emSign- CA Information Request

Meta Information:

Bug ID	1433330
Bug Summary	Add emSign root certificate(s)

General Information

CA Owner Name	eMudhra Technologies Limited
About the CA	**emSign** is the brand for the global digital certificate business that is operated by eMudhra. eMudhra is the largest licensed Certifying Authority and Digital Security Company in India with a strong pedigree as an issuer and solution provider for Digital Certificates. eMudhra has been a licensed CA under Controller of Certifying Authorities which operates the Indian Government Root for more than 10 years and is also a licensed CA in Mauritius under Ministry of IT, Mauritius. eMudhra has **issued over 35 million digital certificates** (3% of India's population). eMudhra is a critical **partner to Digital India** and supports the usage of digital signatures on a variety of eGovernance platforms for Government of India including Company Law Board, Income Tax, Goods and Service Tax (GST / VAT), eProcurement, Travel Portals, Customs, Banking etc. eMudhra's solutions power digital signature and other multifactor authentication for over 35 Banks which include domestic and global Banks. eMudhra also has a proprietary CA solution which is today used by the Indian Army and other defense establishments. eMudhra works through several partners across Asia Pacific and Middle East and Africa to enable digital signature based authentication/signing and setup of National PKI infrastructures. eMudhra is **Vice Chairman of Asia PKI Consortium** where we drive adoption of digital signature technology in other Countries and drive interoperability for trade between various countries. eMudhra is also the **Chairman of India PKI Forum**, which is sponsored by Government of India. eMudhra therefore has setup an independent root to support security infrastructure development across the region which cannot be achieved via its role as an Issuing CA under the Indian Government Root.
CA Email Alias 1	vijay@emudhra.com
CA Email Alias 2	kaushik@emudhra.com
Company Website	www.emsign.com, www.emudhra.com
Organizational Type	Private Corporation
Geographic Focus	Primary focus is India, and Global (serves customers globally, including APAC, EMEA, America)

Primary Market / Customer Base	The primary market for eMudhra is India where we have very strong partner network of over 35 million subscribers and 17000 channel partners who work with end users for digital certificate purchase, usage etc. We also work with large Enterprises (Banks, Government Departments, Insurance, Capital Markets, Financial Services) to protect their infrastructure using PKI. Recently, we have expanded our geographical focus to adjoining countries to work with Governments and Enterprises to deploy PKI infrastructure.
Impact to Mozilla Users	Digital India and driving its adoption is one of the cornerstones of the Indian government's mission. There is a huge focus on Cybersecurity by Government and as a consequence by Private Sector as well. The need to protect infrastructure is resulting in large scale transformational projects where PKI (used to secure communication between end users, websites etc) and digital certificates are becoming critical. Because a lot of such projects deal with issues of national security, data security, data privacy eMudhra is ideally poised bridge that gap of providing trust services to local and global markets where trust services go hand in hand with our security solution offerings for signing, authentication, encryption. Since many of our customers use Mozilla products, adding emSign's Root to NSS will enable eMudhra to provide trust services to various entities who are embarking on digital transformation with a focus on security.

Required and Recommended Practices

Do You, as an official representative of this CA agree to the following Recommended Practices Statement?

Yes. I have reviewed Mozilla's lists of Required and Recommended Practices, and confirm that we follow those practices, with exceptions and clarifications noted in the text box below.

CA Response to Required and Recommended Practices

Publicly Available CP and CPS (Required)	CP-CPS is available at https://repository.emsign.com. The publication and repository obligations including availability and frequency are covered in Section 2.1.3 of the CP/CPS CP/CPS is available in PDF and is in English language only. CP/CPS has reference to Mozilla Root Store Policy in Section 1.1. The CP-CPS addresses the requirements of Mozilla Policy.
Audit Criteria (Required)	The scope and criteria of Audit is covered in Section 8 of the CP/CPS. emSign is audited by BDO for compliance to all Webtrust principles. BDO, Malaysia is a licensed Webtrust practitioner as listed in http://www.webtrust.org/licensed-webtrust-practitioners-international/item64419.aspx
Revocation of Compromised Certificates (Required)	The revocation criteria and procedures for Compromised Certificates is covered in Section 4.9 of the CP/CPS.
Verifying Domain Name Ownership (Required)	The procedures for verification of Domain Ownership is listed in Section 3.2 which has reference to Section 10.1, Appendix A of CP/CPS.
Verifying Email Address Control (Required)	The procedures for verification of Email Address Control is listed in Section 3.2 which has reference to Section 10.7, Appendix A of CP/CPS.

	It states, "The control over email or the domain name of email server, shall be verified in the form of delivery and acceptance of the email, or any other reliable means." The process involves the challenge response procedure sent over email containing a unique tokenised URL. The holder of email should click the URL, and click to verify the control.
DNS names go in SAN (Required)	emSign Certificates are fully compliant with CAB Forum's BRs. Refer to CP/CPS Appendix B. All the DNS Names are part of SAN extension. The common name field may contain any one of the intended domain name which is present in the SAN.
OCSP (Required)	OCSP operations are covered in Section 4.9 and 4.10 of the CP/CPS. Compliance of OCSP with respect to the following have also been validated by Auditors during Webtrust Audit. OCSP URL functions using HTTP at port 80 and the URL is part of the certificate issued to subscriber. The OCSP service is dynamically updated at the earliest possible time, and is well within the period of four days.
Network Security Controls (Required)	Network Security Controls are covered in Section 6.7 Compliance of Network Security Controls with respect to the following have been validated by Auditors during Webtrust Audit. emSign is in compliance with the general protections for the network and supporting systems as outlined in Network and Certificate System Security Requirements, and will continue to do the following network security activities on a regular basis, according to the guidelines issued by the CA/Browser Forum: Maintain network security controls that at minimum meet the Network and Certificate System Security Requirements. Check for mis-issuance of certificates, especially for high-profile domains. Review network infrastructure, monitoring, passwords, etc. for signs of intrusion or weakness. Ensure Intrusion Detection Systems and other monitoring software is up-to-date. Shut down certificate issuance quickly if we are alerted of intrusion.
CA Hierarchy (Recommended)	emSign's CP/CPS applies to all the root certificates submitted. There is no separation of sections for each type of roots. The root certificates are separated by below parameters: • Two Affiliate company (eMudhra, India and eMudhra, USA) • Two Key algorithms (RSA / ECC) • Under RSA, separate 4096 bit root for CodeSign and TimeStamping, and 2048 bit root for other purposes

	Hence, there are 6 root certificates. Please refer to attached CA Hierarchy document for detailed information along with the purpose for each Root and Intermediate certificate. Under each of the roots, there are subordinate CAs that differentiates the certificate policy/purpose of issuances.
Document Handling of IDNs in CP/CPS (Recommended)	Section 3.1.2 of CP/CPS states that "Requests for internationalized domain names (IDNs) in Certificates will be flagged for additional manual review and any necessary risk analysis procedures".
Usage of Appropriate Constraints (Recommended)	Root certificates of SSL and Email trust bits are separate. Nevertheless, the issuing CA also contains respective EKU constraints as appropriate.
Pre-Issuance Linting (Recommended)	Certificate issuance of emSign goes through stringent checks, and application has validated controls to meet the BR and RFC requirements for standards. emSign continues to implement additional tools (as recommended) in order to enhance the pre-issuance checks.

Forbidden and Potentially Problematic Practices

Do you, as an official representative of this CA agree to the following Problematic Practices Statement?

Yes. I have reviewed Mozilla's lists of Forbidden and Potentially Problematic Practices, and confirm that we do not do those practices.

CA Response to Forbidden and Potentially Problematic Practices

Long-lived Certificates (Forbidden)	Refer section 6.3.2 of the CP/CPS. The compliance of certificate lifetimes has been audited by Webtrust auditor.
Non-Standard Email Address Prefixes for Domain Ownership Validation (Forbidden)	Domain Ownership verification complies with the requirements of BR. Refer Appendix A of CP/CPS. When used, the email addresses are restricted only to use subscriber information listed in the "registrant", "technical", or "administrative" WHOIS records and a selected whitelist of local addresses, which are limited to local-parts of "admin", "administrator", "webmaster", "hostmaster", and "postmaster".
Issuing End Entity Certificates Directly From Roots (Forbidden)	emSign does not issue certificates to subscribers directly from Root.
Distributing Generated Private Keys in PKCS#12 Files (Forbidden)	emSign does not generate key-pair for the subscribers of SSL or signing certificates, unless the case where subscriber is guided / assisted / automated at their system to generate the key pairs. The keypairs are never transmitted by emSign, over the network during generation or certificate issuance process. However, for encryption only certificates, subscriber may opt for key-archival in which case emSign may generate the key pair and archive it as per section 4.12 and section 6.2.5 of CP/CPS
Certificates Referencing Local Names or Private IP Addresses (Forbidden)	emSign strictly implements the restriction, not to issue, SSL certificates on local names or reserved IP addresses.

Issuing SSL Certificates for .int Domains (Forbidden)	emSign does not issue SSL certificates to internal domain names.
OCSP Responses Signed by a Certificate Under a Different Root (Forbidden)	OCSP responses are signed only by respective issuer's OCSP responder certificates.
Issuance of SHA-1 Certificates (Forbidden)	emSign does not issue SHA-1 certificates.
Delegation of Domain / Email validation to third parties (Forbidden)	Domain / Email validation process is not and never delegated and is carried on by emSign.
Allowing External Entities to Operate Subordinate CAs (Problematic)	At this point of time, emSign does not allow external entities to operate Sub-CAs.
Generic Names for CAs (Problematic)	emSign does not use generic names for CAs, and uses the brand name to be part of issuer names.
Lack of Communication with End Users (Problematic)	emSign operates a state-of-art customer care facility, which facilitates end users, who are either the subscribers or the users of emSign certificates or any other people.
Backdating the notBefore Date (Problematic)	Certificate validaity (from) dates are not back dated, and the systems / applications are in sync with time servers.
Issuer Encoding in CRL (Problematic)	This has been tested so that issuer field in certificate and CRL follows exactly the same string type and contents. The encoding is exactly the same for equal result.

Policies and Practices

Policy Documentation	The CP/CPS and other documents are provided in English.
CA Document Repository	https://repository.emsign.com
CP-CPS	https://repository.emsign.com
Other Relevant Documents	https://repository.emsign.com
Auditor Name	BDO, Malaysia
Auditor Website	http://www.bdo.my/en-gb/home
Auditor Qualifications	BDO, Malaysia, a member firm of BDO is licensed by AICPA to perform Webtrust for CAs. http://www.webtrust.org/licensed-webtrust-practitioners-international/item64419.aspx
Standard Audit URL	Uploaded in Bugzilla
Standard Audit Type	Webtrust Principles and Criteria for Certification Authorities v2.1
Standard Audit Statement Date	December 15, 2017
BR Audit URL	Uploaded in Bugzilla
BR Audit Type	WebTrust® Principles and Criteria for Certification Authorities – SSL Baseline Requirements with Network Security – Version 2.2
BR Audit Statement Date	December 15, 2017
EV SSL Audit Url	Uploaded in Bugzilla
EV SSL Audit Type	WebTrust for Certification Authorities Extended Validation SSL Audit Criteria - version 1.6.1
EV SSL Audit Statement	Uploaded in Bugzilla

BR Commitment to Comply	Covered in Section 1.1 of CP/CPS
BR Self Assessment	Uploaded in Bugzilla
SSL Verification Procedures	Section 10.1 and 10.2 of Appendix A of CP/CPS
EV SSL Verification Procedures	Section 10.3 and 10.5 of Appendix A of CP/CPS
Organization Verification Procedures	Section 10.2 of Appendix A of CP/CPS
Email Address Verification Procedures	Section 10.7, 10.8 and 10.9 of Appendix A of CP/CPS
Multi-Factor Authentication	Section 4.3.1.5 of CP/CPS.
Network Security	Including, but not limited to, section 6.7 of CP/CPS.
BR Self Assessment	Uploaded in Bugzilla

Technical Information about Root Certificates

Attached as annexure to bug.