Print this page

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**	In Detailed CP/CPS Review

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	emsignroot@emudhra.com		
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	**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: CPS section 12 / Appendix C. 1.2 CAA Domains listed in CP/CPS: CPS section 4.2.4 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?**	Verified

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	In Detailed CP/CPS Review	**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	SHA256WithRSA
Public Key Algorithm	RSA 2048 bits
SHA-1 Fingerprint	8AC7AD8F73AC4EC1B5754DA540F4FCCF7CB58E8C
SHA-256 Fingerprint	40F6AF0346A99AA1CD1D555A4E9CCE62C7F9634603EE406615833DC8C8D00367
Subject + SPKI SHA256	2F5F7B65D92C06EFD67801DDEE03FF143B82F11236946842DA74052246B02530
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	"emSign Root CA - G1" and "emSign ECC Root CA - G3" are owned by eMudhra - India. This is the primary root for global customers, depending on the business, operational and customer requirements that Indian entity will be serving.	**Verified?**	Verified
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	Microsoft	**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	ev-checker exited successfully: Success!	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	http://repository.emsign.com CPS section 4.3.1.2: "emSign PKI creates and operates its own Issuing CAs under this CP/CPS.	**Verified?**	Verified

	Issuing Certifying Authorities are issued out of offline root certificates.		
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." Also see sections 4.1.2 and 4.2.1 of the CPS.	**Verified?**	Verified
Cross Signing	CPS section 1.1: "This CP/CPS addresses the actions of emSign PKI and those of third parties operating with cross certificates issued by emSign PKI."	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	Externally-operated RAs are allowed. See CPS section 1.3.2 and 4.2.1.	**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-v1.03.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	https://repository.emsign.com/cps/CP-CPS-v1.03.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?**	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?**	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?**	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	CPS sections 4.2.1, 4.2.3, Appendix A / Sections 10.1, 10.2, 10.3, and 10.6	**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

Root Case Record # 2

Root Case Information

Root Certificate Name	emSign ECC Root CA - G3	**Root Case No**	R00000518
Request Status	In Detailed CP/CPS Review	**Case Number**	00000262

Certificate Data

Certificate Issuer Common Name	emSign ECC Root CA - G3
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	3CF607A968700EDA8B84
Subject	CN=emSign ECC Root CA - G3; OU=emSign PKI; O=eMudhra Technologies Limited; C=IN
Signature Hash Algorithm	ecdsaWithSHA384
Public Key Algorithm	EC secp384r1
SHA-1 Fingerprint	3043FA4FF257DCA0C380EE2E58EA78B23FE6BBC1
SHA-256 Fingerprint	86A1ECBA089C4A8D3BBE2734C612BA341D813E043CF9E8A862CD5C57A36BBE6B
Subject + SPKI SHA256	98AD944FA2A5BB2DDDB76050690D9ACFFA4AF0A9684FAB3C1ACC3E5E9CE58425
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	"emSign Root CA - G1" and "emSign ECC Root CA - G3" are owned by eMudhra - India. This is the primary root for global customers, depending on the business, operational and customer requirements that Indian entity will be serving.	**Verified?**	Verified
Root Certificate Download URL	https://repository.emsign.com/certs /emSignECCRootCAG3.crt	**Verified?**	Verified
CRL URL(s)	ttp://crl.emsign.com?RootCAG3.crl http://crl.emsign.com?emSignECCEVSSLCAG3.crl http://crl.emsign.com?emSignECCSSLCAG3.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	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints		**Verified?**	Not Applicable

Test Websites or Example Cert

Test Website - Valid	https://testevg3.emsign.com	**Verified?**	Verified
Test Website - Expired	https://testevg3e.emsign.com		
Test Website - Revoked	https://testevg3r.emsign.com		
Example Cert			
Test Notes			

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

Revocation Tested	https://certificate.revocationcheck.com/testevg3.emsign.com	**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	ev-checker exited successfully: Success!	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	http://repository.emsign.com 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.	**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	**Verified?**	Verified

	operate in conformance with this CP/CPS." 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 those of third parties operating with cross certificates issued by emSign PKI."	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	Externally-operated RAs are allowed. See CPS section 1.3.2 and 4.2.1.	**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-v1.03.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	https://repository.emsign.com/cps/CP-CPS-v1.03.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?**	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?**	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?**	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	CPS sections 4.2.1, 4.2.3, Appendix A / Sections 10.1, 10.2, 10.3, and 10.6	**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?**	Verified
Multi-Factor Authentication	CPS section 4.3.1.5.	**Verified?**	Verified
Network Security	CPS section 6.7	**Verified?**	Verified

Root Case Record # 3

Root Case Information

Root Certificate Name	emSign Root CA - C1	**Root Case No**	R00000519
Request Status	In Detailed CP/CPS Review	**Case Number**	00000262

Certificate Data

Certificate Issuer Common Name	emSign Root CA - C1
O From Issuer Field	eMudhra Inc
OU From Issuer Field	emSign PKI
Valid From	2018 Feb 18

Valid To	2043 Feb 18
Certificate Serial Number	00AECF00BAC4CF32F843B2
Subject	CN=emSign Root CA - C1; OU=emSign PKI; O=eMudhra Inc; C=US
Signature Hash Algorithm	SHA256WithRSA
Public Key Algorithm	RSA 2048 bits
SHA-1 Fingerprint	E72EF1DFFCB20928CF5DD4D56737B151CB864F01
SHA-256 Fingerprint	125609AA301DA0A249B97A8239CB6A34216F44DCAC9F3954B14292F2E8C8608F
Subject + SPKI SHA256	CCB6CDFECF7DE18D1BD25E88950D436C85195A9176507BBF69883865BDA5360B
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	"emSign Root CA - C1" and "emSign ECC Root CA - C3" are owned by eMudhra - USA; and used for customers who specifically require US entity based certificates. Typically needed for users from American continents, Middle East, & European countries.	**Verified?**	Verified
Root Certificate Download URL	https://repository.emsign.com/certs/emSignRootCAC1.crt	**Verified?**	Verified
CRL URL(s)	http://crl.emsign.com?RootCAC1.crl http://crl.emsign.com?emSignEVSSLCAC1.crl http://crl.emsign.com?emSignSSLCAC1.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://testevc1.emsign.com	**Verified?**	Verified

Test Website - Expired	https://testevc1e.emsign.com
Test Website - Revoked	https://testevc1r.emsign.com
Example Cert	
Test Notes	

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

Revocation Tested	https://certificate.revocationcheck.com/testevc1.emsign.com	**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	ev-checker exited successfully: Success!	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	http://repository.emsign.com 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.	**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." Also see sections 4.1.2 and 4.2.1 of the CPS.	**Verified?**	Verified
Cross Signing	CPS section 1.1: "This CP/CPS addresses the actions of emSign PKI and those of third parties operating with cross certificates issued by emSign PKI."	**Verified?**	Verified

Technical Constraint on 3rd party Issuer	Externally-operated RAs are allowed. See CPS section 1.3.2 and 4.2.1.	**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-v1.03.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	https://repository.emsign.com/cps/CP-CPS-v1.03.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?**	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?**	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?**	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	CPS sections 4.2.1, 4.2.3, Appendix A / Sections 10.1, 10.2, 10.3, and 10.6	**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

Root Case Record # 4

Root Case Information

Root Certificate Name	emSign ECC Root CA - C3	**Root Case No**	R00000521
Request Status	In Detailed CP/CPS Review	**Case Number**	00000262

Certificate Data

Certificate Issuer Common Name	emSign ECC Root CA - C3
O From Issuer Field	eMudhra Inc
OU From Issuer Field	emSign PKI
Valid From	2018 Feb 18
Valid To	2043 Feb 18
Certificate Serial Number	7B71B68256B8127C9CA8
Subject	CN=emSign ECC Root CA - C3; OU=emSign PKI; O=eMudhra Inc; C=US
Signature Hash Algorithm	ecdsaWithSHA384
Public Key Algorithm	EC secp384r1

SHA-1 Fingerprint	B6AF43C29B81537DF6EF6BC31F1F60150CEE4866
SHA-256 Fingerprint	BC4D809B15189D78DB3E1D8CF4F9726A795DA1643CA5F1358E1DDB0EDC0D7EB3
Subject + SPKI SHA256	7787DB2349664D6D38541977225C6CA7429024291F2CAAD5BE9393D26300A04C
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	"emSign Root CA - C1" and "emSign ECC Root CA - C3" are owned by eMudhra - USA; and used for customers who specifically require US entity based certificates. Typically needed for users from American continents, Middle East, & European countries.	**Verified?**	Verified
Root Certificate Download URL	https://repository.emsign.com/certs /emSignECCRootCAC3.crt	**Verified?**	Verified
CRL URL(s)	http://crl.emsign.com?RootCAC3.crl http://crl.emsign.com?emSignECCEVSSLCAC3.crl http://crl.emsign.com?emSignECCSSLCAC3.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://testevc3.emsign.com	**Verified?**	Verified
Test Website - Expired	https://testevc3e.emsign.com		
Test Website - Revoked	https://testevc3r.emsign.com		
Example Cert			
Test Notes			

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

Revocation Tested	https://certificate.revocationcheck.com/testevc3.emsign.com	**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	ev-checker exited successfully: Success!	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	http://repository.emsign.com 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.	**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." Also see sections 4.1.2 and 4.2.1 of the CPS.	**Verified?**	Verified
Cross Signing	CPS section 1.1: "This CP/CPS addresses the actions of emSign PKI and those of third parties operating with cross certificates issued by emSign PKI."	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	Externally-operated RAs are allowed. See CPS section 1.3.2 and 4.2.1.	**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-v1.03.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	https://repository.emsign.com/cps/CP-CPS-v1.03.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?**	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?**	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?**	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	CPS sections 4.2.1, 4.2.3, Appendix A / Sections 10.1, 10.2, 10.3, and 10.6	**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