emSign CA's BR Self Assessment

CAs Legal Name: eMudhra Technologies Limited

CA Hierarchy:
Document enclosed on CA Hierarchy

Baseline Requirements:
emSign was compliant with Baseline Requirements 1.5.0 but the standard operating procedures are now compliant with Baseline Requirements 1.5.4 since 28 Jan 2018

CA documents:
Available at https://repository.emsign.com

1. CP-CPS: Version 1.01
2. Subscriber Agreement: Version 1.00
3. Relying Party Agreement: Version 1.00

BR Section Number	**List the specific documents and section numbers of those documents which meet the requirements of each BR section**	**Explain how the CA's listed documents meet the requirements of each BR section.**
1.2.1. Revisions Note the Effective Date for each item in the table. Certificates created after each Effective Date are expected to be in compliance with the item. Make sure your CA is in compliance with each of these items. After careful consideration, *indicate if your CA is fully compliant with all items in the table, or clearly indicate action that your CA is taking to improve compliance.*	emSign CP/CPS v1.01	emSign is compliant with all the items of the table 1.2.1 of latest Baseline Requirements.

1.2.2. Relevant Dates Note the Compliance date for each item in the table. Those are the dates by which your CP/CPS and practices are expected to be updated to comply with the item. Make sure your CA is in compliance with each of these items. After careful consideration, *indicate if your CA is fully compliant with all items in the table, or clearly indicate action that your CA is taking to improve compliance.*	emSign CP/CPS v1.01	emSign is compliant with these dates, and has already implemented all compliances. The forthcoming compliance of 825 days maximum validity is also implemented.
1.3.2. Registration Authorities Indicate whether your CA allows for Delegated Third Parties, or not. *Indicate which sections of your CP/CPS specify such requirements, and how the CP/CPS meets the BR requirements for RAs.*	emSign CP/CPS v1.01 Section 1.3.2	For all LRA's, emSign enters into a contract with such LRA's which mandates LRA's to abide by emSign CP/CPS and terms of service. LRA's can issue SSL/TLS certificates only for organizations and domains that have been vetted by emSign
2.1. Repositories *Provide the direct URLs to the CA's repositories*	emSign CP/CPS v1.01 Section 2.1.3	Available at https://repository.emsign.com
2.2. Publication of information "The CA SHALL publicly give effect to these Requirements and represent that it will adhere to the latest published version." *--> Copy the specific text that is used into the explanation in this row. (in English)*	emSign CP/CPS v1.01 Section 2.1.3	This CP/CPS specifies the principles, procedures and practices that the emSign PKI follows to conform to the following policies, guidelines and requirements: 1. RFC 3647 of Internet Engineering Task Force (IETF) for Certificate Policy and Certification Practice Statement. 2. The current version of the CA/Browser Forum (CABF) requirements including: • Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates. • Guidelines for the Issuance and Management of Extended Validation (EV) Certificates, • Guidelines for the Issuance and Management of Extended Validation (EV) Code-Signing Certificates • Network and Certificate System Security Requirements

		3. Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates (Ref: https://aka.ms/csbr) 4. Time-stamping services according to RFC 3161 of IETF and other applicable standards. 5. Adobe Approved Trust List (AATL) Certificate policies. 6. Apple Root Certificate program, Microsoft Trusted Root Certificate Program Audit Requirements, Mozilla Root Store Policy, Oracle Java Root Certificate program, and Root Certificate Policy for the Chromium Projects. If any inconsistency exists between this CP/CPS and aforesaid requirements, then the aforesaid Requirements take precedence over this CP/CPS.
2.2. Publication of information "The CA SHALL host test Web pages that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate. At a minimum, the CA SHALL host separate Web pages using Subscriber Certificates that are (i) valid, (ii) revoked, and (iii) expired." *--> List the URLs to the three test websites (valid, revoked, expired) for each root certificate under consideration. If you are requesting EV treatment, then the TLS cert for each test website must be EV.*		URLs provided to Application Software Providers for each of Valid, Revoked and Expired Certificate. (The list of URLs for each Root is published in Root Certificates Information document attached in the bug.)
2.3. Time or frequency of publication *Indicate your CA's policies/practices to ensure that the BRs are reviewed regularly, and that the CA's CP/CPS is updated annually.*	emSign CP/CPS v1.01 Section 2.1.3 Section 1.1, 1.5.1	The CP/CPS is reviewed by Policy Authority minimum once a year emSign also monitors Baseline Requirements regularly to ensure CP/CPS and Operating Procedures are correct and latest

2.4. Access controls on repositories *Acknowledge that all Audit, CP, CPS documents required by Mozilla's CA Certificate Policy and the BRs will continue to be made publicly available.*	emSign CP/CPS v1.01 Section 2.1.3	emSign will make publicly available all documents required by Mozilla's CA Certificate Policy and BR including Audit Reports, CP/CPS
3.2.2.1 Identity If the Subject Identity Information in certificates is to include the name or address of an organization, *indicate how your CP/CPS meets the requirements in this section of the BRs.*	emSign CP/CPS v1.01 Section 3.2, Appendix A (Section 10.2)	emSign is compliant with Baseline Requirements v1.5.4
3.2.2.2 DBA/Tradename If the Subject Identity Information in certificates is to include a DBA or tradename, *indicate how your CP/CPS meets the requirements in this section of the BRs.*	emSign CP/CPS v1.01 Section 3.2, Appendix A (Section 10.2)	emSign is compliant with Baseline Requirements v1.5.4
3.2.2.3 Verification of Country If the subject:countryName field is present in certificates, *indicate how your CP/CPS meets the requirements in this section of the BRs.*	emSign CP/CPS v1.01 Section 3.2, Appendix A (Section 10.1)	emSign is compliant with Baseline Requirements v1.5.4
3.2.2.4 Validation of Domain Authorization or Control *Indicate which of the methods of domain validation your CA uses, and where this is described in your CP/CPS. The CA's CP/CPS must clearly describe the acceptable methods of domain validation.* ***It is *not* sufficient for the CP/CPS to merely reference the BRs. Enough information must be directly provided in the CP/CPS for the reader to be able to understand how the CA performs domain validation.***	emSign CP/CPS v1.01 Section 3.2, Appendix A (Section 10.1)	emSign is compliant with Baseline Requirements v1.5.4 Domain Validation procedures are captured in Appendix A
3.2.2.4.1 Validating the Applicant as a Domain Contact If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	Not Applicable	Not Applicable

3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	emSign CP/CPS v1.01 Section 3.2, Appendix A (Section 10.1)	emSign is compliant with Baseline Requirements v1.5.4
3.2.2.4.3 Phone Contact with Domain Contact If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	Not Applicable	Not Applicable
3.2.2.4.4 Constructed Email to Domain Contact If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	emSign CP/CPS v1.01 Section 3.2, Appendix A (Section 10.1)	emSign is compliant with Baseline Requirements v1.5.4
3.2.2.4.5 Domain Authorization Document If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	emSign CP/CPS v1.01 Section 3.2, Appendix A (Section 10.1)	emSign is compliant with Baseline Requirements v1.5.4
3.2.2.4.6 Agreed-Upon Change to Website If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	emSign CP/CPS v1.01 Section 3.2, Appendix A (Section 10.1)	emSign is compliant with Baseline Requirements v1.5.4
3.2.2.4.7 DNS Change If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	emSign CP/CPS v1.01 Section 3.2, Appendix A (Section 10.1)	emSign is compliant with Baseline Requirements v1.5.4
3.2.2.4.8 IP Address If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	Not Applicable	Not Applicable

3.2.2.4.9 Test Certificate If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	Not Applicable	Not Applicable
3.2.2.4.10. TLS Using a Random Number If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	Not Applicable	Not Applicable
3.2.2.5 Authentication for an IP Address If your CA allows IP Addresss to be listed in certificates, *indicate how your CA meets the requirements in this section of the BRs.*	emSign CP/CPS v1.01 Section 3.2, Appendix A (Section 10.1)	emSign is compliant with Baseline Requirements v1.5.4
3.2.2.6 Wildcard Domain Validation If your CA allows certificates with a wildcard character (*) in a CN or subjectAltName of type DNS-ID, then *indicate how your CA meets the requirements in this seciton of the BRs.*	emSign CP/CPS v1.01 Section 3.2, Appendix A (Section 10.1)	emSign is compliant with Baseline Requirements v1.5.4
3.2.2.7 Data Source Accuracy *Indicate how your CA meets the requirements in this section of the BRs.*	emSign CP/CPS v1.01 Section 3.2, Appendix A, Section 10 Section 1.6 (definition of reliable data source)	A data source is considered reliable only after emSign verifies for integrity and consistency
3.2.2.8 CAs MUST check and process CAA records *Indicate your CA's understanding that this section is a requirement as of September 8, 2017, and how your CA meets the requirements in this section of the BRs.*	emSign CP/CPS v1.01 Section 4.2.4	emSign verifies the existence of CAA record (RFC 6844) in applicant's DNS. If a CAA record exists and does not list emSign as an authorized CA, Issuing CA will verify that the applicant has authorized issuing CA to issue, despite existence of CAA record.
3.2.3. Authentication of Individual Identity	emSign CP/CPS v1.01 Section 3.2.3	Compliant
3.2.5. Validation of Authority	emSign CP/CPS v1.01 Section 3.2.5	Compliant
3.2.6. Criteria for Interoperation or Certification	emSign CP/CPS v1.01 Section 3.2.6	emSign CA does not have any cross-certificates

Disclose all cross-certificates in the CA hierarchies under evaluation.		
4.1.1. Who Can Submit a Certificate Application Indicate how your CA identifies suspicious certificate requests.	emSign CP/CPS v1.01 Section 4.1.1	emSign system checks high risk organizations and domains before allowing approval of certificates
4.1.2. Enrollment Process and Responsibilities	emSign CP/CPS v1.01 Section 4.1.2	emSign ensures that it receives a certificate request and enforces agreement of subscriber agreement and terms of use as part of the application process
4.2. Certificate application processing	emSign CP/CPS v1.01 Section 4.2	emSign verifies accuracy of information in requested certificate prior to issuance
4.2.1 Re-use of validation information is limited to 825 days *Indicate your CA's understanding that this is a requirement as of March 1, 2018, and indicate how your CA meets the requirements of this section.*	emSign CP/CPS v1.01 Section 3.2.7	emSign acknowledges this requirement and its Operating Procedures ensure this requirement is met
4.2.1. Performing Identification and Authentication Functions *Indicate how your CA identifies high risk certificate requests.*	emSign CP/CPS v1.01 Section 4.2.1	Request for certificates can only be made by verified individuals who have login credentials. emSign system checks high risk organizations and domains before allowing approval of certificates
4.2.2. Approval or Rejection of Certificate Applications	emSign CP/CPS v1.01 Section 4.2.2	Compliant
4.3.1. CA Actions during Certificate Issuance	emSign CP/CPS v1.01 Section 4.3.1	All certificate issuance under Root CA have dual control using trusted personnel with clear segregation of duties in place
4.9.1.1 Reasons for Revoking a Subscriber Certificate *Indicate which section in your CA's CP/CPS contains the list of reasons for revoking certificates.*	emSign CP/CPS v1.01 Section 4.9.1	Compliant
4.9.1.2 Reasons for Revoking a Subordinate CA Certificate *Indicate which section in your CA's CP/CPS contains the list of reasons for revoking subordinate CA certificates.*	emSign CP/CPS v1.01 Section 4.9.1	Compliant
4.9.2. Who Can Request Revocation	emSign CP/CPS v1.01	Compliant

	Section 4.9.2	
4.9.3. Procedure for Revocation Request	emSign CP/CPS v1.01 Section 4.9.3	CP/CPS capture the procedure for revocation request
4.9.5. Time within which CA Must Process the Revocation Request	emSign CP/CPS v1.01 Section 4.9.5	Compliant
4.9.7. CRL Issuance Frequency *Indicate if your CA publishes CRLs. If yes, then please test your CA's CRLs.*	emSign CP/CPS v1.01 Section 4.9.7	24 hours, 30 mins after revocation, Offline Issuing CA's every 3 months
4.9.9. On-line Revocation/Status Checking Availability	emSign CP/CPS v1.01 Section 4.9.9	emSign OCSP responses conform to RFC 6960 and RFC0519
4.9.10. On-line Revocation Checking Requirements *Indicate how your CA meets all of the requirements listed in this section, including support of GET, update frequency, preventing errounious return of "good" status.*	emSign CP/CPS v1.01 Section 4.9.9	emSign OCSP supports both GET and POST methods. It also implements a whitelist based check, so that, 'good' responses are given only for valid vertificates.
4.9.11. Other Forms of Revocation Advertisements Available Indicate if your CA supports OCSP stapling.	NA	NA
4.10.1. Operational Characteristics	emSign CP/CPS v1.01 Section 4.10.1	emSign does not remove revocation entries on CRL/OCSP until after expiry of the revoked certificate
4.10.2. Service Availability	emSign CP/CPS v1.01 Section 4.10.2	emSign digital certificate services are available 24x7x365
5. MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS	emSign CP/CPS v1.01 Section 5	emSign has developed, implemented, and maintains a comprehensive security program that: 1. Protects the confidentiality, integrity, and availability of Certificate Data and Certificate Management Processes; 2. Protects against anticipated threats or hazards to the confidentiality, integrity, and availability of the Certificate Data and Certificate Management Processes; 3. Protects against unauthorized or unlawful access, use, disclosure, alteration, or destruction of any Certificate Data or Certificate Management Processes; 4. Protects against accidental loss or destruction of, or damage to, any Certificate Data or Certificate Management Processes; and

		5. Complies with all other security requirements applicable to the CA by law. emSign conducts risk assessment atleast once a year to identify foreseeable internal and external threats and assess the likelihood and potential damage of these threats and sufficiency of policies, procedures, information systems, technology that emSign has in place to counter such threats emSign's holding entity eMudhra is ISO 27001 certified
5.2.2. Number of Individuals Required per Task	emSign CP/CPS v1.01 Section 5.2.2	Issuing CA Private Key are backed up, stored and recovered using dual control by trusted personnel in a physically secure environment
5.3.1. Qualifications, Experience, and Clearance Requirements	emSign CP/CPS v1.01 Section 5.3.1 and 5.3.2	emSign verifies the identity and trustworthiness for personnel engaged in Certificate Management and uses background check procedures prior to commencement of their duties
5.3.3. Training Requirements and Procedures	emSign CP/CPS v1.01 Section 5.3.3	emSign provides the following initial and continuous training and assessment to ensure personnel trusted with validation maintain a skill level that enable to perform such duties satisfactorily 1) Skills training covering PKI knowledge, authentication 2) Vetting policies and procedures, CP/CPS 3) Common threats to information verification process (phishing, social engineering tactics) emSign maintains documentation of training and that validation specialist possesses the skills required to perform a task before allowing them to perform the task
5.3.4. Retraining Frequency and Requirements	emSign CP/CPS v1.01 Section 5.3.4	emSign shall retrain personnel in trusted roles periodically to ensure they maintain skill levels consistent with CA's training and performance programs
5.3.7. Independent Contractor Controls	emSign CP/CPS v1.01 Section 5.3.7	emSign has so far only utilized internal employees as trusted personnel but will ensure that training requirements and document retention, audit logging requirements/procedures are followed before allowing third party contractors to engage.

5.4.1. Types of Events Recorded *Indicate how your CA meets the requirements of this section.*	emSign CP/CPS v1.01 Section 5.4.1	emSign is compliant with Baseline Requirements v1.5.4 and CP/CPS documents are in accordance with RFC 3647
5.4.3. Retention Period for Audit Logs	emSign CP/CPS v1.01 Section 5.4.3	emSign is compliant with Baseline Requirements v1.5.4 and CP/CPS documents are in accordance with RFC 3647
5.4.8. Vulnerability Assessments *Indicate how your CA meets the requirements of this section.*	emSign CP/CPS v1.01 Section 5.4.8	emSign performs regular internal vulnerability assessments and penetration tests emSign conducts risk assessment atleast once a year to identify foreseeable internal and external threats and assess the likelihood and potential damage of these threats and sufficiency of policies, procedures, information systems, technology that emSign has in place to counter such threats emSign's holding entity eMudhra is ISO 27001 certified
5.5.2. Retention Period for Archive	emSign CP/CPS v1.01 Section 5.4.2	emSign is compliant with Baseline Requirements v1.5.4 and CP/CPS documents are in accordance with RFC 3647 emSign will also retain records over and above the retention period in Baseline Requirements as per any applicable local law
5.7.1. Incident and Compromise Handling Procedures *Indicate how your CA meets the requirements of this section.*	emSign CP/CPS v1.01 Section 5.7.1	emSign has a business continuity plan (BCP), BCP test plan and Incident Response Plan
6.1.1. Key Pair Generation	emSign CP/CPS v1.01 Section 6.1.1	Root CA key generation follows a formal key generation scripts and is only done in the presence of a Qualified Auditor In all cases, emSign Issuing CA keys are generated and used in a physically secured environment using personnel in trusted roles with segregation of duties and multifactor authentication using split passwords/knowledge. The CA keys are generated in cryptographic modules which are FIPS 140-2 Level 3 validated. The HSM or Cryptographic Modules are always stored in a physically secured environment and subject to security controls throughout their lifecycle

6.1.2. Private Key Delivery to Subscriber	emSign CP/CPS v1.01 Section 6.1.2	As applicable in most of the cases, if the Subscriber or intended key holder generates the private key, then there is no need to deliver the Private Key. If someone other than the intended key holder is generating the key on behalf of the intended key holder (assisted mode), they ensure that sufficient security is maintained within the key generation process and any onward issuance process to the Subscriber. At all time, access to private key are protected by a PIN provided by Subscriber.
6.1.5. Key Sizes	emSign CP/CPS v1.01 Section 6.1.5	emSign is compliant with Baseline Requirements v1.5.4 and CP/CPS documents are in accordance with RFC 3647
6.1.6. Public Key Parameters Generation and Quality Checking	emSign CP/CPS v1.01 Section 6.1.6	All CA keys are generated on FIPS 140-2 qualified hardware and meets the requirements of FIPS 186-2, which ensures the proper parameters and their quality for Public Keys. Reasonable techniques are used to validate the suitability of Subscriber Public Keys. Any known weak keys are tested for and rejected at the point of submission.
6.1.7. Key Usage Purposes	emSign CP/CPS v1.01 Section 6.1.7	Private Keys corresponding to Root Certificates are not used to sign Certificates except in the following cases: 1. Self-signed Certificates to represent the Root CA itself; 2. Certificates for Subordinate CAs and Cross Certificates; 3. Certificates for infrastructure purposes (administrative role certificates, internal CA operational device certificates); and 4. Certificates for OCSP Response verification.
6.2. Private Key Protection and Cryptographic Module Engineering Controls	emSign CP/CPS v1.01 Section 6.2	emSign uses HSM or Cryptographic Modules which are FIPS 140-2 Level 3 compliant for storage of Private Keys of Root CA and Issuing CA private keys in a physically secured environment. Root CA & Subordinates are put in separate HSMs and do not share a common one for both purposes.
6.2.5. Private Key Archival	emSign CP/CPS v1.01 Section 6.2.5	After the expiry of CA Certificates, the associated key pair shall be retained securely for a period of minimum 5 years. Such storage of archival shall meet the requirement of private key

		storage (in cryptographic module). Such archived keys shall not be used for any production signing. Issuing CAs under emSign PKI shall not archive copies of Subscriber private keys.
6.2.6. Private Key Transfer into or from a Cryptographic Module	emSign CP/CPS v1.01 Section 6.2.6	CA Keys are always generated in cryptographic modules. They are copied to similar cryptographic modules for recovery / business continuity purposes. Such copying shall also happen in encrypted form, and the private key must never exist in plain text form outside the cryptographic module.
6.2.7. Private Key Storage on Cryptographic Module	emSign CP/CPS v1.01 Section 6.2.7	CA private keys are generated and stored in a physically secure environment within cryptographic modules that are validated to FIPS 140-2 Level-3.
6.3.2 Certificates issued after March 1, 2018, MUST have a Validity Period no greater than 825 days *Indicate how your CA meets the requirements of this section.*	emSign CP/CPS v1.01 Section 6.3.2	emSign has defined Operating Procedures that ensure that validity period is no greater than 825 days
6.5.1. Specific Computer Security Technical Requirements The CA SHALL enforce multi-factor authentication for all accounts capable of directly causing certificate issuance. *Indicate how your CA meets the requirements of this section.*	emSign CP/CPS v1.01 Section 6.5.1	emSign uses multifactor authentication control for all systems capable of directly causing certificate issuance
7.1. Certificate profile CAs SHALL generate non-sequential Certificate serial numbers greater than 0 containing at least 64 bits of output from a CSPRNG. *Indicate how your CA meets the requirements of this section.*	emSign CP/CPS v1.01 Section 7.1, Appendix B	emSign uses CSPRNG to generate serial numbers which are greater than 64 bits.
7.1.1. Version Number(s)	emSign CP/CPS v1.01 Section 7.1.1	X509 v.3
7.1.2. Certificate Content and Extensions; Application of RFC 5280	emSign CP/CPS v1.01 Section 7.1.2	-
7.1.2.1 Root CA Certificate	emSign CP/CPS v1.01	Compliant

	Section 7.1.2, Appendix B	
7.1.2.2 Subordinate CA Certificate	emSign CP/CPS v1.01 Section 7.1.2, Appendix B	Compliant
7.1.2.3 Subscriber Certificate	emSign CP/CPS v1.01 Section 7.1.2, Appendix B	Compliant
7.1.2.4 All Certificates	emSign CP/CPS v1.01 Section 7.1.2, Appendix B	Compliant
7.1.2.5 Application of RFC 5280	emSign CP/CPS v1.01 Section 7.1	Compliant
7.1.3. Algorithm Object Identifiers	emSign CP/CPS v1.01 Section 7.1.5	Compliant
7.1.4. Name Forms	emSign CP/CPS v1.01 Section 7.1.6	Compliant
7.1.4.1 Issuer Information	emSign CP/CPS v1.01 Section 7.1.6	Compliant
7.1.4.2 Subject Information - Subscriber Certificates	emSign CP/CPS v1.01 Section 7.1.6	Compliant
7.1.4.3 Subject Information - Root Certificates and Subordinate CA Certificates	emSign CP/CPS v1.01 Section 7.1.6	Compliant
7.1.5. Name Constraints *Indicate your CA's understanding of Mozilla's requirement to disclose in the CCADB all subordinate CA certificates that are not technically constrained as described in this section.*	Not Documented	Compliant. We understand the disclosure to be made in CCADB for all the Sub-CA certificates that are not technically constrained. These CAs are also subject to full audit as per Section 8 of CPS, and meets the BR requirements.
7.1.6. Certificate Policy Object Identifier	emSign CP/CPS v1.01 Section 7.1.4	Compliant
7.1.6.1 Reserved Certificate Policy Identifiers	emSign CP/CPS v1.01 Section 7.1.4.1	Compliant
7.1.6.2 Root CA Certificates	emSign CP/CPS v1.01 Section 7.1.4.2	Compliant
7.1.6.3 Subordinate CA Certificates	emSign CP/CPS v1.01 Section 7.1.4.3	Compliant
7.1.6.4 Subscriber Certificates	emSign CP/CPS v1.01 Section 7.1.4.4	Compliant
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS	emSign CP/CPS v1.01 Section 8	emSign is compliant with Baseline Requirements v1.5.4. Audit Reports are uploaded in Bugzilla and will be made publicly available in the repository.

8.1. Frequency or circumstances of assessment The period during which the CA issues Certificates SHALL be dividied into an unbroken sequence of audit periods. An audit period MUST NOT exceed one year in duration. For new CA Certificates: The point-in-time readiness assessment SHAL be completed no earlier than twelve months prior to issuing Publicly-Trusted Certificates and SHALL be followed by a complete audit under such scheme within ninety (90) days of issuing the first Publicly-Trusted Certificate. *Indicate your CA's understanding of this requirement, and how your CA meets the requirements of this section.*	emSign CP/CPS v1.01 Section 8.1	Compliant. Section 8.1 and 8.7 of the CP/CPS covers the annual audit and self-audit periods. Currently point-in-time audit is completed in the month of Dec-2017. We should be issuing live certificates soon and subsequently, we will be completing re-assessment within 90 days.
8.2. Identity/qualifications of assessor *Indicate how your CA meets he requirements of this section.*	emSign CP/CPS v1.01 Section 8.2	The audit services described in Section 8.1 are performed by independent, recognised, credible, and established audit firms having significant experience with PKI and cryptographic technologies. The WebTrust audits have been carried out by BDO, Malaysia.
8.4. Topics covered by assessment	emSign CP/CPS v1.01 Section 8.4	Compliant
8.6. Communication of results	emSign CP/CPS v1.01 Section 8.6	Compliant

Also indicate your understanding and compliance with Mozilla's Root Store Policy, which says: "Full-surveillance period-of-time audits MUST be conducted and updated audit information provided no less frequently than annually. Successive audits MUST be contiguous (no gaps). .... The publicly-available documentation relating to each audit MUST contain at least the following clearly-labelled information: - name of the company being audited; - name and address of the organization performing the audit; - Distinguished Name and SHA256 fingerprint of each root and intermediate certificate that was in scope; - audit criteria (with version number) that were used to audit each of the certificates; - a list of the CA policy documents (with version numbers) referenced during the audit; - whether the audit is for a period of time or a point in time; - the start date and end date of the period, for those that cover a period of time; - the point-in-time date, for those that are for a point in time; - the date the report was issued (which will necessarily be after the end date or point-in-time date); and - For ETSI, a statement to indicate if the audit was a full audit, and which parts of the criteria were applied, e.g. DVCP, OVCP, NCP, NCP+, LCP, EVCP, EVCP+, QCP-w, Part1 (General Requirements), and/or Part 2 (Requirements for trust service providers). "	Section 8 of CP/CPS	emSign is compliant with Baseline Requirements v1.5.4 as well as the Mozilla Root Store Policy and its extract provided here. Audit Reports are uploaded in Bugzilla and will be made publicly available once webtrust seal is obtained The contents of audit report covers the required information.
8.7. Self-Audits	emSign CP/CPS v1.01	

	Section 8.7	emSign controls service quality by performing quarterly self-audits against a randomly selected sample of SSL/TLS Certificates being no less than three percent of the certificates issued.
9.6.1. CA Representations and Warranties	emSign CP/CPS v1.01 Section 8.6.1	Compliant
9.6.3. Subscriber Representations and Warranties	emSign CP/CPS v1.01 Section 9.6.3	Compliant
9.8. Limitations of liability	emSign CP/CPS v1.01 Section 9.8	Compliant
9.9.1. Indemnification by CAs	emSign CP/CPS v1.01 Section 9.9.1	Compliant
9.16.3. Severability	emSign CP/CPS v1.01 Section 9.16.3	Compliant