

## 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, 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 code signing (“EV CS”) certificate lifecycle management business practices in applicable versions of its Certification Practice Statements as enumerated in [Appendix B](#), including its commitment to provide EV 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;
- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and EV CS certificates it manages is established and protected throughout their lifecycles; and
  - EV CS subscriber information is properly authenticated (for the registration activities performed by emSign PKI);
- maintained effective controls to provide reasonable assurance that:
  - requests for EV CS Signing Authorities and EV CS Timestamp Authorities are properly authenticated; and
  - certificates issued to EV CS Signing Authorities and EV CS Timestamp Authorities are not valid for a period longer than specified by the CA/Browser Forum; and
- maintained effective controls to provide reasonable assurance that its EV CS Timestamp Authority is operated in conformity with CA/Browser Forum Guidelines

in accordance with the [WebTrust Principles and Criteria for Certification Authorities - Extended Validation Code Signing v1.4.1](#).

### 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 - Extended Validation Code Signing v1.4.1.

### 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 engagement, 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 CS certificate lifecycle management business practices, including its relevant controls over the issuance, renewal and revocation of EV CS certificates, EV CS Signing Authority certificates, and EV CS Timestamp Authority certificates;
- 2) selectively testing transactions executed in accordance with disclosed EV CS 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 conclusion 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 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 - Extended Validation Code Signing v1.4.1.

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 Code Signing v1.4.1 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 Code Signing 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, appearing to be the initials '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 - 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 EV CS CA - G2	3CA9F3D18C08E50959D5	47:95:C9:61:C0:B0:6A:44:10:2F:1A:35:DA:58:B0:96:AA:F6:4B:8E	69:E2:44:8C:5F:03:EE:DE:5E:C2:C9:07:EF:E9:6C:3D:33:AD:67:9B:49:CD:29:C3:8C:51:82:32:31:21:BE:FF
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 CS CA - G3	23BA23AB486AE7D5C0FE	FA:5C:F7:B7:49:4D:5D:6B:F0:32:28:E1:E5:D5:AD:FA:FA:D5:BC:83	0B:AD:A9:79:B7:14:02:FE:86:06:96:03:2C:F4:0E:9D:2A:3F:41:CC:B5:D0:3B:E3:3F:BB:94:A8:0D:7F:FC:7C
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 EV CS CA - C2	00AE0882F16DBA80375653	5B:9F:D5:1A:1D:04:3E:61:B6:65:17:B8:B0:E9:F5:85:F5:48:2D:17	02:49:98:10:12:10:64:4F:68:FA:E9:11:55:43:A5:E6:D2:6A:6D:B0:D2:C1:03:66:FF:2D:5B:B5:05:D8:87:2D
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 CS CA - C3	6004C5E20B62FDD48C46	A7:6A:A4:7D:5D:0E:18:02:D1:3E:EE:04:D6:DF:21:C7:3A:23:61:9C	CB:21:09:79:92:40:20:97:03:37:AE:32:DA:5C:3F:98:1A:9E:05:71:4E:C2:2B:B1:C3:42:1F:E6:95:E5:15:7A

## 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 Code Signing ("EV CS") CA services.

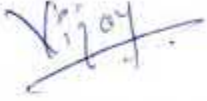
The management of emSign PKI is responsible for establishing and maintaining effective controls over its EV CS CA operations, including its EV CS CA business practices disclosure in its [repository](#), EV CS key lifecycle management controls, EV CS certificate lifecycle management controls, EV CS Signing Authority and EV CS Timestamp Authority 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 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 CS CA services. Based on that assessment, in emSign PKI management's opinion, in providing its EV CS Certification Authority (CA) services at Bangalore, Karnataka, India, throughout the period 20 February 2018 to 19 September emSign PKI has:

- disclosed its extended validation code signing ("EV CS") certificate lifecycle management business practices in applicable versions of its Certification Practice Statement as enumerated in [Appendix B](#), including its commitment to provide EV CS certificates in conformity with the CA/Browser Forum Guidelines on the emSign CA 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 CS certificates it manages is established and protected throughout their lifecycles; and
  - EV CS subscriber information is properly authenticated (for the registration activities performed by emSign PKI);
- maintained effective controls to provide reasonable assurance that:
  - requests for EV CS Signing Authority and EV CS Timestamp Authority certificates are properly authenticated; and
  - certificates issued to EV CS Signing Authorities and EV CS Timestamp Authorities are not valid for a period longer than specified by the CA/Browser Forum; and
- maintained effective controls to provide reasonable assurance that its EV CS Timestamp Authority is operated in conformity with CA/Browser Forum Guidelines

in accordance with the [WebTrust Principles and Criteria for Certification Authorities - Extended Validation Code Signing v1.4.1.](#)



**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 - 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 EV CS CA - G2	3CA9F3D18C08E50959D5	47:95:C9:61:C0:B0:6A:44:10:2F:1A:35:DA:58:B0:96:AA:F6:4B:8E	69:E2:44:8C:5F:03:EE:DE:5E:C2:C9:07:EF:E9:6C:3D:33:AD:67:9B:49:CD:29:C3:8C:51:82:32:31:21:BE:FF
3	emSign ECC Root CA - G3	3CF607A968700EDA8B84	7C:5D:02:84:13:D4:C8:A9B: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 CS CA - G3	23BA23AB486AE7D5C0FE	FA:5C:F7:B7:49:4D:5D:6B:F0:32:28:E1:E5:D5:AD:FA:FA:D5:BC:83	0B:AD:A9:79:B7:14:02:FE:86:06:96:03:2C:F4:0E:9D:2A:3F:41:CC:B5:D0:3B:E3:3F:BB:94:A8:0D:7F:FC:7C
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 EV CS CA - C2	00AE0882F16DBA80375653	5B:9F:D5:1A:1D:04:3E:61:B6:65:17:B8:B0:E9:F5:85:F5:48:2D:17	02:49:98:10:12:10:64:4F:68:FA:E9:11:55:43:A5:E6:D2:6A:6D:B0:D2:C1:03:66:FF:2D:5B:B5:05:D8:87:2D
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 CS CA - C3	6004C5E20B62FDD48C46	A7:6A:A4:7D:5D:0E:18:02:D1:3E:EE:04:D6:DF:21:C7:3A:23:61:9C	CB:21:09:79:92:40:20:97:03:37:AE:32:DA:5C:3F:98:1A:9E:05:71:4E:C2:2B:B1:C3:42:1F:E6:95:E5:15:7A

### 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	-