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 a 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**, emSign PKI has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in applicable versions of its Certification Practice Statements as enumerated in **Appendix B**

- maintained effective controls to provide reasonable assurance that emSign PKI provides its services in accordance with applicable versions of its Certification Practice Statements 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;
  - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
  - subscriber information is properly authenticated (for the registration activities performed by emSign PKI); and
  - 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 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

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

emSign PKI does not escrow its CA keys, does not provide integrated circuit card lifecycle management and certificate suspension services. Accordingly, our procedures did not extend to controls that would address those criteria.

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 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 emSign PKI'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 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 v2.2.2.

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 v2.2.2, nor the suitability of any 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 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 – 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 SSL CA - G1	217AD58B1C713C002091	47B2EFBC3670E7DB4B41F22C51FC02EE84FB2DBF3082A49F2C2688122E9210A1
3	emSign EV SSL CA - G1	626CB92B237FF82E3F50	4334EEB2CC114F82BEE6F8A7E5AEA03A42EB2E1F70CBD66102E414D72F0033B9
4	emSign Class 1 CA - G1	00D59B7C9B36A2D44922EA	CF6D0333D0BE2C69A42D453960DEE9E109D9E8843EA3061A1671D6EAF85EB7D8
5	emSign Class 2 CA - G1	3C5BDA55C0A236A744CD	63A8369DC824A42BC7AE6EE5D26AAFD32DF4AF677CA18B941B7A57E33B1E3559
6	emSign Class 3 CA - G1	00A08870825A326BED9611	42DA1C562F80E46DA7A321244EFC23D0FAA9FEBBB7AA0377D96B42D9E88AB200
7	emSign Device CA - G1	0465835247364A904A8E	4C9198B673550858799AD2744CC083C1BA0027E77D3B8FD6D56CF53620D099E2
8	emSign SMIME CA – G1	00AB98D0B97A5D695A	BA9E8A1FCC4154B094BE734035ECA7E54E9F5619D511B265750EEB982E2C6D06
9	**emSign Root CA - G2**	00864DBF0FE35ED77D8ED8	1AA0C2709E831BD6E3B5129A00BA41F7EEEF020872F1E6504BF0F6C3F24F3AF3
10	emSign CS CA - G2	00C084E666596139A1FA9B	C2E4D1765005D5CA361D400A434B43036DBC931EC6D7B99C17BEC030CC74CA7D
11	emSign EV CS CA - G2	3CA9F3D18C08E50959D5	69E2448C5F03EEDE5EC2C907EFE96C3D33AD679B49CD29C38C5182323121BEFF
12	emSign Time Stamping CA - G2	00BA9E35E51ECFAC6C4740	C3BE06C6B0A92334423180E95EA1E683AAB9C3B7D0F5CB8A4F51FBC1006F3DC0
13	**emSign ECC Root CA - G3**	3CF607A968700EDA8B84	86A1ECBA089C4A8D3BBE2734C612BA341D813E043CF9E8A862CD5C57A36BBE6B
14	emSign ECC SSL CA - G3	72DDC7E9DCE9B0DCFFC7	6B51D1DCF4EB7AEE424185CB1B9580574B39CB963863DE3EC1AD31DDB076CE9F
15	emSign ECC EV SSL CA - G3	01FE3E6C68DEBBEC263E	0116F17F97CDEF4ADE2E63CF2C1B064FD99F404D2B914100BC241F0781853323
16	emSign ECC CS CA - G3	35CF922FB9008249F89C	0D6869A2B4F5DF77A6AFB034225E9BEF345743CF306EDF36EE35B9D05AFAD89C

No.	Common Name	Certificate Serial No.	SHA-256 Fingerprint
17	emSign ECC EV CS CA - G3	23BA23AB486AE7D5C0FE	0BADA979B71402FE860696032CF40E9D2A3F41CCB5D03BE33FBB94A80D7FFC7C
18	emSign ECC Class 1 CA - G3	00FB1E21982EB1B55C5925	ABA6A65DCE8955BAF0685AB88809B7699C174496EF9EE991533251494F43CE10
19	emSign ECC Class 2 CA - G3	23E1BA02DFF3E900EDDD	4E9B731567177E1776A96D66D9120B3DEB28B800937EA4662565B3EF5EC8000B
20	emSign ECC Class 3 CA - G3	00B8EB258324DB08ACC2F5	7066A0F42F530E0DB5AFEE72A3B04DE614E7D2305C67D12C756BB215E37CB975
21	emSign ECC Time stamping CA - G3	0084A863D6F61818464D34	C422AB86C1729E889FBCAF5CD73F217E03C29FE2AC50212F451307D915869F47
22	emSign ECC Device CA - G3	00876282A8FD758C391EC3	70B9BA595412CF8614B76747FD683CCA2759F42642164834FBEFDD88505C4F1C
23	emSign ECC SMIME CA – G3	0E906BB2267EC0FF	F5B3E914CDE2954F65464FA8E9D69F0492622B3C2AC243987B11CBBF1B451307
24	**emSign Root CA - C1**	00AECF00BAC4CF32F843B2	125609AA301DA0A249B97A8239CB6A34216F44DCAC9F3954B14292F2E8C8608F
25	emSign SSL CA - C1	0086766B7F96DF60C46F8B	F91AACA0E4E533747A0880BFCF6F26720DC1D05494C3938DA6802290D5A09B32
26	emSign EV SSL CA - C1	00BADFD29B3F1E678C6960	F6F159286A1401DE5397E21A0090534A85F5E7B9F98FD4A5A47B1DFFD4BFDED4
27	emSign Class 1 CA - C1	7E065336C075C7998B63	0EF7B863FAABC384A694FF632DAAF9BD31CED23E9246559A59ECD7472754CCE6
28	emSign Class 2 CA - C1	1A5C82DEDCBC6A153030	05B30B3FC44F8575334BD812EF9FA8A52A75743E19BC35A5BE3912ECA62C4669
29	emSign Class 3 CA - C1	00B474F64D86392189496E	69B0DD09B98F36A9CC7BD7FFE8A00DCD319A5FC947C9C8AF72C92894D8E81092
30	emSign Device CA - C1	00B19BE3081E2D97B5BFCB	D034B18751BEE10AAAF94C2F14350D3F654E5B934D0DDA592B31E58187A48952
31	emSign Time Stamping CA – C1	00D6CB155EA221A1C4E37A	4D15E5199D88EAB1838E06EBA08BC690E971B4B1FCD77A6530E9C06F17FDF477
32	Soft-Net Secure Signing CA – C1	4D3A149CFA144F9E3115	CCEC157DA0F0BD58E3E8B584054FE0C44F04B4DD8C97B75B788D9140B05142F7
33	**emSign Root CA - C2**	2F0AB76B0DCB4AAF2758	46CD083B47E80402028DF493960EA19C85FE851950D5165F1C7DA4FAA951E2F8

No.	Common Name	Certificate Serial No.	SHA-256 Fingerprint
34	emSign CS CA - C2	00B4E6BA3BE4B674A36434	B0E6BB9D6E7A94BC4A6B89D96743438D2565DBB0A697ABB21457ACA22A13CE4
35	emSign EV CS CA - C2	00AE0882F16DBA80375653	024998101210644F68FAE9115543A5E6D26A6DB0D2C10366FF2D5BB505D8872D
36	emSign Time Stamping CA - C2	63720D6AB070BF2A157D	571FC70654AB8C1AA3B4A261A3D505FAE10BC4558FA17C72849B6B98BC845CAE
37	**emSign ECC Root CA - C3**	7B71B68256B8127C9CA8	BC4D809B15189D78DB3E1D8CF4F9726A795DA1643CA5F1358E1DDB0EDC0D7EB3
38	emSign ECC SSL CA - C3	5B7D9BB1FD33B9BC1D84	A061D445399714C38FC101A6E9AFBDB381F112FA5DE7D5BC14904558D1ED3276
39	emSign ECC EV SSL CA - C3	1B50581F7334B30B2723	C0A578F2109E6F42D3D939948DEEAB729B20F7B23B4237ABD8494DF554CF985C
40	emSign ECC CS CA - C3	00B8973C4278609F2AF2A4	A3AFD72375C1D7A8330E62D577E13581B72332C8062DFA9CF39E51AE65088582
41	emSign ECC EV CS CA - C3	6004C5E20B62FDD48C46	CB21097992402097033 7AE32DA5C3F981A9E05714EC22BB1C3421FE695E5157A
42	emSign ECC Class 1 CA - C3	00BD6A0796AB3F8955521E	FAD2E98649F1C606150F55269EBC035AEA22FFAC131DE64BA6900C75D8447B7E
43	emSign ECC Class 2 CA - C3	00D1142766698BFCDEDA02	DB4591F878F6672F5B70733A66AD7C9537B97E6F0AF5CA49AAB8ECB2CE02F86B
44	emSign ECC Class 3 CA - C3	3D12A1CF78258D580854	5A9A03F2D3FE589BE63CDA11820A9F25F074C92034F51C047D34226D252EC025
45	emSign ECC Time stamping CA - C3	00B94B49C6436D72090201	71D2EE4DDA251D9244F7CE7C6D478EC552D424EF719F02B71030F2821B6BC853
46	emSign ECC Device CA - C3	00D9365F15842A1D0689C3	3D4511D0A80AA949A6D99B253A173471797C4459187A6329E736C37CB5493E46
47	**emSign Root Client Auth G1**	0E4FA878FEA8183E7107189595046D84	8ABFC40FAEAF13CBC8BB67B61C8D097A321CD2FEE047C54256927E0F8BFEADFD
48	**emSign Root Client Auth G3**	0C514FFD18852863D2AAB9B7006346DF	BBD8B3D745EFB79198D93B9C482B9D934537325729EA2F02C129261F91BE2E3D
49	**emSign Root CS CA - G2**	0886217572A7C40CC3BB2EE5D72D6E6C	0D74EF67C88DE3560365E225AEF976F915E901347B73352D81AB5B4132BB2150
50	**emSign Root CS CA - G3**	018FCEC927C116F59C997EDC0CCD2E2B	F2EDAAFF3D9B701FB4D14C9F285F8C0BAD90FC3BCC1FA07D47F4718EDABA34A5

No.	Common Name	Certificate Serial No.	SHA-256 Fingerprint
51	**emSign Root SMIME CA - G1**	0C974F5F068B868F52FC0CF7E5544F51	47911BC8F32A11B029E0BB10A348B459404B87731B870A2F3FA97B4705DC4C25
52	**emSign Root SMIME CA - G3**	009F4F5FF84A1A6DC2C83C0EF9B7031F	F76A0D440C418DC5B362BE8E11E0A5D06023F4396093E4F455827BF55153D8A4
53	**emSign Root TLS CA - G1**	02A27D4E346AEF4E4F04678B5BB6D9EE	CEF71E70B7C29ADDF6C30CD19E614B38FD5F02A435A0EEDDD0087E183D101A51
54	**emSign Root TLS CA - G3**	0E760672F143459FC8FE0AB0BC05E394	7DD78D5F4F13459A83DFF9ABBBA62EDBAF6F2D102BF257FD712F4D9F2746ED8D
55	**emSign Root TSA CA - G2**	065E0E80658A572E5EBDBF93A493E350	1997770A5633FB6D0440ABF7D7E87E15D795F094F8C2959DADB00E785866BF48
56	**emSign Root TSA CA - G3**	0E27F07F8657096CCFD447EA0E2399EC	75D2CE75979CF2A43B172C9F89F733DDA2136031DB4BBF3698B053714C077155

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'S MANAGEMENT ASSERTION

eMudhra Technologies Limited ("emSign PKI") operates the Certification Authority (CA) services known as enumerated in **Appendix A**, and provides the following CA services:

- Subscriber registration
- Certificate renewal
- Certificate rekeys
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation
- Subscriber key generation and management

The management of emSign PKI is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure in its repository, CA business practices management, CA environmental controls, CA key lifecycle management controls, subscriber key lifecycle management controls, certificate lifecycle management controls, and subordinate CA 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 CA services. Based on that assessment, in emSign PKI management's opinion, in providing its Certification Authority (CA) services at Bangalore and Chennai, India throughout the period 01 June 2023 to 31 May 2024, emSign PKI has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its applicable Certification Practice Statements as enumerated in **Appendix B**;

- maintained effective controls to provide reasonable assurance that:
  - emSign PKI provides its services in accordance with its applicable Certification Practice Statements 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;
  - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
  - subscriber information is properly authenticated (for the registration activities performed by emSign PKI; and

- subordinate CA certificate requests are accurate, authenticated, and approved; and

- 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 and Destruction
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management

Subscriber Key Lifecycle Management Controls

- CA-Provided Subscriber Key Generation Services
- CA-Provided Subscriber Key Storage and Recovery Services
- Requirements for Subscriber Key Management

Certificate Lifecycle Management Controls

- Subscriber Registration
- Certificate Renewal
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

Subordinate CA Certificate Lifecycle Management Controls

- Subordinate CA Certificate Lifecycle Management

emSign PKI does not escrow its CA keys, does not provide integrated circuit card lifecycle management and certificate suspension services. Accordingly, our assertion does not extend to controls that would address those criteria.

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 – 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 SSL CA - G1	217AD58B1C713C002091	47B2EFBC3670E7DB4B41F22C51FC02EE84FB2DBF3082A49F2C2688122E9210A1
3	emSign EV SSL CA - G1	626CB92B237FF82E3F50	4334EEB2CC114F82BEE6F8A7E5AEA03A42EB2E1F70CBD66102E414D72F0033B9
4	emSign Class 1 CA - G1	00D59B7C9B36A2D44922EA	CF6D0333D0BE2C69A42D453960DEE9E109D9E8843EA3061A1671D6EAF85EB7D8
5	emSign Class 2 CA - G1	3C5BDA55C0A236A744CD	63A8369DC824A42BC7AE6EE5D26AAFD32DF4AF677CA18B941B7A57E33B1E3559
6	emSign Class 3 CA - G1	00A08870825A326BED9611	42DA1C562F80E46DA7A321244EFC23D0FAA9FEBBB7AA0377D96B42D9E88AB200
7	emSign Device CA - G1	0465835247364A904A8E	4C9198B673550858799AD2744CC083C1BA0027E77D3B8FD6D56CF53620D099E2
8	emSign SMIME CA – G1	00AB98D0B97A5D695A	BA9E8A1FCC4154B094BE734035ECA7E54E9F5619D511B265750EEB982E2C6D06
9	**emSign Root CA - G2**	00864DBF0FE35ED77D8ED8	1AA0C2709E831BD6E3B5129A00BA41F7EEEF020872F1E6504BF0F6C3F24F3AF3
10	emSign CS CA - G2	00C084E666596139A1FA9B	C2E4D1765005D5CA361D400A434B43036DBC931EC6D7B99C17BEC030CC74CA7D
11	emSign EV CS CA - G2	3CA9F3D18C08E50959D5	69E2448C5F03EEDE5EC2C907EFE96C3D33AD679B49CD29C38C5182323121BEFF
12	emSign Time Stamping CA - G2	00BA9E35E51ECFAC6C4740	C3BE06C6B0A92334423180E95EA1E683AAB9C3B7D0F5CB8A4F51FBC1006F3DC0
13	**emSign ECC Root CA - G3**	3CF607A968700EDA8B84	86A1ECBA089C4A8D3BBE2734C612BA341D813E043CF9E8A862CD5C57A36BBE6B
14	emSign ECC SSL CA - G3	72DDC7E9DCE9B0DCFFC7	6B51D1DCF4EB7AEE424185CB1B9580574B39CB963863DE3EC1AD31DDB076CE9F
15	emSign ECC EV SSL CA - G3	01FE3E6C68DEBBEC263E	0116F17F97CDEF4ADE2E63CF2C1B064FD99F404D2B914100BC241F0781853323
16	emSign ECC CS CA - G3	35CF922FB9008249F89C	0D6869A2B4F5DF77A6AFB034225E9BEF345743CF306EDF36EE35B9D05AFAD89C
17	emSign ECC EV CS CA - G3	23BA23AB486AE7D5C0FE	0BADA979B71402FE860696032CF40E9D2A3F41CCB5D03BE33FBB94A80D7FFC7C
18	emSign ECC Class 1 CA - G3	00FB1E21982EB1B55C5925	ABA6A65DCE8955BAF0685AB88809B7699C174496EF9EE991533251494F43CE10
19	emSign ECC Class 2 CA - G3	23E1BA02DFF3E900EDDD	4E9B731567177E1776A96D66D9120B3DEB28B800937EA4662565B3EF5EC8000B
20	emSign ECC Class 3 CA - G3	00B8EB258324DB08ACC2F5	7066A0F42F530E0DB5AFEE72A3B04DE614E7D2305C67D12C756BB215E37CB975
21	emSign ECC Time stamping CA - G3	0084A863D6F61818464D34	C422AB86C1729E889FBCAF5CD73F217E03C29FE2AC50212F451307D915869F47

No.	Common Name	Certificate Serial No.	SHA-256 Fingerprint
22	emSign ECC Device CA - G3	00876282A8FD758C391EC3	70B9BA595412CF8614B76747FD683CCA2759F42642164834FBEFDD88505C4F1C
23	emSign ECC SMIME CA - G3	0E906BB2267EC0FF	F5B3E914CDE2954F65464FA8E9D69F0492622B3C2AC243987B11CBBF1B451307
24	**emSign Root CA - C1**	00AECF00BAC4CF32F843B2	125609AA301DA0A249B97A8239CB6A34216F44DCAC9F3954B14292F2E8C8608F
25	emSign SSL CA - C1	0086766B7F96DF60C46F8B	F91AACA0E4E533747A0880BFCF6F26720DC1D05494C3938DA6802290D5A09B32
26	emSign EV SSL CA - C1	00BADFD29B3F1E678C6960	F6F159286A1401DE5397E21A0090534A85F5E7B9F98FD4A5A47B1DFFD4BFDED4
27	emSign Class 1 CA - C1	7E065336C075C7998B63	0EF7B863FAABC384A694FF632DAAF9BD31CED23E9246559A59ECD7472754CCE6
28	emSign Class 2 CA - C1	1A5C82DEDCBC6A153030	05B30B3FC44F8575334BD812EF9FA8A52A75743E19BC35A5BE3912ECA62C4669
29	emSign Class 3 CA - C1	00B474F64D86392189496E	69B0DD09B98F36A9CC7BD7FFE8A00DCD319A5FC947C9C8AF72C92894D8E81092
30	emSign Device CA - C1	00B19BE3081E2D97B5BFCB	D034B18751BEE10AAAF94C2F14350D3F654E5B934D0DDA592B31E58187A48952
31	emSign Time Stamping CA - C1	00D6CB155EA221A1C4E37A	4D15E5199D88EAB1838E06EBA08BC690E971B4B1FCD77A6530E9C06F17FDF477
32	Soft-Net Secure Signing CA - C1	4D3A149CFA144F9E3115	CCEC157DA0F0BD58E3E8B584054FE0C44F04B4DD8C97B75B788D9140B05142F7
33	**emSign Root CA - C2**	2F0AB76B0DCB4AAF2758	46CD083B47E80402028DF493960EA19C85FE851950D5165F1C7DA4FAA951E2F8
34	emSign CS CA - C2	00B4E6BA3BE4B674A36434	B0E6BB9D6E7A94BC4A6B89D96743438D2565DBB0A697ABB21457ACA22A13CE4
35	emSign EV CS CA - C2	00AE0882F16DBA80375653	024998101210644F68FAE9115543A5E6D26A6DB0D2C10366FF2D5BB505D8872D
36	emSign Time Stamping CA - C2	63720D6AB070BF2A157D	571FC70654AB8C1AA3B4A261A3D505FAE10BC4558FA17C72849B6B98BC845CAE
37	**emSign ECC Root CA - C3**	7B71B68256B8127C9CA8	BC4D809B15189D78DB3E1D8CF4F9726A795DA1643CA5F1358E1DDB0EDC0D7EB3
38	emSign ECC SSL CA - C3	5B7D9BB1FD33B9BC1D84	A061D445399714C38FC101A6E9AFBDB381F112FA5DE7D5BC14904558D1ED3276
39	emSign ECC EV SSL CA - C3	1B50581F7334B30B2723	C0A578F2109E6F42D3D939948DEEAB729B20F7B23B4237ABD8494DF554CF985C
40	emSign ECC CS CA - C3	00B8973C4278609F2AF2A4	A3AFD72375C1D7A8330E62D577E13581B72332C8062DFA9CF39E51AE65088582
41	emSign ECC EV CS CA - C3	6004C5E20B62FDD48C46	CB210979924020970337AE32DA5C3F981A9E05714EC22BB1C3421FE695E5157A
42	emSign ECC Class 1 CA - C3	00BD6A0796AB3F8955521E	FAD2E98649F1C606150F55269EBC035AEA22FFAC131DE64BA6900C75D8447B7E

No.	Common Name	Certificate Serial No.	SHA-256 Fingerprint
43	emSign ECC Class 2 CA - C3	00D1142766698BFCDEDA02	DB4591F878F6672F5B70733A66AD7C9537B97E6F0AF5CA49AAB8ECB2CE02F86B
44	emSign ECC Class 3 CA - C3	3D12A1CF78258D580854	5A9A03F2D3FE589BE63CDA11820A9F25F074C92034F51C047D34226D252EC025
45	emSign ECC Time stamping CA - C3	00B94B49C6436D72090201	71D2EE4DDA251D9244F7CE7C6D478EC552D424EF719F02B71030F2821B6BC853
46	emSign ECC Device CA - C3	00D9365F15842A1D0689C3	3D4511D0A80AA949A6D99B253A173471797C4459187A6329E736C37CB5493E46
47	**emSign Root Client Auth G1**	0E4FA878FEA8183E7107189595046D84	8ABFC40FAEAF13CBC8BB67B61C8D097A321CD2FEE047C54256927E0F8BFEADFD
48	**emSign Root Client Auth G3**	0C514FFD18852863D2AAB9B7006346DF	BBD8B3D745EFB79198D93B9C482B9D934537325729EA2F02C129261F91BE2E3D
49	**emSign Root CS CA - G2**	0886217572A7C40CC3BB2EE5D72D6E6C	0D74EF67C88DE3560365E225AEF976F915E901347B73352D81AB5B4132BB2150
50	**emSign Root CS CA - G3**	018FCEC927C116F59C997EDC0CCD2E2B	F2EDAAFF3D9B701FB4D14C9F285F8C0BAD90FC3BCC1FA07D47F4718EDABA34A5
51	**emSign Root SMIME CA - G1**	0C974F5F068B868F52FC0CF7E5544F51	47911BC8F32A11B029E0BB10A348B459404B87731B870A2F3FA97B4705DC4C25
52	**emSign Root SMIME CA - G3**	009F4F5FF84A1A6DC2C83C0EF9B7031F	F76A0D440C418DC5B362BE8E11E0A5D06023F4396093E4F455827BF55153D8A4
53	**emSign Root TLS CA - G1**	02A27D4E346AEF4E4F04678B5BB6D9EE	CEF71E70B7C29ADDF6C30CD19E614B38FD5F02A435A0EEDDD0087E183D101A51
54	**emSign Root TLS CA - G3**	0E760672F143459FC8FE0AB0BC05E394	7DD78D5F4F13459A83DFF9ABBBA62EDBAF6F2D102BF257FD712F4D9F2746ED8D
55	**emSign Root TSA CA - G2**	065E0E80658A572E5EBDBF93A493E350	1997770A5633FB6D0440ABF7D7E87E15D795F094F8C2959DADB00E785866BF48
56	**emSign Root TSA CA - G3**	0E27F07F8657096CCFD447EA0E2399EC	75D2CE75979CF2A43B172C9F89F733DDA2136031DB4BBF3698B053714C077155

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	-