

## INDEPENDENT ASSURANCE REPORT

*To the management of eMudhra Technologies Limited (“emSign PKI”):*

### Scope

We have engaged, in reasonable assurance engagement, to report on emSign PKI management’s assertion that for its Certification Authority (CA) operations at Bangalore, Karnataka, India, throughout the period 20 February 2018 to 19 September 2018 for its CAs as enumerated in [Appendix A](#), 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 Guidelines 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 Certificate Authorities - Extended Validation SSL v1.6.2](#).

### 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 v1.6.2.

### 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 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 assertion 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 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.

## **Relative effectiveness of controls**

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**

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, throughout the period 20 February 2018 to 19 September 2018, emSign PKI's management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria and Certification Authorities - Extended Validation SSL v1.6.2.

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 - Extended Validation SSL v1.6.2, 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.

A handwritten signature in grey ink that reads 'BDO'.

**BDO Consulting Sdn. Bhd.**

**Kuala Lumpur, Malaysia**

**8 October 2018**



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

No	Common Name	Certificate Serial No	Subject Key Identifier	SHA-256 Fingerprint
1	emSign Root CA - G1	31F5E4620C6C58EDD6D8	FB:EF:0D:86:9E:B0:E3:DD:A9:B9:F1:21:17:7F:3E:FC:F0:77:2B:1A	40:F6:AF:03:46:A9:9A:A1:CD:1D:55:5A:4E:9C:CE:62:C7:F9:63:46:03:EE:40:66:15:83:3D:C8:C8:D0:03:67
2	emSign EV SSL CA - G1	626CB92B237FF82E3F50	B2:9D:CF:41:A7:E9:C3:E0:85:56:40:98:4B:F6:8F:7C:55:29:E7:7E	43:34:EE:B2:CC:11:4F:82:BE:E6:F8:A7:E5:AE:A0:3A:42:EB:2E:1F:70:CB:D6:61:02:E4:14:D7:2F:00:33:B9
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 EV SSL CA - G3	01FE3E6C68DEB BEC263E	D1:AA:B4:D2:D2:25:82:4E:B3:F0:93:60:17:4A:9B:63:7A:F9:1F:0D	01:16:F1:7F:97:CD:EF:4A:DE:2E:63:CF:2C:1B:06:4F:D9:9F:40:4D:2B:91:41:00:BC:24:1F:07:81:85:33:23
5	emSign Root CA - C1	00AECF00BAC4CF32F843B2	FE:A1:E0:70:1E:2A:03:39:52:5A:42:BE:5C:91:85:7A:18:AA:4D:B5	12:56:09:AA:30:1D:A0:A2:49:B9:7A:82:39:CB:6A:34:21:6F:44:DC:AC:9F:39:54:B1:42:92:F2:E8:C8:60:8F
6	emSign EV SSL CA - C1	00BADFD29B3F1E678C6960	C9:71:16:45:43:3B:16:5E:5F:46:FD:EE:35:4D:44:7B:7D:AE:75:07	F6:F1:59:28:6A:14:01:DE:53:97:E2:1A:00:90:53:4A:85:F5:E7:B9:F9:8F:D4:A5:A4:7B:1D:FF:D4:BF:DE:D4
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 EV SSL CA - C3	1B50581F7334B30B2723	48:B7:68:E8:3C:B2:E6:B1:12:44:4C:C4:D7:D3:9A:0B:6F:E9:5A:C6	C0:A5:78:F2:10:9E:6F:42:D3:D9:39:94:8D:EE:AB:72:9B:20:F7:B2:3B:42:37:AB:D8:49:4D:F5:54:CF:98:5C

## Appendix B - Certification Practice Statements in Scope

Certification Practice Statement	Begin Effective Date	End Effective Date
<a href="#">Version 1.01</a>	15 February 2018	4 June 2018
<a href="#">Version 1.02</a>	5 June 2018	25 June 2018
<a href="#">Version 1.03</a>	26 June 2018	-

### EMSIGN PKI MANAGEMENT'S ASSERTION

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

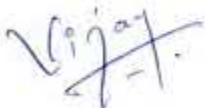
The management of emSign PKI is responsible for establishing and maintaining effective controls over its EV SSL CA operations including its EV SSL CA business practices disclosure in its [repository](#), EV SSL key lifecycle management controls, and EV SSL certificate lifecycle management controls. These 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, Karnataka, India, throughout the period 20 February 2018 to 19 September 2018, 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 v1.6.2](#).



Vijay Kumar M

Senior Vice President - Head of Technology

8 October 2018





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

No	Common Name	Certificate Serial No	Subject Key Identifier	SHA-256 Fingerprint
1	emSign Root CA - G1	31F5E4620C6C58ED D6D8	FB:EF:0D:86:9E:B0:E3 :DD:A9:B9:F1:21:17:7 F:3E:FC:F0:77:2B:1A	40:F6:AF:03:46:A9:9A:A1:C D:1D:55:5A:4E:9C:CE:62:C7 :F9:63:46:03:EE:40:66:15:8 3:3D:C8:C8:D0:03:67
2	emSign EV SSL CA - G1	626CB92B237FF82E 3F50	B2:9D:CF:41:A7:E9:C3 :E0:85:56:40:98:4B:F 6:8F:7C:55:29:E7:7E	43:34:EE:B2:CC:11:4F:82:B E:E6:F8:A7:E5:AE:A0:3A:42 :EB:2E:1F:70:CB:D6:61:02: E4:14:D7:2F:00:33:B9
3	emSign ECC Root CA - G3	3CF607A968700EDA 8B84	7C:5D:02:84:13:D4:C C:8A:9B:81:CE:17:1C: 2E:29:1E:9C:48:63:42	86:A1:EC:BA:08:9C:4A:8D:3 B: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 EV SSL CA - G3	01FE3E6C68DEBBEC 263E	D1:AA:B4:D2:D2:25:8 2:4E:B3:F0:93:60:17: 4A:9B:63:7A:F9:1F:0D	01:16:F1:7F:97:CD:EF:4A:D E:2E:63:CF:2C:1B:06:4F:D9 :9F:40:4D:2B:91:41:00:BC: 24:1F:07:81:85:33:23
5	emSign Root CA - C1	00AECF00BAC4CF32 F843B2	FE:A1:E0:70:1E:2A:03 :39:52:5A:42:BE:5C:9 1:85:7A:18:AA:4D:B5	12:56:09:AA:30:1D:A0:A2:4 9:B9:7A:82:39:CB:6A:34:21 :6F:44:DC:AC:9F:39:54:B1: 42:92:F2:E8:C8:60:8F
6	emSign EV SSL CA - C1	00BADFD29B3F1E67 8C6960	C9:71:16:45:43:3B:16 :5E:5F:46:FD:EE:35:4 D:44:7B:7D:AE:75:07	F6:F1:59:28:6A:14:01:DE:5 3:97:E2:1A:00:90:53:4A:85: F5:E7:B9:F9:8F:D4:A5:A4:7 B:1D:FF:D4:BF:DE:D4
7	emSign ECC Root CA - C3	7B71B68256B8127C 9CA8	FB:5A:48:D0:80:20:40 :F2:A8:E9:00:07:69:1 9:77:A7:E6:C3:F4:CF	BC:4D:80:9B:15:18:9D:78:D B: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 EV SSL CA - C3	1B50581F7334B30B 2723	48:B7:68:E8:3C:B2:E6 :B1:12:44:4C:C4:D7:D 3:9A:0B:6F:E9:5A:C6	C0:A5:78:F2:10:9E:6F:42:D 3:D9:39:94:8D:EE:AB:72:9B :20:F7:B2:3B:42:37:AB:D8: 49:4D:F5:54:CF:98:5C

### Appendix B - Certification Practice Statements in Scope

Certification Practice Statement	Begin Effective Date	End Effective Date
<a href="#">Version 1.01</a>	15 February 2018	4 June 2018
<a href="#">Version 1.02</a>	5 June 2018	25 June 2018
<a href="#">Version 1.03</a>	26 June 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