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, Karnataka, India, as of 19 February 2018 for its CAs as enumerated in **Appendix A**, emSign PKI has, in accordance with the WebTrust for Certification Authorities - Publicly Trusted Code Signing Certificates v1.0,:

- disclosed its code signing ("CS") certificate lifecycle management business practices in its:
    - emSign PKI Certificate Policy & Certificate Practice Statement (CP/CPS) v1.01

  including its commitment to provide CS certificates in conformity with the CA/Browser Forum Guidelines on the emSign PKI website, and provided such services in accordance with its disclosed practices;
- suitably designed, and placed into operation, controls to provide reasonable assurance that:
    - the integrity of keys and CS certificates it manages is established and protected throughout their lifecycles; and
    - CS subscriber information is properly authenticated (for the registration activities performed by emSign PKI);
- suitably designed, and placed into operation, controls to provide reasonable assurance that:
    - requests for CS Signing Authority and CS Timestamp Authority certificates are properly authenticated; and
    - certificates issued to CS Signing Authorities and CS Timestamp Authorities are not valid for a period longer than specified by the CA/Browser Forum; and
- suitably designed, and placed into operation, controls to provide reasonable assurance that its CS Signing Authority and CS Timestamp Authority are operated in conformity with CA/Browser Forum Guidelines.

## Certification authority's responsibilities

emSIgn PKI's management is responsible for these assertions, including the fairness of their presentation, and the provision of its described services in accordance with the WebTrust for Certification Authorities - Publicly Trusted Code Signing Certificates v1.0

## Our independence and quality control

We have complied with the relevant rules of professional conduct / code of ethics applicable to the practice of public accounting and related to assurance engagements, issued by various professional accounting bodies, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies the Canadian Standard on Quality Control 1 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.

## Auditor's responsibilities

Our responsibility is to express an opinion on management's assertions based on our procedures. We conducted our procedures in accordance with Canadian Standard on Assurance Engagements 3000, *Attestation Engagements Other than Audits or Reviews of Historical Financial Information*, set out in the CPA Canada Handbook - Assurance. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertions are fairly stated, and, accordingly, included:

(1) obtaining an understanding of emSign PKI's CS certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of CS certificates, CS Signing Authorities certificates, and CS Timestamp Authority certificates;
(2) evaluating the suitability of the design of the controls; and
(3) performing such other procedures as we considered necessary in the circumstances.

We did not perform procedures to determine the operating effectiveness of controls for any period. Accordingly, we express no opinion on the operating effectiveness of any aspects of emSign PKI's controls individually or in the aggregate.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

**Suitability of controls**

The suitability of the design of the controls at emSign PKI and their effect on assessment of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and replying party locations. We have performed no procedures to evaluate the suitability of the design of the controls at individual subscriber and relying party locations.

**Inherent limitations**

Because of the nature and inherent limitations of controls, emSign PKI's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent or detect and correct, error, fraud, unauthorised access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

**Opinion**

In our opinion, as of 26 February 2018, emSign PKI management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust for Certification Authorities - Publicly Trusted Code Signing Certificates v1.0.

This report does not include any representations as to the quality of emSign PKI's services beyond those covered by the WebTrust for Certification Authorities - Publicly Trusted Code Signing Certificates v1.0, nor the suitability of any of emSign PKI's services for any customer's intended purpose.

**BDO Consulting Sdn Bhd**

**Kuala Lumpur, Malaysia**

**26 February 2018**

Appendix A: Root and Subordinate CAs in Scope

| No | Common Name | Certificate Serial No | Subject Key Identifier | SHA-256 Fingerprint |
|---|---|---|---|---|
| 1 | **emSign Root CA - G2** | 00864DBF0FE35ED77D8ED8 | ED:EC:4D:45:61:18:28:E7:B3:23:28:11:1C:4D:A5:27:0D:5E:EC:F4 | 1A:A0:C2:70:9E:83:1B:D6:E3:B5:12:9A:00:BA:41:F7:EE:EF:02:08:72:F1:E6:50:4B:F0:F6:C3:F2:4F:3A:F3 |
| 2 | emSign CS CA - G2 | 00C084E666596139A1FA9B | 15:86:CA:B6:74:96:17:48:58:34:82:2C:CD:D2:E1:75:9E:AF:44:B7 | C2:E4:D1:76:50:05:D5:CA:36:1D:40:0A:43:4B:43:03:6D:BC:93:1E:C6:D7:B9:9C:17:BE:C0:30:CC:74:CA:7D |
| 3 | **emSign ECC Root CA - G3** | 3CF607A968700EDA8B84 | 7C:5D:02:84:13:D4:CC:8A:9B:81:CE:17:1C:2E:29:1E:9C:48:63:42 | 86:A1:EC:BA:08:9C:4A:8D:3B:BE:27:34:C6:12:BA:34:1D:81:3E:04:3C:F9:E8:A8:62:CD:5C:57:A3:6B:BE:6B |
| 4 | emSign ECC CS CA - G3 | 35CF922FB9008249F89C | E6:1A:AE:5A:79:8C:D0:28:4D:37:E0:9E:6B:C5:2D:5D:B4:6C:F8:EB | 0D:68:69:A2:B4:F5:DF:77:A6:AF:B0:34:22:5E:9B:EF:34:57:43:CF:30:6E:DF:36:EE:35:B9:D0:5A:FA:D8:9C |
| 5 | **emSign Root CA - C2** | 2F0AB76B0DCB4AAF2758 | B3:F7:8A:A4:D6:0F:88:00:59:E8:51:17:4F:D5:7E:EC:86:22:81:9D | 46:CD:08:3B:47:E8:04:02:02:8D:F4:93:96:0E:A1:9C:85:FE:85:19:50:D5:16:5F:1C:7D:A4:FA:A9:51:E2:F8 |
| 6 | emSign CS CA - C2 | 00B4E6BA3BE4B674A36434 | 9A:42:64:A2:E0:62:94:95:C8:12:C3:0F:D5:7E:46:7C:41:2A:B2:2A | B0:E6:BB:9D:6E:7A:94:BC:4A:6B:89:D9:67:43:43:8D:2C:56:5D:BB:0A:69:7A:BB:21:45:7A:CA:22:A1:3C:E4 |
| 7 | **emSign ECC Root CA - C3** | 7B71B68256B8127C9CA8 | FB:5A:48:D0:80:20:40:F2:A8:E9:00:07:69:19:77:A7:E6:C3:F4:CF | BC:4D:80:9B:15:18:9D:78:DB:3E:1D:8C:F4:F9:72:6A:79:5D:A1:64:3C:A5:F1:35:8E:1D:DB:0E:DC:0D:7E:B3 |
| 8 | emSign ECC CS CA - C3 | 00B8973C4278609F2AF2A4 | 74:BF:90:17:0E:A3:70:6E:3C:53:C9:CC:01:51:2E:5B:A7:80:80:BB | A3:AF:D7:23:75:C1:D7:A8:33:0E:62:D5:77:E1:35:81:B7:23:32:C8:06:2D:FA:9C:F3:9E:51:AE:65:08:85:82 |

## emSign PKI MANAGEMENT'S ASSERTION

eMudhra Technologies Limited ("emSign PKI") operates the Certification Authority (CA) services known as enumerated in Appendix A, and provides Code Signing ("CS") CA services.

The management of emSign PKI is responsible for establishing controls over its CS CA operations, including its CS CA business practices disclosure on its repository, CS key lifecycle management controls, CS certificates lifecycle management controls, CS Signing Authority and CS Timestamp Authority certificate lifecycle management controls. These controls contain monitoring mechanism, and actions are taken to correct deficiencies identified.

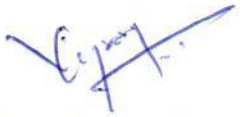
There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, controls placed into operation can only provide reasonable assurance with respect to emSign PKI's Certification Authorities operations.

emSign PKI management has assessed its disclosure of its certificate practices and controls over its CS CA services. Based on that assessment, in emSign PKI management's opinion, in providing its CS Certificate Authority (CA) services at Bangalore, Karnataka, India, as of 19 February 2018, emSign PKI has, in accordance with the WebTrust for Certification Authorities - Publicly Trusted Code Signing Certificates v1.0,:

- disclosed its Code Signing ("CS") certificate lifecycle management business practices in its:
    - emSign PKI Certificate Policy & Certificate Practice Statement (CP/CPS) v1.01

  including its commitment to provide CS certificates in conformity with the CA/Browser Forum Guidelines on the emSign PKI website, and provided such services in accordance with its disclosed practices;
- suitably designed, and placed into operation, controls to provide reasonable assurance that:
    - the integrity of keys and CS certificates it manages is established and protected throughout their lifecycles; and
    - CS subscriber information is properly authenticated (for the registration activities performed by emSign PKI);
- suitably designed, and placed into operation, controls to provide reasonable assurance that:
    - requests for CS Signing Authority and CS Timestamp Authority are properly authenticated; and
    - certificates issued to CS Signing Authorities and CS Timestamp Authorities are not valid for a period longer than specified by the CA/Browser Forum; and

- suitably designed, and placed into operation, controls to provide reasonable assurance that its CS Signing Authority and CS Timestamp Authority are operated in conformity with CA/Browser Forum Guidelines.



**Vijay Kumar M**

**Senior Vice President - Head of Technology**

**26 February 2018**

**eMudhra Technologies Limited.**
Sai Arcade, 3rd Floor, No.56, Outer Ring Road, Devarabeesanahalli, Bangalore – 560103
Phone: +91 80 4227 5300 | Fax: +91 80 4227 5306 | Email: corporate@emudhra.com | Web: www.emudhra.com
CIN - U72200KA2012PLC065153

emudhra Technologies

## Appendix A: Root and Subordinate CAs in Scope

| No | Common Name | Certificate Serial No | Subject Key Identifier | SHA-256 Fingerprint |
|---|---|---|---|---|
| 1 | **emSign Root CA - G2** | 00864DBF0FE35ED77D8ED8 | ED:EC:4D:45:61:18:28:E7:B3:23:28:11:1C:4D:A5:27:0D:5E:EC:F4 | 1A:A0:C2:70:9E:83:1B:D6:E3:B5:12:9A:00:BA:41:F7:EE:EF:02:08:72:F1:E6:50:4B:F0:F6:C3:F2:4F:3A:F3 |
| 2 | emSign CS CA - G2 | 00C084E666596139A1FA9B | 15:86:CA:B6:74:96:17:48:58:34:82:2C:CD:D2:E1:75:9E:AF:44:B7 | C2:E4:D1:76:50:05:D5:CA:36:1D:40:0A:43:4B:43:03:6D:BC:93:1E:C6:D7:B9:9C:17:BE:C0:30:CC:74:CA:7D |
| 3 | **emSign ECC Root CA - G3** | 3CF607A968700EDA8B84 | 7C:5D:02:84:13:D4:CC:8A:9B:81:CE:17:1C:2E:29:1E:9C:48:63:42 | 86:A1:EC:BA:08:9C:4A:8D:3B:BE:27:34:C6:12:BA:34:1D:81:3E:04:3C:F9:E8:A8:62:CD:5C:57:A3:6B:BE:6B |
| 4 | emSign ECC CS CA - G3 | 35CF922FB9008249F89C | E6:1A:AE:5A:79:8C:D0:28:4D:37:E0:9E:6B:C5:2D:5D:B4:6C:F8:EB | 0D:68:69:A2:B4:F5:DF:77:A6:AF:B0:34:22:5E:9B:EF:34:57:43:CF:30:6E:DF:36:EE:35:B9:D0:5A:FA:D8:9C |
| 5 | **emSign Root CA - C2** | 2F0AB76B0DCB4AAF2758 | B3:F7:8A:A4:D6:0F:88:00:59:E8:51:17:4F:D5:7E:EC:86:22:81:9D | 46:CD:08:3B:47:E8:04:02:02:8D:F4:93:96:0E:A1:9C:85:FE:85:19:50:D5:16:5F:1C:7D:A4:FA:A9:51:E2:F8 |
| 6 | emSign CS CA - C2 | 00B4E6BA3BE4B674A36434 | 9A:42:64:A2:E0:62:94:95:C8:12:C3:0F:D5:7E:46:7C:41:2A:B2:2A | B0:E6:BB:9D:6E:7A:94:BC:4A:6B:89:D9:67:43:43:8D:2C:56:5D:BB:0A:69:7A:BB:21:45:7A:CA:22:A1:3C:E4 |
| 7 | **emSign ECC Root CA - C3** | 7B71B68256B8127C9CA8 | FB:5A:48:D0:80:20:40:F2:A8:E9:00:07:69:19:77:A7:E6:C3:F4:CF | BC:4D:80:9B:15:18:9D:78:DB:3E:1D:8C:F4:F9:72:6A:79:5D:A1:64:3C:A5:F1:35:8E:1D:DB:0E:DC:0D:7E:B3 |
| 8 | emSign ECC CS CA - C3 | 00B8973C4278609F2AF2A4 | 74:BF:90:17:0E:A3:70:6E:3C:53:C9:CC:01:51:2E:5B:A7:80:80:BB | A3:AF:D7:23:75:C1:D7:A8:33:0E:62:D5:77:E1:35:81:B7:23:32:C8:06:2D:FA:9C:F3:9E:51:AE:65:08:85:82 |