement in Scope

CP/CPS	Begin Effective Date	End Effective Date
National Certification Authority of Sri Lanka Certificate Policy / Certification Practice Statement version 1.0	7 May 2025	-