# CERTIFICATE POLICY
# &
# CERTIFICATION PRACTICE STATEMENT
# (CP/CPS) For SSL/TLS Certificates

19-August-2025
Version 1.00

**SSL/TLS CP/CPS OID: 1.3.6.1.4.1.50977.1.0.1.1**
© Copyright: eMudhra. All rights reserved.

**emSign**

info@emsign.com | www.emsign.com

# Table of Contents

# 1. Introduction

eMudhra is a group, engaged in Digital Identity, Authentication and transaction management solutions globally. emSign PKI is part of eMudhra group, represented by eMudhra Inc., USA; CERTInext Inc., USA; eMudhra Limited, India; eMudhra Technologies Limited, India; eMudhra PTE Limited, Singapore; eMudhra DMCC, UAE; eMudhra BV, Netherlands; eMudhra Consumer Services Limited, India; P T eMudhra Technologies Indonesia, Indonesia; Cryptas International GmbH and its subsidiaries.

## 1.1. Overview

This emSign PKI (operating under the brand emSign) Certificate Policy and Certification Practice Statement (CP/CPS for Server Authentication) sets forth the principles, procedures, and practices employed by emSign PKI for the issuance, lifecycle management, and oversight of publicly trusted SSL/TLS (Server Authentication) certificates within the emSign PKI hierarchy.

In this document, the terms “emSign,” “emSign CA,” and “emSign PKI” are used interchangeably and refer collectively to all Root Certification Authorities, Issuing Certification Authorities, and affiliates of eMudhra Limited that operate under the emSign brand.

This CP/CPS is applicable to all entities having a defined relationship with the emSign PKI, including:

1. Policy Authorities,
2. Certification Authorities (CAs),
3. Registration Authorities (RAs),
4. Subscribers, and
5. Relying Parties.

Other parties, such as hosting providers, enterprise administrators, or technical integrators, may also perform functions related to certificate lifecycle management, such as issuance or revocation on behalf of Subscribers. In such cases, the principles, procedures, and practices contained in this document shall apply to such parties to the extent practicable, and they shall be held to the same compliance and liability standards as Subscribers, where applicable.

This CP/CPS specifies the principles, procedures, and practices that the emSign PKI follows to conform to the following standards, guidelines, and root program requirements:

1. RFC 3647 of the Internet Engineering Task Force (IETF):
   - Framework for Certificate Policy and Certification Practice Statement structure.
2. The latest versions (as on date of this CP/CPS) of the CA/Browser Forum Requirements (Ref: https://cabforum.org):
   - Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (TLS BR)
   - Baseline Requirements for the Issuance and Management of Extended Validation (EV) Certificates
   - Network and Certificate System Security Requirements
   - *(Note: While other CA/B Forum Baseline Requirements such as for S/MIME and Code Signing exist, they are out of scope for this SSL/TLS CP/CPS and are included here only for completeness and alignment of terminology)*
3. WebTrust: Principles and Criteria for Certification Authorities, including:

- WebTrust: Principles and Criteria for Certification Authorities – Network Security
- WebTrust: Principles and Criteria for Certification Authorities - TLS Baseline
- WebTrust: Principles and Criteria for Certification Authorities – Extended Validation TLS (where applicable)

4. Root Program Requirements of major relying party software providers:
   - Google Chrome Root Program Policy
   - Mozilla Root Store Policy
   - Apple Root Certificate Program
   - Microsoft Root Certificate Program

If any inconsistency exists between this CP/CPS and aforesaid requirements, then the aforesaid Requirements take precedence over this CP/CPS.

All certificates are issued containing the corresponding policy identifier(s) specified in section 1.2 indicating adherence to and conformance with these requirements.

This document is subject to regular review by the emSign Policy Authority, including a formal review at least once annually. It may also be amended, or exceptions granted, in order to mitigate material and imminent impacts to Subscribers, partners, Relying Parties, or other participants in the certificate ecosystem, where practical workarounds do not exist. All such exceptions are tracked, documented, and reported as part of the CA's audit and compliance processes.

All cross-certificates that form part of an established trust relationship are disclosed by emSign PKI. This CP/CPS addresses the actions of emSign PKI in relation to such cross-certificates, including those issued by emSign PKI to third parties and those issued to emSign PKI by other Certification Authorities. However, this CP/CPS does not govern the operations of third-party CAs that issue such certificates; those parties remain subject to their own certificate policies and practice statements.

## 1.2. Document Name and Identification

The OID for emSign PKI is an iso (1) identified-organization (3) dod (6) internet (1) private (4) enterprise (1) eMudhra Technologies Limited (50977) emSign PKI (1).

This document is the emSign PKI Certificate Policy and Certification Practice Statement (CP/CPS) for SSL/TLS. The object identifier (OID) values corresponding to the emSign SSL/TLS CP/CPS are as follows:

| Entity / Certificate Policy | OID |
|---|---|
| Organization | 1.3.6.1.4.1.50977 |
| emSign PKI | 1.3.6.1.4.1.50977.1 |
| emSign SSL CP/CPS | 1.3.6.1.4.1.50977.1.0.1.1 |

**Type of certificate**

The OID for Certificate Policies under emSign PKI is an iso (1) identified-organization (3) dod (6) internet (1) private (4) enterprise (1) eMudhra Technologies Limited (50977) emSign PKI (1) Certificate Type (2).

emSign PKI organizes its OID arcs for the various Certificates described in this CP/CPS as follows:

| Type of Certificate | Policy OID |
|---|---|
| SSL/TLS - Domain Validation | 2.23.140.1.2.1,<br>1.3.6.1.4.1.50977.1.2.100 |
| SSL/TLS - Organization Validation | 2.23.140.1.2.2,<br>1.3.6.1.4.1.50977.1.2.110 |
| SSL/TLS - Individual Validation | 2.23.140.1.2.3,<br>1.3.6.1.4.1.50977.1.2.115 |
| SSL/TLS - Extended Validation | 2.23.140.1.1,<br>1.3.6.1.4.1.50977.1.2.120 |
| OCSP Certificate | 1.3.6.1.4.1.50977.1.2.600 |

This CP/CPS applies to any entity asserting one or more of the emSign OIDs identified above. When a CA issues a Certificate containing one of the above-specified policy identifiers, it asserts that the Certificate was issued and is managed in accordance with the requirements applicable to that respective policy.

Subsequent revisions to this CP might contain new OID assignments for the certificate types identified above, or may be amended with new Certificate Types with corresponding new OIDs.

## 1.3. PKI Participants

### 1.3.1. Certification Authorities

The term Certification Authority (CA) is a trusted third-party entity that issues Certificates and performs all of the functions associated with issuing such Certificates under this CP/CPS. emSign PKI performs the below functions:

1. Perform tasks related to Public Key Infrastructure (PKI) functions, such as:
    a. Certificate lifecycle management
    b. Subscriber registration
    c. Certificate issuance
    d. Certificate renewal and/or rekeying
    e. Certificate distribution (if applicable)
    f. Certificate revocation
2. Provide Certificate revocation information in the form of a Certificate Revocation List (CRL) distribution point and/or Online Certificate Status Protocol (OCSP) responder.

emSign PKI operates secure facilities in order to deliver CA services by itself and/or through infrastructure, personnel and other resources of eMudhra.

The emSign PKI also issues certificates to issuing CAs and subordinate CAs. All such issuing CAs and subordinate CAs are required to operate in conformance with this CP/CPS.

Obligations of the CAs within the emSign PKI include:

- Generating, issuing and distributing public key certificates.
- Distributing CA certificates.

- Generating and publishing certificate status information (such as CRLs).
- Maintaining the security, availability, and continuity of the certificate issuance and CRL.
- signing functions.
- Providing a means for Subscribers to request revocation.
- Revoking public-key certificates.
- Periodically demonstrating internal or external audited compliance with this CP/CPS.

Issuing Certification Authorities (Issuing CAs) under the emSign PKI are operated solely by emSign or by entities that are controlled by emSign or eMudhra. Third-party organizations are not permitted to operate Issuing CAs for publicly trusted SSL/TLS certificate issuance. Issuing CAs are required to act in accordance with their respective Issuing CA Agreements and are bound by the terms of this CP/CPS and applicable industry requirements. Limited functions such as identity validation may be delegated under formal agreements. Issuing CAs may be authorized to issue and manage SSL/TLS certificates as defined in this CP/CPS. All operations are subject to emSign PKI oversight and compliance obligations.

Issuing CAs, if authorized by emSign PKI, may utilize third-party Registration Authorities (RAs) to perform Subscriber identification and domain validation in accordance with this CP/CPS. The Issuing CA remains fully responsible and liable for all validation activities performed by such RAs. All third-party RAs must operate under formal agreements, follow applicable industry requirements, and remain under the oversight of emSign PKI.

### 1.3.2. Registration Authorities

A Registration Authority (RA) is an entity that performs identification and authentication of certificate applicants, initiates or forwards revocation requests, and approves applications for renewal or re-keying of certificates on behalf of emSign CA.

The requirements in this SSL/TLS CP/CPS apply to all RAs. emSign CA may also act as an RA for certificates it issues.

emSign PKI may enter into contractual relationships with authorized entities to operate as Registration Authorities, provided they act under the oversight of emSign PKI and comply with this CP/CPS. Such RAs must follow all applicable industry requirements and the terms of their agreements. RAs may implement more restrictive validation practices internally but must not deviate from the baseline requirements set in this CP/CPS.

- Obligations of Registration Authorities within the emSign PKI include: Process digital certificate application requests
- Identifying and authenticating Subscribers in accordance with this CP/CPS
- Maintain and process all supporting documentation related to certificate application
- Receiving, authenticating and processing certificate revocation requests
- Providing suitable training to personnel performing RA functions.
- Complying with CP/CPS and emSign/Issuer CA Registration Authority Agreement

emSign also can act as a RA for the certificates it directly issues.

### 1.3.3. Subscribers

Subscribers include all end users consisting of natural persons and/or legal entities that successfully apply for the certificate and receive it. Prior to verification of identity and issuance of a Certificate, a Subscriber is an Applicant.

A Subscriber, as used herein, refers to both the Subject of the Certificate and the entity that applied for the certificate or contracted with the Issuing CA for the Certificate issuance.

Technically, CAs are also subscribers of emSign certificates either as a CA issuing a self-signed Certificate to itself (Root CA), or as a CA being issued a Certificate by a superior CA (Issuing CA / Subordinate CA).

References to “end entities” and “subscribers” in this CP/CPS, however, apply only to end-user Subscribers.

Obligations of Subscribers within the emSign PKI include:

- Generating or causing to be generated one or more asymmetric key pairs
- Submitting public keys and credentials for registration
- Providing information to the RA that is accurate and complete to the best of the Subscribers’ knowledge and belief regarding information in their certificates and identification and authentication information
- Taking appropriate measures to protect their private keys from compromise
- Promptly reporting loss or compromise of private key(s) and inaccuracy of certificate information to Issuing CA / RA
- At all times utilize the Digital Certificate in accordance with all applicable laws and regulations.
- Use the signing Key Pairs for electronic signatures in accordance with the Digital Certificate profile and any other limitations known, or which ought to be known, to the Certificate Holder.
- Discontinue the use of the digital signature Key Pair in the event that emSign/Issuing CA notifies the Certificate Holder that the emSign/Issuing CA has been compromised.
- Using its key pair(s) in compliance with this CP/CPS.
- Any other terms as per Subscriber Agreement

When using automated mechanisms such as ACME clients, emSign CERTInext, or emSign APIs for requesting, renewing, or revoking certificates, the Subscriber remains fully responsible for secure key management and adherence to the requirements of this CP/CPS. The use of such automation does not waive or reduce the Subscriber’s obligations regarding identity accuracy, private key protection, or timely revocation reporting.

### 1.3.4. Relying Parties

A Relying Party is an individual or entity that acts in reliance of a TLS certificate issued by an emSign CA. A Relying Party may or may not be a Subscriber of emSign certificates.

While relying on or using a Certificate of emSign PKI, Relying Parties are required to examine the CP/CPS and make their own judgement, and also examine the certificate in repository for expiry or revocation, etc.

Obligations of Relying Parties within the emSign PKI include:

- Confirming the validity of Subscriber public-key certificates.
- Confirming the revocation status of the certificate through CRL / OCSP.
- Verifying that Subscriber possesses the asymmetric private key corresponding to the publickey certificate (e.g., through digital signature verification).
- Confirming that the subscriber uses the public-key in the Subscriber's certificate in compliance with this SSL/TLS CP/CPS.
- Any other terms as per Relying Party Agreement.

All obligations within this section relate to Reasonable Reliance on the validity of a Digital Signature, not the accuracy of the underlying electronic record. A Relying Party must exercise Reasonable Reliance as set out in this section. This CP/CPS does not require a Certificate Holder to ensure that potential relying parties are compliant with the relying party obligations.

### 1.3.5. Other Participants

Other participants may include bridge CAs and CAs that cross-certify Issuing CAs to provide trust among other PKI communities.

emSign Roots and Subordinate CAs shall not cross-certify or bridge any third-party CA where such third-party CA would derive SSL/TLS issuing capabilities under the emSign PKI hierarchy.

#### 1.3.5.1. emSign CERTInext Enterprise and Partner Accounts

Participants within the emSign PKI ecosystem may include authorized entities using the emSign CERTInext platform, such as Enterprise account holders and Partners. These participants may initiate or manage certificate requests through web portals or APIs for their own organizational needs or on behalf of end-user Subscribers. All such activities are performed under emSign's control, and these entities do not operate as Certification Authorities (CAs) or Registration Authorities (RAs).

Enterprise account holders may streamline certificate lifecycle actions (including request, renewal, and revocation) within the boundaries of pre-approved identity and domain validations. Partners are permitted to request certificates for their clients subject to prior authorization and must comply with all applicable agreements and this CP/CPS. emSign PKI retains full responsibility for validation, issuance, and auditability of these interactions.

## 1.4. Certificate Usage

A digital certificate enables individuals or entities to prove their identity in electronic transactions to other participants in such transactions.

### 1.4.1. Appropriate Certificate Uses

Certificates issued under this CP/CPS are intended solely for use in TLS Server Authentication (id-kp-serverAuth, OID 1.3.6.1.5.5.7.3.1), as indicated by the Key Usage and Extended Key Usage (EKU) extensions included in the certificate.

These certificates enable secure communication by authenticating the identity of a server and establishing encrypted TLS sessions with client systems, such as web browsers or applications. Subscribers are responsible for selecting the appropriate certificate type based on the intended usage and assurance level required for their deployment environment.

emSign issues the following SSL/TLS certificate profiles:

- Domain Validated (DV) Certificates: Intended for securing server communications where domain ownership/control has been validated. These certificates are suitable for basic encryption use cases where organizational identity is not required.
- Organization Validated (OV) Certificates: Intended for use where moderate assurance of the server operator's identity is needed. OV certificates include verified organization information in the certificate subject.
- Extended Validation (EV) Certificates: Provide the highest level of assurance by verifying the legal identity, physical presence, and operational existence of the organization. EV certificates clearly identify the legal entity controlling the domain and are issued in accordance with the CA/B Forum EV Guidelines.
- Multi-Domain Certificates (MDCs): Support multiple Fully Qualified Domain Names (FQDNs) listed in the subjectAltName extension. These may be issued under DV, OV, or EV profiles, depending on validation.
- Wildcard Certificates: Enable encryption for all first-level subdomains under a single domain (e.g., *.example.com). Wildcard certificates are available for DV and OV certificates only. Wildcard domain names SHALL NOT be included in EV Certificates, in accordance with CA/B Forum requirements.

The Subscriber must ensure that each certificate is used solely for its intended purpose and in accordance with this CP/CPS, applicable agreements, and published certificate profiles.

This section defines the intended technical usage of certificates as governed by their certificate profile and extensions. It does not constitute a representation or guarantee of fitness for a particular purpose. Assurance levels vary based on certificate type and are subject to applicable validation procedures and the Subscriber Agreement.

### 1.4.2. Prohibited Applications and Certificate Uses

emSign certificates shall not be used for any purpose that is inconsistent with their stated Key Usage or Extended Key Usage (EKU) extensions or outside the scope defined in this CP/CPS and associated certificate profile.

Prohibited uses include, but are not limited to, the following:

1. Use inconsistent with certificate extensions: Any use of the certificate that exceeds the technical purposes indicated by the Key Usage or Extended Key Usage extensions (e.g., using a TLS certificate for code signing or S/MIME).
2. Exceeding reliance limits: Any use that exceeds the designated reliance limits as specified in the emSign Warranty or Subscriber Agreement.
3. Use in high-risk environments: Use of certificates for control or operation of systems where failure could result in death, personal injury, or severe environmental harm, including but not limited to:
    - Nuclear facilities
    - Aircraft navigation or communication systems
    - Life support or medical devices
    - Critical infrastructure or fail-safe systems
4. Use in unlawful or harmful activities: Use of certificates in connection with or to facilitate illegal or harmful conduct, including but not limited to:

- Fraud
- Pornography or child sexual abuse material (CSAM)
- Obscenity
- Defamation or harassment
- Hate speech
- Any activity contrary to public policy or applicable law

5. Man-in-the-middle (MITM) or unauthorized interception: Use of certificates for MITM attacks or inspection of encrypted traffic involving domains or IP addresses not legitimately owned or controlled by the Subscriber is strictly prohibited.
6. Certificate misuse by role:
    - End-entity certificates must not be used to issue other certificates or act as a Certification Authority (CA).
    - CA certificates must not be used to perform end-entity functions, such as document signing or server authentication.
7. Violation of laws or regulations: Use of certificates must comply with all applicable laws, statutes, regulations, court orders, and governmental mandates.

emSign certificates do not guarantee that the Subject is reputable, trustworthy, or operating a secure system, nor do they imply that the device or software where the certificate is installed is free from defect, malware, or vulnerabilities.

The Key Usage and Extended Key Usage extensions are intended to technically enforce permitted usage. All Subscribers and relying parties must ensure that certificates are only used for the designated purposes, consistent with applicable agreements and this CP/CPS.

## 1.5. Policy Administration

These emSign PKI policies are administered by emSign Policy Authority.

Obligations of the emSign PKI Policy Authority include:

- Approving and maintaining this CP/CPS.
- Interpreting adherence to this CP/CPS.
- Specifying the content of public-key certificates.
- Resolving or causing resolution of disputes related to this CP/CPS.
- Remaining current regarding security threats and ensuring that appropriate actions are taken to counteract significant threats.

### 1.5.1. Organization Administering the Document

emSign PKI Policy Authority can be contacted at the following address:

emSign PKI Policy Authority
eMudhra Technologies Limited (eMudhra Group Company)
12-P1-A & 12-P1-B, Hi-Tech Defence and Aerospace Park (IT sector),
Jala Hobli, B.K. Palya,
Bangalore - 562149, Karnataka, India
Phone: +91 80 48484090
Email: info@emsign.com
Website: www.emsign.com

### 1.5.2. Contact Person

emSign PKI Policy Director can be contacted at the following address:

Attn: Policy Director emSign
PKI Policy Authority
eMudhra Technologies Limited (eMudhra Group Company)
12-P1-A & 12-P1-B, Hi-Tech Defence and Aerospace Park (IT sector),
Jala Hobli, B.K. Palya
Bangalore - 562149, Karnataka, India
Phone: +91 80 48484090
Email: info@emsign.com
Website: www.emsign.com

### 1.5.3. Certificate Problem Reporting

To report problems with a certificate issued by emSign or request revocation, parties may contact emSign or use one of the supported automated mechanisms.

#### 1.5.3.1. Email Contact

Certificate-related issues such as key compromise, certificate misuse, or suspected fraudulent issuance may be reported via email:
Attn: Revocation Support
Email: problem-reporting@emsign.com

#### 1.5.3.2. CERTInext Portal

Subscribers, partners, and authorized users may initiate certificate revocation requests through the emSign CERTInext Portal using the certificate management dashboard that is available via Login using:
URL: https://www.emsign.com

#### 1.5.3.3. Enterprise API / Partner Integrations

Enterprise customers and authorized partners integrated with emSign via secure APIs may submit certificate revocation requests programmatically. API access must be pre-authorized and authenticated in accordance with the emSign API Specifications.

#### 1.5.3.4. ACME revokeCert Endpoint

For ACME-enabled accounts, certificate revocation may also be requested using the ACME revokeCert method if the Subscriber is in possession of the corresponding private key.

ACME Directory: https://acme.emsign.com/v1/directory
RevokeCert Endpoint: https://acme.emsign.com/v1/acme/revokeCert

emSign authenticates all revocation requests based on the requester's identity and relationship to the certificate. Requests submitted through trusted channels by Subscribers or Subject Organizations are verified using registered credentials or account-based validation. Requests from third parties may undergo additional investigation or corroboration prior to revocation. All revocation requests and corresponding actions are logged and processed in accordance with this CP/CPS.

### 1.5.4. Person Determining CP/CPS Suitability for the Policy

The CP/CPS suitability for the functions and uses of participants is decided by the Policy Authority of emSign PKI. The Policy Authority consists of representatives from executive management, PKI operations and legal.

### 1.5.5. CPS Approval Procedures

The CP/CPS shall be reviewed and updated by emSign at least annually, or more frequently as needed to reflect changes in applicable standards, policies, or operational practices. All changes are subject to approval by the emSign Policy Authority. Updates may be initiated in response to new or revised CA/Browser Forum Baseline Requirements, root store policies, or other compliance obligations that require corresponding modifications to the CP or CPS.

## 1.6. Definitions & Acronyms

### 1.6.1. Definitions

**Affiliate**: A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.

**Applicant Representative:** A natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: (i) who signs and submits, or approves a certificate request on behalf of the Applicant; and/or (ii) who signs and submits a Subscriber Agreement on behalf of the Applicant; and/or (iii) who acknowledges the Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA or is the CA.

**Applicant**: The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual certificate request.

**Application Software Supplier**: A supplier of Internet browser software or other relying-party application software that displays or uses Certificates and incorporates Root Certificates.

**Attestation Letter**: A letter attesting that Subject Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information.

**Audit Period**: In a period-of-time audit, the period between the first day (start) and the last day of operations (end) covered by the auditors in their engagement. (This is not the same as the period of time when the auditors are on-site at the CA.) The coverage rules and maximum length of audit periods are defined in this CP/CPS.

**Audit Report:** A report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the mandatory provisions of these Requirements.

**Authorization Domain Name**: The Domain Name used to obtain authorization for certificate issuance for a given FQDN. The CA may use the FQDN returned from a DNS CNAME lookup as the FQDN for the

purposes of domain validation. If the FQDN contains a wildcard character, then the CA MUST remove all wildcard labels from the left most portion of requested FQDN. The CA may prune zero or more labels from left to right until encountering a Base Domain Name and may use any one of the intermediate values for the purpose of domain validation.

**Authorized Port**: One of the following ports: 80 (http), 443 (http), 115 (sftp), 25 (smtp), 22 (ssh).

**Base Domain Name:** The portion of an applied for FQDN that is the first domain name node left of a registry controlled or public suffix plus the registry controlled or public suffix (e.g. "example.co.uk" or "example.com"). For FQDNs where the right most domain name node is a gTLD having ICANN Specification 13 in its registry agreement, the gTLD itself may be used as the Base Domain Name.

**Baseline Requirements (BR)**: Means the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, published at https://www.cabforum.org

**Basic Constraints**: Means an extension that specifies whether the subject of the Certificate may act as a CA or only as an end-entity

**CA Key Pair**: A Key Pair where the Public Key appears as the Subject Public Key Info in one or more Root CA Certificate(s) and/or Subordinate CA Certificate(s)

**CAA**: The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify the Certification Authorities (CAs) authorized to issue certificates for that domain. Publication of CAA Resource Records allows a public Certification Authority to implement additional controls to reduce the risk of unintended certificate misuse.

**Certificate Data**: Certificate requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA's possession or control or to which the CA has access.

**Certificate Management Process**: Processes, practices, and procedures associated with the use of keys, software, and hardware, by which the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.

**Certificate Policy**: A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.

**Certificate Problem Report**: Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.

**Certificate Profile**: A set of documents or files that defines requirements for Certificate content and Certificate extensions in accordance with Section 7, e.g. a Section in a CA's CPS or a certificate template file used by CA software.

**Certificate Revocation List**: A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.

**Certificate System**: Means the system used by emSign or a delegated third party in providing identity verification, registration and enrollment, Certificate approval, issuance, validity status, support, and other PKI-related services

**Certificate Transparency**: Means the protocol described in RFC 6962 for publicly logging the existence of Transport Layer Security (TLS) certificates as they are issued or observed.

**Certificate**: An electronic document that uses a digital signature to bind a public key and an identity.

**Certificate Data**: Certificate requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA's possession or control or to which the CA has access.

**Certification Authority Authorization (CAA)**: Means a DNS domain holder specify one or more CAs authorized to issue certificates for that domain name. This is described in RFC 8659

**Certification Authority**: An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Roots CAs and Subordinate CAs.

**Certification Practice Statement**: One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.

**Common Criteria**: Is a framework in which computer system users can specify their security functional and assurance requirements (SFRs and SARs respectively) in a Security Target (ST), and may be taken from Protection Profiles (PPs). It is an international standard (ISO/IEC 15408) for computer security certification

**Control**: "Control" (and its correlative meanings, "controlled by" and "under common control with") means possession, directly or indirectly, of the power to: (1) direct the management, personnel, finances, or plans of such entity; (2) control the election of a majority of the directors; or (3) vote that portion of voting shares required for "control" under the law of the entity's Jurisdiction of Incorporation or Registration but in no case less than 10%.

**Country**: Either a member of the United Nations OR a geographic region recognized as a Sovereign State by at least two UN member nations.

**Critical Vulnerability**: A system vulnerability that has a CVSS v2.0 score of 7.0 or higher according to the NVD or an equivalent to such CVSS rating (see http://nvd.nist.gov/home.cfm https://nvd.nist.gov/vuln-metrics/cvss), or as otherwise designated as a Critical Vulnerability by the CA or the CA/Browser Forum

**Cross Certificate**: A certificate that is used to establish a trust relationship between two Root CAs.

**CSPRNG**: A random number generator intended for use in cryptographic system.

**Delegated Third Party**: A natural person or Legal Entity that is not the CA but is authorized by the CA to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.

**Domain Authorization Document**: Documentation provided by, or a CA's documentation of a communication with, a Domain Name Registrar, the Domain Name Registrant, or the person or entity listed in WHOIS as the Domain Name Registrant (including any private, anonymous, or proxy registration service) attesting to the authority of an Applicant to request a Certificate for a specific Domain Namespace.

**Domain Contact**: The Domain Name Registrant, technical contact, or administrative contract (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record.

**Domain Label**: From RFC 8499 (http://tools.ietf.org/html/rfc8499): "An ordered list of zero or more octets that makes up a portion of a domain name. Using graph theory, a label identifies one node in a portion of the graph of all possible domain names."

**Domain Name Registrant**: Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.

**Domain Name Registrar**: A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN); (ii) a national Domain Name authority/registry; or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns).

**Domain Name**: The label assigned to a node in the Domain Name System.

**Domain Namespace**: The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.

**Enterprise RA**: An employee or agent of an organization unaffiliated with the CA who authorizes issuance of Certificates to that organization.

**EV Code Signing Certificate**: CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates published at https://www.cabforum.org

**EV Guidelines (EVG)**: CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates published at https://www.cabforum.org

**Expiry Date**: The "Not After" date in a Certificate that defines the end of a Certificate's validity period.

**Fully-Qualified Domain Name**: A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.

**Government Entity**: A government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).

**Grace Period**: Means the period during which the Subscriber must make a revocation request.

**High Risk Certificate Request**: A Request that the CA flags for additional scrutiny by reference to internal criteria and databases maintained by the CA, which may include names at higher risk for phishing or other fraudulent usage, names contained in previously rejected certificate requests or revoked Certificates, names listed on the Miller Smiles phishing list or the Google Safe Browsing list, or names that the CA identifies using its own risk-mitigation criteria.

**Internal Name**: A string of characters (not an IP address) in a Common Name or Subject Alternative Name field of a Certificate that cannot be verified as globally unique within the public DNS at the time of certificate issuance because it does not end with a Top Level Domain registered in IANA's Root Zone Database.

**IP Address**: A 32-bit or 128-bit number assigned to a device that uses the Internet Protocol for communication.

**Issuing CA**: In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.

**Key Compromise**: A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, an unauthorized person has had access to it, or there exists a practical technique by which an unauthorized person may discover its value. A Private Key is also considered compromised if methods have been developed that can easily calculate it based on the Public Key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys) or if there is clear evidence that the specific method used to generate the Private Key was flawed.

**Key Generation Script**: A documented plan of procedures for the generation of a CA Key Pair.

**Key Pair**: The Private Key and its associated Public Key.

**Legal Entity**: An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.

**Multi-Perspective Issuance Corroboration**: A process in which the results of domain validation and CAA checking performed by the Primary Network Perspective are confirmed by additional Network Perspectives prior to issuing a certificate.

**Network Perspective**: Related to Multi-Perspective Issuance Corroboration. A Network Perspective refers to a system (such as a cloud-hosted server) or a group of network elements (like a VPN and its supporting infrastructure) used to send outbound Internet traffic during domain control validation and/or CAA checking. The location of a Network Perspective is defined as the point where outbound Internet traffic before any encapsulation is initially passed to the Internet service provider or network infrastructure responsible for connectivity.

**Object Identifier**: A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.

**OCSP Responder**: An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests.

**Online Certificate Status Protocol**: An online Certificate-checking protocol that enables relying party application software to determine the status of an identified Certificate.

Online Channel: Refers to emSign's online platforms such as CERTInext, ACME, API, and any other internet-based interfaces or services that enable Subscribers or Relying Parties to access emSign services through automated or self-service mechanisms.

**Parent Company**: A company that Controls a Subsidiary Company.

**Private Key**: The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

**Public Key Infrastructure**: A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.

**Public Key**: The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

**Publicly-Trusted Certificate**: A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software.

**Qualified Auditor**: A natural person or Legal Entity that meets the requirements of this CP/CPS.

**Random Value**: A value specified by a CA to the Applicant that exhibits at least 112 bits of entropy.

**Registered Domain Name**: A Domain Name that has been registered with a Domain Name Registrar.

**Registration Authority (RA)**: Any Legal Entity that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the certificate application process or revocation process or both. When “RA” is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.

**Reliable Data Source**: An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate. The accuracy of the Reliable Data Source is evaluated for the source for its reliability, accuracy, and resistance to alteration or falsification. Such evaluation considers the age of the information, update frequency by such source, the data provider and the purpose of data collection, the accessibility of such data to public, the relative difficulty in falsifying or altering the data. The database maintained by emSign PKI where it was primarily collected for fulfilling the validation is not qualified as the Reliable Data Source.

**Reliable Method of Communication**: A method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Representative.

**Relying Party Agreement**: means an agreement between emSign and a Relying Party that must be read and accepted by a Relying Party prior to validating, relying on or using a Certificate and is available for reference in the Repository.

**Relying Party**: Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such Supplier merely displays information relating to a Certificate.

**Repository**: An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.

**Request Token**: A value derived in a method specified by the CA which binds this demonstration of control to the certificate request. The Request Token SHALL incorporate the key used in the certificate request. A Request Token MAY include a timestamp to indicate when it was created. A Request Token MAY include other information to ensure its uniqueness. A Request Token that includes a timestamp SHALL remain valid for no more than 30 days from the time of creation. A Request Token that includes a timestamp SHALL be treated as invalid if its timestamp is in the future. A Request Token that does not include a timestamp is valid for a single use and the CA SHALL NOT re-use it for a subsequent validation. The binding SHALL use a digital signature algorithm or a cryptographic hash algorithm at least as strong as that to be used in signing the certificate request.

**Required Website Content**: Either a Random Value or a Request Token, together with additional information that uniquely identifies the Subscriber, as specified by the CA.

**Reserved IP Address**: An IPv4 or IPv6 address that the IANA has marked as reserved:
http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml
http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml

**Root CA System**: Means a system used to create a Root Certificate or to generate, store, or sign with the Private Key associated with a Root Certificate.

**Root CA**: The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.

**Root Certificate**: The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.

**Sovereign State**: A state or country that administers its own government, and is not dependent upon, or subject to, another power.

**Subject Identity Information**: Information that identifies the Certificate Subject. Subject Identity Information does not include a domain name listed in the subjectAltName extension or the Subject commonName field.

**Subject**: The Subject is either the Subscriber or a device under the control and operation of the Subscriber.

**Subordinate CA**: A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.

**Subscriber Agreement**: An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.

**Subscriber**: A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use.

**Subsidiary Company**: A company that is controlled by a Parent Company.

**Technically Constrained Subordinate CA Certificate**: A Subordinate CA certificate which uses a combination of Extended Key Usage settings and Name Constraint settings to limit the scope within which the Subordinate CA Certificate may issue Subscriber or additional Subordinate CA Certificates.

**Terms of Use**: Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with these Requirements when the Applicant/Subscriber is an Affiliate of the CA or is the CA.

**Test Certificate**: A Certificate with a maximum validity period of 30 days and which: (i) includes a critical extension with the specified Test Certificate CABF OID, or (ii) is issued under a CA where there are no certificate paths/chains to a root certificate subject to these Requirements.

**Trustworthy System**: Computer hardware, software, and procedures that are: reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy.

**Unregistered Domain Name**: A Domain Name that is not a Registered Domain Name.

**Valid Certificate**: A Certificate that passes the validation procedure specified in RFC 5280.

**Validation Specialists**: Someone who performs the information verification duties specified in this CP/CPS . This includes the RA / Trusted Personnel of CA.

**Validity Period:** The period of time measured from the date when the Certificate is issued until the Expiry Date.

**Verified Method of Communication**: Method of communication as defined and verified in conformance with Section 11.5 of the EVG

**WebTrust for Certification Authorities**: Means the current program for CAs located at CPA Canada Webtrust Principles and Criteria.

**WHOIS**: Information retrieved directly from the Domain Name Registrar or registry operator via the protocol defined in RFC 3912, the Registry Data Access Protocol defined in RFC 7482, or an HTTPS website

**Wildcard Certificate**: A Certificate containing an asterisk (*) in the left-most position of any of the Subject Fully-Qualified Domain Names contained in the Certificate.

**Wildcard Domain Name**: A Domain Name consisting of a single asterisk character followed by a single full stop character (*.) followed by a FQDN

**X.509**: Means the ITU-T standard for Certificates and their corresponding authentication framework

### 1.6.2. Acronyms

| # | Acronyms | Meaning |
|---|---|---|
| 1 | ACME | Automated Certificate Management Environment |
| 2 | AICPA | American Institute of Certified Public Accountants |
| 3 | API | Application Programming Interface |
| 4 | CA | Certification Authority |
| 5 | CAA | Certification Authority Authorization |
| 6 | CABF | CA/Browser Forum |
| 7 | ccTLD | Country Code Top-Level Domain |
| 8 | CICA | Canadian Institute of Chartered Accountants |
| 9 | CP | Certificate Policy |
| 10 | CPS | Certification Practice Statement |
| 11 | CRL | Certificate Revocation List |
| 12 | CSR | Certificate Signing Request |
| 13 | DBA | Doing Business As |
| 14 | DBA | Database Administrator |
| 15 | DN | Distinguished Names |
| 16 | DNS | Domain Name System |
| 17 | DSA | Digital Signature Algorithm |
| 18 | DV | Domain Validated |
| 19 | ECDSA | Elliptic Curve Digital Signature Algorithm |
| 20 | EKU | Extended Key Usage |
| 21 | EV | Extended Validation |
| 22 | FIPS | (US Government) Federal Information Processing Standard |
| 23 | FQDN | Fully-Qualified Domain Name |
| 24 | GET | Get Everything Transmitted |
| 25 | HTTP | Hypertext Transfer Protocol |
| 26 | IANA | Internet Assigned Numbers Authority |
| 27 | ICANN | Internet Corporation for Assigned Names and Numbers |
| 28 | IDN | Internationalized domain names |
| 29 | IDS | Intrusion Detection System |
| 30 | IETF | Internet Engineering Task Force |
| 31 | IPS | Intrusion Prevention System |

| | | |
|---|---|---|
| 32 | ISO | International Organization for Standardization |
| 33 | MITM | Man-in-the-middle |
| 34 | MPIC | Multi-Perspective Issuance Corroboration |
| 35 | NIST | National Institute of Standards and Technology (USA) |
| 36 | NTP | Network Time Protocol |
| 37 | OCSP | Online Certificate Status Protocol |
| 38 | OID | Object Identifier |
| 39 | OV | Organization Validated |
| 40 | PKI | Public Key Infrastructure |
| 41 | POST | Power-On Self-Test |
| 42 | PQC | Post Quantum Cryptography |
| 43 | PSL | public suffix list |
| 44 | RA | Registration Authority |
| 45 | RSA | Rivest Shamir Adleman |
| 46 | SMIME | Secure MIME (Multipurpose Internet Mail Extensions) |
| 47 | SAN | Subject Alternative Name |
| 48 | SOA | Statement of Applicability |
| 49 | SSL | Secure Sockets Layer |
| 50 | TLS | Transport Layer Security |
| 51 | TSA | Time Stamp Authority |
| 52 | URL | Uniform Resource Locator |
| 53 | UTC | Coordinated Universal Time |
| 54 | VESDA | Very Early Smoke Detection Appliance |

# 2. Publication and Repository Responsibilities

## 2.1. Repositories

The emSign PKI online repository is available at:
https://repository.emsign.com

The repository ensures that emSign PKI's Root Certificates, publicly trusted Subordinate CA Certificates, and revocation data (CRLs and/or OCSP responses) are available 24 hours a day, 7 days a week, with a minimum availability of 99.5% annually, excluding scheduled maintenance downtime not exceeding 0.5% per year.

Each Issuing CA operating under the emSign PKI hierarchy shall ensure that relevant certification information, including Root and Subordinate CA Certificates, Cross-Certificates (if any), revocation data, this CP/CPS, and applicable Subscriber and Relying Party Agreements, is published in the emSign repository or other designated location, in accordance with applicable policies and obligations.

emSign PKI reserves the right to withhold publication of any information deemed confidential or security-sensitive.

Repository Responsibilities Include:

- Storing and distributing public key certificates
- Storing and distributing certificate status information (CRLs and/or OCSP)

- Publishing this CP/CPS and updates thereto
- Publishing applicable Subscriber and Relying Party Agreements

### 2.2. Publication of Certificate Information

emSign and other Issuer CAs shall make the following information publicly accessible on the web:

- All publicly trusted root Certificates.
- Cross Certificates (If applicable).
- Certificate Revocation Lists (CRLs)
- Test websites for the roots (wherever applicable)
- CP/CPS
- Subscriber and Relying Party Agreements

Pointers to repository information in CA and end entity Certificates shall only contain valid Uniform Resource Identifiers (URIs) that are accessible by relying parties.

### 2.3. Time or Frequency of Publication

emSign and other Issuer CA shall publish CA certificates and revocation data as soon as possible after issuance.

CAs shall publish new or modified versions of CP/CPS within seven days of their approval. The CP/CPS is subjected to minimum of one annual review, even if there are no external factors influencing the changes in CP/CPS. Such review shall amend the version and date of publication of CP/CPS, as approved by Policy Authority.

### 2.4. Access Controls on Repository

The information published in the emSign PKI online repository is publicly accessible and provided with unrestricted, read-only access. This includes CA certificates, CRLs, CP/CPS documents, and Subscriber and Relying Party Agreements.

emSign has implemented appropriate logical and physical safeguards to prevent unauthorized modification, insertion, or deletion of repository content. Only duly authorized personnel may manage repository contents, ensuring the integrity, authenticity, and availability of published information at all times.

## 3. Identification and Authentication

emSign issues different types of SSL/TLS certificates, and the verification process depends on the type of certificate being requested. Before issuance, relevant checks are performed to confirm domain ownership, verify organization details, and validate the authority of the requester where applicable. These identification and authentication activities are carried out either by emSign or by Registration Authorities authorized by emSign, following the requirements defined in this CP/CPS.

## 3.1. Naming

### 3.1.1. Types of Names

All names included in SSL/TLS certificates issued by emSign PKI conform to X.500 and X.501 Distinguished Name (DN) standards. The Subject field is populated according to the applicable certificate profile and is used to identify the certificate subscriber. The specific DN attributes included may vary based on the certificate type and profile but are never left empty.

### 3.1.2. Need for Names to be Meaningful

All certificates issued under this CP/CPS whether for Root CAs, Issuing CAs, or end-entity Subscribers contain Subject Distinguished Names (DNs) that are meaningful and conform to X.500/X.501 and RFC 5280 standards.

For SSL/TLS end-entity certificates, the Subject DN is constructed to allow relying parties to reliably identify the entity controlling the domain(s) listed. The Common Name (CN) typically contains a fully qualified domain name (FQDN), and the Organization (O) attribute, when present, reflects the legal name of the Subscriber. The subjectAlternativeName (SAN) extension is always present and is the primary identifier used for domain validation.

For Root and Issuing CA certificates, the Subject DN identifies the CA entity and clearly reflects its role and authoritative namespace. The Subject name in a CA certificate MUST match the Issuer name in certificates it issues, as required by RFC 5280.

Requests involving internationalized domain names (IDNs) are subject to additional review and risk analysis before certificate issuance.

### 3.1.3. Anonymity or Pseudonymity of Subscribers

CA and subscriber certificates shall not contain anonymous or pseudonymous identities.

### 3.1.4. Rules for Interpreting Various Name Forms

Distinguished Names in Certificates are interpreted using X.500 standards and ASN.1 syntax. For URIs and HTTP References, refer RFC 2253 and 2616 for further information on how X.500 distinguished names in certificates are interpreted.

### 3.1.5. Uniqueness of Names

Each certificate issued by emSign under this CP/CPS includes a unique serial number generated using a cryptographically secure random process. While the Subject Distinguished Name (DN) may be reused across multiple certificates for the same Subscriber, the domain names listed in the subjectAlternativeName extension are validated for control by the Subscriber. Domain name uniqueness is inherently managed by ICANN as part of the global DNS infrastructure.

### 3.1.6. Recognition, Authentication, and Role of Trademarks

emSign requires that Certificate Applicants avoid including names in their certificate requests that may infringe upon the intellectual property rights of others. While emSign evaluates subject information in line with applicable certificate validation requirements, it does not independently assess trademark ownership, nor does it adjudicate disputes related to trademarks, service marks, or trade names.

If emSign becomes aware of a potential rights conflict, it reserves the right to deny or revoke a certificate application to protect the integrity of the PKI. In the case of Extended Validation (EV) SSL/TLS Certificates, any subject information containing an organization's name, trade name, or related identifiers is verified through documented processes as specified in this CP/CPS and aligned with EV SSL/TLS Certificate guidelines of CAB Forum.

## 3.2. Initial Identity Validation

emSign PKI, through its Issuing CAs or authorized Registration Authorities, validates the identity of Applicants prior to issuing SSL/TLS certificates. For domain validation, emSign uses methods approved under the CA/Browser Forum Baseline Requirements, such as DNS record verification, HTTP file-based validation, and CAA record checking. For Organization Validated (OV) and Extended Validation (EV) certificates, emSign verifies the legal existence, identity, and operational presence of the Applicant using trusted government records or qualified information sources. Reuse of validated Applicant information is permitted only when associated with a verified account and if the information remains current and within the validity period defined by this CP/CPS. Identity validation procedures may be revised to meet updated policy, compliance, or legal obligations.

### 3.2.1. Method to Prove Possession of Private Key

For SSL/TLS certificates, the Applicant must demonstrate control of the private key corresponding to the public key in the certificate request. This is typically done by submitting a PKCS#10 Certificate Signing Request (CSR) that is signed using the private key. Other industry-approved methods may be used, subject to emSign PKI's validation and approval.

emSign PKI does not generate key pairs for end-entity SSL/TLS certificates that include the id-kp-serverAuth or anyExtendedKeyUsage EKU values. The Subscriber is responsible for secure key generation and protection. This ensures the Subscriber maintains sole control over the private key, as required by the CA/Browser Forum Baseline Requirements.

### 3.2.2. Authentication of Organization Identity

If a Certificate asserts the identity of an Organization, emSign or its authorized Registration Authorities shall validate the organization's legal name, address, and existence using reliable third-party sources such as government business registries. Operational existence may also be confirmed as applicable. All validations are conducted in accordance with the certificate type and procedures outlined in Appendix A.

### 3.2.3. Authentication of Individual Identity

If a Certificate asserts the identity of an individual, emSign or its authorized Registration Authorities shall validate the individual's name and identity using reliable government-issued photo identification and trusted data sources. The specific procedures followed depend on the certificate type and are described in Appendix A.

### 3.2.4. Non-Verified Certificate Holder Information

emSign does not include unverified information in publicly trusted SSL/TLS certificates. Any information appearing in a certificate is subject to verification as per the applicable validation requirements. However, in limited cases, non-verified information may be included in certificates

issued solely for internal demonstration or testing purposes. These certificates are clearly marked as Test or Demonstration Certificates and are not intended for public trust or use in production environments.

### 3.2.5. Validation Of Authority

When a certificate request includes an Organizational Name, emSign or its authorized Registration Authorities shall validate that the Applicant is duly authorized to act on behalf of the Organization. This validation includes confirming the Applicant's role, position, or explicit authorization using verified organizational records, direct confirmation from authoritative contacts within the Organization, or other reliable and documented sources. The method of validation may vary based on the certificate type and ensures that only appropriately authorized individuals can submit certificate requests on behalf of the Organization.

### 3.2.6. Criteria for interoperation

Cross-certification, where performed, does not grant any certificate issuance rights or control over CA private keys to external entities. Any interoperation for trust path compatibility must fully comply with this CP/CPS, maintain exclusive control by emSign or eMudhra over all issuance processes and keys, and be subject to approval by the emSign Policy Authority.

## 3.3. Identification and authentication for re-key requests

For CA Certificates, re-keying is permitted by issuing a new certificate with an extended validity period for the same Distinguished Name (DN).

For Subscriber Certificates, re-keying (renewal) may be allowed using previously validated information only if the original identification and authentication (I&A) was performed within the respective periods outlined below in the table in 3.3.1. for Domain Validated (DV) and Organization Validated (OV) TLS certificates, or as specified for Extended Validation (EV) certificates, based on applicable guidelines and certificate type.

In such cases, and only if the certificate has not been revoked, emSign PKI may accept the renewal request using a previously verified Certificate Signing Request (CSR), or permit re-authentication via secure methods such as a passphrase, shared secret, account-based authentication, or any other mechanism approved by emSign PKI. Renewal or re-keying based on a revoked certificate is explicitly prohibited.

### 3.3.1. Identification and Authentication for Routine Re-Key

Re-keying is a process where new private key / key pair is generated by the subscriber and a request is made to provide certificate, with information similar to a previous certificate.

Subscribers may request Re-key any number of times during the validity period of the certificate. Rekeyed Certificate has a 'Valid Till' date which equals the 'Valid Till' date of the certificate that is being re-issued.

Where the initial Subscriber identification & authentication process as per this CP/CPS will be been performed as below:

| Validation Type | Certificate Issued On or After | Certificate Issued Before | Maximum Data Reuse Period | Re-Key Authentication Condition |
|---|---|---|---|---|
| Subject Identity Information Validation | March 15, 2026 | | 825 days | Re-key allowed using passphrase, shared secret, or other mechanism if initial identification completed within 825 days. |
| Subject Identity Information Validation | | March 15, 2026 | 398 days | Re-key allowed using passphrase, shared secret, or other mechanism if initial identification completed within 398 days. |
| Domain Name and IP Address Validation | March 15, 2026 | | 398 days | Must be validated within this period prior to certificate issuance. |
| Domain Name and IP Address Validation | March 15, 2026 | March 15, 2027 | 200 days | Must be validated within this period prior to certificate issuance. |
| Domain Name and IP Address Validation | March 15, 2027 | March 15, 2029 | 100 days | Must be validated within this period prior to certificate issuance. |
| Domain Name and IP Address Validation | March 15, 2029 | | 10 days | Must be validated within this period prior to certificate issuance. |
| EV (Extended Validation) | — | — | As per EV guidelines | Re-key authentication must follow EV Guidelines. |

### 3.3.2. Identification and Authentication for Re-Key After Revocation

Identification and Authentication for Re-Key after revocation is based on the same requirements as issuance of new Certificates.

## 3.4. Identification and Authentication for Revocation Requests

A request to revoke keys or digital certificates may be submitted by the Subscriber or an individual authorized under applicable contractual agreements. Revocation requests may be initiated through secure mechanisms such as emSign's subscriber portal, CERTInext enterprise and partner platforms, ACME clients, or authorized APIs integrated with emSign PKI.

To validate a revocation request, emSign PKI requires the requester to authenticate using secure challenge-response methods, such as logging in with verified credentials, demonstrating domain/email control, or signing the request using the corresponding private key.

emSign PKI may revoke a certificate without authentication in circumstances where there is evidence or reasonable suspicion of key compromise, misuse, fraud, or based on instructions from a competent legal or regulatory authority or an event that triggers revocation of one or more certificates based on inconsistencies identified between practice and policy. All such revocation actions are logged, and validation personnel ensure traceability of the requester (where applicable), action taken, and reason.

Requests related to CA certificate revocation are subject to elevated review and must be authorized by the emSign Policy Authority.

# 4. Certificate Life-Cycle Operation Requirements

## 4.1. Certificate Application

SSL/TLS certificate requests may be submitted through authorized online channel including the CERTInext portal, enterprise integrations using emSign APIs, or automated systems such as ACME. Each application must include sufficient information to allow emSign to confirm the identity of the requesting entity, validate control over the domain names to be certified, and verify that the individual submitting the request is authorized to act on behalf of the applicant organization, where applicable. Additionally, the application must enable validation that the public key submitted corresponds to a private key legitimately held by the applicant.

All applications are subject to verification procedures appropriate to the certificate type requested. Issuance proceeds only after successful completion of identity and domain validation steps by emSign or its authorized Registration Authorities. Applicants must review the issued certificate for accuracy and promptly report any errors or inconsistencies.

### 4.1.1. Who Can Submit a Certificate Application

Certificate applications must be submitted by individuals or entities authorized to act on behalf of the Applicant. Submissions may occur through approved emSign interfaces, including the CERTInext portal, emSign enterprise API integrations, or automated protocols such as ACME.

All required registration details must be provided in accordance with this CP/CPS and the applicable Certificate Holder Agreement or Subscriber Agreement. Each application is subject to review, approval, and acceptance by emSign or its authorized Registration Authorities.

EV certificate applications must be submitted by an authorized Certificate Requester and approved by a designated Certificate Approver, and must be accompanied by a signed Subscriber Agreement from a Contract Signer.

Applications will not be accepted from individuals or entities listed on government sanctions, denied-persons, or prohibited lists relevant to the jurisdiction of the Issuing CA entity .

### 4.1.2. Enrolment Process and Responsibilities

Applicants seeking SSL/TLS Certificates under the emSign PKI shall complete an enrollment process designed to ensure the integrity, authenticity, and accountability of all issued certificates. While Issuing CAs may define specific implementation workflows, the enrollment process shall include the following minimum steps:

- The Applicant's identity whether representing an organization or an individual shall be verified in accordance with the procedures outlined in Appendix A.
- The Applicant shall generate a secure cryptographic key pair and demonstrate possession of the private key, typically through submission of a digitally signed Certificate Signing Request (CSR).
- The verified identity shall be bound to the public key in accordance with this CP/CPS.
- The Applicant must enter into a binding Subscriber Agreement. The Issuing CA shall operate under a formal agreement with emSign PKI.
- All communications supporting the application and issuance process whether electronic or out-of-band shall maintain the confidentiality and integrity of transmitted data using cryptographic methods appropriate to the key size and security profile.

Applicants are responsible for submitting accurate and complete information, responding to validation requests in a timely manner, and protecting the confidentiality of their private keys. Certificates shall only be issued once all validation requirements have been fulfilled and applicable agreements accepted.

## 4.2. Certificate Application Processing

### 4.2.1. Performing Identification and Authentication Functions

Certificate applications may be submitted directly to emSign or through authorized Registration Authorities (RAs), including enterprise interfaces such as the emSign CERTInext portal, API-based integrations, or automated channels like ACME. All applications are ultimately processed and issued by emSign's Issuing CAs.

Prior to issuance, emSign or its authorized RAs perform validation procedures to ensure:

- The Applicant is eligible to request the specified certificate type;
- A valid Certificate Signing Request (CSR) is submitted;
- The submitted public key is appropriately bound to the Applicant's identity;
- The Subscriber Agreement has been accepted by the Applicant;
- The certificate request conforms with applicable requirements outlined in Section 3.1 and Appendix A.

For SSL/TLS Certificates, emSign performs DNS-based Certification Authority Authorization (CAA) checks in accordance with RFC 8659 and CAB Forum TLS Baseline Requirements. If CAA records exist for any FQDN or wildcard domain in the certificate request, issuance shall proceed only if the CAA records authorize emSign using the issue or issuewild property tags with the value emsign.com.

If the Relevant RRset for a Fully Qualified Domain Name (FQDN) or wildcard domain name contains no restrictive tags, such as if it contains only iodef or unrecognized property tags, then CAA does not restrict issuance.

If emSign issues a certificate after performing a CAA check, issuance shall occur within the Time-To-Live (TTL) of the CAA record or within 8 hours, whichever is shorter.

Subscribers who already have CAA records in their DNS zones and intend to request Server TLS certificates from emSign must include a CAA record with the appropriate issue, issuewild, or issuemail property set to "emsign.com" to explicitly authorize emSign to issue the corresponding certificate type.

Where applicable, emSign will also apply Multi-Perspective Issuance Corroboration (MPIC) to ensure that domain validation checks are not biased by single-network visibility and reflect globally reachable DNS resolution.

### 4.2.2. Approval or Rejection Of Certificate Applications

emSign or its authorized Registration Authorities (RAs) shall approve a certificate application only after successful completion of all required validation procedures as defined in this CP/CPS and Appendix A. The Issuing CA shall reject any application that fails validation or where the submitted information cannot be verified. Additionally, emSign reserves the right to reject a certificate application at its discretion, including but not limited to cases where:

- The Applicant or request is associated with high-risk domains, prohibited geographies, or restricted entities;
- Issuance may compromise the trustworthiness, security, or reputation of emSign;
- The domain is a newly delegated gTLD that is not yet approved for public issuance;
- There is suspected misuse, fraud, or conflict with applicable laws or industry standards.

emSign is not obligated to provide specific reasons for the rejection of an application. Applicants whose requests have been denied may submit a new application following corrective action.

Subscribers are responsible for ensuring the ongoing accuracy of the information provided in their certificate applications. Failure to notify emSign of changes that affect certificate validity may result in certificate revocation in accordance with Section 4.9 and the terms of the Subscriber Agreement.

### 4.2.3. Time to Process Certificate Applications

Registration Authorities and Issuing CAs operating within the emSign PKI are under no obligation to process Digital Certificate Applications other than within a commercially reasonable time.

### 4.2.4. Certificate Authority Authorization (CAA)

For any certificate application involving domain names intended for server authentication, emSign shall perform Certification Authority Authorization (CAA) checks in accordance with RFC 8659.

If a CAA DNS Resource Record is present for the domain, emSign shall verify whether the record authorizes certificate issuance by emSign. If the domain's CAA record does not include emsign.com (for the relevant issue or issuewild property tags, as applicable), the certificate application shall be rejected.

emSign recognizes the following domain name values in CAA records as granting authorization for issuance by emSign PKI:

- emsign.com

If no CAA record exists for the domain, issuance may proceed. The results of all CAA checks are logged for audit purposes.

## 4.3. Certificate Issuance

### 4.3.1. Certification Authority Actions During Certificate Issuance

Issuing CAs operating under this CP/CPS shall comply with all applicable requirements and processes defined in the emSign PKI CP/CPS for SSL/TLS. Certificate issuance shall occur only after successful validation of the Applicant and verification of all certificate data in accordance with the applicable certificate profile and Appendix A.

#### 4.3.1.1. emSign Root Certification Authority

The Root CA Certificates are self-signed and generated in an offline environment. Root CA private keys are maintained in secure, offline cryptographic modules in compliance with industry standards and are only used to sign Subordinate CA certificates and CRLs/OCSP responses as required.

emSign PKI publishes its Root CA Certificates, along with their certificate chains, in the online repository: https://repository.emsign.com.

#### 4.3.1.2. emSign Issuing Certification Authority Certificates

emSign operates its own Issuing CAs under this CP/CPS. These CAs are directly subordinate to an emSign-operated offline Root CA. All Issuing CA certificates are published in the repository, including the hierarchy path to the Root.

Where necessary, emSign may operate issuing CAs under other emSign subordinate CAs within the same hierarchy, subject to strict internal controls and authorization by the emSign Policy Authority.

#### 4.3.1.3. emSign PKI Registration Authority Appointment

Any Issuing CA (under emSign PKI) can appoint external Registration Authorities, who must accept the terms and conditions of emSign PKI Registration Authority Agreement. Upon final approval of the application by Issuing CA, the Registration Authority becomes duly appointed. Upon appointment, they shall be appropriately trained and qualified staff members of the Registration Authority are eligible for Registration Authority Officer Digital Certificates.

#### 4.3.1.4. Registration Authority Officer's Certificate

As part of the application process, Registration Authorities are required to nominate one or more persons within their Organisation to take responsibility for the operation of their Registration Authority functions. Those nominated persons will each be issued a Registration Authority Officer's Digital Certificate.

#### 4.3.1.5. Certificate Holder Certificates

Upon the Applicant's acceptance of the terms and conditions of the Certificate Holder Agreement or other relevant agreement, the successful completion of the application process and final approval of the application by the Issuing CA, the Issuing CA issues the Digital Certificate to the Applicant or Device.

emSign deploys multi-factor authentication for all accounts capable of directly causing certificate issuance.

#### 4.3.1.6. Issuance Safeguards

- All issuance systems are subject to automated and manual controls to prevent misissuance.

- Certificates SHALL NOT be backdated to circumvent policy requirements.
- Linting and pre-issuance validation tools (e.g., PKILint, ZLint, x509lint) are employed prior to issuance to detect non-compliant fields.
- All certificate issuance actions are logged, and evidence of validation (whether internal or via authorized RA) is retained for audit and compliance purposes.
- The Root CA does not support automated issuance. All operations involving Root key usage are performed manually by authorized personnel under controlled environments.

#### 4.3.2. Notification to subscriber by the CA of issuance of certificate

The Issuing CA shall notify the Subscriber of the issuance of a Certificate in a convenient and appropriate way based on information submitted during the enrolment process.

### 4.4. Certificate Acceptance

Certificate acceptance is governed by the requirements outlined in this CP/CPS. A certificate is considered accepted when the Subscriber uses the certificate, downloads or installs it, or authorizes its use by another entity. Acceptance may also be inferred if 30 days pass from the date of issuance without objection.

By accepting a certificate, the Subscriber:

- Agrees to be bound by the terms of the Subscriber Agreement and this CP/CPS;
- Confirms that the certificate contents are accurate and truthful as submitted during the application process;
- Warrants that no unauthorized individual has had access to the private key associated with the certificate; and
- Accepts the responsibility to securely retain and control the private key, use a trustworthy system, and take reasonable precautions to prevent its compromise, misuse, or unauthorized disclosure.

If a certificate is not accepted, eMudhra reserves the right to revoke the certificate. However, use of the certificate or any reliance upon it constitutes deemed acceptance, binding the Subscriber to the terms and conditions stated herein.

#### 4.4.1. Conduct Constituting Certificate Acceptance

The downloading, installing or otherwise taking delivery (through physical or electronic means via certificate delivered over link/download in the Issuing CA website or in email, etc) by the subscriber, or by an entity authorized/consented by subscriber, of a Digital Certificate constitutes acceptance of a Digital Certificate within the emSign PKI.

#### 4.4.2. Publication of the Certificate by the Certification Authority

Issuing CAs may publish a Certificate by sending the Certificate to the Subscriber and/or publishing in a suitable Repository.

The Issuing CA MUST submit a pre-certificate to publicly trusted Certificate Transparency (CT) logs prior to issuing an SSL/TLS certificate.

The Issuing CA MUST also submit the final issued SSL/TLS certificate (post-certificate logging) to publicly trusted CT logs after issuance.

#### 4.4.3. Notification of Certificate Issuance by the Certification Authority to Other Entities

In addition to the Subscriber, emSign may notify:

- Registration Authorities or authorized enterprise portals involved in processing the application;
- Reseller partners or web host integrators through their designated notification channels; and
- The emSign Policy Authority, in cases involving CA certificate issuance;

### 4.5. Key Pair And Certificate Usage

#### 4.5.1. Subscriber Private Key and Certificate Usage

By accepting the SSL/TLS Certificate, the Subscriber agrees to use the Certificate strictly in accordance with its designated key usage extensions as defined in the Certificate Profile. Subscribers must ensure that their private keys are protected against unauthorized access, disclosure, or use, and must only use the key for lawful purposes and in line with the intended use.

Subscribers are responsible for:

- Generating and storing private keys in a secure environment,
- Preventing loss, modification, or unauthorized access to the private key,
- Promptly notifying emSign if there is any suspicion of key compromise.

#### 4.5.2. Relying Party Public Key and Certificate Usage

Relying Parties are individuals or entities that depend on the validity of a Digital Certificate issued under this CP/CPS to establish trust in digital communications or transactions. A Relying Party may accept a Digital Certificate only to the extent that:

- They are authorized to do so by contract with the Certificate Holder, or
- It is permitted by applicable law or regulation in the jurisdiction where the Certificate is issued.

For SSL/TLS Certificates:

- Relying Parties are expected to use software that complies with X.509 standards, the SSL/TLS protocol, and other applicable industry standards.
- emSign PKI does not guarantee or warrant that third-party software enforces the certificate validation procedures, and Relying Parties must obtain independent legal or technical advice if needed.
- Relying Parties must validate the certificate before relying on it, by checking its revocation status using emSign PKI-provided CRL or OCSP services.
- emSign PKI assumes no responsibility for any risk or damages resulting from reliance on a certificate that has not been properly validated.

Any entity querying the existence or validity of an emSign PKI-issued certificate is deemed to have accepted the Relying Party Agreement and the terms of this CP/CPS.

Relying Parties must assess, at a minimum:

- That the certificate is not being used in a manner prohibited by this CP/CPS;
- The appropriateness of the certificate for the intended purpose;

- That the certificate's usage aligns with its key usage and extended key usage fields;
- That the certificate is valid at the time of reliance by checking its status via CRL or OCSP mechanisms.

Warranties provided under this CP/CPS are only valid if the Relying Party has performed the above verification and assessment steps.

## 4.6. Certificate Renewal

### 4.6.1. Circumstances for Certificate Renewal

An Issuing CA may process a renewal request if all of the following conditions are met:

- The public key remains valid and suitable for continued use.
- The associated private key has not been compromised.
- The certificate subject information and Subscriber attributes remain unchanged.
- No additional validation is required under the applicable certificate type.

Renewal may be permitted even after certificate expiration, provided the above conditions are met. However, the original certificate shall not be further renewed, rekeyed, or modified once expired.

### 4.6.2. Who may request renewal

Renewal may be requested by the original Subscriber or by a Registration Authority acting on their behalf. All renewal requests must be authenticated using approved subscriber authentication methods, such as passphrases, shared secrets, or account-based authentication. Submission of a CSR is optional, but if used, it must contain the same public key.

### 4.6.3. Processing Certificate Renewal Requests

emSign PKI reserves the right to request re-authentication or updated information prior to processing a renewal request. In such cases, the same validation procedures applicable to new issuance may be applied. The original certificate may remain valid or may be revoked at emSign's discretion.

### 4.6.4. Notification of new certificate issuance to subscriber

Notification of the renewed certificate shall follow the same process as for new certificate issuance, as defined in Section 4.3.2 of this CP/CPS. Subscribers may also receive email reminders about impending certificate expiration as a courtesy, typically within 60 days prior to expiry.

### 4.6.5. Conduct constituting acceptance of a renewal certificate

Subscriber conduct constituting acceptance of a renewed certificate shall be the same as defined under Section 4.4.1. This includes usage, installation, or download of the certificate.

### 4.6.6. Publication of the Renewed Digital Certificate by Certification Authority

Renewed certificates shall be published using the same mechanisms as those for new certificate issuance, including delivery to the Subscriber and publication in the emSign certificate repository and CT logs, if applicable.

#### 4.6.7. Notification of certificate issuance by the CA to other entities

The CA may notify relevant Registration Authorities involved in the renewal process. No additional notifications are sent to external entities unless specifically required under applicable practices or agreements.

### 4.7. Certificate Re-Key

Certificate re-key refers to the issuance of a new certificate with a newly generated public key, while retaining the same subject information as the original certificate. All re-key operations must comply with the requirements of this CP/CPS, including due diligence in key pair generation, validation, and secure delivery.

#### 4.7.1. Circumstance For Certificate Re-Key

An Issuing CA may re-key a Certificate upon request as long as:

- The original Certificate to be re-keyed has not been revoked;
- All retained details within the Certificate remain accurate and no new or additional validation is required.

#### 4.7.2. Who may request certification of a new public key

Re-key requests may be initiated by:

- The original Certificate Subscriber
- An authorized PKI Sponsor or delegated Registration Authority acting on behalf of the Subscriber

#### 4.7.3. Processing Certificate Re-Key Request

Re-key requests are processed using the same procedures applicable to new certificate issuance. The Subscriber must authenticate as required for routine re-keying under this CP/CPS.

If the private key has not been compromised and the subject and domain information remain unchanged, a replacement certificate may be issued based on a previously validated certificate request (CSR).

#### 4.7.4. Notification of new certificate issuance to subscriber

The notification to subscriber on new certificate issuance (for re-key certificate) shall be same as the process defined in this CP/CPS for new certificate issuance notification to Certificate Holder.

#### 4.7.5. Conduct constituting acceptance of a Re-Key Digital Certificate

The conduct constituting the certificate acceptance for re-key shall be same as the process defined in this CP/CPS for new certificate acceptance.

#### 4.7.6. Publication of the Re-Key Digital Certificate by Certification Authority

The publication of certificate in case of re-key shall be same as the process defined in this CP/CPS for new certificate publication.

#### 4.7.7. Notification of Re-Key Digital Certificate Issuance by the Certification Authority to other entities

The notification to other entities for re-key certificate shall be same as the process defined in this CP/CPS for new certificate issuance notification to other entities.

### 4.8. Certificate Modification

emSign PKI does not support modifying SSL/TLS certificates after they are issued. If any certificate information needs to change, the Subscriber must request a new certificate.

The new request will follow the full validation process as required for the certificate type.

#### 4.8.1. Circumstance for certificate modification

No stipulation.

#### 4.8.2. Who may request certificate modification

No stipulation.

#### 4.8.3. Processing certificate modification requests

No stipulation.

#### 4.8.4. Notification of new certificate issuance to subscriber

No stipulation.

#### 4.8.5. Conduct constituting acceptance of modified certificate

No stipulation.

#### 4.8.6. Publication of the modified certificate by the CA

No stipulation.

#### 4.8.7. Notification of certificate issuance by the CA to other entities

No stipulation.

### 4.9. Certificate Revocation and Suspension

#### 4.9.1. Circumstances For Revocation

Issuing CAs shall revoke Digital Certificates when the private key associated with the Digital Certificate is compromised or suspected to be compromised or when any of the information on a Digital Certificate change or becomes obsolete.

Issuing CA SHALL revoke a Digital Certificate of Subscriber within 24 hours when any of the following conditions are met:

- The Subscriber requests revocation of the Certificate.
- The original certificate request was not authorized by the Subscriber and retroactive authorization is not granted.

- The Private Key associated with or used to sign the Certificate has been compromised or misused.
- The Issuing CA becomes aware of a demonstrated or proven method (e.g., Debian weak keys) that exposes the Subscriber's Private Key to compromise or makes it computable based on the Public Key.
- The Certificate was used to sign, publish, or distribute malware or other harmful content.
- The Issuing CA obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon.
- The Certificate was used to authenticate a misleading or fraudulent subordinate domain name.

Issuing CA SHOULD revoke a Digital Certificate of Subscriber within 24 hours but MUST revoke within 5 days when any of the following conditions are met:

- Any information appearing in the Certificate was or became inaccurate or misleading.
- The Certificate was not issued in accordance with this CP/CPS or applicable industry standards.
- The Applicant has lost its rights to a trademark or the domain name listed in the Certificate.
- The Subscriber breached a material obligation under this CP/CPS or the Subscriber Agreement.
- A government or regulatory order is received by the Issuing CA to revoke the Certificate.
- The Subscriber was added to a denied party or prohibited persons list (e.g., export control or sanctions list).
- The binding between the subject and the subject's Public Key in the Certificate is no longer valid.
- For Certificates that have organizational affiliation, the Issuer CA or the RA shall require the Affiliated Organization to inform it if the subscriber affiliation changes. If the Affiliated Organization no longer authorizes the affiliation of a Subscriber, then the Issuer CA shall revoke any Certificates issued to that Subscriber containing the organizational affiliation. If an Affiliated Organization terminates its relationship with the Issuer CA or RA such that it no longer provides affiliation information, the Issuer CA shall revoke all Certificates affiliated with that Affiliated Organization.
- The Issuing CA ceases operations or its right to manage Certificates is revoked, and it has not arranged another CA for revocation support.
- The Issuing CA is compromised.
- The Certificate Holder is subject to bankruptcy or liquidation.
- The Certificate Holder is deceased.
- If not revoking the Certificate would compromise the trust status of the Issuing CA or affiliated systems.

The Issuing CA SHALL revoke a Subordinate CA Certificate within seven (7) days if one or more of the following occurs:

- The Subordinate CA requests revocation in writing;
- The Subordinate CA notifies the Issuing CA that the original certificate request was not authorized and does not retroactively grant authorization;
- If the Certificate no longer complies with the requirements specified in Sections 6.1.5 and 6.1.6 of the TLS Baseline Requirements.
- The Issuing CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of this CP/CPS.
- The Issuing CA obtains evidence that the Certificate was misused;

- The Issuing CA is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with this CP or the applicable Certificate Policy or Certification Practice Statement;
- The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
- The Issuing CA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
- The Issuing CA's or Subordinate CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository;
- Revocation is required by the Issuing CA's Certificate Policy and/or Certification Practice Statement;
- The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable.)

**Revocation Reason Options:**

- keyCompromise (1): The certificate subscriber must choose the "keyCompromise" revocation reason when they have reason to believe that the private key of their certificate has been compromised, e.g. an unauthorized person has had access to the private key of their certificate.
- affiliationChanged (3): The certificate subscriber should choose the "affiliationChanged" revocation reason when their organization's name or other organizational information in the certificate has changed.
- Superseded (4): The certificate subscriber should choose the "superseded" revocation reason when they request a new certificate to replace their existing certificate.
- cessationOfOperation (5): The certificate subscriber should choose the "cessationOfOperation" revocation reason when they no longer own all of the domain names in the certificate or when they will no longer be using the certificate because they are discontinuing their website.
- privilegeWithdrawn (9): The certificate subscriber should choose the "privilegeWithdrawn" revocation reason when the original Certificate request was not authorized and does not retroactively grant authorization.

### 4.9.2. Who Can Request Revocation

A revocation request for an SSL/TLS certificate may be submitted by the Subscriber, an authorized representative of the Subscriber's organization, or a Registration Authority (RA). The Issuing CA may also revoke a certificate at its discretion, without receiving a formal request, if it determines that revocation is necessary for security or compliance reasons. Additionally, third parties such as security researchers or relying parties may report suspected key compromise, misuse, or other certificate-related issues using the contact details provided in Section 1.5.2.1.

**Certificate Problem Reporting**

Any party including Security Researchers, Anti-Malware Organizations, Subscribers, Relying Parties, Application Software Suppliers, or other third parties may report suspected Private Key compromise, certificate misuse, fraud, or any other concerns related to certificates.

Reports should be submitted via email to the contact listed in Section 1.5.2 of this CP/CPS. To ensure proper handling, it is recommended to include “Certificate Problem Report” in the subject line. The report should include:

- Identity and contact information of the reporting party, and
- A clear explanation of the issue or reason for the revocation request.

All reports will be evaluated and acted upon as appropriate, in accordance with the provisions of Section 4.9.3 of this CP/CPS.

### 4.9.3. Procedure For Revocation Request

Issuing CAs and RAs will revoke a Digital Certificate upon receipt of a valid request and may provide automated mechanisms for requesting and authenticating revocation requests. A revocation request may be sent by the Certificate Holder or Affiliated Organization through any one or many of the following modes, as may be provided by Issuing CA:

- Submit the revocation request via the emSign CERTInext platform
- Submit the revocation request via the Issuing CA Support Line
- Issuing CA website
- Contact administrators of Issuing CA or Registration Authority directly

Certificate Holders or Affiliated Organization may use a passphrase or any kind of shared secret or any other form of subscriber authentication mechanism, that will be used to activate the revocation process.

If revocation is requested by someone other than an authorized representative of the Subscriber or Affiliated Organization, the Issuer CA or RA shall investigate the alleged basis for the revocation request and take appropriate action.

### 4.9.4. Revocation Request Grace Period

The revocation request grace period is the time available to the subscriber within which the subscriber must make a revocation request after reasons for revocation have been identified. Subscribers shall request revocation as soon as possible if the Private Key corresponding to the Certificate is lost or compromised or if the certificate data is no longer valid. Issuing CAs will revoke Digital Certificates as soon as reasonably practical following verification of a revocation request.

### 4.9.5. Time within which CA must process the revocation request

The Issuer CA shall revoke Digital Certificates within such time, as reasonably practical, after validating the revocation request within timelines as mentioned in section 4.9 of this CP/CPS.

### 4.9.6. Revocation Checking Requirement for Relying Parties

Certificate Revocation List is provided in the emSign PKI Repository and Relying Parties are required to validate the suitability of the certificate to the purpose intended and ensure that the Certificate remains valid at the time of usage by checking against the Certificate Revocation List.

### 4.9.7. Certificate Revocation List Issuance Frequency

The CRL which provides the status of Subscriber Certificates (Issuing CAs), the CRL shall be:

1. Generated once within seven (7) days, or within thirty (30) minutes of any revocation made.

2. Valid for NOT more than ten (10) days from the date of generation.

For other certificates (Root CA and/or CAs that has Sub CAs), the CRL shall be:

1. Generated once within twelve (12) months, or within twenty-four (24) hours of any revocation made.
2. Valid for NOT more than twelve (12) months from the date of generation.

### 4.9.8. Maximum Latency for Certificate Revocation List publication

CRLs are published to repository within 10 minutes of generation

### 4.9.9. On-Line Revocation/Status Checking Availability

emSign or Issuing CAs seek to provide online status checking availability for the certificates 7 days a week, 24 hours a day, subject to routine maintenance.

### 4.9.10. On-Line Revocation Checking Requirement

Relying Parties shall check the validity of a certificate via CRL or OCSP before relying on the Certificate.

Failure to do so negates the ability of the Relying Party to claim that it acted on the Digital Certificate with reasonable reliance.

The OCSP URL is provided as part of the Digital Certificate, wherever applicable. The OCSP requests supports both GET and POST requests. The OCSP responder does not respond 'good' response, in case the certificate has not been issued.

For the subscriber certificates, the update of OCSP is provided at least once in every 4 days and has a maximum expiration time of 10 days. Whereas for Subordinate CA certificates, the updates are made at a minimum of once in 12 months, or within 24 hours of a revocation of Subordinate CA.

### 4.9.11. Other Forms of Revocation Advertisements Available

Not applicable.

### 4.9.12. Special Requirements in Relation to Key Compromise

emSign PKI uses commercially reasonable efforts to notify Subscribers if it becomes aware of, or suspects, a compromise of a Subscriber's private key. This may include newly discovered vulnerabilities, incident reports, or discretionary assessment based on credible evidence.
To report a suspected key compromise, the reporting party MUST submit **proof** using one of the following formats:

- The compromised private key itself; OR
- A Certificate Signing Request (CSR) signed with the compromised private key, using the Common Name: "Proof of Key Compromise for emSign"

Supporting information such as vulnerability references, technical descriptions, or incident sources is strongly encouraged.

Reports must be submitted via email to the contact listed in Section 1.5.2, with the subject line "Certificate Problem Report", and MUST include the identity and contact details of the reporter along with a clear explanation.

emSign will review each report in accordance with Section 4.9.3 of this CP/CPS.

#### 4.9.13. Circumstances For Suspension
Not Applicable.

#### 4.9.14. Who Can Request Suspension
Not Applicable.

#### 4.9.15. Procedure For Suspension Request
Not Applicable.

#### 4.9.16. Limits On Suspension Period
Not Applicable.

### 4.10. Certificate Status Services

#### 4.10.1. Operational Characteristics
Issuer CAs shall make certificate status information available via CRL or OCSP.

#### 4.10.2. Service Availability
Digital Certificate status services are available 24x7 throughout the year.

#### 4.10.3. Optional Features
No stipulation.

### 4.11. End Of Subscription
A Subscriber's subscription to emSign PKI services shall be considered ended under the following circumstances:

- The Subscriber allows all SSL/TLS Certificates issued by emSign to expire without requesting renewal or re-key;
- The Subscriber requests revocation of all valid Certificates without applying for replacement;
- The Subscriber Agreement between emSign and the Subscriber is terminated or expires without renewal;
- emSign or the relevant Issuing CA ceases operations impacting the service;
- emSign revokes all Certificates issued to the Subscriber due to non-compliance with the CP/CPS or applicable policies and agreements.

The end of subscription does not absolve the Subscriber from responsibilities accrued prior to termination, including the continued obligation to prevent misuse of any previously issued Certificates.

### 4.12. Key escrow and recovery
Private Keys associated with SSL/TLS Certificates shall not be escrowed or archived under any circumstance, except in specific enterprise TLS automation scenarios described below.

emSign PKI does not support private key escrow for general-purpose TLS subscriber certificates. However, under the CERTInext brand, emSign PKI may optionally offer automation services which necessitates TLS subscriber private keys to be temporarily escrowed under certain use cases, to enterprise customers, based on explicit agreement. In such cases, CERTInext acts as the escrow agent and stores the Subscriber Private Key in securely encrypted form to facilitate the automation. The process is strictly limited to the enterprise requesting the automation services, and any escrow retrieval action automatically triggers revocation of the corresponding certificate to prevent further use.

#### 4.12.1. Key escrow and recovery policy and practices

Key recovery is only applicable to enterprise TLS certificates issued under CERTInext where automation services necessitate private key escrow and have been contractually agreed. Recovery may be initiated only under the following conditions:

- The Private Key has been lost or corrupted.
- The Subscriber organization is no longer operational or is otherwise unavailable.
- A competent legal or governmental authority mandates key recovery.
- Recovery is deemed critical by the Subscriber organization under contractual terms.

Only duly authorized administrators of the enterprise account may initiate recovery. All escrowed keys remain encrypted and are protected against unauthorized access. No escrow or recovery is permitted for SSL/TLS certificates outside of such explicitly approved enterprise agreements.

An entity receiving Private Key escrow services shall:

- Notify Subscribers that their Private Keys are escrowed,
- Protect escrowed keys from unauthorized disclosure,
- Protect any authentication mechanisms that could be used to recover escrowed Private Keys,
- Release escrowed keys only for properly authenticated and authorized requests for recovery, and Comply with any legal obligations to disclose or keep confidential escrowed keys, escrowed key-related information, or the facts concerning any key recovery request or process.

#### 4.12.2. Session Key Encapsulation and Recovery Policy and Practices

No Stipulation.

# 5. Facility, Management, And Operational Controls

## 5.1. Physical Controls

All Issuing CAs of emSign PKI shall implement appropriate physical controls for the following:

1. Physical access control to the hardware used in connection with CA operations.
2. Physical access control over the relevant software.
3. Fire safety protection
4. Protection against failure of supporting utilities like power, telecommunications, etc.
5. Protection against theft.
6. Disaster recovery procedures.

### 5.1.1. Site Location and construction

All Issuing CAs of emSign PKI shall perform their CA operations from a secure datacentre with the following features:

1. The datacentre shall be equipped with physical and logical controls that makes the CA operations inaccessible to unauthorised persons.
2. The data centre shall be a facility made of concrete and steel construction.
3. The data centre shall have security protection mechanisms such as guards, door locks.
4. The data centre shall be with raised floor construction and an array of resilient security and environmental systems.

For SSL/TLS Issuing CAs operated in colocation environments, physical access to the racks, HSMs, and related CA infrastructure is fully controlled and managed exclusively by emSign personnel. These systems are physically isolated and are not accessible to the datacenter provider or other tenants.

### 5.1.2. Physical Access

All Issuing CAs of emSign PKI's systems are located in a secure datacentre. Entry into this secure facility is allowed only to security-cleared and authorised personnel, whose movements within the facility are logged and audited. Physical access to this facility is also video recorded on a 24/7 basis. Further physical access to this facility is monitored 24/7 by onsite security personnel.

### 5.1.3. Power and Air-Conditioning

The supply of power to All Issuing CAs of emSign PKI systems are protected with dual power feeds through the use of Uninterrupted Power Supply (UPS) systems and generators in order to prevent abnormal shutdown in the event of a power failure.

Climate control systems have been implemented to ensure that the temperature within all Issuing CAs of emSign PKI facility is maintained within reasonable operating limits

### 5.1.4. Water Exposures

The facility is located outside any flood prone area. Further, it is located on an upper floor with raised flooring, which provide protection against water exposures. Further the outside walls are also sealed to provide protection from water exposure.

### 5.1.5. Fire Prevention and Protection

The datacentre is equipped with smoke detection system. It is also equipped with necessary Fire Suppression system (FM200) and Very Early Smoke Detection Appliance (VESDA) for fire protection.

### 5.1.6. Media Storage

All magnetic media containing emSign PKI information, including backup media, are stored in containers, cabinets or safes with fire protection capabilities. Further they are located either within the emSign PKI service operations area or in a secure off-site storage area and are protected from any unauthorised physical access.

### 5.1.7. Waste Disposal

All Issuing CAs of emSign PKI shall dispose of commercially sensitive or confidential information as under:

- In case of paper or other printed material containing such information, it shall be shredded or destroyed in a generally accepted procedure.
- In case of magnetic media containing trusted elements of CA or commercially sensitive or confidential information it shall be securely disposed of by physical damage to, or complete destruction of, the asset or by use of an approved utility to wipe or overwrite the magnetic media;

### 5.1.8. Off-Site Backup

An off-site location is used for the storage and retention of backup software and data.

The off-site storage:

- is available to authorised personnel 24 hours per day seven days per week for the purpose of retrieving software and data; and
- has appropriate levels of physical security in place
- Are stored in fire-rated safes and containers.

## 5.2. Procedural Controls

All Issuing CAs of emSign PKI shall ensure that they adhere to all Administrative processes and procedures as detailed in this CP/CPS and as dealt with and described in detail in the various documents used within and supporting the emSign PKI.

### 5.2.1. Trusted Roles

Trusted roles are created in the emSign PKI system in order to ensure that one person acting alone cannot circumvent security safeguards implemented in the CA system. To ensure this the responsibilities are shared by multiple roles and individuals. This is accomplished by creating separate roles and accounts on various components of the CA system, and each role has a limited amount of capability. This method allows a system of "checks and balances" to occur among the various roles.

The trusted roles within the emSign PKI system defined includes various roles like Admin Officer, Audit Officer, Registration Officer, Security Officer, Systems Officer, etc. These are defined in detail along with their responsibilities as part of internal policy documents, and may be confidential in nature.

### 5.2.2. Number of Persons Required Per Task

At least two people are assigned to each trusted role to prevent the possibility of accidental or intentional compromise of any component of the CA infrastructure. Each Issuer CA shall require that at least two people acting in a trusted role take action requiring a trusted role, such as activating the Issuer CA's Private Keys, generating a CA Key Pair, or creating a backup of a CA Private Key. Such sensitive operations also require the active participation and oversight of senior management.

Issuing CAs will utilize commercially reasonable practices to ensure that one person acting alone cannot circumvent safeguards. Issuing CAs shall use commercially reasonable efforts to identify a separate individual for each trusted role. Issuing CAs must ensure that no single individual may gain access to any Private Key (other than the individual's own Private Key).

### 5.2.3. Identification and Authentication for Each Role

All Issuing CAs of emSign PKI shall perform appropriate security screening procedure including background check before appointing a person to the trusted role. Each role described here are identified and authenticated in a manner to guarantee that the right person has the right role to support the CA.

### 5.2.4. Roles Requiring Separation of Duties

Issuing CAs shall enforce role separation for each of the roles and Individual trusted-personnel shall be specifically designated to the roles Identified & defined in this CP/CPS and/or as part of CA's Operating procedures.

It is not permitted for any one person to serve on more than one role at the same time for a specific activity or a task.

## 5.3. Personnel Controls

All Issuing CAs of emSign PKI shall conduct appropriate background checks on all persons selected to take up a trusted role in accordance with the designated security screening procedure, prior to the commencement of their duties. CA shall determine the nature and extent of any background checks, in its sole discretion.

CA shall not be liable for employee conduct that is outside of their duties and for which CA has no control including, without limitation, acts of espionage, sabotage, criminal conduct, or malicious interference.

All employees, agents or independent contractors performing trusted roles, shall be bound by these personnel controls requirements.

### 5.3.1. Qualifications, Experience, and Clearance Requirements

All Issuing CAs of emSign PKI requires that personnel meet a certain minimum standard with regards to background, Qualifications, Experience, and clearance requirements for each trusted role. Selection of personnel are made against this criteria.

### 5.3.2. Background Check Procedures

Background check procedures may include but are not limited to checks and confirmation of:

- Previous employment
- Professional references
- Educational qualifications
- Identity Verification
- Other relevant government records (e.g. national identifiers, etc.)

Where the checks and confirmations cannot be obtained due to a prohibition or limitation of law or other circumstances, All Issuing CAs of emSign PKI will utilize available substitute investigation techniques that provide similar information, including background checks performed by applicable Government and/or Private agencies.

### 5.3.3. Training Requirements

All Issuing CAs of emSign PKI shall provide its personnel with on the job training covering the following areas to the extent relevant for the role of the concerned personnel.

- Basic PKI concepts
- This SSL/TLS CP/CPS
- Documented emSign PKI security and operational policies and procedures
- The use and operation of PKI system software.
- Common threats to the validation process including phishing and other social engineering Tactics
- CA/Browser Forum Guidelines.

### 5.3.4. Retraining Frequency and Requirements

Whenever there is any change in the Issuer CA's or RA's operations appropriate training is provided to the individuals acting in trusted roles so that they are aware of the changes. Apart from this a general yearly training update is provided to all personnel on related topics

### 5.3.5. Job Rotation Frequency and Sequence

No Stipulation.

### 5.3.6. Sanctions for Unauthorised Actions

Appropriate disciplinary actions will be taken for unauthorised actions by any of the personnel, including potential termination of employment and criminal actions.

### 5.3.7. Independent Contractor Requirements

All Issuing CAs of emSign PKI may employ independent contractors as may be necessary. When independent contractors are employed they will be subjected to the same process, procedures and controls as prescribed in this CP/CPS and other related documents.

### 5.3.8. Documentation Supplied to Personnel

All Issuing CAs of emSign PKI provides personnel in trusted roles with the documentation necessary to perform their roles including this CP/CPS.

## 5.4. Audit Logging Procedures

### 5.4.1. Types Of Events Recorded

Audit log shall be maintained for:

1. CA & Certificate Lifecycle Management Events:
    a. Generation, certification, backup, recovery and/or destruction of the CA Key Pairs are recorded. This includes all configuration data used in the process.
    b. Successful and unsuccessful Certificate applications, Certificate issuances, Certificate re-issuances and Certificate renewals for Subscriber Certificates. Also, the revocation requests for Subscriber Certificate including revocation reason
    c. Generations and issuances of CRLs.
    d. Custody of keys, devices and media holding keys
    e. Compromise of a Private Key

2. Security Related Events:
    a. Firewall and router activities
    b. Any downtime in system, software crashes and hardware failures.
    c. CA system actions performed by trusted personnel, including software updates, hardware replacements and upgrades.
    d. Successful and unsuccessful PKI system access attempts
    e. Cryptographic hardware security module events, such as usage, de-installation, service or repair and retirement
    f. CA facility entry/exit
    g. Each movement of the removable media

3. Certificate Application Information:
    a. All documentation & related information provided by the Applicant for application validation process
    b. Physical and/or electronic storage locations of applicant provided documents

All logs include the following elements:

- Date and time of entry
- Sequence number of entry
- Description of the entry
- Identity of person/device making log entry

The Audit log files for all events relating to the security and services of the Issuing CA shall be generated and maintained. Where possible, the security audit logs shall be automatically generated. Where this is not possible, a logbook in paper form, or other physical mechanism shall be used. Security audit logs of all events as above shall be retained and made available during compliance audits.

The access to the systems are either protected by PIN protected Crypto Tokens or in the form of username - password as may be required by specific system or software or database. The administrative passwords in such cases are ensured to be split, so that minimum of two person will be required to perform critical / administrative activity.

### 5.4.2. Frequency Of Processing Log

Audit logs shall be verified at least monthly to see for any evidence of malicious activity.

### 5.4.3. Retention Period For Audit Log

The retention period for audit logs, as mentioned in Section 5.4.1, and applicable to all Issuing CAs of the emSign PKI, shall be as follows:

1. Logs of CA key management activity minimum 2 years
2. CA system logs of certificate management activity minimum 2 years
3. Operating system logs minimum 2 years
4. Physical access system logs minimum 2 years
5. Manual logs of physical access minimum 2 years
6. Video recording of CA facility accesses 90 days

### 5.4.4. Protection Of Audit Log

In all Issuing CAs of emSign PKI, Audit logs are protected using a combination of physical and logical access controls. The events are logged in a way that they cannot be deleted or destroyed for any period of time that they are retained. The events are logged in a manner to ensure that only individuals with authorized trusted access are able to perform any operations based on their profile without modifying integrity, authenticity and confidentiality of the data.

The records of events are protected in a manner to prevent alteration and detect tampering.

### 5.4.5. Audit Log Backup Procedures

All Issuing CAs of emSign PKI shall do onsite back up of the system generated audit logs on a daily basis. At least on a monthly basis all audit logs and audit summaries shall be backed-up in a secure off site location. These shall be under the control of an authorized trusted role. Audit log backup should be protected to the same degree as originals.

### 5.4.6. Audit collection system (internal vs. external)

The security audit process of each Issuing CA must be initiated at system start up and may finish only at system shutdown. The audit collection system should ensure the integrity and availability of the data collected. If necessary, the audit collection system should protect the data confidentiality. In the case of a problem occurring during the process of the audit collection the Issuing CAs must determine whether to suspend Issuing CA operations until the problem is remedied.

Automated audit data is generated and recorded at the application, network, and operating system level. Manually generated audit data is recorded by the trusted-personnel.

### 5.4.7. Notification To Event-Causing Subject

No stipulation.

### 5.4.8. Vulnerability Assessment

All Issuing CAs of emSign PKI shall perform regular vulnerability assessments. Such vulnerability assessments should focus on internal and external threats that could result in unauthorized access, tampering, modification, alteration or destruction of the Certificate issuance process.

The Vulnerability Assessments shall also include application scanning, as well as Penetration Testing. Any negative results out of such reports shall be put under corrective actions for such negative result. No common security vulnerabilities shall exist on public facing websites, hosted in the network.

The results of such vulnerability assessment tests shall be used to enhance the security of the environment.

## 5.5. Records Archival

All Issuing CAs of emSign PKI shall maintain an archive of the relevant records as per the record retention policies set forth in this CP/CPS and any record retention policies that apply by law. The CA shall include sufficient detail in archived records to show that a Certificate was issued in accordance with the CP/CPS.

### 5.5.1. Types Of Records Archived

All Issuing CAs of emSign PKI archives records that will include all relevant evidence in the Issuing CA's possession including:

- Audit logs;
- Digital Certificate requests and all related actions;
- Contents of issued Digital Certificates;
- Evidence of Digital Certificate acceptance and signed (electronically or otherwise) Certificate Holder Agreements;
- Revocation requests and all related actions;
- Archive and retrieval requests;
- Digital Certificate Revocation Lists posted;
- Audit Opinions as discussed in this emSign PKI CP/CPS; and

For each Digital Certificate, the records contain information related to creation, issuance, intended use, revocation and expiration. Upon authorized request, the CA makes available, documentation related to each Digital Certificate subject to the emSign PKI Document Access Policy.

### 5.5.2. Retention Period For Archive

All Issuing CAs of emSign PKI archives and retains audit logs in accordance the audit log retention policy described in this CP/CPS.

### 5.5.3. Protection Of Archive

All Issuing CAs of emSign PKI archives and protects audit logs in accordance the audit log protection policy described in this CP/CPS.

### 5.5.4. Archive Backup Procedures

All Issuing CAs of emSign PKI maintains and implements backup procedures so that backup copies of the archived records are stored in a separate location so that in the event of the loss or destruction of the primary archives a complete set of backup copies is readily available.

### 5.5.5. Requirements For Time-Stamping Of Records

All Issuing CAs of emSign PKI shall automatically timestamp its records as they are created. All events that are recorded within the emSign PKI include the date and time of when the event took place. This date and time are based on the system time on which the CA system is operating. emSign PKI uses procedures to review and ensure that all systems operating within the emSign PKI rely on a trusted time source.

### 5.5.6. Archive collection system (internal or external)

emSign PKI’s Archive Collection System is internal.

### 5.5.7. Procedures To Obtain And Verify Archive Information

Only specific Trusted Roles and auditors may view the archives in whole. The Issuer CA may allow Subscribers to obtain a copy of their archived information. The contents of the archives will not be released, except as required by law.

## 5.6. Key Changeover

To enable smooth transition of expiring CA certificates, new CA Private key shall be certified towards the end of old certificate expiry date. The new CA private key and certificate will be commissioned and used for issuing new subscriber certificates henceforth.

In this case, both old and new CA private keys may be concurrently active.

Old CA Private Keys used to sign previous Subscriber Certificates are maintained till such time that all Subscriber Certificates underneath that gets expired. Until then, the old private key will be used for purposes including CRL and OCSP.

## 5.7. Compromise And Disaster Recovery

### 5.7.1. Incident and compromise handling procedures

The CA Operations Disaster & Recovery Plan is in place with all CAs under emSign PKI, in the form of Business Continuity Plan. This plan fulfils the purpose towards restoring the core business operations when operations and/or systems have been adversely and significantly impacted. This restoration shall be made as quickly as practicable. Such plan shall provide immediate resumption of revocation services in the event of an unexpected emergency.

The disaster recovery and business resumption plan is proprietary, security-sensitive, and confidential. Accordingly, it is not intended to be made publicly available.

All Issuing CAs under emSign PKI have in place an appropriate Key compromise plan detailing the activities taken in the event of a compromise of an emSign Issuing CA Private Key. Such plans include procedures for:

- Revoking all Digital Certificates signed with that emSign Issuing CA's Private Key;
- Notifying emSign Issuing CA and all of the Holders of Digital Certificates issued by that emSign PKI's Issuing CA.

### 5.7.2. Computing resources, software, and/or data are corrupted

Any compromise detected on emSign PKI's computing resources, software, or data operations, it shall be investigated to the extent of the compromise and the risk presented to affected parties. Depending on the extent of the compromise, if it is determined that a continued operation could pose a significant risk to Relying Parties or Subscribers, such operation shall be suspended until it is ensured that the risk is mitigated.

### 5.7.3. Entity private key compromise procedures

The CA Private Keys are classified as highly critical to the business operations and continuity. If any of the CA's private signing keys were compromised or were suspected of having been compromised, an assessment shall be made to determine the nature and extent of the compromise. In the most severe circumstances, all Certificates ever issued by the use of those keys shall be revoked and a notification shall be sent to all owners of Certificates of that revocation, and offer to re-issue the Certificates to the customers with an alternative /new key.

### 5.7.4. Business continuity capabilities after a disaster

emSign PKI's Business Continuity Plan shall provide for a minimum of:

- Private Key compromise procedures as well as Public Key Revocation procedures.
- Incident & compromise handling procedures.
- Software, Computing resources and/or Corrupted data handling procedures.
- Business continuity capabilities and procedures after a disaster.

The stated goals of this plan shall ensure that certificate status services be only minimally affected by any disaster involving CA facility and that it shall be capable of maintaining other services or resuming them as quickly as possible following a disaster. The business continuity plans are made available to the auditors and audited during defined audit cycles. These are also subjected to annual test, review, and update of the procedures.

## 5.8. CA or RA termination

When it is necessary to terminate an Issuing CA or Registration Authority service, emSign PKI shall:

- Provide notice & information about the termination by sending notice by email to its customers, Vendors, cross-certifiers (if any), and any other applicable entities.
- By posting such information on the web site
- Minimize any disruption caused by the termination of an Issuing CA
- Take care of retention of archived records of the Issuing CA
- Check and transfer all responsibilities to a qualified successor entity.

All CAs under emSign PKI specify the procedures they will follow when terminating all or a portion of their Digital Certificate issuance and management operations.

The successor CA should assume the same obligations, duties and rights of terminating CA, and issue new keys / certificates to all users whose keys / certificates were revoked by terminating CA. Such new certificate issuance shall comply by, user making an application and meeting the requirements of identification & authentication requirements as well as Subscriber agreement of new issuing CA.

Where practical, Key / Digital Certificate revocation shall be timed to coincide with the progressive & planned rollout of new Keys and Digital Certificates by a successor Issuing CA.

# 6. Technical Security Controls

emSign Certification Authority has put in place sufficient security controls to protect the private keys and access to various modules within the Certifying Authority environment.

The Issuing CA Private Keys are stored securely in a Hardware Security Module which is compliant with FIPS 140-2 Level 3+ Standard. Access to systems/module within the Certification Authority environment are restricted using tokens or smartcards and associated pass phrases in such a manner that no single member holds total control over any component of the system. The Hardware Security Modules are always stored in a physically secure environment that is subject to security control.

## 6.1. Key Pair Generation and Installation

### 6.1.1. Key Pair Generation

Issuing CA key pairs are generated in a secure manner as part of a key ceremony in a physically trusted environment by trusted personnel. Issuing CA key generation is carried out in a secure device that is at least FIPS 140-2 Level 3 compliant.

Subscriber key pairs:

1. Subscriber key pairs are generally generated by the Subscriber using secure methods (software or hardware) prior to submitting a Certificate Signing Request (CSR).
2. For SSL/TLS certificates, key generation typically occurs within the Subscriber's server or secure cryptographic device.

Issuing CA SHALL reject a certificate request if one or more of the following conditions are met:

1. The Key Pair does not meet the requirements set forth in Section 6.1.5 and/or Section 6.1.6;
2. There is clear evidence that the specific method used to generate the Private Key was flawed;
3. Issuing CA is aware of a demonstrated or proven method that exposes the Applicant's Private Key to compromise;
4. Issuing CA has previously been made aware that the Applicant's Private Key has suffered a Key Compromise, such as through the provisions of Section 4.9.1;
    a) In the case of Debian weak keys vulnerability (https://wiki.debian.org/SSLkeys), the Issuer CA shall reject all keys found at https://github.com/cabforum/Debian-weak-keys/ for each key type (e.g. RSA, ECDSA).
    b) In the case of ROCA vulnerability, the Issuer CA shall reject keys identified by the tools available at https://github.com/crocs-muni/roca or equivalent.

In the case of Close Primes vulnerability (https://fermatattack.secvuln.info/), the Issuer CA shall reject weak keys which can be factored within 100 rounds using Fermat's factorization method.

### 6.1.2. Private Key Delivery to Certificate Holder

For TLS certificates, emSign does not generate or deliver private keys. The Subscriber is solely responsible for generating the key pair and ensuring the private key remains confidential and protected at all times. emSign does not retain, archive, or transmit private keys for TLS certificate Subscribers, except for the limited use case when automation services are contracted, as per Section 4.12..

### 6.1.3. Public Key Delivery to Certificate Issuer

For TLS certificates, the Subscriber delivers the public key to the Issuing CA as part of a Certificate Signing Request (CSR). The CSR must be delivered over a secure channel and contain a valid digital signature that demonstrates the Subscriber's possession of the corresponding private key. The Issuing CA ensures the integrity of the public key during transmission and verifies that it corresponds to the Subscriber's verified identity before certificate issuance.

### 6.1.4. Certification Authority Public Key to Relying Parties

All Issuing CAs of emSign PKI shall ensure that Public Key delivery to Relying Parties is done in a secure manner to serve as a trust anchor in commercial browsers and operating system root stores, or may be specified in a Certificate validation or path discovery policy file. CA may deliver its Public Key certificate through its repository available on emSign or Issuer website.

### 6.1.5. Key Sizes

Within the emSign PKI, key algorithms and lengths for TLS certificates are defined by certificate profiles and comply with CA/Browser Forum Baseline Requirements.

For TLS Subscriber Certificates:

- RSA keys MUST have a minimum key length of 2048 bits.
- Elliptic Curve Cryptography (ECC) keys MUST use curves with a strength of at least NIST P-256 (also known as secp256r1).

For TLS CA Certificates (Root and Subordinate):

- RSA keys MUST have a minimum key length of 3072 bits for CA Certificates created after 1 Jan 2021.
- ECC keys MUST use at least NIST P-256.

The Issuing CA SHALL ensure that all key lengths and algorithms are compliant with current Baseline Requirements and are sufficient to protect against known cryptographic attacks.

Following points shall be noted on Hash algorithms:

1. All Signature Algorithms are used in conjunction with Digest Algorithm of SHA-256 or a hash algorithm that is equally or more resistant to a collision attack.
2. MD5 is not supported.

### 6.1.6. Public Key Parameters Generation And Quality Checking

All CA keys are generated on FIPS 140-2 qualified hardware and meets the requirements of FIPS 1862, 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 shall be tested for and rejected at the point of submission.

### 6.1.7. Key Usage Purposes (As Per X.509 V3 Key Usage Field)

The Key Usage and Extended Key Usage extensions included in certificates issued under emSign PKI comply with RFC 5280, CA/Browser Forum Baseline Requirements, and are set according to the certificate type and its intended use.

- Root CA Certificates are used only to sign Subordinate CA Certificates and CRLs.
- Issuing CA Certificates are used to sign end-entity certificates and CRLs.
- TLS Subscriber Certificates include key usages appropriate for server authentication

For TLS certificates, key usages are limited to:

- For RSA keys: digitalSignature, keyEncipherment
- For ECC keys: digitalSignature only

The specific key usages and extended key usages for each certificate type are defined in the Certificate Profiles section of this CP/CPS.

## 6.2. Private Key Protection And Cryptographic Module Engineering Controls

Issuing CA, RA, Subscribers and other participates are required to take appropriate and adequate steps to protect Private Keys in line with the requirements of this CP/CPS.

This includes:

- Securing their Private Key

- Taking necessary precautions to prevent loss, damage, disclosure, alteration or unauthorized access or use of their Private Key
- Exercise sole and complete control and use of the Private Key

### 6.2.1. Cryptographic Module Standards and Controls

All CA Private Keys under emSign PKI must be generated and maintained in a Hardware Security Module that is compliant with Federal Information Protection Standards 140-2 Level 3+.

### 6.2.2. Private key (n out of m) multi-person control

All Issuer CA Private Keys are accessed / activated in CA System through n-of-m multiple trusted person control including for any Private Key backups.

### 6.2.3. Private Key Escrow

Private keys associated with TLS CA certificates are not escrowed. emSign PKI does not support private key escrow for general-purpose TLS subscriber certificates. However, under the CERTInext brand, emSign PKI may optionally offer automation services that require TLS subscriber private keys to be temporarily escrowed for certain enterprise use cases, based on explicit agreement with the Subscriber. In such cases, CERTInext acts as the escrow agent and stores the Subscriber's private key in securely encrypted form. This process is strictly limited to the enterprise requesting the automation service, and any retrieval of an escrowed private key automatically triggers revocation of the corresponding certificate to prevent further use.

### 6.2.4. Private Key Backup

Issuing CAs under emSign PKI may backup their Private Keys using a secure cryptographic device and store the Private Keys in an encrypted state if private keys are stored outside the cryptographic module.

Subscribers may choose to backup up their Private Keys using a secure manner. Issuing CA may provide backup services of Private Key for Subscriber provided that the backups shall be secured in a manner that only the Subscriber can control the Private Key.

### 6.2.5. Private key archival

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.

### 6.2.6. Private Key Transfer into or from a Cryptographic Module

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

CA Private Keys shall be stored on a Hardware Security Module that is compliant with FIPS 140-2 Level 3 Standard.

Subscriber Private Keys can be stored on a Cryptographic Module.

### 6.2.8. Method Of Activating Private Key

CA Private Keys are activated in accordance with the specifications of the Cryptographic Module Manufacturer.

### 6.2.9. Method Of Deactivating Private Key

When not in use, Issuing CA shall deactivate its Private Keys by ending (logging out) the sessions with cryptographic modules. These are based on specifications of the Cryptographic Module Manufacturer.

### 6.2.10. Method Of Destroying Private Key

Issuing CA shall use individuals in trusted roles to destroy Private Keys when they are no longer needed or upon expiry or upon revocation of the Certificate by deleting or overwriting the data or using physical destruction.

Subscribers may destroy their Private Keys when the corresponding Certificate is revoked or expired of if the Private Key is no longer needed. This must be done in a secure manner so as to ensure that there is no loss, theft, compromise or unauthorized disclosure or use.

### 6.2.11. Cryptographic Module Rating

The rating of the Cryptographic Module shall meet the requirements laid down in "Cryptographic Module Standards and Controls" section of this CP/CPS.

## 6.3. Other Aspects of Key Pair Management

### 6.3.1. Public Key Archival

Issuer CA shall archive a copy of each public key.

### 6.3.2. Certificate Operational Periods and Key Pair Usage Periods

The maximum validity periods for Digital Certificates issued within the emSign CA PKI are:

| **Type** | **Private Key Use (signing the certificates)** | **Private Key Use (signing the CRL)** | **Certificate Term** |
|---|---|---|---|
| Root CA Certificate | 20 years | 25 years | 25 years |
| All Subordinate CAs of Root CA | 12 years | 15 years | 15 years |
| Subscriber Certificates with Server Authentication EKU | Not Applicable | Not Applicable | 398 Days |

While the validity period of Issuing CA certificates may be defined in accordance with this Policy, emSign limits the operational use of any Issuing CA certificate to a maximum of five (5) years from the date of issuance. The certificate will be replaced prior to exceeding this operational limit, even if the remaining validity period allows for continued use.

Reference for maximum Validity Periods of Subscriber Certificates

| Certificate Issued On or After | Certificate Issued Before | Maximum Validity Period |
|---|---|---|
| – | March 15, 2026 | 398 days |
| March 15, 2026 | March 15, 2027 | 200 days |
| March 15, 2027 | March 15, 2029 | 100 days |
| March 15, 2029 | – | 47 days |

All certificates including subscriber certificates or any subordinate CA certificate end date shall not exceed the end date of its signing certificate (issuer).

## 6.4. Activation Data

### 6.4.1. Activation Data Generation and Installation

Issuing CAs under emSign PKI shall ensure that activation data used to protect access to private keys such as PINs, passphrases, or cryptographic tokens has sufficient entropy and strength to prevent unauthorized access. Activation mechanisms must include multi-factor authentication wherever applicable.

All personnel involved in CA operations, including emSign PKI Officers, shall use strong, complex passwords or cryptographic authentication methods to safeguard sensitive systems, in line with emSign PKI's internal security policies.

### 6.4.2. Activation Data Protection

If activation data must be transmitted to subscribers, it shall be via a channel of appropriate protection, and distinct in time and place from the associated Cryptographic Module. Personal Identification Codes may be supplied to Subscriber in a secure manner.

### 6.4.3. Other Aspects of Activation Data

Where a PIN or Passphrase is used, User is required to enter PIN or Passphrase along with other personal identification details to be able to access and install their keys or digital certificates.

## 6.5. Computer Security Controls

### 6.5.1. Specific computer security technical requirements

emSign PKI has an Information Security Policy that documents the policies, standards and guidelines relating to information security. This Information Security Policy has been approved by the emSign Policy Authority and is communicated to all employees that pertain to the emSign PKI business.

Some of the security controls and policies include:

- Clearly defined processes, systems and safeguards for ensuring physical, logical access to the systems
- Usage of HSM for protection of Issuing CA Private key material.
- Access controls to Certificate Authority services and PKI roles.
- Enforced separation of duties for Certificate Authority Services and PKI roles.
- Trusted personnel checks, roles of responsibility in the emSign PKI.
- Application, Session and Database security
- Archival process for Certificate Authority history and Audit data.
- Controls are in place to prevent unauthorized or illegitimate software from executing within its systems, including but not limited to anti-virus and anti-malware software.
- Comprehensive incident response plan to respond to compromise or breach of its online systems as well as its certificate issuance systems.
- Enforcement of Multi-factor authentication for all accounts capable of directly causing a certificate issuance.

### 6.5.2. Computer Security Rating

No stipulation.

## 6.6. Life Cycle Technical Controls

Following lifecycle controls are required to be followed to ensure mitigation of risk during operation of emSign PKI ecosystem.

- Hardware and software procured should follow methodologies that ensure no scope for any particular component to be tampered
- Systems used within emSign PKI shall be developed using strict change control procedures
- Only trusted personnel shall be authorized to use core systems of emSign PKI
- Issuing CA shall not install applications or component software that is not part of the Issuing CA configuration
- The Issuer CA shall purchase or develop updates in the same manner as original equipment, and shall use trusted trained personnel to install the software and equipment.
- System administrators in network do not have access to certificate issuance systems due to proper segmentation of duties and least privilege principles.

### 6.6.1. System Development Controls

Adequate controls are put in place for System Development as follows

- Software Development Lifecycle practices are followed for development and implementation of new systems.
- Security analysis is conducted at the design stage.
- Outsourcing of projects (if any) is closely monitored and controlled.

### 6.6.2. Security Management Controls

Issuing CA installation, configuration, as well as any modifications are documented and controlled by Issuing CA through formal mechanisms.

Issuing CA change control process shall include procedures to detect unauthorized modification to the Issuing CA systems. Any third-party software procured shall be verified for integrity, appropriate versioning and for being free of any modifications.

#### 6.6.3. Life Cycle Security Controls

emSign PKI periodically verifies the integrity of the Certifying Authority software and monitors the configuration of CA systems.

### 6.7. Network Security Controls

Issuing CA shall ensure that the network in which the CA system is hosted is protected by network firewalls and other systems that to the extent possible prevent unauthorized access by parties. Other measures include:

- Turning off any unused network ports or services.
- Firewalls and filtering routers used for CA equipment limits services to and from the CA equipment to those required to perform CA functions.
- 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.
- Shut down certificate issuance quickly if we are alerted of intrusion.
- Review network infrastructure, monitoring, passwords, etc. for signs of intrusion or weakness.
- Ensure IDS (Intrusion Detection System) and IPS (Intrusion Prevention System) systems, and other monitoring software are in place and are up-to-date.
- Segmentation of key certificate issuance systems from non-related servers and systems such as marketing websites, etc.

### 6.8. Time-Stamping

Issuing CAs shall ensure that their components are regularly synchronized with a time service such an atomic clock or Network Time Protocol. The system time on computers shall be updated using the Network Time Protocol (NTP) to synchronize system clocks at least once every eight hours.

This shall be used for establishing the time of:

- Initial validity time of a CA Certificate;
- Revocation of a CA Certificate;
- Posting of CRL updates; and
- Issuance of Subscriber Certificates

An internal NTP server is maintained that synchronizes with external sources and maintains the accuracy of its clock within one second or less.

## 7. Certificate, CRL, And OCSP Profiles

### 7.1. Certificate Profile

All emSign PKI Digital Certificates conform to Digital Certificate and Certificate Revocation List profiles as described in RFC 5280 and utilise the ITU-T X.509 version 3 Digital Certificate standards.

Refer to APPENDIX B for Certificate contents that are specific to the individual classes of Digital Certificates.

### 7.1.1. Version Number(s)

All Certificates issued by emSign are X.509 version 3.

### 7.1.2. Certificate Extensions

Certificate extensions shall be in conformance to RFC 5280 and the Baseline Requirements.

The certificates are with the extensions required by respective certificate profiles. Private extensions are permissible, but the use of private extensions is not warranted under this CP/CPS unless specifically included by reference.

#### 7.1.2.1. Key Usage

This permits the standard Key Usage values, and the criticality field of the *KeyUsage* extension is generally set to TRUE.

#### 7.1.2.2. Certificate Policies Extension

The *certificatePolicies* extension in TLS certificates issued under emSign PKI shall include the appropriate object identifier (OID) corresponding to the certificate policy defined in this CP/CPS. The *critical* field of this extension SHALL be set to FALSE.

Additional policy OIDs MAY be included to reflect compliance with relevant standards or program requirements, such as the CA/Browser Forum Baseline Requirements or other industry-specific criteria, where applicable.

Reserved Certificate Policy Identifiers

emSign Issuing CAs MAY include certificate policy identifiers corresponding to Domain Validation (DV), Organization Validation (OV), Extended Validated (EV) or Individual Validation (IV) as defined in the CA/Browser Forum Baseline Requirements. When such identifiers are present, the subject field SHALL be populated in accordance with the respective validation requirements.

**Root CA Certificates**

emSign Root CA Certificates SHALL NOT contain the certificatePolicies extension.

**Subordinate CA Certificates**

- Subordinate CAs operated by emSign MAY include the *anyPolicy* OID (2.5.29.32.0) or an explicit policy OID to assert policy compliance.
- Subordinate CAs not operated by emSign (i.e., external subordinate CAs) SHALL include only explicit policy OIDs and SHALL NOT include the *anyPolicy* OID.

**Subscriber Certificates**

- Subscriber Certificates SHALL include one or more policy OIDs.

- One policy OID MAY represent the emSign CPS and include a URI pointing to the CP/CPS document.
- Additional policy OIDs SHALL represent the certificate's validation level and compliance with verification, issuance, and other requirements, as specified in Appendix A and Appendix B, and referenced in Section 1.2 of this CP/CPS.

### 7.1.3. Algorithm Object Identifiers

The certificate contains the Signing Algorithm information as per RFC 5280 specifications.

### 7.1.4. Name Forms

The certificates with name forms compliant to RFC 5280. Each certificate includes a unique certificate serial number (non-sequential) among respective Issuing CA, that exhibits at least 80 bits of output from a CSPRNG.

The Issuer Name shall be populated in each Certificate issued containing the Country, Organization Name and the Common Name of the Issuer CA. The Distinguished Name for each Certificate type is set forth as per the respective certificate profile. Optional Sub fields in the Subject contains only verified information, or left empty. The subject fields shall not contain values as meta data of period, hyphen, empty space, etc (Eg: '.' OR '-' OR ' ') indicating the field as not applicable.

After April 30, 2019, Subject Alternative Name (subjectAltName) Extension shall not contain underscore characters ("_") in dNSName entries. There are no certificates issued with underscore in dNSName entires, prior to this date.

For internationalized domain names, the Common Name and each SAN dnsName entry is represented as a Domain Name consisting of multiple puny-coded label / values.

### 7.1.5. Name constraints

emSign PKI includes Name Constraints in Subordinate CA Certificates when relevant. emSign PKI places Name Constraints in a non-critical nameConstraints extension within the CA certificate. emSign PKI does not include the anyExtendedKeyUsage EKU in Name Constrained CA certificates.

### 7.1.6. Certificate policy object identifier

The OIDs used by emSign PKI are listed in Section 1.2.

### 7.1.7. Usage of Policy Constraints extension

No stipulation.

### 7.1.8. Policy qualifiers syntax and semantics

emSign PKI includes in End Entity Certificates a non-critical Certificate Policies extension as defined in RFC5280. It includes a one or more PolicyInformation extension that includes the Certificate Policy Identifier and a single Policy Qualifier referring to the CPS URI or a userNotice.

### 7.1.9. Processing semantics for the critical Certificate Policies extension

No stipulation.

## 7.2. CRL Profile

Certificate Revocation Lists are issued in the X.509 version 2 format in accordance with RFC 5280.

### 7.2.1. Version Number(s)

Issuing CAs within the emSign PKI issue X.509 version 2 Certificate Revocation Lists.

### 7.2.2. CRL and CRL entry extensions

#### 7.2.2.1. Fields in CRL

The CRL contains following fields:

1. Issuer DN
2. Effective date of CRL issuance
3. Next update date
4. Signature Algorithm
5. Signature Hash Algorithm

#### 7.2.2.2. CRL Extensions

CRL contains the following extensions:

1. CRL Number: Sequential number for CRL under specific issuer.
2. Authority Key Identifier: Identifier of Issuing CA.

#### 7.2.2.3. CRL Entries

CRL contains the entries of certificates revoked under that issuer. Each of these entries contain:

1. Certificate Serial Number
2. Revocation Date
3. Revocation reason

## 7.3. OCSP Profile

Issuer CA may operate an Online Certificate Status Protocol responder in compliance with necessary requirements. OCSP responders conform to RFC 5019 and/or RFC 6960. The OCSP requests and responses shall be compliant with the requirements of RFC.

### 7.3.1. Version Number(s)

Issuing CAs within the emSign PKI issue Version 1 OCSP Responses.

### 7.3.2. OCSP Extensions

No Stipulation

# 8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

## 8.1. Frequency or circumstances of assessment

All Issuing Certification Authorities under the emSign PKI are subject to an annual compliance audit. These audits are conducted by qualified independent auditors and are designed to confirm conformance with the latest versions of AICPA/CICA:

- WebTrust: for Certification Authorities
- WebTrust: Principles and Criteria for Certification Authorities – Network Security
- WebTrust: for Certification Authorities – Baseline Requirements for TLS
- WebTrust: for Extended Validation SSL, where applicable

These assessments ensure that emSign PKI's practices align with the CA/Browser Forum's Baseline Requirements and applicable browser root program policies. Additional assessments may be performed in response to significant changes in CA operations, incidents, or at the discretion of the Policy Authority.

## 8.2. Identity and Qualifications of Assessor

External compliance audits of emSign PKI's Issuing Certification Authorities are conducted by a Qualified Auditor who is independent of emSign, credible, and recognized by AICPA/WebTrust. The auditor must have substantial experience in auditing Information Security systems, PKI operations, and cryptographic technologies. The auditor is bound by applicable laws, regulations, or professional codes of ethics and must maintain professional liability or errors and omissions insurance with coverage of at least USD 1,000,000. The auditor must be authorized to conduct WebTrust audits, including for Certification Authorities, Baseline Requirements for TLS, and Extended Validation SSL where applicable.

emSign PKI audits have been carried out by BDO.

## 8.3. Assessor's Relationship to Assessed Entity

emSign PKI has selected an auditor that is completely independent from emSign CA

## 8.4. Topics Covered by Assessment

Topics covered by the Assessment include but are not limited to CA business practice disclosure (CP/CPS), service integrity of emSign Operations and emSign's operational compliance to this CP/CPS and to the WebTrust guidelines.

## 8.5. Actions Taken As a Result of Deficiency

For any material non-compliance or deficiency presented by the Auditors, emSign, at its sole discretion will determine an appropriate corrective action plan with appropriate time frame to remove the deficiency.

## 8.6. Communication of results

Results of the audit are reported to the Policy Authority for analysis and resolution of any deficiency through a subsequent corrective action plan.

## 8.7. Self Audits

emSign PKI controls service quality through ongoing internal audits at least a quarterly basis, against a randomly selected sample of certificates. The sample size of certificates issued would be at least 3%. This sample size period should begin from the first time the certificate is issued, or immediately after the previous self-audit sample was taken

# 9. Other Business and Legal Matters

## 9.1. Fees

### 9.1.1. Certificate Issuance or Renewal Fees

emSign PKI charges fee to its customers for certificate issuance and renewal. The fees are indicated to the customers through suitable web interface or through sales and marketing materials. The fees can be changed from time to time at emSign's discretion.

### 9.1.2. Certificate Access Fees

emSign PKI may charge access fee for bulk access to its certificate databases/repository as specified in applicable agreements.

### 9.1.3. Revocation or Status Information Access Fees

No fee will be charged by emSign CA for revocation of a certificate. Further no fee will be charged for a relying party to check the validity of the existing certificate using a CRL.

However, emSign PKI reserves the right to charge a fee for providing certificate status information via OCSP.

### 9.1.4. Fees for Other Services

emSign PKI reserves the right to charge fee for enterprise support and/or any other additional services.

### 9.1.5. Refund Policy

emSign PKI will provide refund to subscribers under certain circumstances and subject to certain conditions. The details of these will be contained in the relevant contractual document.

## 9.2. Financial Responsibilities

### 9.2.1. Insurance Cover

emSign maintains Commercial General Liability insurance with a policy limit of at least two million US dollars ($2,000,000) in coverage and Errors and Omissions/Professional Liability insurance with a policy limit of at least Five million US dollars ($ 5,000,000) in coverage.

### 9.2.2. Other Assets

No stipulation.

### 9.2.3. Insurance or warranty coverage for end-entities

Subscribers and Relying parties can apply to Commercial Insurance Providers for Financial Protection against accidental occurrences such as theft, corruption, loss or unintentional disclosure of the private key that corresponds to the public key in their emSign Certificate.

#### 9.2.4. Financial Records

emSign PKI shall maintain its financial records, including books of accounts, in a commercially reasonable manner.

#### 9.2.5. No Partnership or Agency

No partnership or agency is implied in any subscriber or relying party agreement under this CP/CPS. Hence emSign is not the agent, fiduciary trustee or other representative of subscribers or the relying parties. Further the subscribers and relying parties shall not represent themselves as agent, partner, affiliate, employee or representative of emSign and shall have no authority to commit anything on behalf of emSign.

### 9.3. Confidentiality of Business Information

#### 9.3.1. Scope of Confidential Information

emSign PKI considers the following information as confidential information and protects them from disclosure using a reasonable degree of care:

1. Private Keys;
2. Activation data used to access Private Keys or to gain access to the CA system;
3. Business continuity, incident response, contingency, and disaster recovery plans;
4. Other security practices used to protect the confidentiality, integrity, or availability of information;
5. Information held by emSign PKI as private information in accordance with this CP/CPS;
6. Audit logs and archive records;
7. Transaction records, financial audit records, and external or internal audit trail records and any audit reports (with the exception of an auditor's letter confirming the effectiveness of the controls set forth in this CPS).
8. Any other information relating to subscriber or emSign PKI, which may be sensitive in nature.

#### 9.3.2. Information not Within the Scope of Confidential Information

Any information other than information indicated as confidential in this CP/CPS shall be deemed public. Further Information appearing in certificates and in the Repository, are considered public.

#### 9.3.3. Responsibility to Protect Private Information

emSign PKI's employees, agents and contractors are contractually obliged to protect confidential information. Further emSign provides training to employees on protection of confidential information.

### 9.4. Privacy of Personal Information

#### 9.4.1. Privacy Plan

emSign PKI protects personal information as per the Privacy Policy published in emSign Repository.

#### 9.4.2. Information Treated as Private

All personal information about an applicant that is not publicly available in the contents of a Certificate or CRL are treated as private information by emSign PKI.

#### 9.4.3. Information not deemed private
Any certificate content and certificate status information is deemed not private in emSign PKI.

#### 9.4.4. Responsibility to Protect Private Information
emSign PKI shall store private information in accordance with the published Privacy Policy document published in emSign repository. All private information is securely stored and protected against accidental disclosure.

#### 9.4.5. Notice and Consent to Use Private Information
Personal information obtained from an applicant during the application or identity verification process, to the extent not included in a certificate, is considered private information. Such private information will be used by emSign PKI only after obtaining the subject's consent or as required by applicable law or regulation. All subscribers are deemed to have consented to the global transfer and publication of any personal data contained in a Certificate.

#### 9.4.6. Disclosure pursuant to Judicial or Administrative Process
emSign PKI may disclose private information without notice to the applicants or subscribers where such disclosure is required by law or regulation.

#### 9.4.7. Other information disclosure circumstances
No stipulation.

### 9.5. Intellectual Property Rights
emSign does not knowingly violate the intellectual property rights of third parties.

All Intellectual Property Rights including all copyright in all Certificates, all documents including this CP/CPS and all proprietary marks belong to and will remain the property of eMudhra. eMudhra retains the exclusive right to use and licence its intellectual property.

Certificates are the exclusive property of emSign PKI. emSign PKI gives permission to reproduce and distribute Certificates on a royalty free, non-exclusive basis, provided that they are reproduced and distributed in full.

emSign PKI reserves the right to revoke a Certificate at any time and at its sole discretion.

Public keys and Private keys are the property of the applicable Certificate Holders who rightfully hold them.

emSign excludes all liability for breach of any other intellectual property rights.

### 9.6. Representations and Warranties

#### 9.6.1. Certification Authority Representation and Warranties
emSign PKI represents that it complies, in all material respects, with the provisions of this CP/CPSSSL/TLS CP/CPS and all applicable laws and regulations.

emSign PKI further warrants that:

1. Reasonable steps are taken to verify that the information contained in any Certificate is accurate at the time of issuance and is validated in accordance with this CP/CPS, the CA/Browser Forum Baseline Requirements, and EV Guidelines, where applicable.
2. Certificates will be revoked promptly upon discovery or notification that the Certificate's contents are no longer accurate, or that the associated Private Key has been compromised.

emSign PKI also provides the representations and warranties required under the CA/Browser Forum Baseline Requirements and, where applicable, the CA/Browser Forum Guidelines for Extended Validation (EV) SSL Certificates.

No other warranties are made by emSign. All other warranties, whether express, implied, statutory, or otherwise including, but not limited to, implied warranties of merchantability and fitness for a particular purpose are disclaimed to the fullest extent permitted by applicable law.

### 9.6.2. RA representations and warranties

RAs and LRAs warrant that:

1. They carry out the issuance process in compliance with this CP/CPS.
2. The information provided by them does not contain any false or misleading information.
3. Translations performed by them are an accurate translation of the original information.
4. All Certificates requested by them meet all material requirements of this CP/CPS.

Additional representations and warranties may be contained in emSign's agreement with RA/LRAs.

### 9.6.3. Subscriber Representation and Warranties

Subscribers represent and warrant to emSign PKI, Relying Parties and other parties that, for each Certificate, the Subscriber will:

1. Securely generate its Private Keys and protect its Private Keys from compromise,
2. Provide accurate and complete information when communicating with emSign,
3. Confirm the accuracy of the certificate data prior to using the Certificate,
4. Promptly request revocation of a Certificate, cease using it and its associated Private Key and notify emSign PKI if there is any actual or suspected misuse or compromise of the Private Key associated with the Public Key included in the certificate,
5. Promptly request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate,
6. Use the Certificate only for authorized and legal purposes, consistent with the certificate purpose, this CPS, any applicable CP, and the relevant Subscriber Agreement, including only installing SSL Certificates on servers accessible at the domain listed in the Certificate and
7. Promptly cease using the Certificate and related Private Key after the Certificate's expiration.

Subscribers represent and warrant as specified in CA Browser Forum Requirements & Guidelines.

### 9.6.4. Relying Party Representation and Warranties

The Relying Party is solely responsible for making the decision to rely on a emSign PKI Certificate.

A Relying Party accepts that to reasonably rely on a emSign PKI Certificate, the Relying Party must have:

1. Obtained sufficient knowledge on the use of digital Certificates and PKI,
2. Studied the applicable limitations on the usage of Certificates and agrees to emSign's limitations on liability related to the use of Certificates,
3. Read, understood, and agreed to the emSign's Relying Party Agreement and this CP/CPS,
4. Verified both the emSign Certificate and the Certificates in the certificate chain using the relevant CRL or OCSP
5. Not used a emSign Certificate which has expired or been revoked,
6. Taken all reasonable steps to minimize the risk associated with relying on a digital signature certificate after considering:
    a) applicable law and the legal requirements for identification of a party, protection of the confidentiality or privacy of information, and enforceability of the transaction;
    b) the intended use of the Certificate as listed in the certificate or this CPS,
    c) the data listed in the Certificate,
    d) the economic value of the transaction or communication,
    e) the potential loss or damage that would be caused by an erroneous identification or a loss of confidentiality or privacy of information in the application, transaction, or communication,
    f) the Relying Party's previous course of dealing with the Subscriber,
    g) the Relying Party's understanding of trade, including experience with computer-based methods of trade, and
    h) any other indicia of reliability or unreliability pertaining to the Subscriber and/or the application, communication, or transaction.

Any unauthorized reliance on a Certificate is at the Relying Party's own risk.

#### 9.6.5. Representation and Warranties of Other Parties

No stipulation.

## 9.7. Disclaimer of Warranties

emSign PKI hereby disclaims all warranties including warranty on merchantability and /or fitness to a particular purpose other than to the extent prohibited by law or otherwise expressly provided in this CP/CPS.

## 9.8. Limitation of Liability

All Issuing CAs under emSign PKI provides the service on best effort basis. The security and suitability of the service will not be guaranteed by Issuing CAs under emSign PKI.

Issuing CAs under emSign PKI shall not be liable for delay or omission to issue/revoke/activate a digital certificate or any other consequences arising from events beyond the control of Issuing CAs under emSign PKI. emSign PKI shall not be liable, for any certificates obtained from it, by representing false or inaccurate or misleading or untrue information.

All warranties and any disclaimers thereof, and any limitations of liability among Issuing CAs under emSign PKI, its Intermediaries (RAs/partners) and their respective customers shall be in strict adherence to the terms and conditions of the Agreement amongst them.

To the extent Issuing CAs under emSign PKI has issued and managed the certificate in accordance with this CP/CPS, Issuing CAs under emSign PKI shall not have any liability to the Subscriber, Relying Party or any Third Parties for any losses or damages suffered as a result of use or reliance on such a certificate.

Issuing CAs under emSign PKI shall be liable to Certificate Holders or Relying Parties for direct loss arising from any breach of this CP/CPS or for any other liability it may incur in contract, tort or otherwise, including liability for negligence up to the following limits per Subscriber or Relying Party or Third Party per Certificate, provided the Subscriber, the Relying Party or the Third Party is in full compliance of this CP/CPS.

Limits of Liability per Subscriber or Relying party or Third Party per certificate:

(1) US Dollars One Thousand only (USD 1,000/-)
(2) US Dollars Two Thousand only (USD 2,000/-) for Extended validation certificates.

The limit for aggregate maximum liability for all claims related to a single certificate or service shall be a liability of US Dollars Ten Thousand (USD 10,000/- only) or the amount paid by the subscriber in respect of that certificate or service during the past 12 months, whichever is higher.

The aggregate maximum liability for all claims, regardless of the number and source of claims shall be USD 1 million (USD 1,000,000/-) only.

Issuing CA's liability, under emSign PKI, to any person for damages arising under, out of or related in any way to this CP/CPS, Subscriber Agreement, the applicable contract or any related agreement, whether in contract, warranty, tort or otherwise, shall be limited to actual damages suffered by that person. Issuing CAs under emSign PKI shall not be liable for indirect, consequential, incidental, special, exemplary, or punitive damages with respect to any person, even if emSign PKI has been advised of the possibility of such damages, regardless of how such damages or liability may arise, whether in tort, negligence, equity, contract, statute, common law, or otherwise.

By participating within the Issuing CAs under emSign PKI, any person that participates within the emSign PKI irrevocably agrees that they shall not apply for or otherwise seek either indirect, exemplary, consequential, special, incidental, or punitive damages and irrevocably confirms to Issuing CAs under emSign PKI their acceptance of the foregoing and the fact that emSign has relied upon the foregoing as a condition and inducement to permit that person to participate within the emSign Public Key Infrastructure.

## 9.9. Indemnities

### 9.9.1. Indemnification by emSign PKI

emSign PKI shall indemnify each Application Software Vendor against any claim, damage, or loss suffered by an Application Software Vendor related to an EV Certificate issued by emSign PKI, except where the claim, damage, or loss suffered by the Application Software Vendor was directly caused by the Application Software Vendor's software displaying either:

(1) a valid and trustworthy EV Certificate as not valid or trustworthy or
(2) displaying as trustworthy
    (i) an EV Certificate that has expired or

(ii) a revoked EV Certificate where the revocation status is available online but the Application Software Vendor's software failed to check or ignored the status.

### 9.9.2. Indemnification by Subscribers

Any subscriber of a emSign Certificate, shall indemnify and hold harmless emSign PKI , its partners, any trusted root entities and their respective directors, officers, employees, agents, and contractors from any and all damages and losses arising out of:

(1) use of the emSign PKI Certificate in a manner not authorised by emSign PKI;
(2) tampering with the emSign Certificate; or
(3) misrepresentation or omission of material fact in order to obtain or use a Certificate, whether or not such misrepresentation or omission was intentional.

In addition, Subscribers shall indemnify and hold harmless emSign PKI from any and all damages (including legal fees) for lawsuits, claims or actions by third-parties relying on or otherwise using a emSign Certificate relating to:

(1) Subscriber's breach of their obligations under the Subscriber Agreement or this CP/CPS;
(2) Subscriber's failure to protect its private key; or
(3) claims (including without limitation infringement claims) pertaining to content or other information or data supplied by Certificate Holder.

### 9.9.3. Indemnification by Relying Parties

Any relying party of a emSign Certificate, , shall indemnify and hold harmless emSign PKI , its partners, any trusted root entities and their respective directors, officers, employees, agents, and contractors from any and all damages and losses arising out of:

(1) breach of the Relying Party Agreement, this CPS, or applicable law;
(2) unreasonable reliance on a Certificate;
(3) failure to check the Certificate's status prior to use.
(4) use of the emSign Certificate in a manner not authorised by emSign PKI;
(5) tampering with the emSign Certificate; or
(6) misrepresentation or omission of material fact in order to obtain or use a Certificate, whether or not such misrepresentation or omission was intentional.

## 9.10. Term and Termination

### 9.10.1. Term

This CP/CPS and any amendments to this shall become effective upon publication in the emSign repository and shall remain in effect until it is replaced by a newer version.

### 9.10.2. Termination

This CP/CPS and any amendments shall remain in force until it is amended or replaced by a newer version.

#### 9.10.3. Effect of Termination and Survival

Upon termination of this CPS, emSign PKI Participants are nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates. At a minimum, all responsibilities related to protecting confidential information will survive termination.

### 9.11. Individual Notices and Communications with Participants

Notices related to this CP/CPS may be submitted to emSign PKI in either paper or electronic form, using the contact details provided in Section 1.5.2 of this document. A notice is considered effective only upon receipt of a valid and signed acknowledgment from emSign PKI. If an acknowledgment is not received within seven (7) calendar days, the sender is required to resend the notice in physical form to the postal address specified in this CP/CPS, using a courier service that provides delivery confirmation.

emSign PKI may send required notices to Participants via electronic or physical means, unless otherwise explicitly agreed upon in writing.

### 9.12. Amendments

#### 9.12.1. Procedure for Amendment

Amendments to this CP/CPS are approved by emSign Policy Authority. Upon any amendment the amended CP/CPS shall be posted on the online repository within the duration defined in this CP/CPS.

#### 9.12.2. Notification Mechanism and Period

emSign PKI may make changes to this CP/CPS without notice; further emSign PKI does not guarantee or set a notice-and-comment period.

#### 9.12.3. Circumstances under which OID must be changed

No stipulation.

### 9.13. Dispute Resolution Procedures

If any dispute arises between the parties participating in the emSign PKI the parties shall first attempt to solve the dispute by good faith negotiations by referring directly to emSign, before resorting to any other dispute resolution mechanism. If such good faith negotiations fail then the parties may refer the matter to arbitration or adjudication.

### 9.14. Governing Law

This CP/CPS is governed by the laws of India except in circumstances where issuing CAs under emSign PKI have explicitly agreed with the subscriber / relying party / any other party to be governed by the laws of any other country. The construction and interpretation of this CPS will be in accordance with laws of India or the laws of the agreed jurisdiction as indicated above. Venue with respect to any disputes will be in Bangalore, India or any venue explicitly agreed in the subscriber / relying party / any other party agreement for the certificate with reference to which the dispute arises.

### 9.15. Compliance with Applicable Law

The certificates issued under emSign PKI shall be used by the subscribers and relying parties only in accordance with the laws and regulations of the jurisdiction in which they are used or relied upon.

Issuing CAs under emSign PKI may refuse to issue or may revoke Certificates if, in their opinion, issuance or the continued use of the emSign PKI Certificates would violate applicable laws or regulations.

## 9.16. Miscellaneous Provisions

### 9.16.1. Entire Agreement

No stipulation.

### 9.16.2. Assignment

Issuing CAs, subscribers, relying parties, Registering Authorities or any other entities operating under this CP/CPS are not entitled to assign any of their rights or obligations under this CP/CPS without the prior written consent of eMudhra.

### 9.16.3. Severability

If any of the provisions of this CP/CPS is held invalid by a competent authority in the applicable jurisdiction, the remainder of the CP/CPS will remain valid and enforceable.

### 9.16.4. Enforcement (attorneys' fees and waiver of rights)

Issuing CAs under emSign PKI may seek indemnification and attorneys' fees from a party for damages, losses and expenses related to that party's conduct.

emSign PKI's failure to enforce a provision of this CP/CPS does not waive emSign PKI 's right to enforce the same provision later or right to enforce any other provision of this CP/CPS.

No waiver to any party shall be effective unless it is given in writing by respective issuing CAs under emSign PKI.

In its specific agreements with subscribers, relying parties or any other parties emSign PKI may agree to further provisions relating to enforcement.

### 9.16.5. Force Majeure

emSign PKI accepts no liability for any delay or failure to perform an obligation under this CP/CPS to the extent those delay or failure is caused by events beyond its reasonable control.

## 9.17. Other Provisions

No stipulation.

# 10. Appendix A: Verification Requirements for Subscriber

## 10.1. SSL/TLS - DV

| **Usage/Purpose** | Secure Websites |
|---|---|
| **Domain Verification** | Domain name(s) to be listed in the Certificate shall be checked with any one or more of the following procedures, for satisfactory proof of right-to-use the domain:<br><br>1. Validating the request by sending a Random Value to an email address created by prepending 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' in the local part, followed by the at-sign ("@"), followed by the Authorization Domain Name and obtaining a response utilizing the Random Value (Baseline Requirements Section 3.2.2.4.4)<br>2. Validating the request by confirming the presence of a Random Value in a DNS CNAME or TXT record on the Authorization Domain Name (Baseline Requirements Section 3.2.2.4.7)<br>3. Validating the request by sending a Random Value to an email address of DNS CAA Email Contact. The relevant CAA Resource Record Set MUST be found using the search algorithm defined in RFC 8659 Section 3 (Baseline Requirements Section 3.2.2.4.13)<br>4. Validating the request by sending a Random Value to a DNS TXT Record Email Contact via email and then receiving a confirming response utilizing the Random Value (Baseline Requirements Section 3.2.2.4.14)<br>5. Validating the request by calling the DNS TXT Record Phone Contact's phone number and obtaining a confirming response to validate the Authorization Domain Name. (Baseline Requirements Section 3.2.2.4.16)<br>6. Validating the request by confirming the presence of a Random Value within a file under the "/.well-known/pki-validation" directory on the Authorization Domain Name that is accessible by the CA via HTTP/HTTPS over an Authorized Port. (Baseline Requirements Section 3.2.2.4.18)<br>7. Validating the request by using the ACME HTTP Challenge method in accordance to RFC 8555 (Baseline Requirements Section 3.2.2.4.19)<br>8. ACME DNS Challenge (Labelled with Account ID) DNS validation using ACME with account-specific labels (Baseline Requirements Section 3.2.2.4.21)<br><br>**Wildcard domains:** These shall undergo additional checks, to not to wrongly issue, for a domain listed in public suffix list (PSL). If the domain is listed in PSL, the application shall be refused, unless applicant proves ownership of entire domain namespace.<br>**Country:** If the Country is present in application, it shall be validated against, the domain names ccTLD, or the domain registrar provided information, or by IP address range allocation (by country) checked for the domain or the applicant's IP address.<br>**IP Address**: If the IP address is requested for the certificate, in place of domain name, it shall be verified to have the applicant's control over the IP as per Baseline Requirements Section 3.2.2.5, by means of (i) change in agreed information in an URL containing the IP address, OR (ii)<br>IP assignment document of IANA or Regional Internet Registry, OR (iii) Email, Fax, SMS, or Postal Mail to IP Address Contact OR (iv) Phone Contact with IP |

| | |
|---|---|
| | Address Contact OR (v) ACME “http-01” method for IP Addresses OR (vi) ACME “tls-alpn-01” method for IP Addresses performing r-DNS lookup resulting in a domain name verified by above procedure.<br>**MPIC:**<br>emSign implements Multi-Perspective Issuance Corroboration (MPIC) to improve protection against Border Gateway Protocol (BGP) hijacks and DNS manipulation during domain validation. MPIC is applied to the following validation methods:<br>1. DNS-based validation methods, including DNS TXT and CNAME records<br>2. HTTP-based domain validation methods, including file-based challenges<br>3. ACME HTTP-01 challenge methods<br>4. CAA record checks<br>emSign SHALL corroborate validation results using at least two independent Network Perspectives. These Network Perspectives MUST be geographically separated by a straight-line distance of at least 500 kilometers.<br>Each Network Perspective MAY use a recursive DNS resolver that is not co-located with the Network Perspective. However, the DNS resolver used by the Network Perspective MUST fall within the same Regional Internet Registry (RIR) service region as the Network Perspective relying upon it.<br>emSign SHALL ensure that no Network Perspective reuses or shares DNS cache or validation results with any other perspective. DNS queries and HTTP validations MUST be performed independently from each perspective. Validation results from one perspective SHALL NOT influence or substitute for validation results from another.<br>MPIC SHALL be used to detect and prevent certificate issuance in the presence of routing or DNS anomalies, including BGP hijacks, DNS poisoning, or other forms of network-level interference. Any inconsistencies detected during MPIC SHALL result in the validation being treated as a failure, and the certificate SHALL NOT be issued. |

### 10.2. SSL/TLS - IV/OV

| **Usage/Purpose** | Secure Websites |
|---|---|
| **Individual Verification** | For Individual Validated (IV), Verification of the identity & address of the applicant shall be made using, any one or more the following:<br>1. Identity & address of the applicant shall be verified by obtaining a legible copy, which noticeably shows the Applicant's face, of at least one currently valid government-issued photo ID proof (passport, national ID, driver's license, government employment ID, or any other equivalent document type). The copy of the document shall be inspected for any indication of alteration or falsification.<br>2. If address is not part of identity proof and/or requires any further assurance, this may be checked by taking an additional form of identification, such as recent utility bills, telephone bills, financial account statements, credit card, an additional ID proof, or any other equivalent document type.<br>3. Additional cross-checks may be made the Applicant's name & address for consistency with a Reliable Data Source.<br>4. Confirmation may be taken that the Applicant is able to receive communication by telephone, postal mail/courier, or fax.<br>5. If the verification is not satisfactorily achieved by any of the above process OR an alternate process is necessary, it may completed by accepting a Declaration of Identity, that is attested by a the RA, Trusted Agent, notary, lawyer, certified/practicing accountant, Bank officer (above specified grades), Postal Officer(above specified grades), or a Government Officer (above specified grades). |
| **Organization Verification** | For Organization Validated (OV), Verification of the identity & address of the applicant shall be made using, any one or more the following:<br>1. A Reliable Data Source including a government/third-party databases, or through a physical/electronic/telephonic communication with the entity or jurisdiction governing the organization's legal creation, existence, or recognition.<br>2. A site visit verification by CA or RA.<br>3. An attestation letter that is signed by a practicing/qualified accountant, lawyer, government official, or any other reliable third party.<br>4. Any DBA Names 'to-be-included' included in the Certificate is also verified using a government source, attestation letter, third party or any other reliable form of identification.<br>5. For address & validity verification, it can also be made using, a utility bill, bank statement, credit card statement, tax document, or any other reliable form of identification. |
| **Domain Verification** | Domain name(s) to be listed in the Certificate shall be checked with any one or more of the following procedures, for satisfactory proof of right-to-use the domain:<br><br>1. Validating the request by sending a Random Value to an email address created by prepending 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' in the local part, followed by the at-sign ("@"), followed by |

| | |
|---|---|
| | the Authorization Domain Name and obtaining a response utilizing the Random Value (Baseline Requirements Section 3.2.2.4.4)<br>2. Validating the request by confirming the presence of a Random Value in a DNS CNAME or TXT record on the Authorization Domain Name (Baseline Requirements Section 3.2.2.4.7)<br>3. Validating the request by sending a Random Value to an email address of DNS CAA Email Contact. The relevant CAA Resource Record Set MUST be found using the search algorithm defined in RFC 8659 Section 3 (Baseline Requirements Section 3.2.2.4.13)<br>4. Validating the request by sending a Random Value to a DNS TXT Record Email Contact via email and then receiving a confirming response utilizing the Random Value (Baseline Requirements Section 3.2.2.4.14)<br>5. Validating the request by calling the DNS TXT Record Phone Contact's phone number and obtaining a confirming response to validate the Authorization Domain Name. (Baseline Requirements Section 3.2.2.4.16)<br>6. Validating the request by confirming the presence of a Random Value within a file under the "/.well-known/pki-validation" directory on the Authorization Domain Name that is accessible by the CA via HTTP/HTTPS over an Authorized Port. (Baseline Requirements Section 3.2.2.4.18)<br>7. Validating the request by using the ACME HTTP Challenge method in accordance to RFC 8555 (Baseline Requirements Section 3.2.2.4.19)<br>8. ACME DNS Challenge (Labelled with Account ID) DNS validation using ACME with account-specific labels (Baseline Requirements Section 3.2.2.4.21)<br><br>**Wildcard domains:** These shall undergo additional checks, to not to wrongly issue, for a domain listed in public suffix list (PSL). If the domain is listed in PSL, the application shall be refused, unless applicant proves ownership of entire domain namespace.<br>**Country:** If the Country is present in application, it shall be validated against, the domain names ccTLD, or the domain registrar provided information, or by IP address range allocation (by country) checked for the domain or the applicant's IP address.<br>**IP Address**: If the IP address is requested for the certificate, in place of domain name, it shall be verified to have the applicant's control over the IP as per Baseline Requirements Section 3.2.2.5, by means of (i) change in agreed information in an URL containing the IP address, OR (ii)<br>IP assignment document of IANA or Regional Internet Registry, OR (iii) Email, Fax, SMS, or Postal Mail to IP Address Contact OR (iv) Phone Contact with IP Address Contact OR (v) ACME "http-01" method for IP Addresses OR (vi) ACME "tls-alpn-01" method for IP Addresses performing r-DNS lookup resulting in a domain name verified by above procedure.<br>**MPIC:**<br>emSign implements Multi-Perspective Issuance Corroboration (MPIC) to improve protection against Border Gateway Protocol (BGP) hijacks and DNS manipulation during domain validation. MPIC is applied to the following validation methods:<br>1. DNS-based validation methods, including DNS TXT and CNAME records |

| | |
|---|---|
| | 2. HTTP-based domain validation methods, including file-based challenges<br>3. ACME HTTP-01 challenge methods<br>4. CAA record checks<br>emSign SHALL corroborate validation results using at least two independent Network Perspectives. These Network Perspectives MUST be geographically separated by a straight-line distance of at least 500 kilometers.<br>Each Network Perspective MAY use a recursive DNS resolver that is not co-located with the Network Perspective. However, the DNS resolver used by the Network Perspective MUST fall within the same Regional Internet Registry (RIR) service region as the Network Perspective relying upon it.<br>emSign SHALL ensure that no Network Perspective reuses or shares DNS cache or validation results with any other perspective. DNS queries and HTTP validations MUST be performed independently from each perspective. Validation results from one perspective SHALL NOT influence or substitute for validation results from another.<br>MPIC SHALL be used to detect and prevent certificate issuance in the presence of routing or DNS anomalies, including BGP hijacks, DNS poisoning, or other forms of network-level interference. Any inconsistencies detected during MPIC SHALL result in the validation being treated as a failure, and the certificate SHALL NOT be issued. |
| **Telephone Verification** | If Telephone is to be present in the certificate, telephone number shall<br>1. Either be a part of a pre-verified source, including bank verified information, etc<br>2. Or, be verified by sending a challenge-response SMS text message or by recording the applicant's voice during a communication to/by that telephone number. |
| **Email Verification** | If Email is to be present in the certificate, The control over email or the domain name of email server,<br>1. Either be a part of a pre-verified source, including bank verified information, etc<br>2. Or, be verified in the form of delivery and acceptance of the email. |

### 10.3. SSL/TLS - EV

| | |
|---|---|
| **Usage/Purpose** | Secure Websites |
| **Physical Verification** | As per EV requirements, mentioned below. |
| **Individual Verification** | As per EV requirements, mentioned below. |
| **Organization Verification** | As per EV requirements, mentioned below. |

| | |
|---|---|
| **Domain Verification** | Domain name(s) to be listed in the Certificate shall be checked with any one or more of the following procedures, for satisfactory proof of right-to-use the domain:<br><br>1. Validating the request by sending a Random Value to an email address created by prepending 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' in the local part, followed by the at-sign ("@"), followed by the Authorization Domain Name and obtaining a response utilizing the Random Value (Baseline Requirements Section 3.2.2.4.4)<br>2. Validating the request by confirming the presence of a Random Value in a DNS CNAME or TXT record on the Authorization Domain Name (Baseline Requirements Section 3.2.2.4.7)<br>3. Validating the request by sending a Random Value to an email address of DNS CAA Email Contact. The relevant CAA Resource Record Set MUST be found using the search algorithm defined in RFC 8659 Section 3 (Baseline Requirements Section 3.2.2.4.13)<br>4. Validating the request by sending a Random Value to a DNS TXT Record Email Contact via email and then receiving a confirming response utilizing the Random Value (Baseline Requirements Section 3.2.2.4.14)<br>5. Validating the request by calling the DNS TXT Record Phone Contact's phone number and obtaining a confirming response to validate the Authorization Domain Name. (Baseline Requirements Section 3.2.2.4.16)<br>6. Validating the request by confirming the presence of a Random Value within a file under the "/.well-known/pki-validation" directory on the Authorization Domain Name that is accessible by the CA via HTTP/HTTPS over an Authorized Port. (Baseline Requirements Section 3.2.2.4.18)<br>7. Validating the request by using the ACME HTTP Challenge method in accordance to RFC 8555 (Baseline Requirements Section 3.2.2.4.19)<br>8. ACME DNS Challenge (Labelled with Account ID) DNS validation using ACME with account-specific labels (Baseline Requirements Section 3.2.2.4.21) |
| **Telephone Verification** | As per EV requirements, mentioned below. |
| **Email Verification** | As per EV requirements, mentioned below. |
| **EV Verification** | Section 11 of EV guidelines of CABF |
| **MPIC** | emSign implements Multi-Perspective Issuance Corroboration (MPIC) to improve protection against Border Gateway Protocol (BGP) hijacks and DNS manipulation during domain validation. MPIC is applied to the following validation methods:<br>1. DNS-based validation methods, including DNS TXT and CNAME records<br>2. HTTP-based domain validation methods, including file-based challenges<br>3. ACME HTTP-01 challenge methods<br>4. CAA record checks |

| | |
|---|---|
| | emSign SHALL corroborate validation results using at least two independent Network Perspectives. These Network Perspectives MUST be geographically separated by a straight-line distance of at least 500 kilometers.<br>Each Network Perspective MAY use a recursive DNS resolver that is not co-located with the Network Perspective. However, the DNS resolver used by the Network Perspective MUST fall within the same Regional Internet Registry (RIR) service region as the Network Perspective relying upon it.<br>emSign SHALL ensure that no Network Perspective reuses or shares DNS cache or validation results with any other perspective. DNS queries and HTTP validations MUST be performed independently from each perspective. Validation results from one perspective SHALL NOT influence or substitute for validation results from another.<br>MPIC SHALL be used to detect and prevent certificate issuance in the presence of routing or DNS anomalies, including BGP hijacks, DNS poisoning, or other forms of network-level interference. Any inconsistencies detected during MPIC SHALL result in the validation being treated as a failure, and the certificate SHALL NOT be issued. |

# 11. Appendix B: Certificate Profiles

## 11.1. Root Certificates

| | |
|---|---|
| Version | V3 |
| Serial Number | Unique Non-Sequential CSPRNG Number and is greater than zero. |
| Signature Algorithm | SHA-256, SHA-384 or SHA-512 with RSA Encryption or ECDSA with SHA-256, SHA-384 or SHA-512 |
| Issuer: CN | <Issuing CA Common Name> |
| Issuer: O | <Issuing CA Organization name> |
| Issuer: OU | <Issuing CA Organization unit> |
| Issuer: C | <Issuing CA Country> |
| Valid From | Start date expressed in UTC format |
| Valid To | Start date expressed in UTC format |
| Public Key | RSA 4096 (OR) RSA 8192<br>ECC curves NIST P-256, P-384, or P-521 |
| Subject: CommonName | Common Name of Root CA |
| Subject: OrganizationName | Legal Name of CA Organization |
| Subject: OrganizationalUnitName | Variable Information |
| Subject: CountryName | Country of CA |
| Key Usage | Critical=TRUE<br>Certificate Signing, Off-line CRL Signing, CRL Signing (06) |

| | |
|---|---|
| Subject Key Identifier | Critical=FALSE<br>160 bit hash (SHA-1) |
| Basic Constraints | Critical=TRUE<br>Subject Type=CA, Path Length Constraint=None |

## 11.2. Subordinate CA Certificates (Issuer / Intermediate)

| | |
|---|---|
| Version | V3 |
| Serial Number | Unique Non-Sequential CSPRNG Number and is greater than zero. |
| Signature Algorithm | SHA-256, SHA-384 or SHA-512 with RSA Encryption or ECDSA with SHA-256, SHA-384 or SHA-512 |
| Issuer: CN | <Issuing CA Common Name> |
| Issuer: O | <Issuing CA Organization name> |
| Issuer: OU | <Issuing CA Organization unit> |
| Issuer: C | <Issuing CA Country> |
| Valid From | Start date expressed in UTC format |
| Valid To | Start date expressed in UTC format |
| Public Key | RSA 4096 (OR) RSA 8192<br>ECC curves NIST P-256, P-384, or P-521 |
| Subject: CommonName | Common Name of CA |
| Subject: OrganizationName | Legal Name of CA Organization |
| Subject: OrganizationalUnitName | Variable Information |
| Subject: CountryName | Country of CA |
| Key Usage | Critical=TRUE<br>Certificate Signing, Off-line CRL Signing, CRL Signing (06) |
| Enhanced Key Usage | In case the CA issues Server Authentication certificates: |
| | Critical=FALSE<br>Server Authentication, Client Authentication |
| Certificate Policies | Critical=FALSE<br>1. Policy ID=2.5.29.32.0, http://repository.emsign.com |
| Subject Key Identifier | Critical=FALSE<br>160 bit hash (SHA-1) |
| Authority Key Identifier | Critical=FALSE<br>160 bit hash (SHA-1) |
| Basic Constraints | Critical=TRUE<br>Subject Type=CA, Path Length Constraint=n |
| Authority Information access | Critical=FALSE<br>Access Method=OCSP (1.3.6.1.5.5.7.48.1),<br>URL=http://ocsp.emSign.com |

| | |
|---|---|
| CRL Distribution Points | Critical=FALSE<br>CRL HTTP URL = http://crl.emsign.com?<IssuerName>.crl |

### 11.3. SSL/TLS - DV

| | |
|---|---|
| Version | V3 |
| Serial Number | Unique Non-Sequential CSPRNG Number and is greater than zero. |
| Signature Algorithm | SHA-256, SHA-384 or SHA-512 with RSA Encryption or ECDSA with SHA-256, SHA-384 or SHA-512 |
| Issuer: CN | <Issuing CA Common Name> |
| Issuer: O | <Issuing CA Organization name> |
| Issuer: OU | <Issuing CA Organization unit> |
| Issuer: C | <Issuing CA Country> |
| Valid From | Start date expressed in UTC format |
| Valid To | Start date expressed in UTC format |
| Public Key | As per Section 6.1.5. |
| Subject: CommonName | FQDN or Single IP |
| Subject Alternative Name | Critical=FALSE<br>DNS (multiple) = FQDN or Single IP |
| Key Usage | Critical=TRUE<br>Digital Signature, (in case of RSA algorithm, it shall also contain Key Encipherment (a0)) |
| Enhanced Key Usage | Critical=FALSE<br>Server Authentication |
| Certificate Policies | Critical=FALSE<br>1. Policy ID=1.3.6.1.4.1.50977.1.2.100 (User Notice, Domain Validated SSL/TLS Certificate) 2. Policy ID=1.3.6.1.4.1.50977.1.0.1 (CPS), http://repository.emsign.com |
| Subject Key Identifier | Critical=FALSE<br>160 bit hash (SHA-1) |
| Authority Key Identifier | Critical=FALSE<br>160 bit hash (SHA-1) |
| Basic Constraints | Critical=TRUE<br>Subject Type=End Entity, Path Length Constraint=None |
| Authority Information access | Critical=FALSE<br>Access Method=OCSP (1.3.6.1.5.5.7.48.1), URL=http://ocsp.emSign.com |
| CRL Distribution Points | Critical=FALSE<br>CRL HTTP URL = http://crl.emsign.com?<IssuerName>.crl |

### 11.4. SSL/TLS - OV

| | |
|---|---|
| Version | V3 |
| Serial Number | Unique Non-Sequential CSPRNG Number and is greater than zero. |
| Signature Algorithm | SHA-256, SHA-384 or SHA-512 with RSA Encryption or ECDSA with SHA-256, SHA-384 or SHA-512 |
| Issuer: CN | <Issuing CA Common Name> |
| Issuer: O | <Issuing CA Organization name> |
| Issuer: OU | <Issuing CA Organization unit> |
| Issuer: C | <Issuing CA Country> |
| Valid From | Start date expressed in UTC format |
| Valid To | Start date expressed in UTC format |
| Public Key | As per Section 6.1.5. |
| Subject: CommonName | FQDN or Single IP |
| Subject: OrganizationName | Legal Name of the Organization with allowed variations |
| Subject: StreetAddress | Verified Street Address (Optional) |
| Subject: LocalityName | Verified Locality (Optional) |
| Subject: StateOrProvinceName | Verified State/Province |
| Subject: CountryName | Verified Country |
| Subject: PostalCode | Verified Postal Code (Optional) |
| Subject Alternative Name | Critical=FALSE<br>DNS (multiple) = FQDN or Single IP |
| Key Usage | Critical=TRUE<br>Digital Signature, (in case of RSA algorithm, it shall also contain Key Encipherment (a0)) |
| Enhanced Key Usage | Critical=FALSE<br>Server Authentication |
| Certificate Policies | Critical=FALSE<br>1. Policy ID=1.3.6.1.4.1.50977.1.2.110 (User Notice, Organization Validated SSL/TLS Certificate) 2. Policy ID=1.3.6.1.4.1.50977.1.0.1 (CPS, http://repository.emsign.com |
| Subject Key Identifier | Critical=FALSE<br>160 bit hash (SHA-1) |
| Authority Key Identifier | Critical=FALSE<br>160 bit hash (SHA-1) |
| Basic Constraints | Critical=TRUE<br>Subject Type=End Entity, Path Length Constraint=None |

| | |
|---|---|
| Authority Information access | Critical=FALSE<br>Access Method=OCSP (1.3.6.1.5.5.7.48.1),<br>URL=http://ocsp.emSign.com |
| CRL Distribution Points | Critical=FALSE<br>CRL HTTP URL = http://crl.emsign.com?<IssuerName>.crl |

### 11.5. SSL/TLS - EV

| | |
|---|---|
| Version | V3 |
| Serial Number | Unique Non-Sequential CSPRNG Number and is greater than zero. |
| Signature Algorithm | SHA-256, SHA-384 or SHA-512 with RSA Encryption or ECDSA with SHA-256, SHA-384 or SHA-512 |
| Issuer: CN | <Issuing CA Common Name> |
| Issuer: O | <Issuing CA Organization name> |
| Issuer: OU | <Issuing CA Organization unit> |
| Issuer: C | <Issuing CA Country> |
| Valid From | Start date expressed in UTC format |
| Valid To | Start date expressed in UTC format |
| Public Key | As per Section 6.1.5. |
| Subject: CommonName | FQDN or Single IP |
| Subject: OrganizationName | Legal Name of the Organization with allowed variations |
| Subject: StreetAddress | Verified Street Address (Optional) |
| Subject: LocalityName | Verified Locality (Optional) |
| Subject: StateOrProvinceName | Verified State/Province |
| Subject: CountryName | Verified Country |
| Subject: PostalCode | Verified Postal Code (Optional) |
| Subject: BusinessCategory | Verified Information as per EV criteria |
| Subject: SerialNumber | Verified Information as per EV criteria |
| Subject: JurisdictionLocalityName | Verified Information as per EV criteria |
| Subject: JurisdictionStateOrProvinceName | Verified Information as per EV criteria |
| Subject: JurisdictionCountryName | Verified Information as per EV criteria |
| Subject Alternative Name | Critical=FALSE<br>DNS (multiple) = FQDN or Single IP |
| Key Usage | Critical=TRUE<br>Digital Signature, (in case of RSA algorithm, it shall also contain Key Encipherment (a0)) |
| Enhanced Key Usage | Critical=FALSE<br>Server Authentication |

| | |
|---|---|
| Certificate Policies | Critical=FALSE<br>1. Policy ID=1.3.6.1.4.1.50977.1.2.120 (User Notice, Extended Validated SSL/TLS Certificate) 2. Policy ID=1.3.6.1.4.1.50977.1.0.1 (CPS, http://repository.emsign.com |
| Subject Key Identifier | Critical=FALSE<br>160 bit hash (SHA-1) |
| Authority Key Identifier | Critical=FALSE<br>160 bit hash (SHA-1) |
| Basic Constraints | Critical=TRUE<br>Subject Type=End Entity, Path Length Constraint=None |
| Authority Information access | Critical=FALSE<br>Access Method=OCSP (1.3.6.1.5.5.7.48.1), URL=http://ocsp.emSign.com |
| CRL Distribution Points | Critical=FALSE CRL<br>HTTP URL = http://crl.emsign.com?<IssuerName>.crl |

# 12. Appendix C: Change History

This section contains the summary of changes made to the CP-CPS. Please check the archived document versions for detailed comparative differences.

**Version 1.00: 19-August-2025**

- Base Version