Tel: +603 2616 2888
Fax: +603 2616 3190
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 a reasonable assurance engagement, to report on emSign PKI management's assertion that for its Certification Authority (CA) operations at the locations enumerated in Appendix A throughout the period 1 June 2025 to 31 May 2026 for its CAs as enumerated in Appendix B(i), emSign PKI has:

- disclosed its extended validation TLS ("EV TLS") certificate lifecycle management business practices in applicable versions of its Certification Practice Statements in Appendix C, including its commitment to provide EV TLS 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 TLS certificates it manages is established and protected throughout their lifecycles; and
  - EV TLS 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 TLS v2.0.1.

The CAs enumerated in Appendix B(ii) did not issue any EV TLS certificates for the audit period.

Certification authority's responsibilities

emSign PKI'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 TLS v2.0.1.

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.

BDO PLT (201906000013 [LLP0018825-LCA & AF 0206]), Chartered Accountants, a Limited Liability Partnership, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms.

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 TLS certificate lifecycle management business practices, including its relevant controls over the issuance, renewal and revocation of EV TLS certificates;
(2) selectively testing transactions executed in accordance with disclosed EV TLS 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 2025 to 31 May 2026, 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 TLS v2.0.1.

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 TLS v2.0.1, nor the suitability of any of emSign PKI's services for any customer's intended purpose.

Other Matter

Without modifying our opinion, we noted the following other matters during our procedures and have considered the nature of these matters in our risk assessment and in determining the nature, timing, and extent of our procedures. This included performing procedures to understand the root cause disclosed by the CA, and if facts and circumstances noted in our examination agreed with what has been disclosed. We have also considered the procedures the CA has designed and noted if implemented properly and operated effectively, the controls would address the root cause. We did not perform any procedures subsequent to this report as to the effectiveness of the controls implemented.

Matter Topic		Matter Description
1.	Certificate Problem Report Handling	eMudhra disclosed in Mozilla Bug #1970727 that Certificate Problem Reports were not responded to within the required 24-hour timeframe.
2.	Certificate Status Validation / CRL Integrity	eMudhra disclosed in Mozilla Bug #1970728 that CRLs for six newly created TLS Intermediate CAs were signed using an incorrect CA key configuration, resulting in invalid CRL signatures. No end-entity certificates had been issued under the affected Intermediate CAs.
3.	Policy Document Governance	eMudhra disclosed in Mozilla Bug #1973341 that certificates were issued with RSA key sizes greater than 2048 bits, while its CP/CPS end-entity certificate profile only referenced "RSA 2048".
4.	Dual-Purpose Root Transition / Trust Separation	eMudhra disclosed in Mozilla Bug #2018979 its transition plan for existing dual-purpose root certificates in accordance with MRSP §7.5.3.

While the emSign PKI assertion notes all issues disclosed on Bugzilla from 1 June 2025 through the date of this report, we have only noted those instances relevant to the CAs enumerated in Appendix B(i) and Appendix B(ii) and applicable to the WebTrust Principles and Criteria for Certification Authorities – Extended Validation TLS v2.0.1.

Use of the WebTrust seal

emSign PKI's use of the WebTrust for Certification Authorities – Extended Validation TLS 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
201906000013 (LLP0018825-LCA) & AF 0206
Chartered Accountants

Kuala Lumpur, Malaysia
6 August 2026

APPENDIX A – LIST OF LOCATIONS IN SCOPE

Location Name	Location Type	Location	In-Scope for Physical and Environmental Control Testing
eMudhra Digital Campus	Main Office	Bangalore, India	No
Offline key storage 1	Data Centre 1	Bangalore, India	Yes
Offline key storage 2	Data Centre 2	Chennai, India	Yes
Online CA hosting 1	Data Centre 1	Bangalore, India	Yes
Online CA hosting 2	Data Centre 2	Chennai, India	Yes
Online CA hosting 3	Data Centre 3	Utah, United States	Yes
Online CA hosting 4	Data Centre 4	New Jersey, United States	Yes
MPIC Servers	AWS	Mumbai, Asia Pacific	No
MPIC Servers	AWS	N. Virginia, United States	No
MPIC Servers	AWS	Frankfurt, Europe	No
MPIC Servers	AWS	N. California, United States	No
MPIC Servers	AWS	Sao Paulo, South America	No
MPIC Servers	AWS	Singapore, Asia Pacific	No

APPENDIX B(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 Root TLS CA - G1	00F7AB65559E10812DF6484347586A25	9B913476EAB476E21E0887DBCDE44345D1359D28116B83B7CD3E87BD807EBF68
4*	**emSign ECC Root CA - G3**	3CF607A968700EDA8B84	86A1ECBA089C4A8D3BBE2734C612BA341D813E043CF9E8A862CD5C57A36BBE6B
5	emSign ECC EV SSL CA - G3	01FE3E6C68DEBBEC263E	0116F17F97CDEF4ADE2E63CF2C1B064FD99F404D2B914100BC241F0781853323
6	emSign Root TLS CA - G3	00961A3EFB1359576ED04005B4684A5B	3094025792039A68AF6E553686410BDAB7C0D4A36B9084CBA64202E35D6EBBDD
7*	**emSign Root CA - C1**	00AECF00BAC4CF32F843B2	125609AA301DA0A249B97A8239CB6A34216F44DCAC9F3954B14292F2E8C8608F
8	emSign EV SSL CA - C1	00BADFD29B3F1E678C6960	F6F159286A1401DE5397E21A0090534A85F5E7B9F98FD4A5A47B1DFFD4BFDED4
9*	**emSign ECC Root CA - C3**	7B71B68256B8127C9CA8	BC4D809B15189D78DB3E1D8CF4F9726A795DA1643CA5F1358E1DDB0EDC0D7EB3
10	emSign ECC EV SSL CA - C3	1B50581F7334B30B2723	C0A578F2109E6F42D3D939948DEEAB729B20F7B23B4237ABD8494DF554CF985C
11*	**emSign Root TLS CA - G1**	02A27D4E346AEF4E4F04678B5BB6D9EE	CEF71E70B7C29ADDF6C30CD19E614B38FD5F02A435A0EEDDD0087E183D101A51
12	emSign TLS CA - G1	437E0DB6D4E846134D00AD35463A7D	DE029E40F6BB851DA4B804C65121D8535084FDF6B3B47DDF7E94B4E46A6C3437
13	EM EV TLS CA - G2A-1	35ACF2A0E598C8E849D5EE7E724C82	684B11E56AB72502B75DACA1CD009E3DD4BEAB3AC1FE448902D272766CCA797E
14	EM EV TLS CA - G2B	008F06A3F1D6A2FC71D29393C71CD48E	E072B30D7F5B8BCF0080E51D6CC7765767072DB2319E9BB1CD3D02A086898750
15	EM EV TLS CA - G2C	00B28103309375C0CBB9E9B80B66C430	C3BC2B480FB1A1AB4D0BA1ED6C7B53E09644704573362 0991A32D6798D77AA20
16	InCommon Intermediate CA - EVG2C	0E9098B1015D2FDA128A5342BDB088	A83559D892F4692DA9A088A1B759773015D7AA6FB2B50B18C5F9F89CC27631E1

No.	Common Name	Certificate Serial No.	SHA-256 Fingerprint
17*	**emSign Root TLS CA - G3**	0E760672F143459FC8FE0AB0BC05E394	7DD78D5F4F13459A83DFF9ABBBA62EDBAF6F2D102BF257FD712F4D9F2746ED8D
18	emSign TLS CA - G3	3B6ECEC869F677EFF33445C0E3EDC5	04E6DEA261B8720E0525E9DA23282100352BDEBC119CFC3DBD812C3D68A2BCDD
19	EM EV TLS CA - G3A-1	00B28971D9989A629CA9B4E206067211	BA0A3DA706F47DAC1A9C33C4EE1E4D86B726EF48E70D4319F3C949EC673A1975
20	EM EV TLS CA - G3B	00C7C41EFE92D825F05EAE841A4A82C1	E7568FE6E12331F4FD7DE61DA4C7559D0F8EB192A218D4741A3BA75184333838
21	EM EV TLS CA - G3C	008009928A64107601AF05FA2F19F109	432EC25F0D28DE9006D97BF752F17BBB2CD41F669933FCB072D9A1148D0261F3
22	InCommon Intermediate CA - EVG3C	00C61D1CF77FA6D4C88875A43BEB4AE4	5F2F050F9CDD928FE50102244733CBA7EA72204D9A7686949CE59E402AD1AAB9

Reflects Root CA certificates

LIST OF CROSS SIGNED CAs:

No.	Common Name	Certificate Serial No.	SHA-256 Fingerprint
1	EM EV TLS CA - G2A-1	46057D09344E92BB7064D4C7219F3C2D	A57FACB931C9A20376E6FE212F7234EFF7B8811436A421BEFF26F5DEA9BCC4F1
2	EM EV TLS CA - G2B	00E84B4F5D5B7BEDF7C770DAA72EE04732	43785B01437218B8D57C2A5B5979976ECAF06B35A710A5CA4BB3C0C1BA65A078
3	EM EV TLS CA - G2C	00EDE78290C6A3193FCEA950E66DF34D20	0307BC756AAEA5398BF3B47D433D2BCB83470F7FEA640753877ADEFD910E8BF3
4	EM EV TLS CA - G3A-1	00AABA43C0D684BA96FE14CE7397A4EE35	D62657961AC9C5A9A522549E34CADE585ECBFD3869A780C97EDF52E0EC90CEFC
5	EM EV TLS CA - G3B	00D8F8685E4F2BD9D82402A85A1C1EB731	579480AEA166290BD3C643589E795FC0D0E54E86505D180F1DFF99EFD3199512
6	EM EV TLS CA - G3C	05F078752DECE7A1BB8595D303167171	FD9D5C2DBBD4995AB69B8D50C439D9527B00529199C2FD01B2174EB58F07021F

APPENDIX B(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

No.	Common Name	Certificate Serial No.	SHA-256 Fingerprint
3	emSign Class 2 CA - G1	3C5BDA55C0A236A744CD	63A8369DC824A42BC7AE6E E5D26AAFD32DF4AF677CA 18B941B7A57E33B1E3559
4	emSign Class 3 CA - G1	00A08870825A326BED9611	42DA1C562F80E46DA7A321 244EFC23D0FAA9FEBBB7A A0377D96B42D9E88AB200
5	emSign Device CA - G1	0465835247364A904A8E	4C9198B673550858799AD2 744CC083C1BA0027E77D3B 8FD6D56CF53620D099E2
6	emSign ECC SSL CA - G3	72DDC7E9DCE9B0DCFFC7	6B51D1DCF4EB7AEE424185 CB1B9580574B39CB963863 DE3EC1AD31DDB076CE9F
7	emSign ECC Class 1 CA - G3	00FB1E21982EB1B55C5925	ABA6A65DCE8955BAF0685 AB88809B7699C174496EF9 EE991533251494F43CE10
8	emSign ECC Class 2 CA - G3	23E1BA02DFF3E900EDDD	4E9B731567177E1776A96D 66D9120B3DEB28B800937E A4662565B3EF5EC8000B
9	emSign ECC Class 3 CA - G3	00B8EB258324DB08ACC2F5	7066A0F42F530E0DB5AFEE 72A3B04DE614E7D2305C67 D12C756BB215E37CB975
10	emSign ECC Device CA - G3	00876282A8FD758C391EC3	70B9BA595412CF8614B767 47FD683CCA2759F4264216 4834FBEFDD88505C4F1C
11	emSign SSL CA - C1	0086766B7F96DF60C46F8B	F91AACA0E4E533747A0880 BFCF6F26720DC1D05494C3 938DA6802290D5A09B32
12	emSign Class 1 CA - C1	7E065336C075C7998B63	0EF7B863FAABC384A694FF 632DAAF9BD31CED23E9246 559A59ECD7472754CCE6
13	emSign Class 2 CA - C1	1A5C82DEDCBC6A153030	05B30B3FC44F8575334BD8 12EF9FA8A52A75743E19BC 35A5BE3912ECA62C4669
14	emSign Class 3 CA - C1	00B474F64D86392189496E	69B0DD09B98F36A9CC7BD 7FFE8A00DCD319A5FC947C 9C8AF72C92894D8E81092
15	emSign Device CA - C1	00B19BE3081E2D97B5BFCB	D034B18751BEE10AAAF94C 2F14350D3F654E5B934D0D DA592B31E58187A48952
16	emSign ECC SSL CA - C3	5B7D9BB1FD33B9BC1D84	A061D445399714C38FC101 A6E9AFBDB381F112FA5DE7 D5BC14904558D1ED3276
17	emSign ECC Class 1 CA - C3	00BD6A0796AB3F8955521E	FAD2E98649F1C606150F55 269EBC035AEA22FFAC131D E64BA6900C75D8447B7E
18	emSign ECC Class 2 CA - C3	00D1142766698BFCDEDA02	DB4591F878F6672F5B7073 3A66AD7C9537B97E6F0AF5 CA49AAB8ECB2CE02F86B
19	emSign ECC Class 3 CA - C3	3D12A1CF78258D580854	5A9A03F2D3FE589BE63CDA 11820A9F25F074C92034F5 1C047D34226D252EC025

No.	Common Name	Certificate Serial No.	SHA-256 Fingerprint
20	emSign ECC Device CA - C3	00D9365F15842A1D0689C3	3D4511D0A80AA949A6D99B253A173471797C4459187A6329E736C37CB5493E46
21	EM DV TLS CA - G2A-1	00B6391A6D28C7886AE6FCCED2F3C1A7	3F13597D3355D341BD09328AEE567D7F4E002D9919B986F9962DAFF197EA75D1
22	EM DV TLS CA - G2B	00F0A030825E22BB2E1D88E3889DC073	829EC444B8BE3DFD2D030A0D9E7A1D0DD2A3C2C325D39589C27AC9A065BAE793
23	EM DV TLS CA - G2C	00AB5DEA38BDC920D5FA4736DA54BEBE	0427EA3CB4A7B4CB205E77A7B166D332BEDB8E8EF469BC5E883169C8D0AC876D
24	EM OV TLS CA - G2A-1	59491409E797EA968F05E0FF331FEC	291804EC866837CD5AF5F4D652F1DCC79BEC622D4F9BF4870E5E4D8639DF3AD4
25	EM OV TLS CA - G2B	00C164DB9804F563241ED32C4100A566	6A7A93861982B664001710A0EFD04C8A72F6A23E252B280911797E0BF1BD9012
26	EM OV TLS CA - G2C	00CBDCFA0D64112709CF14B7E4858250	DE767792E870BD32F331029FC89DC24C53F9DF970DC70F1EA30CF29DB3F94BA9
27	EM DV TLS CA - G3A-1	00A3E5AD9D0C0374A342E5E2A3F506DD	4896D51F6537A5326272C412BC75990E15D4F5ECDC2946C19776923B8E169E93
28	EM DV TLS CA - G3B	00A4AEE678F23362B4C0E460B772F214	42C4ACCD12C4F59597925E1A08A7A90102608543809308D50EC427E118BA1493
29	EM DV TLS CA - G3C	588B2E3C2BB8CDA13E1A1209254321	0164D7CEAE5BB909C272AF151FF44B1177AE9B47D9424B94F1D9558C30934D19
30	EM OV TLS CA - G3A-1	00C5FB5F2D43071F5B5623B5D132878C	259FF0963A0665BF40D92E05E95B960CCB423DBD117482AE647BC7FD5F5CE644
31	EM OV TLS CA - G3B	6CADA367FB1C100088120EA202D568	98B896625C0C230ADEEC3EB2CF6AAD5001ECF9156A68644E82374CE5833BC25B
32	EM OV TLS CA - G3C	296926C227A3A1526392B19482A504	CB6E15165AC802E9B3F993F16C25D41F4E81C21EBDE71AE1B012AC00BF9C7C3F

LIST OF CROSS SIGNED CAs:

No.	Common Name	Certificate Serial No.	SHA-256 Fingerprint
1	EM DV TLS CA - G2A-1	45D2438F4CAE023D3D78A052A5A9DB94	122A5433D8A2A8C501D5E680AB216885A6019326A189DF91E8895F8B5AD488DD
2	EM DV TLS CA - G2B	6D3091E911E878BA6E196CC2A186FF01	5F0D6380B345D409C641D089B081D7B43B365FD414394403301671C3CBC6A3E5
3	EM DV TLS CA - G2C	00DF5AD8718C74A3CFEE80D5B5FB94AE03	8FE4701D088C2250317BB3A77EDC1707E38E1112E8A334F615CFA9D46F175B04

No.	Common Name	Certificate Serial No.	SHA-256 Fingerprint
4	EM DV TLS CA - G3A-1	00FBF771754D6A8760263B3E115432593F	ECB8D30846BEF4B340C90152659F452FD81A7A4F41429B890F1E2B3467058565
5	EM DV TLS CA - G3B	00A024FDF4BA665C785CE4A020483858B7	45A883F349AEDFD5F3A649B5498FFB121712BA8B448F3F2A91DBC5A766FCDDBE
6	EM DV TLS CA - G3C	0091F347F1A5B7D39962B95E0EE4E299D1	62B7F9868263F72F6911FC78CEAF72C1979158B7368BF648683BB2AA39B02E72
7	EM OV TLS CA - G2A-1	49CA1A0221C19698975E1EC6F4EDA4D1	E0DA30FF7384B9873EDE9FB2DBA7F1353C7E60ED59BB9A43779F9E8494A47BAC
8	EM OV TLS CA - G2B	2923D7603B9D92DEDD54733C594811DA	121C42490FECA63B63E7D068046CC4C5FC58436BF71C97283746F37A9DD67799
9	EM OV TLS CA - G2C	119AF942CF007231271F37B0CDAE9928	ED82135F7D946673F8298BF758DC830BAD20FB37F5BB9EAC52B236563FEC931E
10	EM OV TLS CA - G3A-1	00ADA1791F3D515E1A4080D208AE888A01	1159D471B5746802C2F2CB2FFFE6D5C332B9319BD52ACEBFA93AEC07544E7C5D
11	EM OV TLS CA - G3B	00E94223BDE92F914E5AB9ACABFDAC3710	5F1DED4DD590AF74631290CF073B122A2AAC6A1FA479778A0BD43579BD832699
12	EM OV TLS CA - G3C	008D5A4811939EF447D77111CDD9849AE9	7485B51C0ED192878FA1D2F948FB529AE1842CC5086C4B67F7BE5B2039DE9489

APPENDIX C – CERTIFICATION PRACTICE STATEMENTS IN SCOPE

CERTIFICATION PRACTICE STATEMENT (CP/CPS) FOR SSL/TLS

Certification Practice Statement	Begin Effective Date	End Effective Date
Version 1.00	19 August 2025	8 September 2025
Version 1.01	9 September 2025	18 November 2025
Version 1.02	19 November 2025	27 November 2025
Version 1.03	28 November 2025	1 April 2026
Version 1.04	2 April 2026	20 April 2026
Version 1.05	21 April 2026	9 July 2026
Version 1.06	10 July 2026	-

CERTIFICATION PRACTICE STATEMENT (CP/CPS) FOR INCOMMON CA TLS

Certification Practice Statement	Begin Effective Date	End Effective Date
Version 1.04	8 April 2026	20 April 2026
Version 1.05	21 April 2026	9 July 2026
Version 1.06	10 July 2026	-

EMSIGN PKI'S MANAGEMENT ASSERTION

eMudhra Technologies Limited ("emSign PKI") operates the Certification Authority (CA) services enumerated in **Appendix B(i)**, and provides Extended Validation TLS ("EV TLS") CA services.

The management of emSign PKI is responsible for establishing and maintaining effective controls over its EV TLS CA operations, including its EV TLS CA business practices disclosure in its repository, EV TLS key lifecycle management controls, and EV TLS 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 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 TLS CA services. Based on that assessment, in emSign PKI management's opinion, in providing its EV TLS Certification Authority (CA) services at the locations enumerated in **Appendix A**, throughout the period 01 June 2025 to 31 May 2026, emSign PKI has:

- disclosed its extended validation TLS ("EV TLS") certificate lifecycle management business practices in applicable versions of its Certification Practice Statements as enumerated in **Appendix C**, including its commitment to provide EV TLS 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 TLS certificates it manages is established and protected throughout their lifecycles; and
  - EV TLS 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 TLS v2.0.1.

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

emSign PKI has disclosed the following matters publicly Mozilla's Bugzilla platform. These matters were included below due to being open during the period 01 June 2025 through the date of this report.

Bug ID	Summary	Opened	Closed	Resolution
#1965559	eMudhra: Delayed Publication of Issuing CA Certificates In CCADB	09/05/2025	01/07/2025	Fixed
#1970727	eMudhra: Failure to respond to a Problem Report within 24 hours	05/06/2025	16/07/2025	Fixed
#1970728	eMudhra: Invalid CRL signatures	05/06/2025	16/07/2025	Fixed
#1973341	eMudhra emSign PKI Services: Policy Document Inconsistency	21/06/2025	19/08/2025	Fixed
#1974435	eMudhra emSign PKI Services: Delayed Revocation of TLS Certificates due to Policy Inconsistency	27/06/2025	19/08/2025	Fixed
#1999241	eMudhra emSign PKI Services: Delayed Publication of Issuing CA Certificates in CCADB	10/11/2025	24/12/2025	Fixed
#2007297	eMudhra emSign PKI Services: CRL URL Mismatch Between CCADB Disclosure and Issued Certificates	21/12/2025	23/02/2026	Fixed
#2048995	eMudhra emSign PKI Services: OCSP Responder Returned "Unauthorized" for Some Pecertificates	19/06/2026	30/07/2026	Fixed
#2018979	eMudhra: Transition Plan for Existing Dual-Purpose Roots	24/02/2026	-	Open
#2043837	eMudhra emSign PKI Services: www Subdomain Inclusion in Certificate SAN via ACME Issuance Workflow	30/05/2026	-	Open

Venu Madhava

Signed by Venu Madhava
Date: 2026.08.06 10:33:15

Venu Madhava,

Director.

06 August 2026

APPENDIX A – LIST OF LOCATIONS IN SCOPE

Location Name	Location Type	Location	In-Scope for Physical and Environmental Control Testing
eMudhra Digital Campus	Main Office	Bangalore, India	No
Offline key storage 1	Data Centre 1	Bangalore, India	Yes
Offline key storage 2	Data Centre 2	Chennai, India	Yes
Online CA hosting 1	Data Centre 1	Bangalore, India	Yes
Online CA hosting 2	Data Centre 2	Chennai, India	Yes
Online CA hosting 3	Data Centre 3	Utah, United States	Yes
Online CA hosting 4	Data Centre 4	New Jersey, United States	Yes
MPIC Servers	AWS	Mumbai, Asia Pacific	No
MPIC Servers	AWS	N. Virginia, United States	No
MPIC Servers	AWS	Frankfurt, Europe	No
MPIC Servers	AWS	N. California, United States	No
MPIC Servers	AWS	Sao Paulo, South America	No
MPIC Servers	AWS	Singapore, Asia Pacific	No

APPENDIX B(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 Root TLS CA - G1	00F7AB65559E10812DF6484347586A25	9B913476EAB476E21E0887DBCDE44345D1359D28116B83B7CD3E87BD807EBF68
4*	**emSign ECC Root CA - G3**	3CF607A968700EDA8B84	86A1ECBA089C4A8D3BBE2734C612BA341D813E043CF9E8A862CD5C57A36BBE6B
5	emSign ECC EV SSL CA - G3	01FE3E6C68DEBBEC263E	0116F17F97CDEF4ADE2E63CF2C1B064FD99F404D2B914100BC241F0781853323
6	emSign Root TLS CA - G3	00961A3EFB1359576ED04005B4684A5B	3094025792039A68AF6E553686410BDAB7C0D4A36B9084CBA64202E35D6EBBDD
7*	**emSign Root CA - C1**	00AECF00BAC4CF32F843B2	125609AA301DA0A249B97A8239CB6A34216F44DCAC9F3954B14292F2E8C8608F
8	emSign EV SSL CA - C1	00BADFD29B3F1E678C6960	F6F159286A1401DE5397E21A0090534A85F5E7B9F98FD4A5A47B1DFFD4BFDED4
9*	**emSign ECC Root CA - C3**	7B71B68256B8127C9CA8	BC4D809B15189D78DB3E1D8CF4F9726A795DA1643CA5F1358E1DDB0EDC0D7EB3
10	emSign ECC EV SSL CA - C3	1B50581F7334B30B2723	C0A578F2109E6F42D3D939948DEEAB729B20F7B23B4237ABD8494DF554CF985C
11*	**emSign Root TLS CA - G1**	02A27D4E346AEF4E4F04678B5BB6D9EE	CEF71E70B7C29ADDF6C30CD19E614B38FD5F02A435A0EEDDD0087E183D101A51
12	emSign TLS CA - G1	437E0DB6D4E846134D00AD35463A7D	DE029E40F6BB851DA4B804C65121D8535084FDF6B3B47DDF7E94B4E46A6C3437
13	EM EV TLS CA - G2A-1	35ACF2A0E598C8E849D5EE7E724C82	684B11E56AB72502B75DACA1CD009E3DD4BEAB3AC1FE448902D272766CCA797E
14	EM EV TLS CA - G2B	008F06A3F1D6A2FC71D29393C71CD48E	E072B30D7F5B8BCF0080E51D6CC7765767072DB2319E9BB1CD3D02A086898750
15	EM EV TLS CA - G2C	00B28103309375C0CBB9E9B80B66C430	C3BC2B480FB1A1AB4D0BA1ED6C7B53E09644704573362099 1A32D6798D77AA20
16	InCommon Intermediate CA - EVG2C	0E9098B1015D2FDA128A5342BDB088	A83559D892F4692DA9A088A1B759773015D7AA6FB2B50B18C5F9F89CC27631E1
17*	**emSign Root TLS CA - G3**	0E760672F143459FC8FE0AB0BC05E394	7DD78D5F4F13459A83DFF9ABBBA62EDBAF6F2D102BF257FD712F4D9F2746ED8D

No	Common Name	Certificate Serial No.	SHA-256 Fingerprint
18	emSign TLS CA - G3	3B6ECEC869F677EFF33445C0E3EDC5	04E6DEA261B8720E0525E9DA23282100352BDEBC119CFC3DBD812C3D68A2BCDD
19	EM EV TLS CA - G3A-1	00B28971D9989A629CA9B4E206067211	BA0A3DA706F47DAC1A9C33C4EE1E4D86B726EF48E70D4319F3C949EC673A1975
20	EM EV TLS CA - G3B	00C7C41EFE92D825F05EAE841A4A82C1	E7568FE6E12331F4FD7DE61DA4C7559D0F8EB192A218D4741A3BA75184333838
21	EM EV TLS CA - G3C	008009928A64107601AF05FA2F19F109	432EC25F0D28DE9006D97BF752F17BBB2CD41F669933FCB072D9A1148D0261F3
22	InCommon Intermediate CA - EVG3C	00C61D1CF77FA6D4C88875A43BEB4AE4	5F2F050F9CDD928FE50102244733CBA7EA72204D9A7686949CE59E402AD1AAB9

Reflects Root CA certificates

LIST OF CROSS SIGNED CAs:

No	Common Name	Certificate Serial No.	SHA-256 Fingerprint
1	EM EV TLS CA - G2A-1	46057D09344E92BB7064D4C7219F3C2D	A57FACB931C9A20376E6FE212F7234EFF7B8811436A421BEFF26F5DEA9BCC4F1
2	EM EV TLS CA - G2B	00E84B4F5D5B7BEDF7C770DAA72EE04732	43785B01437218B8D57C2A5B5979976ECAF06B35A710A5CA4BB3C0C1BA65A078
3	EM EV TLS CA - G2C	00EDE78290C6A3193FCEA950E66DF34D20	0307BC756AAEA5398BF3B47D433D2BCB83470F7FEA640753877ADEFD910E8BF3
4	EM EV TLS CA - G3A-1	00AABA43C0D684BA96FE14CE7397A4EE35	D62657961AC9C5A9A522549E34CADE585ECBFD3869A780C97EDF52E0EC90CEFC
5	EM EV TLS CA - G3B	00D8F8685E4F2BD9D82402A85A1C1EB731	579480AEA166290BD3C643589E795FC0D0E54E86505D180F1DFF99EFD3199512
6	EM EV TLS CA - G3C	05F078752DECE7A1BB8595D303167171	FD9D5C2DBBD4995AB69B8D50C439D9527B00529199C2FD01B2174EB58F07021F

APPENDIX B(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
21	EM DV TLS CA - G2A-1	00B6391A6D28C7886AE6FCCED2F3C1A7	3F13597D3355D341BD09328AEE567D7F4E002D9919B986F9962DAFF197EA75D1
22	EM DV TLS CA - G2B	00F0A030825E22BB2E1D88E3889DC073	829EC444B8BE3DFD2D030A0D9E7A1D0DD2A3C2C325D39589C27AC9A065BAE793

No	Common Name	Certificate Serial No.	SHA-256 Fingerprint
23	EM DV TLS CA - G2C	00AB5DEA38BDC920D5FA4736DA54BEBE	0427EA3CB4A7B4CB205E77A7B166D332BEDB8E8EF469BC5E883169C8D0AC876D
24	EM OV TLS CA - G2A-1	59491409E797EA968F05E0FF331FEC	291804EC866837CD5AF5F4D652F1DCC79BEC622D4F9BF4870E5E4D8639DF3AD4
25	EM OV TLS CA - G2B	00C164DB9804F563241ED32C4100A566	6A7A93861982B664001710A0EFD04C8A72F6A23E252B280911797E0BF1BD9012
26	EM OV TLS CA - G2C	00CBDCFA0D64112709CF14B7E4858250	DE767792E870BD32F331029FC89DC24C53F9DF970DC70F1EA30CF29DB3F94BA9
27	EM DV TLS CA - G3A-1	00A3E5AD9D0C0374A342E5E2A3F506DD	4896D51F6537A5326272C412BC75990E15D4F5ECDC2946C19776923B8E169E93
28	EM DV TLS CA - G3B	00A4AEE678F23362B4C0E460B772F214	42C4ACCD12C4F59597925E1A08A7A90102608543809308D50EC427E118BA1493
29	EM DV TLS CA - G3C	588B2E3C2BB8CDA13E1A1209254321	0164D7CEAE5BB909C272AF151FF44B1177AE9B47D9424B94F1D9558C30934D19
30	EM OV TLS CA - G3A-1	00C5FB5F2D43071F5B5623B5D132878C	259FF0963A0665BF40D92E05E95B960CCB423DBD117482AE647BC7FD5F5CE644
31	EM OV TLS CA - G3B	6CADA367FB1C100088120EA202D568	98B896625C0C230ADEEC3EB2CF6AAD5001ECF9156A68644E82374CE5833BC25B
32	EM OV TLS CA - G3C	296926C227A3A1526392B19482A504	CB6E15165AC802E9B3F993F16C25D41F4E81C21EBDE71AE1B012AC00BF9C7C3F

LIST OF CROSS SIGNED CAs:

No	Common Name	Certificate Serial No.	SHA-256 Fingerprint
1	EM DV TLS CA - G2A-1	45D2438F4CAE023D3D78A052A5A9DB94	122A5433D8A2A8C501D5E680AB216885A6019326A189DF91E8895F8B5AD488DD
2	EM DV TLS CA - G2B	6D3091E911E878BA6E196CC2A186FF01	5F0D6380B345D409C641D089B081D7B43B365FD413994403301671C3CBC6A3E5
3	EM DV TLS CA - G2C	00DF5AD8718C74A3CFEE80D5B5FB94AE03	8FE4701D088C2250317BB3A77EDC1707E38E1112E8A334F615CFA9D46F175B04
4	EM DV TLS CA - G3A-1	00FBF771754D6A8760263B3E115432593F	ECB8D30846BEF4B340C90152659F452FD81A7A4F41429B890F1E2B3467058565
5	EM DV TLS CA - G3B	00A024FDF4BA665C785CE4A020483858B7	45A883F349AEDFD5F3A649B5498FFB121712BA8B448F3F2A91DBC5A766FCDDBE
6	EM DV TLS CA - G3C	0091F347F1A5B7D39962B95E0EE4E299D1	62B7F9868263F72F6911FC78CEAF72C1979158B7368BF648683BB2AA39B02E72

No	Common Name	Certificate Serial No.	SHA-256 Fingerprint
7	EM OV TLS CA - G2A-1	49CA1A0221C19698975E1EC6F4EDA4D1	E0DA30FF7384B9873EDE9FB2DBA7F1353C7E60ED59BB9A43779F9E8494A47BAC
8	EM OV TLS CA - G2B	2923D7603B9D92DEDD54733C594811DA	121C42490FECA63B63E7D068046CC4C5FC58436BF71C97283746F37A9DD67799
9	EM OV TLS CA - G2C	119AF942CF007231271F37B0CDAE9928	ED82135F7D946673F8298BF758DC830BAD20FB37F5BB9EAC52B236563FEC931E
10	EM OV TLS CA - G3A-1	00ADA1791F3D515E1A4080D208AE888A01	1159D471B5746802C2F2CB2FFFE6D5C332B9319BD52ACEBFA93AEC07544E7C5D
11	EM OV TLS CA - G3B	00E94223BDE92F914E5AB9ACABFDAC3710	5F1DED4DD590AF74631290CF073B122A2AAC6A1FA479778A0BD43579BD832699
12	EM OV TLS CA - G3C	008D5A4811939EF447D77111CDD9849AE9	7485B51C0ED192878FA1D2F948FB529AE1842CC5086C4B67F7BE5B2039DE9489

APPENDIX C – CERTIFICATION PRACTICE STATEMENTS IN SCOPE

Certification Practice Statement (CP/CPS) for SSL/TLS

Certification Practice Statement	Begin Effective Date	End Effective Date
Version 1.00	19 August 2025	8 September 2025
Version 1.01	9 September 2025	18 November 2025
Version 1.02	19 November 2025	27 November 2025
Version 1.03	28 November 2025	1 April 2026
Version 1.04	2 April 2026	20 April 2026
Version 1.05	21 April 2026	9 July 2026
Version 1.06	10 July 2026	-

Certification Practice Statement (CP/CPS) for InCommon CA TLS

Certification Practice Statement	Begin Effective Date	End Effective Date
Version 1.04	8 April 2026	20 April 2026
Version 1.05	21 April 2026	9 July 2026
Version 1.06	10 July 2026	-