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 eMudhra Technologies Limited ("emSign PKI"):

Scope

We have been engaged, in reasonable assurance engagement, to report on emSign PKI management's assertion that for its Certification Authority (CA) operations at Bangalore and Chennai, India throughout the period 1 June 2023 to 31 May 2024 for its CAs as enumerated in **Appendix A(i)**, emSign PKI has:

- disclosed its extended validation SSL ("EV SSL") certificate lifecycle management business practices in applicable versions of its Certification Practice Statements in **Appendix B**, including its commitment to provide EV SSL certificates in conformity with the CA/Browser Forum Requirements on the emSign PKI's 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 emSign PKI)

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

The CAs enumerated in **Appendix A(ii)** did not issue any EV SSL certificate for the audit period.

Certification authority's responsibilities

emSign PKI's management is responsible for its assertion, including the fairness of its presentation, and 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 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 emSign PKI's EV SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal 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 emSign PKI 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 1 June 2023 to 31 May 2024, emSign PKI 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 emSign PKI'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 emSign PKI's services for any customer's intended purpose.

Use of the WebTrust seal

emSign PKI'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.
Kuala Lumpur, Malaysia
19 August 2024

Appendix A(i) – List of Root and Subordinate CAs in Scope

No.	Common Name	Certificate Serial No.	SHA-256 Fingerprint
1	**emSign Root CA - G1**	31F5E4620C6C58EDD6D8	40F6AF0346A99AA1CD1D555A4E9CCE62C7F9634603EE406615833DC8C8D00367
2	emSign EV SSL CA - G1	626CB92B237FF82E3F50	4334EEB2CC114F82BEE6F8A7E5AEA03A42EB2E1F70CBD66102E414D72F0033B9
3	**emSign ECC Root CA - G3**	3CF607A968700EDA8B84	86A1ECBA089C4A8D3BBE2734C612BA341D813E043CF9E8A862CD5C57A36BBE6B
4	emSign ECC EV SSL CA - G3	01FE3E6C68DEBBEC263E	0116F17F97CDEF4ADE2E63CF2C1B064FD99F404D2B914100BC241F0781853323
5	**emSign Root CA - C1**	00AECF00BAC4CF32F843B2	125609AA301DA0A249B97A8239CB6A34216F44DCAC9F3954B14292F2E8C8608F
6	emSign EV SSL CA - C1	00BADFD29B3F1E678C6960	F6F159286A1401DE5397E21A0090534A85F5E7B9F98FD4A5A47B1DFFD4BFDED4
7	**emSign ECC Root CA - C3**	7B71B68256B8127C9CA8	BC4D809B15189D78DB3E1D8CF4F9726A795DA1643CA5F1358E1DDB0EDC0D7EB3
8	emSign ECC EV SSL CA - C3	1B50581F7334B30B2723	C0A578F2109E6F42D3D939948DEEAB729B20F7B23B4237ABD8494DF554CF985C
9	**emSign Root TLS CA - G1**	02A27D4E346AEF4E4F04678B5BB6D9EE	CEF71E70B7C29ADDF6C30CD19E614B38FD5F02A435A0EEDDD0087E183D101A51
10	**emSign Root TLS CA - G3**	0E760672F143459FC8FE0AB0BC05E394	7DD78D5F4F13459A83DFF9ABBBA62EDBAF6F2D102BF257FD712F4D9F2746ED8D

Appendix A(ii) – List of Subordinate CAs in Scope

No.	Common Name	Certificate Serial No.	SHA-256 Fingerprint
1	emSign SSL CA - G1	217AD58B1C713C002091	47B2EFBC3670E7DB4B41F22C51FC02EE84FB2DBF3082A49F2C2688122E9210A1
2	emSign Class 1 CA - G1	00D59B7C9B36A2D44922EA	CF6D0333D0BE2C69A42D453960DEE9E109D9E8843EA3061A1671D6EAF85EB7D8
3	emSign Class 2 CA - G1	3C5BDA55C0A236A744CD	63A8369DC824A42BC7AE6EE5D26AAFD32DF4AF677CA18B941B7A57E33B1E3559
4	emSign Class 3 CA - G1	00A08870825A326BED9611	42DA1C562F80E46DA7A321244EFC23D0FAA9FEBBB7AA0377D96B42D9E88AB200

No.	Common Name	Certificate Serial No.	SHA-256 Fingerprint
5	emSign Device CA - G1	0465835247364A904A8E	4C9198B673550858799AD2744CC083C1BA0027E77D3B8FD6D56CF53620D099E2
6	emSign ECC SSL CA - G3	72DDC7E9DCE9B0DCFFC7	6B51D1DCF4EB7AEE424185CB1B9580574B39CB963863DE3EC1AD31DDB076CE9F
7	emSign ECC Class 1 CA - G3	00FB1E21982EB1B55C5925	ABA6A65DCE8955BAF0685AB88809B7699C174496EF9EE991533251494F43CE10
8	emSign ECC Class 2 CA - G3	23E1BA02DFF3E900EDDD	4E9B731567177E1776A96D66D9120B3DEB28B800937EA4662565B3EF5EC8000B
9	emSign ECC Class 3 CA - G3	00B8EB258324DB08ACC2F5	7066A0F42F530E0DB5AFEE72A3B04DE614E7D2305C67D12C756BB215E37CB975
10	emSign ECC Device CA - G3	00876282A8FD758C391EC3	70B9BA595412CF8614B76747FD683CCA2759F42642164834FBEFDD88505C4F1C
11	emSign SSL CA - C1	0086766B7F96DF60C46F8B	F91AACA0E4E533747A0880BFCF6F26720DC1D05494C3938DA6802290D5A09B32
12	emSign Class 1 CA - C1	7E065336C075C7998B63	0EF7B863FAABC384A694FF632DAAF9BD31CED23E9246559A59ECD7472754CCE6
13	emSign Class 2 CA - C1	1A5C82DEDCBC6A153030	05B30B3FC44F8575334BD812EF9FA8A52A75743E19BC35A5BE3912ECA62C4669
14	emSign Class 3 CA - C1	00B474F64D86392189496E	69B0DD09B98F36A9CC7BD7FFE8A00DCD319A5FC947C9C8AF72C92894D8E81092
15	emSign Device CA - C1	00B19BE3081E2D97B5BFCB	D034B18751BEE10AAAF94C2F14350D3F654E5B934D0DDA592B31E58187A48952
16	emSign ECC SSL CA - C3	5B7D9BB1FD33B9BC1D84	A061D445399714C38FC101A6E9AFBDB381F112FA5DE7D5BC14904558D1ED3276
17	emSign ECC Class 1 CA - C3	00BD6A0796AB3F8955521E	FAD2E98649F1C606150F55269EBC035AEA22FFAC131DE64BA6900C75D8447B7E
18	emSign ECC Class 2 CA - C3	00D1142766698BFCDEDA02	DB4591F878F6672F5B70733A66AD7C9537B97E6F0AF5CA49AAB8ECB2CE02F86B
19	emSign ECC Class 3 CA - C3	3D12A1CF78258D580854	5A9A03F2D3FE589BE63CDA11820A9F25F074C92034F51C047D34226D252EC025
20	emSign ECC Device CA - C3	00D9365F15842A1D0689C3	3D4511D0A80AA949A6D99B253A173471797C4459187A6329E736C37CB5493E46

Appendix B – Certification Practice Statements in Scope

Certification Practice Statement	Begin Effective Date	End Effective Date
Version 1.12	26 September 2022	15 August 2023
Version 1.13	16 August 2023	29 August 2023
Version 1.14	30 August 2023	16 June 2024
Version 1.15	17 June 2024	-

EMSIGN PKI MANAGEMENT'S ASSERTION

eMudhra Technologies Limited ("emSign PKI") operates the Certification Authority (CA) services known as enumerated in Appendix A(i), and provides Extended Validation SSL ("EV SSL") CA services.

The management of emSign PKI is responsible for establishing and maintaining effective controls over its EV SSL CA operations including its EV SSL CA business practices disclosure in its repository, EV SSL key lifecycle management controls, and EV 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 emSign PKI's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

emSign PKI management has assessed its disclosures of its certificate practices and controls over its EV SSL CA services. Based on that assessment, in emSign PKI management's opinion, in providing its EV SSL Certification Authority (CA) services at Bangalore and Chennai, India, throughout the period 01 June 2023 to 31 May 2024, emSign PKI has:

- disclosed its extended validation SSL ("EV SSL") certificate lifecycle management business practices in applicable versions of its Certification Practice Statements as enumerated in Appendix B, including its commitment to provide EV SSL certificates in conformity with the CA/Browser Forum Guidelines on the emSign PKI 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 emSign PKI)

in accordance with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL V1.8.

The CAs enumerated in Appendix A(ii) are not used for EV SSL certificate services although technically capable of such issuance. The management has put in place internal controls to prevent EV SSL issuance under these CAs.

Venu Madhava

Signed by Venu Madhava
Date: 2024.08.19
12:02:36

Venu Madhava
Executive Vice President - Legal, HR and GRC
19 August 2024

Appendix A(i) – List of Root and Subordinate CAs in Scope

No	Common Name	Certificate Serial No	SHA-256 Fingerprint
1	**emSign Root CA - G1**	31F5E4620C6C58EDD6D8	40F6AF0346A99AA1CD1D555A4E9CCE62C7F9634603EE406615833DC8C8D00367
2	emSign EV SSL CA - G1	626CB92B237FF82E3F50	4334EEB2CC114F82BEE6F8A7E5AEA03A42EB2E1F70CBD66102E414D72F0033B9
3	**emSign ECC Root CA - G3**	3CF607A968700EDA8B84	86A1ECBA089C4A8D3BBE2734C612BA341D813E043CF9E8A862CD5C57A36BBE6B
4	emSign ECC EV SSL CA - G3	01FE3E6C68DEBBEC263E	0116F17F97CDEF4ADE2E63CF2C1B064FD99F404D2B914100BC241F0781853323
5	**emSign Root CA - C1**	00AECF00BAC4CF32F843B2	125609AA301DA0A249B97A8239CB6A34216F44DCAC9F3954B14292F2E8C8608F
6	emSign EV SSL CA - C1	00BADFD29B3F1E678C6960	F6F159286A1401DE5397E21A0090534A85F5E7B9F98FD4A5A47B1DFFD4BFDED4
7	**emSign ECC Root CA - C3**	7B71B68256B8127C9CA8	BC4D809B15189D78DB3E1D8CF4F9726A795DA1643CA5F1358E1DDB0EDC0D7EB3
8	emSign ECC EV SSL CA - C3	1B50581F7334B30B2723	C0A578F2109E6F42D3D939948DEEAB729B20F7B23B4237ABD8494DF554CF985C
9	**emSign Root TLS CA - G1**	02A27D4E346AEF4E4F04678B5BB6D9EE	CEF71E70B7C29ADDF6C30CD19E614B38FD5F02A435A0EEDDD0087E183D101A51
10	**emSign Root TLS CA - G3**	0E760672F143459FC8FE0AB0BC05E394	7DD78D5F4F13459A83DFF9ABBBA62EDBAF6F2D102BF257FD712F4D9F2746ED8D

Appendix A(ii) - List of Subordinate CAs in Scope

No	Common Name	Certificate Serial No	SHA-256 Fingerprint
1	emSign SSL CA - G1	217AD58B1C713C002091	47B2EFBC3670E7DB4B41F22C51FC02EE84FB2DBF3082A49F2C2688122E9210A1
2	emSign Class 1 CA - G1	00D59B7C9B36A2D44922EA	CF6D0333D0BE2C69A42D453960DEE9E109D9E8843EA3061A1671D6EAF85EB7D8
3	emSign Class 2 CA - G1	3C5BDA55C0A236A744CD	63A8369DC824A42BC7AE6EE5D26AAFD32DF4AF677CA18B941B7A57E33B1E3559
4	emSign Class 3 CA - G1	00A08870825A326BED9611	42DA1C562F80E46DA7A321244EFC23D0FAA9FEBBB7AA0377D96B42D9E88AB200
5	emSign Device CA - G1	0465835247364A904A8E	4C9198B673550858799AD2744CC083C1BA0027E77D3B8FD6D56CF53620D099E2
6	emSign ECC SSL CA - G3	72DDC7E9DCE9B0DCFFC7	6B51D1DCF4EB7AEE424185CB1B9580574B39CB963863DE3EC1AD31DDB076CE9F
7	emSign ECC Class 1 CA - G3	00FB1E21982EB1B55C5925	ABA6A65DCE8955BAF0685AB88809B7699C174496EF9EE991533251494F43CE10
8	emSign ECC Class 2 CA - G3	23E1BA02DFF3E900EDDD	4E9B731567177E1776A96D66D9120B3DEB28B800937EA4662565B3EF5EC8000B
9	emSign ECC Class 3 CA - G3	00B8EB258324DB08ACC2F5	7066A0F42F530E0DB5AFEE72A3B04DE614E7D2305C67D12C756BB215E37CB975
10	emSign ECC Device CA - G3	00876282A8FD758C391EC3	70B9BA595412CF8614B76747FD683CCA2759F42642164834FBEFDD88505C4F1C

No	Common Name	Certificate Serial No	SHA-256 Fingerprint
11	emSign SSL CA - C1	0086766B7F96DF60C46F8B	F91AACA0E4E533747A0880BFCF6F26720DC1D05494C3938DA6802290D5A09B32
12	emSign Class 1 CA - C1	7E065336C075C7998B63	0EF7B863FAABC384A694FF632DAAF9BD31CED23E9246559A59ECD7472754CCE6
13	emSign Class 2 CA - C1	1A5C82DEDCBC6A153030	05B30B3FC44F8575334BD812EF9FA8A52A75743E19BC35A5BE3912ECA62C4669
14	emSign Class 3 CA - C1	00B474F64D86392189496E	69B0DD09B98F36A9CC7BD7FFE8A00DCD319A5FC947C9C8AF72C92894D8E81092
15	emSign Device CA - C1	00B19BE3081E2D97B5BFCB	D034B18751BEE10AAAF94C2F14350D3F654E5B934D0DDA592B31E58187A48952
16	emSign ECC SSL CA - C3	5B7D9BB1FD33B9BC1D84	A061D445399714C38FC101A6E9AFBDB381F112FA5DE7D5BC14904558D1ED3276
17	emSign ECC Class 1 CA - C3	00BD6A0796AB3F8955521E	FAD2E98649F1C606150F55269EBC035AEA22FFAC131DE64BA6900C75D8447B7E
18	emSign ECC Class 2 CA - C3	00D1142766698BFCDEDA02	DB4591F878F6672F5B70733A66AD7C9537B97E6F0AF5CA49AAB8ECB2CE02F86B
19	emSign ECC Class 3 CA - C3	3D12A1CF78258D580854	5A9A03F2D3FE589BE63CDA11820A9F25F074C92034F51C047D34226D252EC025
20	emSign ECC Device CA - C3	00D9365F15842A1D0689C3	3D4511D0A80AA949A6D99B253A173471797C4459187A6329E736C37CB5493E46

Appendix B - Certification Practice Statements in Scope

Certification Practice Statement	Begin Effective Date	End Effective Date
Version 1.12	26 September 2022	15 August 2023
Version 1.13	16 August 2023	29 August 2023
Version 1.14	30 August 2023	16 June 2024
Version 1.15	17 June 2024	-