

INDEPENDENT ASSURANCE REPORT

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

Scope

We have 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 Principles and Criteria for Certification Authorities v2.1](#),:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
 - [emSign PKI Certificate Policy & Certificate Practice Statement \(CP/CPS\) v1.01](#);
- suitably designed, and placed into operations, controls to provide reasonable assurance that:
 - emSign PKI provides its services in accordance with its Certificate Practice Statement;
- suitably designed, and placed into operations, controls to provide reasonable assurance that:
 - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
 - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
 - subscriber information is properly authenticated (for the registration activities performed by emSign PKI); and
 - subordinate CA certificate requests are accurate, authenticated, and approved; and
- suitably designed, and placed into operations, 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 system integrity.

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 v2.1.

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 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 key and certificate lifecycle management business practices and its controls over key and certificate integrity, over the authenticity and confidentiality of subscriber and relying party information, over the continuity of key and certificate lifecycle management operations and over development, maintenance and operation of system integrity;
- (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 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's management's assertion, as referred to above, is fairly stated, in all materials respects in accordance with the WebTrust Principles and Criteria for Certification Authority v2.1.

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 v2.1, nor the suitability of any of emSign PKI's services for any customer's intended purpose.

A handwritten signature in black ink, appearing to be 'S. Yusoff', written in a cursive style.

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:B 9:F1:21:17:7F:3E:FC:F0:77:2B: 1A | 40:F6:AF:03:46:A9:A1:CD:1D:55:5 A: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:99:2 B:7D:89:6A:57:69:AD:95:AF:E3 :37 | 47:B2:EF:BC:36:70:E7:DB:4B:41:F2:2 C:51:FC:02:EE:84:FB:2D:BF:30:82:A4: 9F:2C:26:88:12:2E:92:10:A1 |
| 3 | emSign EV SSL CA - G1 | 626CB92B237FF82E3F50 | B2:9D:CF:41:A7:E9:C3:E0:85:5 6:40:98:4B: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:D6:6 1:02:E4:14:D7:2F:00:33:B9 |
| 4 | emSign Class 1 CA - G1 | 00D59B7C9B36A2D44922EA | DC:60:8F:0A:DE:B1:99:84:9B:8 4:40:03:E3:75:03:32:03:80:00: 90 | CF:6D:03:33:D0:BE:2C:69:A4:2D:45:3 9:60:DE:E9:E1:09:D9:E8:84:3E:A3:06: 1A:16:71:D6:EA:F8:5E:B7:D8 |
| 5 | emSign Class 2 CA - G1 | 3C5BDA55C0A236A744CD | E6:DD:0D:B9:9B:D2:15:40:CF: 23:08:2D:6C:19:B8:5C:68:32:5 2:32 | 63:A8:36:9D:C8:24:A4:2B:C7:AE:6E:E 5:D2:6A:AF:D3:2D:F4:AF:67:7C:A1:8B :94:1B:7A:57:E3:3B:1E:35:59 |
| 6 | emSign Class 3 CA - G1 | 00A08870825A326BED9611 | 5C:A5:9C:41:EF:6E:41:61:46:7 9:2C:DF:D8:55:45:05:D5:A7:1A :86 | 42:DA:1C:56:2F:80:E4:6D:A7:A3:21:2 4:4E:FC:23:D0:FA:A9:FE:BB:B7:AA:03 :77:D9:6B:42:D9:E8:8A:B2:00 |
| 7 | emSign Device CA - G1 | 0465835247364A904A8E | 0B:93:78:E2:E0:35:07:6D:DF:8 6:77:8F:8C:51:8D:E3:35:7C:A9 :77 | 4C:91:98:B6:73:55:08:58:79:9A:D2:74 :4C:C0:83:C1:BA:00:27:E7:7D:3B:8F: D6:D5:6C:F5:36:20:D0:99:E2 |
| 8 | emSign Root CA - G2 | 00864DBF0FE35ED77D8ED8 | ED:EC:4D:45:61:18:28:E7:B3:2 3:28:11:1C:4D:A5:27:0D:5E:EC :F4 | 1A:A0:C2:70:9E:83:1B:D6:E3:B5:12:9 A:00:BA:41:F7:EE:EF:02:08:72:F1:E6: 50:4B:F0:F6:C3:F2:4F:3A:F3 |
| 9 | emSign CS CA - G2 | 00C084E666596139A1FA9B | 15:86:CA:B6:74:96:17:48:58:3 4:82:2C:CD:D2:E1:75:9E:AF:44 :B7 | C2:E4:D1:76:50:05:D5:CA:36:1D:40:0 A:43:4B:43:03:6D:BC:93:1E:C6:D7:B9 :9C:17:BE:C0:30:CC:74:CA:7D |
| 10 | emSign EV CS CA - G2 | 3CA9F3D18C08E50959D5 | 47:95:C9:61:C0:B0:6A:44:10:2 F:1A:35:DA:58:B0:96:AA:F6:4B :8E | 69:E2:44:8C:5F:03:EE:DE:5E:C2:C9:0 7:EF:E9:6C:3D:33:AD:67:9B:49:CD:29 :C3:8C:51:82:32:31:21:BE:FF |

| | | | |
|----|----------------------------------|------------------------|---|
| 11 | emSign Time Stamping CA - G2 | 00BA9E35E51ECFAC6C4740 | C0:0F:C1:F7:CF:9E:26:FF:8B:7 1:4A:CB:EC:F6:09:9F:2E:FA:C4 :A1 7C:5D:02:84:13:D4:CC:8A:9B:8 1:CE:17:1C:2E:29:1E:9C:48:63 :42 13:8D:4C:28:99:E1:62:B7:D2:E 0:53:E3:18:D1:62:DC:1C:CA:66 :FA D1:AA:B4:D2:D2:25:82:4E:B3:F 0:93:60:17:4A:9B:63:7A:F9:1F :0D E6:1A:AE:5A:79:8C:D0:28:4D:3 7:E0:9E:6B:C5:2D:5D:B4:6C:F8 :EB FA:5C:F7:B7:49:4D:5D:6B:F0:3 2:28:E1:E5:D5:AD:FA:FA:D5:B C:83 46:BE:80:C3:C8:27:FE:EC:9B:5 8:2B:1A:62:5D:B2:D5:D1:02:38 :68 E0:16:FE:BD:C4:E1:65:C6:A5:9 9:4C:89:5E:71:8E:D4:5D:67:F1 :FD 22:62:4A:BC:7E:6D:A1:30:B7:2 A:C9:95:7E:2A:23:DE:3D:27:F3 :8D F1:DD:23:B0:F4:F1:1D:EB:24:3 5:64:63:3C:10:A9:D9:54:8F:08 :3F A5:AC:F9:1F:5A:25:8E:10:B0:2 9:DA:19:00:26:86:E8:A1:E6:E8 :D9 FE:A1:E0:70:1E:2A:03:39:52:5 |
| 12 | emSign ECC Root CA - G3 | 3CF607A968700EDA8B84 | C3:BE:06:C6:B0:A9:23:34:42:31:80:E9 :5E:A1:E6:83:AA:B9:C3:B7:D0:F5:CB: 8A:4F:51:FB:C1:00:6F:3D:C0 86:A1:EC:BA:08:9C:4A:8D:3B:BE:27:3 4:C6:12:BA:34:1D:81:3E:04:3C:F9:E8: A8:62:CD:5C:57:A3:6B:BE:6B 6B:51:D1:DC:F4:EB:7A:EE:42:41:85:C B:1B:95:80:57:4B:39:CB:96:38:63:DE: 3E:C1:AD:31:DD:B0:76:CE:9F 01:16:F1:7F:97:CD:EF:4A:DE:2E:63:C F:2C:1B:06:4F:D9:9F:40:4D:2B:91:41: 00:BC:24:1F:07:81:85:33:23 0D:68:69:A2:B4:F5:DF:77:A6:AF:B0:3 4:22:5E:9B:EF:34:57:43:CF:30:6E:DF: 36:EE:35:B9:D0:5A:FA:D8:9C 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 AB:A6:A6:5D:CE:89:55:BA:F0:68:5A:B 8:88:09:B7:69:9C:17:44:96:EF:9E:E9: 91:53:32:51:49:4F:43:CE:10 4E:9B:73:15:67:17:7E:17:76:A9:6D:66 :D9:12:0B:3D:EB:28:B8:00:93:7E:A4:6 6:25:65:B3:EF:5E:C8:00:0B 70:66:A0:F4:2F:53:0E:0D:B5:AF:EE:72 :A3:B0:4D:E6:14:E7:D2:30:5C:67:D1:2 C:75:6B:B2:15:E3:7C:B9:75 C4:22:AB:86:C1:72:9E:88:9F:BC:AF:5 C:D7:3F:21:7E:03:C2:9F:E2:AC:50:21: 2F:45:13:07:D9:15:86:9F:47 70:B9:BA:59:54:12:CF:86:14:B7:67:47 :FD:68:3C:CA:27:59:F4:26:42:16:48:3 4:FB:EF:DD:88:50:5C:4F:1C 12:56:09:AA:30:1D:A0:A2:49:B9:7A:8 |
| 13 | emSign ECC SSL CA - G3 | 72DDC7E9DCE9B0DCFFC7 | |
| 14 | emSign ECC EV SSL CA - G3 | 01FE3E6C68DEBBEC263E | |
| 15 | emSign ECC CS CA - G3 | 35CF922FB9008249F89C | |
| 16 | emSign ECC EV CS CA - G3 | 23BA23AB486AE7D5C0FE | |
| 17 | emSign ECC Class 1 CA - G3 | 00FB1E21982EB1B55C5925 | |
| 18 | emSign ECC Class 2 CA - G3 | 23E1BA02DFF3E900EDDD | |
| 19 | emSign ECC Class 3 CA - G3 | 00B8EB258324DB08ACC2F5 | |
| 20 | emSign ECC Time stamping CA - G3 | 0084A863D6F61818464D34 | |
| 21 | emSign ECC Device CA - G3 | 00876282A8FD758C391EC3 | |
| 22 | emSign Root CA - C1 | 00AECF00BAC4CF32F843B2 | |

| | | | | |
|----|------------------------------|------------------------|--|--|
| 23 | emSign SSL CA - C1 | 0086766B7F96DF60C46F8B | A:42:BE:5C:91:85:7A:18:AA:4D :B5 FC:C5:15:40:F1:AF:4F:13:B2:9 8:F2:71:0E:63:15:37:D1:94:6B: 74 C9:71:16:45:43:3B:16:5E:5F:4 6:FD:EE:35:4D:44:7B:7D:AE:75 :07 3B:0E:EF:29:3B:11:48:29:2C:0 1:15:D1:8E:7B:79:69:05:7B:C9 :52 26:68:C0:F3:FC:40:1C:F7:CA:1 2:4B:4F:92:C3:8B:14:94:48:3B :FD 7B:9E:A6:C5:27:7E:64:97:AB:8 4:01:3A:EA:26:96:6B:92:4E:87 :E1 92:C5:7C:AD:63:20:E5:4C:23:C F:69:11:CF:A7:87:FB:81:F4:91 :F8 B3:F7:8A:A4:D6:0F:88:00:59:E 8:51:17:4F:D5:7E:EC:86:22:81 :9D 9A:42:64:A2:E0:62:94:95:C8:1 2:C3:0F:D5:7E:46:7C:41:2A:B2 :2A 5B:9F:D5:1A:1D:04:3E:61:B6:6 5:17:B8:B0:E9:F5:85:F5:48:2D :17 C1:41:93:9D:9D:EF:34:CC:72:F D:D8:40:A6:1E:D6:B7:2A:43:A A:E9 FB:5A:48:D0:80:20:40:F2:A8:E 9:00:07:69:19:77:A7:E6:C3:F4: | 2:39:CB:6A:34:21:6F:44:DC:AC:9F:39: 54:B1:42:92:F2:E8:C8:60:8F F9:1A:AC:A0:E4:E5:33:74:7A:08:80:B F:CF:6F:26:72:0D:C1:D0:54:94:C3:93: 8D:A6:80:22:90:D5:A0:9B:32 F6:F1:59:28:6A:14:01:DE:53:97:E2:1A :00:90:53:4A:85:F5:E7:B9:F9:8F:D4:A 5:A4:7B:1D:FF:D4:BF:DE:D4 0E:F7:B8:63:FA:AB:C3:84:A6:94:FF:6 3:2D:AA:F9:BD:31:CE:D2:3E:92:46:55 :9A:59:EC:D7:47:27:54:CC:E6 05:B3:0B:3F:C4:4F:85:75:33:4B:D8:12 :EF:9F:A8:A5:2A:75:74:3E:19:BC:35:A 5:BE:39:12:EC:A6:2C:46:69 69:B0:DD:09:B9:8F:36:A9:CC:7B:D7:F F:E8:A0:0D:CD:31:9A:5F:C9:47:C9:C8 :AF:72:C9:28:94:D8:E8:10:92 D0:34:B1:87:51:BE:E1:0A:AA:F9:4C:2 F:14:35:0D:3F:65:4E:5B:93:4D:0D:DA: 59:2B:31:E5:81:87:A4:89:52 46:CD:08:3B:47:E8:04:02:02:8D:F4:93 :96:0E:A1:9C:85:FE:85:19:50:D5:16:5 F:1C:7D:A4:FA:A9:51:E2:F8 B0:E6:BB:9D:6E:7A:94:BC:4A:6B:89:D 9:67:43:43:8D:2C:56:5D:BB:0A:69:7A: BB:21:45:7A:CA:22:A1:3C:E4 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 57:1F:C7:06:54:AB:8C:1A:A3:B4:A2:6 1:A3:D5:05:FA:E1:0B:C4:55:8F:A1:7C: 72:84:9B:6B:98:BC:84:5C:AE BC:4D:80:9B:15:18:9D:78:DB:3E:1D:8 C:F4:F9:72:6A:79:5D:A1:64:3C:A5:F1: |
| 24 | emSign EV SSL CA - C1 | 00BADFD29B3F1E678C6960 | | |
| 25 | emSign Class 1 CA - C1 | 7E065336C075C7998B63 | | |
| 26 | emSign Class 2 CA - C1 | 1A5C82DEDCBC6A153030 | | |
| 27 | emSign Class 3 CA - C1 | 00B474F64D86392189496E | | |
| 28 | emSign Device CA - C1 | 00B19BE3081E2D97B5BFCB | | |
| 29 | emSign Root CA - C2 | 2F0AB76B0DCB4AAF2758 | | |
| 30 | emSign CS CA - C2 | 00B4E6BA3BE4B674A36434 | | |
| 31 | emSign EV CS CA - C2 | 00AE0882F16DBA80375653 | | |
| 32 | emSign Time Stamping CA - C2 | 63720D6AB070BF2A157D | | |
| 33 | emSign ECC Root CA - C3 | 7B71B68256B8127C9CA8 | | |

| | | | | |
|----|----------------------------------|------------------------|---|---|
| 34 | emSign ECC SSL CA - C3 | 5B7D9BB1FD33B9BC1D84 | CF E3:E8:97:1E:BF:C4:3D:3A:B0:D C:F7:1D:9D:3F:5F:2C:B1:6D:EB :6C 48:B7:68:E8:3C:B2:E6:B1:12:4 4:4C:C4:D7:D3:9A:0B:6F:E9:5A :C6 74:BF:90:17:0E:A3:70:6E:3C:5 3:C9:CC:01:51:2E:5B:A7:80:80 :BB A7:6A:A4:7D:5D:0E:18:02:D1:3 E:EE:04:D6:DF:21:C7:3A:23:61 :9C 8C:D9:9F:A0:21:35:3E:FC:B4:3 A:99:6C:2E:F2:0A:29:6F:F0:EC :92 56:4C:89:B8:25:C8:98:EE:BD:F 2:7C:62:2D:AE:69:39:3A:B6:17 :2C F1:66:AB:96:8C:A4:0D:D2:26:6 2:33:2F:9A:55:09:5D:D9:E6:48 :4A 0B:BF:47:0B:3D:65:F5:4E:73:4 C:1C:AD:1E:4E:67:52:09:2D:26 :BD 04:F6:54:AF:2E:B4:DD:A7:44:1 E:CA:F0:63:9C:24:15:43:58:2F :CF | 35:8E:1D:DB:0E:DC:0D:7E:B3 A0:61:D4:45:39:97:14:C3:8F:C1:01:A 6:E9:AF:BD:B3:81:F1:12:FA:5D:E7:D5: BC:14:90:45:58:D1:ED:32:76 C0:A5:78:F2:10:9E:6F:42:D3:D9:39:94 :8D:EE:AB:72:9B:20:F7:B2:3B:42:37:A B:D8:49:4D:F5:54:CF:98:5C A3:AF:D7:23:75:C1:D7:A8:33:0E:62:D 5:77:E1:35:81:B7:23:32:C8:06:2D:FA: 9C:F3:9E:51:AE:65:08:85:82 CB:21:09:79:92:40:20:97:03:37:AE:32 :DA:5C:3F:98:1A:9E:05:71:4E:C2:2B:B 1:C3:42:1F:E6:95:E5:15:7A FA:D2:E9:86:49:F1:C6:06:15:0F:55:26 :9E:BC:03:5A:EA:22:FF:AC:13:1D:E6:4 B:A6:90:0C:75:D8:44:7B:7E DB:45:91:F8:78:F6:67:2F:5B:70:73:3A :66:AD:7C:95:37:B9:7E:6F:0A:F5:CA:4 9:AA:B8:EC:B2:CE:02:F8:6B 5A:9A:03:F2:D3:FE:58:9B:E6:3C:DA:1 1:82:0A:9F:25:F0:74:C9:20:34:F5:1C: 04:7D:34:22:6D:25:2E:C0:25 71:D2:EE:4D:DA:25:1D:92:44:F7:CE:7 C:6D:47:8E:C5:52:D4:24:EF:71:9F:02: B7:10:30:F2:82:1B:6B:C8:53 3D:45:11:D0:A8:0A:A9:49:A6:D9:9B:2 5:3A:17:34:71:79:7C:44:59:18:7A:63: 29:E7:36:C3:7C:B5:49:3E:46 |
| 35 | emSign ECC EV SSL CA - C3 | 1B50581F7334B30B2723 | | |
| 36 | emSign ECC CS CA - C3 | 00B8973C4278609F2AF2A4 | | |
| 37 | emSign ECC EV CS CA - C3 | 6004C5E20B62FDD48C46 | | |
| 38 | emSign ECC Class 1 CA - C3 | 00BD6A0796AB3F8955521E | | |
| 39 | emSign ECC Class 2 CA - C3 | 00D1142766698BFCDEDA02 | | |
| 40 | emSign ECC Class 3 CA - C3 | 3D12A1CF78258D580854 | | |
| 41 | emSign ECC Time stamping CA - C3 | 00B94B49C6436D72090201 | | |
| 42 | emSign ECC Device CA - C3 | 00D9365F15842A1D0689C3 | | |

emSign PKI MANAGEMENT'S ASSERTION

eMudhra Technologies Limited ("emSign PKI") operates the Certification Authority (CA) services known as enumerated in Appendix A, and provides the following CA services:

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation
- Subscriber key generation and management

The management of emSign PKI is responsible for establishing controls over its CA operations, including its CA business practices disclosure on its repository, CA business practices management, CA environmental controls, CA key lifecycle management controls, subscriber key lifecycle management controls, certificate lifecycle management controls, and subordinate CA 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 Certification Authority operations.

emSign PKI management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in emSign PKI management's opinion, in providing its Certification Authority (CA) services at Bangalore, Karnataka, India as of 19 February 2018, emSign PKI has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
 - emSign PKI Certificate Policy & Certificate Practice Statement (CP/CPS) v1.01;
- suitably designed, and placed into operations, controls to provide reasonable assurance that:
 - emSign PKI provides its services in accordance with its Certificate Practice Statement;

eMudhra Technologies Limited.

- suitably designed, and placed into operations, controls to provide reasonable assurance that:
 - the integrity of keys and certificates it manages is established and protected through their lifecycles;
 - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
 - subscriber information is properly authenticated (for the registration activities performed by emSign PKI); and
 - subordinate CA certificate requests are accurate, authenticated, and approved; and
- 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

in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.1, including the following:

CA Business Practices Disclosure

- Certificate Policy & Certificate Practice Statement (CP/CPS)

CA Business Practices Management

- CP/CPS Management

CA Environmental Controls

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical & Environmental Security
- Operations Management
- System Access Management
- System Development and Maintenance
- Business Continuity Management
- Monitoring and Compliance

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

- Audit Logging

CA Key Lifecycle Management Controls

- CA Key Generation
- CA Key Storage, Backup and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Archival and Destruction
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management

Subscriber Key Lifecycle Management Controls

- CA-Provided Subscriber Key Generation Services
- CA-Provided Subscriber Key Storage and Recovery Services
- Requirements for Subscriber Key Management

Certificate Lifecycle Management Controls

- Subscriber Registration
- Certificate Renewal
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

Subordinate CA Certificate Lifecycle Management Controls

- Subordinate CA Certificate Lifecycle Management



Vijay Kumar M

Senior Vice President - Head of Technology

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 | 31F5E4620C6C58E DD6D8 | FB:EF:0D:86:9E:B0: E3:DD:A9:B9:F1:21: 17:7F:3E:FC:F0:77:2 B:1A | 40:F6:AF:03:46:A9:9A:A1 :CD:1D:55:5A:4E:9C:CE:6 2:C7:F9:63:46:03:EE:40:6 6:15:83:3D:C8:C8:D0:03: 67 |
| 2 | emSign SSL CA - G1 | 217AD58B1C713C 002091 | 34:D1:F7:39:32:45:4 0:4A:99:2B:7D:89:6 A:57:69:AD:95:AF:E 3:37 | 47:B2:EF:BC:36:70:E7:DB :4B:41:F2:2C:51:FC:02:E E:84:FB:2D:BF:30:82:A4: 9F:2C:26:88:12:2E:92:10: A1 |
| 3 | emSign EV SSL CA - G1 | 626CB92B237FF82 E3F50 | B2:9D:CF:41:A7:E9: C3:E0:85:56:40:98:4 B:F6:8F:7C:55:29:E7 :7E | 43:34:EE:B2:CC:11:4F:82 :BE:E6:F8:A7:E5:AE:A0:3 A:42:EB:2E:1F:70:CB:D6: 61:02:E4:14:D7:2F:00:33: B9 |
| 4 | emSign Class 1 CA - G1 | 00D59B7C9B36A2 D44922EA | DC:60:8F:0A:DE:B1: 99:84:9B:84:40:03:E 3:75:03:32:03:80:00 :90 | CF:6D:03:33:D0:BE:2C:69 :A4:2D:45:39:60:DE:E9:E 1:09:D9:E8:84:3E:A3:06:1 A:16:71:D6:EA:F8:5E:B7: D8 |
| 5 | emSign Class 2 CA - G1 | 3C5BDA55C0A236 A744CD | E6:DD:0D:B9:9B:D2: 15:40:CF:23:08:2D: 6C:19:B8:5C:68:32: 52:32 | 63:A8:36:9D:C8:24:A4:2B :C7:AE:6E:E5:D2:6A:AF:D 3:2D:F4:AF:67:7C:A1:8B: 94:1B:7A:57:E3:3B:1E:35: 59 |
| 6 | emSign Class 3 CA - G1 | 00A08870825A326 BED9611 | 5C:A5:9C:41:EF:6E: 41:61:46:79:2C:DF: D8:55:45:05:D5:A7: 1A:86 | 42:DA:1C:56:2F:80:E4:6D :A7:A3:21:24:4E:FC:23:D 0:FA:A9:FE:BB:B7:AA:03: 77:D9:6B:42:D9:E8:8A:B2 :00 |
| 7 | emSign Device CA - G1 | 0465835247364A9 04A8E | 0B:93:78:E2:E0:35:0 7:6D:DF:86:77:8F:8 C:51:8D:E3:35:7C:A 9:77 | 4C:91:98:B6:73:55:08:58: 79:9A:D2:74:4C:C0:83:C1 :BA:00:27:E7:7D:3B:8F:D 6:D5:6C:F5:36:20:D0:99: E2 |
| 8 | emSign Root CA - G2 | 00864DBF0FE35ED 77D8ED8 | ED:EC:4D:45:61:18: 28:E7:B3:23:28:11:1 C:4D:A5:27:0D:5E:E C:F4 | 1A:A0:C2:70:9E:83:1B:D6 :E3:B5:12:9A:00:BA:41:F 7:EE:EF:02:08:72:F1:E6:5 0:4B:F0:F6:C3:F2:4F:3A:F 3 |
| 9 | emSign CS CA - G2 | 00C084E66659613 9A1FA9B | 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:43:0 3:6D:BC:93:1E:C6:D7:B9: 9C:17:BE:C0:30:CC:74:CA :7D |
| 10 | emSign EV CS CA - G2 | 3CA9F3D18C08E5 0959D5 | 47:95:C9:61:C0:B0: 6A:44:10:2F:1A:35: | 69:E2:44:8C:5F:03:EE:DE :5E:C2:C9:07:EF:E9:6C:3 |

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

| | | | | |
|--------|-------------------------------------|----------------------------|---|---|
| | | | DA:58:B0:96:AA:F6: 4B:8E | D:33:AD:67:9B:49:CD:29: C3:8C:51:82:32:31:21:BE :FF |
| 1 1 | emSign Time Stamping CA - G2 | 00BA9E35E51ECF AC6C4740 | C0:0F:C1:F7:CF:9E: 26:FF:8B:71:4A:CB: EC:F6:09:9F:2E:FA: C4:A1 | C3:BE:06:C6:B0:A9:23:34 :42:31:80:E9:5E:A1:E6:83 :AA:B9:C3:B7:D0:F5:CB:8 A:4F:51:FB:C1:00:6F:3D: C0 |
| 1 2 | emSign ECC Root CA - G3 | 3CF607A968700ED A8B84 | 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:3 4:1D:81:3E:04:3C:F9:E8: A8:62:CD:5C:57:A3:6B:BE :6B |
| 1 3 | emSign ECC SSL CA - G3 | 72DDC7E9DCE9B0 DCFFC7 | 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:3 E:C1:AD:31:DD:B0:76:CE: 9F |
| 1 4 | emSign ECC EV SSL CA - G3 | 01FE3E6C68DEBB EC263E | D1:AA:B4:D2:D2:25: 82:4E:B3:F0:93:60:1 7:4A:9B:63:7A:F9:1 F:0D | 01:16:F1:7F:97:CD:EF:4A :DE:2E:63:CF:2C:1B:06:4 F:D9:9F:40:4D:2B:91:41: 00:BC:24:1F:07:81:85:33: 23 |
| 1 5 | emSign ECC CS CA - G3 | 35CF922FB900824 9F89C | 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:E F:34:57:43:CF:30:6E:DF:3 6:EE:35:B9:D0:5A:FA:D8: 9C |
| 1 6 | emSign ECC EV CS CA - G3 | 23BA23AB486AE7 D5C0FE | 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:E 3:3F:BB:94:A8:0D:7F:FC: 7C |
| 1 7 | emSign ECC Class 1 CA - G3 | 00FB1E21982EB1B 55C5925 | 46:BE:80:C3:C8:27: FE:EC:9B:58:2B:1A: 62:5D:B2:D5:D1:02: 38:68 | AB:A6:A6:5D:CE:89:55:BA :F0:68:5A:B8:88:09:B7:69 :9C:17:44:96:EF:9E:E9:91 :53:32:51:49:4F:43:CE:10 |
| 1 8 | emSign ECC Class 2 CA - G3 | 23E1BA02DFF3E90 0EDDD | E0:16:FE:BD:C4:E1: 65:C6:A5:99:4C:89: 5E:71:8E:D4:5D:67: F1:FD | 4E:9B:73:15:67:17:7E:17: 76:A9:6D:66:D9:12:0B:3D :EB:28:B8:00:93:7E:A4:66 :25:65:B3:EF:5E:C8:00:0B |
| 1 9 | emSign ECC Class 3 CA - G3 | 00B8EB258324DB0 8ACC2F5 | 22:62:4A:BC:7E:6D: A1:30:B7:2A:C9:95: 7E:2A:23:DE:3D:27: F3:8D | 70:66:A0:F4:2F:53:0E:0D: B5:AF:EE:72:A3:B0:4D:E6 :14:E7:D2:30:5C:67:D1:2 C:75:6B:B2:15:E3:7C:B9: 75 |
| 2 0 | emSign ECC Time stamping CA - G3 | 0084A863D6F6181 8464D34 | F1:DD:23:B0:F4:F1: 1D:EB:24:35:64:63:3 C:10:A9:D9:54:8F:0 8:3F | C4:22:AB:86:C1:72:9E:88 :9F:BC:AF:5C:D7:3F:21:7 E:03:C2:9F:E2:AC:50:21: 2F:45:13:07:D9:15:86:9F: 47 |

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

| | | | | |
|--------|------------------------------|----------------------------|---|---|
| 2 1 | emSign ECC Device CA - G3 | 00876282A8FD758 C391EC3 | A5:AC:F9:1F:5A:25: 8E:10:B0:29:DA:19: 00:26:86:E8:A1:E6:E 8:D9 | 70:B9:BA:59:54:12:CF:86 :14:B7:67:47:FD:68:3C:C A:27:59:F4:26:42:16:48:3 4:FB:EF:DD:88:50:5C:4F: 1C |
| 2 2 | emSign Root CA - C1 | 00AECF00BAC4CF 32F843B2 | FE:A1:E0:70:1E:2A: 03:39:52:5A:42:BE:5 C:91:85:7A:18:AA:4 D:B5 | 12:56:09:AA:30:1D:A0:A2 :49:B9:7A:82:39:CB:6A:3 4:21:6F:44:DC:AC:9F:39: 54:B1:42:92:F2:E8:C8:60: 8F |
| 2 3 | emSign SSL CA - C1 | 0086766B7F96DF6 0C46F8B | FC:C5:15:40:F1:AF: 4F:13:B2:98:F2:71:0 E: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:C3:93:8 D:A6:80:22:90:D5:A0:9B: 32 |
| 2 4 | emSign EV SSL CA - C1 | 00BADFD29B3F1E 678C6960 | C9:71:16:45:43:3B:1 6:5E: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:D 4 |
| 2 5 | emSign Class 1 CA - C1 | 7E065336C075C79 98B63 | 3B:0E:EF:29:3B:11:4 8:29:2C:01:15:D1:8 E:7B:79:69:05:7B:C 9:52 | 0E:F7:B8:63:FA:AB:C3:84 :A6:94:FF:63:2D:AA:F9:B D:31:CE:D2:3E:92:46:55: 9A:59:EC:D7:47:27:54:CC :E6 |
| 2 6 | emSign Class 2 CA - C1 | 1A5C82DEDCBC6A 153030 | 26:68:C0:F3:FC:40: 1C:F7:CA:12:4B:4F: 92:C3:8B:14:94:48:3 B:FD | 05:B3:0B:3F:C4:4F:85:75: 33:4B:D8:12:EF:9F:A8:A5 :2A:75:74:3E:19:BC:35:A 5:BE:39:12:EC:A6:2C:46: 69 |
| 2 7 | emSign Class 3 CA - C1 | 00B474F64D86392 189496E | 7B:9E:A6:C5:27:7E: 64:97:AB:84:01:3A: EA:26:96:6B:92:4E:8 7:E1 | 69:B0:DD:09:B9:8F:36:A9 :CC:7B:D7:FF:E8:A0:0D:C D:31:9A:5F:C9:47:C9:C8: AF:72:C9:28:94:D8:E8:10 :92 |
| 2 8 | emSign Device CA - C1 | 00B19BE3081E2D9 7B5BFCB | 92:C5:7C:AD:63:20: E5:4C:23:CF:69:11: CF:A7:87:FB:81:F4: 91:F8 | D0:34:B1:87:51:BE:E1:0A :AA:F9:4C:2F:14:35:0D:3 F:65:4E:5B:93:4D:0D:DA: 59:2B:31:E5:81:87:A4:89: 52 |
| 2 9 | emSign Root CA - C2 | 2F0AB76B0DCB4A AF2758 | B3:F7:8A:A4:D6:0F: 88:00:59:E8:51:17:4 F:D5:7E:EC:86:22:8 1:9D | 46:CD:08:3B:47:E8:04:02 :02:8D:F4:93:96:0E:A1:9 C:85:FE:85:19:50:D5:16:5 F:1C:7D:A4:FA:A9:51:E2: F8 |
| 3 0 | emSign CS CA - C2 | 00B4E6BA3BE4B67 4A36434 | 9A:42:64:A2:E0:62:9 4:95:C8:12:C3:0F:D 5:7E:46:7C:41:2A:B 2:2A | B0:E6:BB:9D:6E:7A:94:BC :4A:6B:89:D9:67:43:43:8 D:2C:56:5D:BB:0A:69:7A: BB:21:45:7A:CA:22:A1:3C :E4 |

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

| | | | | |
|--------|---------------------------------|----------------------------|---|---|
| 3 1 | emSign EV CS CA - C2 | 00AE0882F16DBA8 0375653 | 5B:9F:D5:1A:1D:04: 3E:61:B6:65:17:B8:B 0: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:D8:87:2 D |
| 3 2 | emSign Time Stamping CA - C2 | 63720D6AB070BF2 A157D | C1:41:93:9D:9D:EF: 34:CC:72:FD:D8:40: A6:1E:D6:B7:2A:43: AA:E9 | 57:1F:C7:06:54:AB:8C:1A :A3:B4:A2:61:A3:D5:05:F A:E1:0B:C4:55:8F:A1:7C: 72:84:9B:6B:98:BC:84:5C :AE |
| 3 3 | emSign ECC Root CA - C3 | 7B71B68256B8127 C9CA8 | FB:5A:48:D0:80:20: 40:F2:A8:E9:00:07:6 9:19:77:A7:E6:C3:F 4:CF | BC:4D:80:9B:15:18:9D:78 :DB:3E:1D:8C:F4:F9:72:6 A:79:5D:A1:64:3C:A5:F1: 35:8E:1D:DB:0E:DC:0D:7E :B3 |
| 3 4 | emSign ECC SSL CA - C3 | 5B7D9BB1FD33B9 BC1D84 | 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:B 3:81:F1:12:FA:5D:E7:D5: BC:14:90:45:58:D1:ED:32 :76 |
| 3 5 | emSign ECC EV SSL CA - C3 | 1B50581F7334B30 B2723 | 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:A B:D8:49:4D:F5:54:CF:98: 5C |
| 3 6 | emSign ECC CS CA - C3 | 00B8973C4278609 F2AF2A4 | 74:BF:90:17:0E:A3:7 0:6E:3C:53:C9:CC:0 1:51:2E: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:9 C:F3:9E:51:AE:65:08:85:8 2 |
| 3 7 | emSign ECC EV CS CA - C3 | 6004C5E20B62FD D48C46 | 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:B 1:C3:42:1F:E6:95:E5:15:7 A |
| 3 8 | emSign ECC Class 1 CA - C3 | 00BD6A0796AB3F 8955521E | 8C:D9:9F:A0:21:35: 3E:FC:B4:3A:99:6C: 2E:F2:0A:29:6F:F0:E C:92 | FA:D2:E9:86:49:F1:C6:06 :15:0F:55:26:9E:BC:03:5 A:EA:22:FF:AC:13:1D:E6: 4B:A6:90:0C:75:D8:44:7B :7E |
| 3 9 | emSign ECC Class 2 CA - C3 | 00D1142766698BF CDEDA02 | 56:4C:89:B8:25:C8: 98:EE:BD:F2:7C:62: 2D:AE:69:39:3A:B6: 17:2C | DB:45:91:F8:78:F6:67:2F: 5B:70:73:3A:66:AD:7C:95 :37:B9:7E:6F:0A:F5:CA:4 9:AA:B8:EC:B2:CE:02:F8: 6B |
| 4 0 | emSign ECC Class 3 CA - C3 | 3D12A1CF78258D 580854 | F1:66:AB:96:8C:A4: 0D:D2:26:62:33:2F: 9A:55:09:5D:D9:E6: 48:4A | 5A:9A:03:F2:D3:FE:58:9B :E6:3C:DA:11:82:0A:9F:2 5:F0:74:C9:20:34:F5:1C:0 4:7D:34:22:6D:25:2E:C0: 25 |

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

| | | | | |
|--------|-------------------------------------|----------------------------|---|---|
| 4 1 | emSign ECC Time stamping CA - C3 | 00B94B49C6436D7 2090201 | 0B:BF:47:0B:3D:65: F5:4E:73:4C:1C:AD: 1E:4E:67:52:09:2D:2 6:BD | 71:D2:EE:4D:DA:25:1D:92 :44:F7:CE:7C:6D:47:8E:C 5:52:D4:24:EF:71:9F:02:B 7:10:30:F2:82:1B:6B:C8:5 3 |
| 4 2 | emSign ECC Device CA - C3 | 00D9365F15842A1 D0689C3 | 04:F6:54:AF:2E:B4: DD:A7:44:1E:CA:F0: 63:9C:24:15:43:58:2 F:CF | 3D:45:11:D0:A8:0A:A9:49 :A6:D9:9B:25:3A:17:34:7 1:79:7C:44:59:18:7A:63:2 9:E7:36:C3:7C:B5:49:3E: 46 |