BDO

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's 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 Principles and Criteria for Certification Authorities - SSL Baseline with Network Security v2.2,:

- disclosed its SSL certificate lifecycle management business practices in its:
  - emSign PKI Certificate Policy & Certification Practice Statement (CP/CPS) v1.01;

  including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirement on the emSign PKI's 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 SSL certificates it manages is established and protected throughout their lifecycles; and
  - SSL 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:
  - 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; and
- suitably designed, and placed into operation, controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum.

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 Principles and Criteria for Certification Authorities - SSL Baseline with Network Security v2.2.

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 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 SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of SSL certificates, and obtaining an understanding of emSign PKI's network and certificate system security to meet the requirements set forth by the CA/Browser Forum;

(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 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 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 Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.2.

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 – SSL Baseline with Network Security v2.2, 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 - 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 SSL CA - G1	217AD58B1C713C002091	34:D1:F7:39:32:45:40:4A:99:2B:7D:89:6A:57:69:AD:95:AF:E3:37	47:B2:EF:BC:36:70:E7:DB:4B:41:F2:2C:51:FC:02:EE:84:FB:2D:BF:30:82:A4:9F:2C:26:88:12:2E:92:10:A1
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 SSL CA - G3	72DDC7E9DCE9B0DCFFC7	13:8D:4C:28:99:E1:62:B7:D2:E0:53:E3:18:D1:62:DC:1C:CA:66:FA	6B:51:D1:DC:F4:EB:7A:EE:42:41:85:CB:1B:95:80:57:4B:39:CB:96:38:63:DE:3E:C1:AD:31:DD:B0:76:CE:9F
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 SSL CA - C1	0086766B7F96DF60C46F8B	FC:C5:15:40:F1:AF:4F:13:B2:98:F2:71:0E:63:15:37:D1:94:6B:74	F9:1A:AC:A0:E4:E5:33:74:7A:08:80:BF:CF:6F:26:72:0D:C1:D0:54:94:C3:93:8D:A6:80:22:90:D5:A0:9B:32
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 SSL CA - C3	5B7D9BB1FD33B9BC1D84	E3:E8:97:1E:BF:C4:3D:3A:B0:DC:F7:1D:9D:3F:5F:2C:B1:6D:EB:6C	A0:61:D4:45:39:97:14:C3:8F:C1:01:A6:E9:AF:BD:B3:81:F1:12:FA:5D:E7:D5:BC:14:90:45:58:D1:ED:32:76

emudhra Technologies

emSign PKI MANAGEMENT'S ASSERTION

eMudhra Technologies Limited ("emSign PKI") operates the Certification Authority ("CA") services listed as in **Appendix A** and provides SSL CA services.

The management of emSign PKI is responsible for establishing controls over its SSL CA operations, including its network and certificate security system controls, its SSL CA business practices disclosure on its website at http://repository.emsign.com/, SSL key lifecycle management controls, and SSL 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, controls placed into operation can only provide reasonable assurance with respect to emSign PKI's CA operations.

emSign PKI's management has assessed its disclosures of its certificate practices and controls over its SSL CA services. Based on that assessment, in emSign PKI's opinion, in providing its SSL Certification Authority (CA) services at Bangalore, Karnataka, India, as of 19 February 2018, emSign PKI has, in accordance with the WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security v2.2,:

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

  including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirement on emSign PKI's 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 SSL certificates it manages is established and protected throughout their lifecycles; and
    - SSL 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:
    - 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; and

- suitably designed, and placed into operation, controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum.

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 - 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 SSL CA - G1	217AD58B1C713C002091	34:D1:F7:39:32:45:40:4A:99:2B:7D:89:6A:57:69:AD:95:AF:E3:37	47:B2:EF:BC:36:70:E7:DB:4B:41:F2:2C:51:FC:02:EE:84:FB:2D:BF:30:82:A4:9F:2C:26:88:12:2E:92:10:A1
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 SSL CA - G3	72DDC7E9DCE9B0DCFFC7	13:8D:4C:28:99:E1:62:B7:D2:E0:53:E3:18:D1:62:DC:1C:CA:66:FA	6B:51:D1:DC:F4:EB:7A:EE:42:41:85:CB:1B:95:80:57:4B:39:CB:96:38:63:DE:3E:C1:AD:31:DD:B0:76:CE:9F
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 SSL CA - C1	0086766B7F96DF60C46F8B	FC:C5:15:40:F1:AF:4F:13:B2:98:F2:71:0E:63:15:37:D1:94:6B:74	F9:1A:AC:A0:E4:E5:33:74:7A:08:80:BF:CF:6F:26:72:0D:C1:D0:54:94:C3:93:8D:A6:80:22:90:D5:A0:9B:32
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 SSL CA - C3	5B7D9BB1FD33B9BC1D84	E3:E8:97:1E:BF:C4:3D:3A:B0:DC:F7:1D:9D:3F:5F:2C:B1:6D:EB:6C	A0:61:D4:45:39:97:14:C3:8F:C1:01:A6:E9:AF:BD:B3:81:F1:12:FA:5D:E7:D5:BC:14:90:45:58:D1:ED:32:76