

## 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 and at Utah and New Jersey, United States throughout the period 1 June 2024 to 31 May 2025 for its CAs as enumerated in [Appendix A\(i\)](#), emSign PKI has:

- disclosed its S/MIME certificate lifecycle management business practices in applicable versions of its Certification Practice Statements as enumerated in [Appendix B](#) including its commitment to provide S/MIME certificates in conformity with the CA/Browser Forum Requirements 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 S/MIME certificates it manages is established and protected throughout their lifecycles; and
  - S/MIME subscriber information is properly authenticated (for the registration activities performed by emSign PKI)
- 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 - S/MIME Certificate v1.0.3](#).

The CAs enumerated in [Appendix A\(ii\)](#) did not issue any S/MIME 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 the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities - S/MIME Certificates v1.0.3.



## **Our independence and quality control**

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 S/MIME certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of S/MIME certificates;
- (2) selectively testing transactions executed in accordance with disclosed S/MIME 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 factor 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 2024 to 31 May 2025, 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 - S/MIME Certificates v1.0.3.

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 - S/MIME Certificates v1.0.3, 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 - S/MIME Certificates 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.

A handwritten signature in black ink that reads 'BDO Consulting Sdn Bhd'.

BDO Consulting Sdn. Bhd.  
Kuala Lumpur, Malaysia  
19 August 2025

**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                 | 40F6AF0346A99AA1CD1D55<br>5A4E9CCE62C7F9634603EE<br>406615833DC8C8D00367 |
| 2   | emSign SMIME CA - G1      | 00AB98D0B97A5D695A                   | BA9E8A1FCC4154B094BE73<br>4035ECA7E54E9F5619D511<br>B265750EEB982E2C6D06 |
| 3   | emSign Root SMIME CA - G1 | 0091685541577A36E8AE09<br>ADEBE4CFAF | A65160E9770D70D8ACE8EC<br>3670A7B4EF1F87F4F507B1<br>CE3D6FC623ADED0694C1 |
| 4   | emSign ECC Root CA - G3   | 3CF607A968700EDA8B84                 | 86A1ECBA089C4A8D3BBE2<br>734C612BA341D813E043CF<br>9E8A862CD5C57A36BBE6B |
| 5   | emSign ECC SMIME CA - G3  | 0E906BB2267EC0FF                     | F5B3E914CDE2954F65464F<br>A8E9D69F0492622B3C2AC2<br>43987B11CBBF1B451307 |
| 6   | emSign Root SMIME CA - G3 | 00B33EBCAC96AC83A823E2<br>786D76B6D8 | B4CEEBA48EF8CCC6090F6D<br>2A62A85DBB51C5A106A7D<br>C7EC5408270020F91C222 |
| 7   | emSign Root SMIME CA - G1 | 0C974F5F068B868F52FC0C<br>F7E5544F51 | 47911BC8F32A11B029E0BB<br>10A348B459404B87731B87<br>0A2F3FA97B4705DC4C25 |
| 8   | emSign SMIME CA - G1      | 00FE04E642637D4020947D<br>6C5F4E0BD0 | B9E2588E93B5E53617B842<br>E6ED34854EE46BA3D6721E<br>C45DC650CE4439F514BE |
| 9   | emSign Root SMIME CA - G3 | 009F4F5FF84A1A6DC2C83C<br>0EF9B7031F | F76A0D440C418DC5B362BE<br>8E11E0A5D06023F4396093<br>E4F455827BF55153D8A4 |
| 10  | emSign SMIME CA - G3      | 13BCE369D10F5CA4408D91<br>B84155CB   | 30444F40CAC26FFF497B1C<br>D00DDF4D81453A8A176272<br>CC34ABE35FD564602B1B |

**Appendix A(ii):**

**List of Root and Subordinate CAs in Scope:**

| No. | Common Name                | Certificate Serial No. | SHA-256 Fingerprint  |
|-----|----------------------------|------------------------|--|
| 1   | emSign Class 1 CA - G1     | 00D59B7C9B36A2D44922EA | CF6D0333D0BE2C69A42D45<br>3960DEE9E109D9E8843EA3<br>061A1671D6EAF85EB7D8 |
| 2   | emSign Class 2 CA - G1     | 3C5BDA55C0A236A744CD   | 63A8369DC824A42BC7AE6E<br>E5D26AAFD32DF4AF677CA<br>18B941B7A57E33B1E3559 |
| 3   | emSign Class 3 CA - G1     | 00A08870825A326BED9611 | 42DA1C562F80E46DA7A321<br>244EFC23D0FAA9FEBBB7AA<br>0377D96B42D9E88AB200 |
| 4   | emSign Device CA - G1      | 0465835247364A904A8E   | 4C9198B673550858799AD2<br>744CC083C1BA0027E77D3B<br>8FD6D56CF53620D099E2 |
| 5   | emSign ECC Class 1 CA - G3 | 00FB1E21982EB1B55C5925 | ABA6A65DCE8955BAF0685<br>AB88809B7699C174496EF9<br>EE991533251494F43CE10 |

| No. | Common Name                     | Certificate Serial No. | SHA-256 Fingerprint  |
|-----|---------------------------------|------------------------|--|
| 6   | emSign ECC Class 2 CA - G3      | 23E1BA02DFF3E900EDDD   | 4E9B731567177E1776A96D<br>66D9120B3DEB28B800937E<br>A4662565B3EF5EC8000B |
| 7   | emSign ECC Class 3 CA - G3      | 00B8EB258324DB08ACC2F5 | 7066A0F42F530E0DB5AFEE<br>72A3B04DE614E7D2305C67<br>D12C756BB215E37CB975 |
| 8   | emSign ECC Device CA - G3       | 00876282A8FD758C391EC3 | 70B9BA595412CF8614B767<br>47FD683CCA2759F4264216<br>4834FBEFDD88505C4F1C |
| 9   | <b>emSign Root CA - C1</b>      | 00AECF00BAC4CF32F843B2 | 125609AA301DA0A249B97A<br>8239CB6A34216F44DCAC9F<br>3954B14292F2E8C8608F |
| 10  | emSign Class 1 CA - C1          | 7E065336C075C7998B63   | 0EF7B863FAABC384A694FF<br>632DAAF9BD31CED23E9246<br>559A59ECD7472754CCE6 |
| 11  | emSign Class 2 CA - C1          | 1A5C82DEDCBC6A153030   | 05B30B3FC44F8575334BD8<br>12EF9FA8A52A75743E19BC<br>35A5BE3912ECA62C4669 |
| 12  | emSign Class 3 CA - C1          | 00B474F64D86392189496E | 69B0DD09B98F36A9CC7BD<br>7FFE8A00DCD319A5FC947C<br>9C8AF72C92894D8E81092 |
| 13  | emSign Device CA - C1           | 00B19BE3081E2D97B5BFCB | D034B18751BEE10AAAF94C<br>2F14350D3F654E5B934D0D<br>DA592B31E58187A48952 |
| 14  | Soft-Net Secure Signing CA - C1 | 4D3A149CFA144F9E3115   | CCEC157DA0F0BD58E3E8B<br>584054FE0C44F04B4DD8C9<br>7B75B788D9140B05142F7 |
| 15  | <b>emSign ECC Root CA - C3</b>  | 7B71B68256B8127C9CA8   | BC4D809B15189D78DB3E1D<br>8CF4F9726A795DA1643CA5<br>F1358E1DDB0EDC0D7EB3 |
| 16  | emSign ECC Class 1 CA - C3      | 00BD6A0796AB3F8955521E | FAD2E98649F1C606150F55<br>269EBC035AEA22FFAC131D<br>E64BA6900C75D8447B7E |
| 17  | emSign ECC Class 2 CA - C3      | 00D1142766698BFCDEDA02 | DB4591F878F6672F5B7073<br>3A66AD7C9537B97E6F0AF5<br>CA49AAB8ECB2CE02F86B |
| 18  | emSign ECC Class 3 CA - C3      | 3D12A1CF78258D580854   | 5A9A03F2D3FE589BE63CDA<br>11820A9F25F074C92034F5<br>1C047D34226D252EC025 |
| 19  | emSign ECC Device CA - C3       | 00D9365F15842A1D0689C3 | 3D4511D0A80AA949A6D99B<br>253A173471797C4459187A<br>6329E736C37CB5493E46 |

#### Appendix B - Certification Practice Statement in Scope

| Certification Practice Statement | Begin Effective Date | End Effective Date |
|----------------------------------|----------------------|--------------------|
| <a href="#">Version 1.14</a>     | 30 August 2023       | 16 June 2024       |
| <a href="#">Version 1.15</a>     | 17 June 2024         | 4 September 2024   |
| <a href="#">Version 1.16</a>     | 5 September 2024     | 29 November 2024   |
| <a href="#">Version 1.17</a>     | 30 November 2024     | 13 March 2025      |
| <a href="#">Version 1.18</a>     | 14 March 2025        | 5 June 2025        |
| <a href="#">Version 1.19</a>     | 6 June 2025          | 7 July 2025        |
| <a href="#">Version 1.20</a>     | 8 July 2025          | -                  |

## EMSIGN PKI'S MANAGEMENT ASSERTION

eMudhra Technologies Limited (“emSign PKI”) operates the Certification Authority (CA) services known as enumerated in [Appendix A\(i\)](#) and provides S/MIME CA services.

The management of emSign PKI is responsible for establishing and maintaining effective controls over its S/MIME operations, including its S/MIME CA business practices disclosure on its [repository](#), S/MIME key lifecycle management controls, and S/MIME 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 CA 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 S/MIME CA services. Based on that assessment, in providing its S/MIME CA services at Bangalore and Chennai, India and at Utah and New Jersey, United States, throughout the period 01 June 2024 to 31 May 2025, emSign PKI has:

- Disclosed its S/MIME certificate lifecycle management business practices in applicable versions of its Certification Practice Statements as enumerated in [Appendix B](#), including its commitment to provide S/MIME certificates in conformity with the CA/Browser Forum Requirements 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 S/MIME certificates it manages is established and protected throughout their lifecycles; and
  - S/MIME subscriber information is properly authenticated (for the registration activities performed by emSign PKI);
- Maintained effected 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 - S/MIME Certificates v1.0.3](#).

The CAs enumerated in [Appendix A\(ii\)](#) are not used for S/MIME certificate services although technically capable of such issuance. The management has put in place internal controls to prevent S/MIME issuance under these CAs.

*Venu Madhava*

Signed by Venu Madhava  
Date: 2025.08.15  
17:05:20

**Venu Madhava,**  
**Executive Vice President- Legal, HR and GRC.**  
**15 August 2025.**

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

| No. | Common Name                      | Certificate Serial No.           | SHA-256 Fingerprint  |
|-----|----------------------------------|----------------------------------|--|
| 1   | <b>emSign Root CA - G1</b>       | 31F5E4620C6C58EDD6D8             | 40F6AF0346A99AA1CD1D555A4E9CCE62C7F9634603EE406615833DC8C8D00367 |
| 2   | emSign SMIME CA - G1             | 00AB98D0B97A5D695A               | BA9E8A1FCC4154B094BE734035ECA7E54E9F5619D511B265750EEB982E2C6D06 |
| 3   | emSign Root SMIME CA - G1        | 0091685541577A36E8AE09ADEBE4CFAF | A65160E9770D70D8ACE8EC3670A7B4EF1F87F4F507B1CE3D6FC623ADED0694C1 |
| 4   | <b>emSign ECC Root CA - G3</b>   | 3CF607A968700EDA8B84             | 86A1ECBA089C4A8D3BBE2734C612BA341D813E043CF9E8A862CD5C57A36BBE6B |
| 5   | emSign ECC SMIME CA - G3         | 0E906BB2267EC0FF                 | F5B3E914CDE2954F65464FA8E9D69F0492622B3C2AC243987B11CBBF1B451307 |
| 6   | emSign Root SMIME CA - G3        | 00B33EBCAC96AC83A823E2786D76B6D8 | B4CEEBA48EF8CCC6090F6D2A62A85DBB51C5A106A7DC7EC5408270020F91C222 |
| 7   | <b>emSign Root SMIME CA - G1</b> | 0C974F5F068B868F52FC0CF7E5544F51 | 47911BC8F32A11B029E0BB10A348B459404B87731B870A2F3FA97B4705DC4C25 |
| 8   | emSign SMIME CA - G1             | 00FE04E642637D4020947D6C5F4E0BD0 | B9E2588E93B5E53617B842E6ED34854EE46BA3D6721EC45DC650CE4439F514BE |
| 9   | <b>emSign Root SMIME CA - G3</b> | 009F4F5FF84A1A6DC2C83C0EF9B7031F | F76A0D440C418DC5B362BE8E11E0A5D06023F4396093E4F455827BF55153D8A4 |
| 10  | emSign SMIME CA - G3             | 13BCE369D10F5CA4408D91B84155CB   | 30444F40CAC26FFF497B1CD00DDF4D81453A8A176272CC34ABE35FD564602B1B |

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

| No | Common Name                | Certificate Serial No.  | SHA-256 Fingerprint  |
|----|----------------------------|-------------------------|--|
| 1  | emSign Class 1 CA - G1     | 00D59B7C9B36A2D44922EA  | CF6D0333D0BE2C69A42D453960DEE9E109D9E8843EA3061A1671D6EAF85EB7D8 |
| 2  | emSign Class 2 CA - G1     | 3C5BDA55C0A236A744CD    | 63A8369DC824A42BC7AE6EE5D26AAFD32DF4AF677CA18B941B7A57E33B1E3559 |
| 3  | emSign Class 3 CA - G1     | 00A08870825A326BED9611  | 42DA1C562F80E46DA7A321244EFC23D0FAA9FEBBB7AA0377D96B42D9E88AB200 |
| 4  | emSign Device CA - G1      | 0465835247364A904A8E    | 4C9198B673550858799AD2744CC083C1BA0027E77D3B8FD6D56CF53620D099E2 |
| 5  | emSign ECC Class 1 CA - G3 | 00FB1E21982EB1B55C5925  | ABA6A65DCE8955BAF0685AB88809B7699C174496EF9EE991533251494F43CE10 |
| 6  | emSign ECC Class 2 CA - G3 | 23E1BA02DFF3E900EDDD    | 4E9B731567177E1776A96D66D9120B3DEB28B800937EA4662565B3EF5EC8000B |
| 7  | emSign ECC Class 3 CA - G3 | 00B8EB258324DB08ACC2F5  | 7066A0F42F530E0DB5AFEE72A3B04DE614E7D2305C67D12C756BB215E37CB975 |
| 8  | emSign ECC Device CA - G3  | 00876282A8FD758C391EC3  | 70B9BA595412CF8614B76747FD683CCA2759F42642164834FBFDD88505C4F1C  |
| 9  | <b>emSign Root CA - C1</b> | 00AECF00BAC4CF32F843B2  | 125609AA301DA0A249B97A8239CB6A34216F44DCA9F3954B14292F2E8C8608F  |
| 10 | emSign Class 1 CA - C1     | 7E065336C075C7998B63    | 0EF7B863FAABC384A694FF632DAAF9BD31CED23E9246559A59ECD7472754CCE6 |
| 11 | emSign Class 2 CA - C1     | 1A5C82DEDCCBC6A153030   | 05B30B3FC44F8575334BD812EF9FA8A52A75743E19BC35A5BE3912ECA62C4669 |
| 12 | emSign Class 3 CA - C1     | 00B474F64D86392189496E  | 69B0DD09B98F36A9CC7BD7FFE8A00DCD319A5FC947C9C8AF72C92894D8E81092 |
| 13 | emSign Device CA - C1      | 00B19BE3081E2D97B5BFBCB | D034B18751BEE10AAAF94C2F14350D3F654E5B934D0DDA592B31E58187A48952 |

| No | Common Name                     | Certificate Serial No. | SHA-256 Fingerprint  |
|----|---------------------------------|------------------------|--|
| 14 | Soft-Net Secure Signing CA - C1 | 4D3A149CFA144F9E3115   | CCEC157DA0F0BD58E3E8B584054FE0C44F04B4DD8C97B75B788D9140B05142F7 |
| 15 | <b>emSign ECC Root CA - C3</b>  | 7B71B68256B8127C9CA8   | BC4D809B15189D78DB3E1D8CF4F9726A795DA1643CA5F1358E1DDB0EDC0D7EB3 |
| 16 | emSign ECC Class 1 CA - C3      | 00BD6A0796AB3F8955521E | FAD2E98649F1C606150F55269EBC035AEA22FFAC131DE64BA6900C75D8447B7E |
| 17 | emSign ECC Class 2 CA - C3      | 00D1142766698BFCDEDA02 | DB4591F878F6672F5B70733A66AD7C9537B97E6F0AF5CA49AAB8ECB2CE02F86B |
| 18 | emSign ECC Class 3 CA - C3      | 3D12A1CF78258D580854   | 5A9A03F2D3FE589BE63CDA11820A9F25F074C92034F51C047D34226D252EC025 |
| 19 | emSign ECC Device CA - C3       | 00D9365F15842A1D0689C3 | 3D4511D0A80AA949A6D99B253A173471797C4459187A6329E736C37CB5493E46 |

### Appendix B - Certification Practice Statements in Scope

| Certification Practice Statement | Begin Effective Date | End Effective Date |
|----------------------------------|----------------------|--------------------|
| <a href="#">Version 1.14</a>     | 30 August 2023       | 16 June 2024       |
| <a href="#">Version 1.15</a>     | 17 June 2024         | 4 September 2024   |
| <a href="#">Version 1.16</a>     | 5 September 2024     | 29 November 2024   |
| <a href="#">Version 1.17</a>     | 30 November 2024     | 13 March 2025      |
| <a href="#">Version 1.18</a>     | 14 March 2025        | 5 June 2025        |
| <a href="#">Version 1.19</a>     | 6 June 2025          | 7 July 2025        |
| <a href="#">Version 1.20</a>     | 8 July 2025          | -                  |