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) that in generating and protecting its emSign Root TLS CA - G1, emSign Root SMIME CA - G1, emSign Root Client Auth CA - G1, emSign Root TSA CA - G2, emSign Root CS CA - G2, emSign Root TLS CA - G3, emSign Root SMIME CA - G3, emSign Root Client Auth CA - G3, emSign Root TSA CA - G3 and emSign Root CS CA - G3 (collectively, "emSign PKI Root CAs") on 8 February 2024 at Bangalore, with the following identifying information:

Root Name	Subject Key Identifier	Certificate Serial Number
emSign Root TLS CA - G1	641DC9D8F8C4EC044B2281F5329A5EB9E79352F9	02A27D4E346AEF4E4F04678B5BB6D9EE
emSign Root SMIME CA - G1	756C0C2036DB1C88D425BEB7FA69D3B18E6CA7AB	0C974F5F068B868F52FC0CF7E5544F51
emSign Root Client Auth CA - G1	DB577BCEB185DE3A4EAFC62740236F5511144524	0E4FA878FEA8183E7107189595046D84
emSign Root TSA CA - G2	FA22B01A0E0F0713237A38FCD037313688D83825	065E0E80658A572E5EBDBF93A493E350
emSign Root CS CA - G2	E61CC6AA27B48BF2BD85645FAFF4BA72A6D00175	0886217572A7C40CC3BB2EE5D72D6E6C
emSign Root TLS CA - G3	E13AAB217CF1E34D54AED472B7FD8B5942209054	0E760672F143459FC8FE0AB0BC05E394
emSign Root SMIME CA - G3	BDB1C020F9330DB3A35A7DC5BE3B31601D655C0A	009F4F5FF84A1A6DC2C83C0EF9B7031F
emSign Root Client Auth CA - G3	49F5CFF70D58CF9E8171788AAC393E93C63EE6F2	0C514FFD18852863D2AAB9B7006346DF
emSign Root TSA CA - G3	40C9218A784245B988B1EECAC1F668F56A0933B7	0E27F07F8657096CCFD447EA0E2399EC
emSign Root CS CA - G3	687403F885CA8D5450571D16E0C8DE450DABCD2D	018FCEC927C116F59C997EDC0CCD2E2B

emSign PKI has:

- Followed the CA key generation and protection requirements in its:
  - Certificate Policy and Certification Practice Statement (CP/CPS) as emSign Certificate Policy and Certification Practice Statement v1.14

- included appropriate, detailed procedures and controls in its Root Key Generation Script(s): Root Key Generation Script version 1.0, dated 8 February 2024.

- Maintained effective controls to provide reasonable assurance that the emSign PKI Root CAs were generated and protected in conformity with the procedures described in its CP/CPS and its Root Key Generation Script

- Performed, during the root key generation process, all procedures required by the Root Key Generation Script

- generated the CA keys in a physically secured environment as described in its CP/CPS

- generated the CA keys using personnel in trusted roles under multiple person control and split knowledge

- generated the CA keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in its CP/CPS

in accordance with CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.2.2.

Certification authority's responsibilities

emSign PKI's management is responsible for its assertion, including the fairness of its presentation, and for generating and protecting its CA keys in accordance with CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.2.2.

Our independence and quality management

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies International Standard on Quality Management (ISQM) 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements* 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.

Practitioner's responsibilities

Our responsibility is to express an opinion on management's assertion based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. 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 documented plan of procedures to be performed for the generation of the certification authority key pairs for the emSign PKI Root CAs;
2. reviewing the detailed CA key generation script(s) for conformance with industry standard practices;
3. testing and evaluating, during the CA key generation process, the effectiveness of controls over the integrity, confidentiality, and availability of all private keys, including back-up copies, and access keys (including physical keys, tokens, and passwords), used in the establishment of the service;
4. physical observation of all procedures performed during the root key generation process to ensure that the procedures actually performed on 8 February 2024 were in accordance with the Root Key Generation Script for the emSign PKI Root CAs; and
5. 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

Opinion

In our opinion, on 8 February 2024, emSign PKI management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.2.2.

This report does not include any representation as to the quality of emSign PKI's services beyond those covered by CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.2.2., nor the suitability of any of emSign PKI's services for any customer's intended purpose

Digital Age Strategies Private Limited,
Bengaluru, Karnataka, India,
15 February 2024.

DINESH
SHIVAR
AM
SHASTRI

Digitally signed
by DINESH
SHIVARAM
SHASTRI
Date: 2024.02.15
10:17:10 +05'30'

EMSIGN PKI'S MANAGEMENT ASSERTION

eMudhra Technologies Limited ("emSign PKI") has deployed a public key infrastructure. As part of this deployment, it was necessary to create a hierarchy consistent of self-signed Root CAs known as emSign Root TLS CA - G1, emSign Root SMIME CA - G1, emSign Root Client Auth CA - G1, emSign Root TSA CA - G2, emSign Root CS CA - G2, emSign Root TLS CA - G3, emSign Root SMIME CA - G3, emSign Root Client Auth CA - G3, emSign Root TSA CA - G3 and emSign Root CS CA - G3 (collectively, "emSign PKI Root CAs"). These CA's will serve as Root CAs for client certificate services. In order to allow the CA's to be installed in a final production configuration, a Root Key Generation Ceremony was conducted, the purpose of which was to formally witness and document the creation of the CA's private signing key. This helps assure the non-refutability of the integrity of the emSign PKI's Root CAs' key pairs, and in particular, the private signing keys.

emSign PKI management has securely generated key pairs, each consisting of a public and private key, in support of its CA operations. The key pairs were generated in accordance with procedures described in emSign PKI's Certificate Policy (CP) and Certification Practice Statement (CPS), and its Root Key Generation Script, which are in accordance with CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.2.2.

emSign PKI management established and maintained effective controls over the generation of these keys. These controls were designed to provide reasonable assurance of adherence to the above-mentioned practices throughout the root key generation process.

emSign PKI management is responsible for establishing and maintaining procedures over its CA root key generations, and over the integrity and confidentiality of all private keys and access keys (including physical keys, tokens, and passwords) used in the establishment of the emSign PKI Root CAs, and for the CA environment controls relevant to the generation and protection of its CA keys.

emSign PKI management has assessed the procedures and controls for the generation of the CA keys. Based on that assessment, in management's opinion, in generation and protecting its CA keys for the emSign PKI Root CA's on 8 February 2024 at Bangalore, with the following identifying information:

Root Name	Subject Key Identifier	Certificate Serial Number
emSign Root TLS CA - G1	641DC9D8F8C4EC044B2281F53 29A5EB9E79352F9	02A27D4E346AEF4E4F04678B5 BB6D9EE
emSign Root SMIME CA - G1	756C0C2036DB1C88D425BEB7F A69D3B18E6CA7AB	0C974F5F068B868F52FC0CF7E5 544F51
emSign Root Client Auth CA - G1	DB577BCEB185DE3A4EAFC6274 0236F5511144524	0E4FA878FEA8183E7107189595 046D84
emSign Root TSA CA - G2	FA22B01A0E0F0713237A38FCD 037313688D83825	065E0E80658A572E5EBDBF93A 493E350
emSign Root CS CA - G2	E61CC6AA27B48BF2BD85645FA FF4BA72A6D00175	0886217572A7C40CC3BB2EE5D 72D6E6C

Root Name	Subject Key Identifier	Certificate Serial Number
emSign Root TLS CA - G3	E13AAB217CF1E34D54AED472B7FD8B5942209054	0E760672F143459FC8FE0AB0BC05E394
emSign Root SMIME CA - G3	BDB1C020F9330DB3A35A7DC5BE3B31601D655C0A	009F4F5FF84A1A6DC2C83C0EF9B7031F
emSign Root Client Auth CA - G3	49F5CFF70D58CF9E8171788AAC393E93C63EE6F2	0C514FFD18852863D2AAB9B7006346DF
emSign Root TSA CA - G3	40C9218A784245B988B1EECAC1F668F56A0933B7	0E27F07F8657096CCFD447EA0E2399EC
emSign Root CS CA - G3	687403F885CA8D5450571D16E0C8DE450DABCD2D	018FCEC927C116F59C997EDC0CCD2E2B

emSign PKI has:

- followed the CA key generation and protection requirements in its:
    - Certificate Policy and Certification Practice Statement (CP/CPS) as emSign Certificate Policy and Certification Practice Statement v1.14
- included appropriate, detailed procedures and controls in its Root Key Generation Script(s): Root Key Generation Script version 1.0, dated 8 February 2024.
- maintained effective controls to provide reasonable assurance that the emSign PKI Root CAs were generated and protected in conformity with the procedures described in its CP/CPS and its Root Key Generation Script
- performed, during the root key generation process, all procedures required by the Root Key Generation Script
- generated the CA keys in a physically secured environment as described in its CP/CPS
- generated the CA keys using personnel in trusted roles under multiple person control and split knowledge
- generated the CA keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in its CP/CPS

in accordance with CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.2.2.

VENU
MAD
HAVA

Digitally signed by VENU MADHAVA
Date: 2024.02.14 21:17:02 +05'30'

Venu Madhava
Director
14 February 2024