Mozilla - CA Program

Case Information

Case Number	00000262	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	eMudhra Technologies Limited	**Request Status**	Information Verification In Process

Additional Case Information

Subject	Include emSign root certificates	**Case Reason**	

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org /show_bug.cgi?id=1442337

General information about CA's associated organization

CA Email Alias 1			
CA Email Alias 2			
Company Website	https://www.emudhra.com/	**Verified?**	Verified
Organizational Type	Private Corporation	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Not Applicable
Geographic Focus	India, Global	**Verified?**	Verified
Primary Market / Customer Base	emSign is a brand of digital certificates operated by eMudhra.	**Verified?**	Verified
Impact to Mozilla Users	eMudhra provides certs for eGovernance platforms, travel portals, banks, etc.	**Verified?**	Verified

Required and Recommended Practices

Recommended Practices	https://wiki.mozilla.org/CA/Required_or_Recommended_Practices	**Recommended Practices Statement**	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's Response to Recommended Practices	1. Publicly Available CP and CPS: CPS section 2.1.3 1.1 Revision Table, updated annually: Not found NEED: https://wiki.mozilla.org/CA/Required_or_Recommended_Practices#CP.2FCPS_Revision_Table 1.2 CAA Domains listed in CP/CPS: Not found NEED: https://wiki.mozilla.org/CA/Required_or_Recommended_Practices#CAA_Domains_listed_in_CP.2FCPS 2. Audit Criteria: CPS section 8 3. Revocation of Compromised Certificates: CPS section 4.9.1 4. Verifying Domain Name Ownership: CPS sections 10.1, 10.2, 10.3 5. Verifying Email Address Control: CPS sections 10.2, 10.6, 10.7, 10.8, 10.9 6. DNS names go in SAN: CPS sections 11.3, 11.4, 11.5 7. OCSP: CPS sections 4.9.9 - OCSP SHALL NOT respond "Good" for unissued certs: test succeeded 8. Network Security Controls: CPS section 6.7	**Verified?**	Need Response From CA

Forbidden and Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org/CA/Forbidden_or_Problematic_Practices	**Problematic Practices Statement**	I have reviewed Mozilla's lists of Forbidden and Potentially Problematic Practices, and confirm that we do not do those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Problematic Practices	1. Long-lived Certificates: CPS section 6.3.2 2. Non-Standard Email Address Prefixes for Domain Ownership Validation: CPS sections 10.1, 10.2, 10.3 3. Issuing End Entity Certificates Directly From Roots: CPS section 4.3.1.2 4. Distributing Generated Private Keys in PKCS#12 Files: CPS section 3.2.1 5. Certificates Referencing Local Names or Private IP Addresses: CPS section 10.1, 10.2, 10.3 6. Issuing SSL Certificates for .int Domains: No 7. OCSP Responses Signed by a Certificate Under a Different Root: No 8. Issuance of SHA-1 Certificates: CPS section 6.1.5 9. Delegation of Domain / Email Validation to Third Parties: CPS sections 1.3.1, 1.3.2, 4.1.2, 4.2.1, 4.3.1.2	**Verified?**	Verified

Root Case Record # 1

Root Case Information

Root Certificate Name	emSign Root CA - G1	**Root Case No**	R00000515
Request Status	Information Verification In Process	**Case Number**	00000262

Certificate Data

Certificate Issuer Common Name	emSign Root CA - G1
O From Issuer Field	eMudhra Technologies Limited
OU From Issuer Field	emSign PKI
Valid From	2018 Feb 18
Valid To	2043 Feb 18
Certificate Serial Number	31f5e4620c6c58edd6d8
Subject	CN=emSign Root CA - G1, OU=emSign PKI, O=eMudhra Technologies Limited, C=IN
Signature Hash Algorithm	sha256WithRSAEncryption
Public Key Algorithm	RSA 2048 bits
SHA-1 Fingerprint	8A:C7:AD:8F:73:AC:4E:C1:B5:75:4D:A5:40:F4:FC:CF:7C:B5:8E:8C
SHA-256 Fingerprint	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
Certificate ID	2F:5F:7B:65:D9:2C:06:EF:D6:78:01:DD:EE:03:FF:14:3B:82:F1:12:36:94:68:42:DA:74:05:22:46:B0:25:30
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	NEED justification for each of the 6 root certs in this inclusion request.	**Verified?**	Need Response From CA
Root Certificate Download URL	https://repository.emsign.com/certs /emSignRootCAG1.crt	**Verified?**	Verified
CRL URL(s)	http://crl.emsign.com?RootCAG1.crl http://crl.emsign.com?emSignEVSSLCAG1.crl http://crl.emsign.com?emSignSSLCAG1.crl CPS section 4.9.7: valid not more than 10 days.	**Verified?**	Verified
OCSP URL(s)	http://ocsp.emsign.com	**Verified?**	Verified
Mozilla Trust Bits	Email; Websites	**Verified?**	Verified
SSL Validation Type	DV; OV; EV	**Verified?**	Verified
Mozilla EV Policy OID(s)	2.23.140.1.1	**Verified?**	Verified
Root Stores Included In		**Verified?**	Verified
Mozilla Applied Constraints		**Verified?**	Not Applicable

Test Websites or Example Cert

Test Website - Valid	https://testevg1.emSign.com	**Verified?**	Verified

Test Website - Expired	https://testevg1e.emsign.com
Test Website - Revoked	https://testevg1r.emsign.com
Example Cert	https://bugzilla.mozilla.org/attachment.cgi?id=8955229
Test Notes	

Test Results (When Requesting the SSL/TLS Trust Bit)

Revocation Tested	https://certificate.revocationcheck.com/testevg1.emsign.com No errors	**Verified?**	Verified
CA/Browser Forum Lint Test	Tests ran, successful test output provided: https://bugzilla.mozilla.org/attachment.cgi?id=8955230	**Verified?**	Verified
Test Website Lint Test	Tests ran, successful test output provided: https://bugzilla.mozilla.org/attachment.cgi?id=8955230	**Verified?**	Verified
EV Tested	Tests ran, successful test output provided: https://bugzilla.mozilla.org/attachment.cgi?id=8955230	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	CPS section 4.3.1.2: "emSign PKI creates and operates its own Issuing CAs under this CP/CPS. Issuing Certifying Authorities are issued out of offline root certificates. However, on a need basis, emSign PKI may create and operate issuing CAs under a subordinate under Root CA. emSign PKI publishes all Issuing CA Certificates along with its Hierarchy to its Root CA, in its repository available at http://repository.emsign.com emSign PKI may also appoint external Issuing CAs..."	**Verified?**	Verified
Externally Operated SubCAs	Externally-operated issuing sub-CAs are allowed. CPS Section 1.3.1: "The emSign PKI also issues certificates to issuing CAs, subordinate CAs, including CAs owned by third parties. All such issuing CAs and subordinate CAs are required to operate in conformance with this CP/CPS."	**Verified?**	Verified

	Also see sections 4.1.2 and 4.2.1 of the CPS.		
Cross Signing	CPS section 1.1: "This CP/CPS addresses the actions of emSign PKI and not those of third parties operating with cross certificates issued by emSign PKI." NEED Clarification -- The above sentence seems to contradict sections 1.3.1, 4.1.2, and 4.2.1.	**Verified?**	Need Response From CA
Technical Constraint on 3rd party Issuer	Externally-operated RAs are allowed. CPS section 1.3.2: "emSign PKI may enter into contractual relationship with third party Issuing CAs, who may operate their own RA & authorize the issuance of certificates. Such third party issuing CAs and their RAs must comply with all the requirements of this CP/CPS and the terms of their contract. This may also refer to additional criteria as recommended by the CA Browser Forum. RAs may implement more restrictive vetting practices as per their internal policy." CPS Section 4.2.1 of the CPS. "Initial identity validation shall be performed by an Issuing CAs validation team or by Registration Authorities under contract as set forth in this CP/CPS." ... "Identification and Authentication requirements for each Digital Certificate profile is given in Appendix A."	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	CP/CPS are provided in English only.	**Verified?**	Verified
CA Document Repository	https://repository.emsign.com	**Verified?**	Verified
CP Doc Language	English		
CP	https://repository.emsign.com/cps/CP-CPS-v1.01.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	https://repository.emsign.com/cps/CP-CPS-v1.01.pdf	**Verified?**	Verified
Other Relevant Documents	Subscriber Agreement: https://repository.emsign.com/cps/SA-v1.00.pdf Relying Party Agreement: https://repository.emsign.com/cps/RPA-v1.00.pdf	**Verified?**	Verified
Auditor	BDO International Limited	**Verified?**	Verified

Auditor Location	Malaysia	**Verified?**	Verified
Standard Audit	https://repository.emsign.com/downloads/auditreports/1-A-CA_opt.pdf	**Verified?**	Not Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	2/26/2018	**Verified?**	Verified
BR Audit	https://repository.emsign.com/downloads/auditreports/2-A-SSL_opt.pdf	**Verified?**	Not Verified
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	2/26/2018	**Verified?**	Verified
EV SSL Audit	https://repository.emsign.com/downloads/auditreports/3-A-EVSSL_opt.pdf	**Verified?**	Not Verified
EV SSL Audit Type	WebTrust	**Verified?**	Verified
EV SSL Audit Statement Date	2/26/2018	**Verified?**	Verified
BR Commitment to Comply	CPS section 1.1	**Verified?**	Verified
BR Self Assessment	https://bugzilla.mozilla.org/attachment.cgi?id=8955225	**Verified?**	Verified
SSL Verification Procedures	Appendix A / Sections 10.1, 10.2, 10.3, and 10.6 CPS section 4.2.1: "emSign CA or Issuing CAs shall maintain systems and processes to sufficiently authenticate the Applicant's identity in compliance with its CP/CPS." ... "Identification and Authentication requirements for each Digital Certificate profile is given in Appendix A." CPS section 4.2.3: "A Registration Authority will approve or reject Certificate Holder applications based upon the Certificate Holders meeting the requirements of this CP/CPS in Appendix A."	**Verified?**	Verified
EV SSL Verification Procedures	CPS Appendix A / Section 10.3	**Verified?**	Verified
Organization Verification Procedures	CPS Appendix A / Sections 10.2 and 10.3	**Verified?**	Verified
Email Address Verification Procedures	CPS Appendix A / Sections 10.2, 10.6, 10.7, 10.8, 10.9	**Verified?**	Verified
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	**Verified?**	Not Applicable
Multi-Factor Authentication	CPS section 4.3.1.5.	**Verified?**	Verified

Network Security	CPS section 6.7	**Verified?**	Verified