# CERTIFICATE POLICY

# &

# CERTIFICATION PRACTICE STATEMENT

# (CP/CPS)

26-July-2021
Version 1.09

**CP/CPS OID: 1.3.6.1.4.1.50977.1.0.1**


**emSign**
info@emsign.com | www.emsign.com

emudhra
Trust Delivered

# 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, eMudhra Limited, India, eMudhra Technologies Limited, India, eMudhra PTE Limited, Singapore, eMudhra DMCC, UAE.

## 1.1. Overview

This emSign PKI (operating under the brand emSign) Certificate Policy and Certification Practice Statement (the "CP/CPS") presents the principles, procedures and practices employed in the issuance and life cycle management within emSign PKI Hierarchy. This CP/CPS and all amendments thereto are incorporated by a reference into emSign Certificates issued under this CP/CPS.

In this document, the words "emSign" and "emSign CA" and "emSign PKI" are used interchangeably and include all root CAs, Issuing CAs and Affiliates of eMudhra.

This CP/CPS is applicable to all entities with relationship with emSign PKI including policy authorities, certification authorities, registration authorities, subscribers, and relying parties. Any other parties may also perform some functions relating to issuance and/or revocation of certificates, on behalf of subscribers. In such cases, the principles, procedures and practices contained in this document shall be applicable to such parties, as if they were the subscribers, to the extent practicable.

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

1. RFC 3647 of Internet Engineering Task Force (IETF) for Certificate Policy and Certification Practice Statement.
2. The latest versions (as on date of this CP/CPS) of the CA/Browser Forum (CABF) requirements including: (Ref: https://cabforum.org)
   - Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates.
   - Guidelines for the Issuance and Management of Extended Validation (EV) Certificates,
   - Guidelines for the Issuance and Management of Extended Validation (EV) Code-Signing Certificates
   - Network and Certificate System Security Requirements
3. Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates (Ref: https://aka.ms/csbr)
4. Time-stamping services according to RFC 3161 of IETF and other applicable standards.
5. Adobe Approved Trust List (AATL) Certificate policies.
6. Apple Root Certificate program, Microsoft Trusted Root Certificate Program Audit Requirements, Mozilla Root Store Policy, Oracle Java Root Certificate program, and Root Certificate Policy for the Chromium Projects.

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

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 emSign Policy Authority and subject to amendment as well as exceptions to mitigate material, imminent impacts to subscribers, partners, relying parties, and/or others within the certificate ecosystem where practical workarounds do not exist. Such exceptions are tracked, documented and reported as part of the audit process.

All the Cross Certificates in an established trust relationship are disclosed by emSign PKI. This CP/CPS addresses the actions of emSign PKI and those of third parties operating with cross certificates issued by emSign PKI.

## 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). The object identifier (OID) values corresponding to the emSign 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 CP/CPS Document | 1.3.6.1.4.1.50977.1.0.1 |

**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 |
| Code Signing - Organization Validation | 2.23.140.1.4.1,<br>1.3.6.1.4.1.50977.1.2.200 |
| Code Signing - Extended Validation | 2.23.140.1.3,<br>1.3.6.1.4.1.50977.1.2.210 |

| | |
|---|---|
| Device Certificate | 1.3.6.1.4.1.50977.1.2.300 |
| Client Certificates - Class 1 | 1.3.6.1.4.1.50977.1.2.400 |
| Client Certificates - Class 2 | 1.3.6.1.4.1.50977.1.2.410 |
| Client Certificates - Class 3 | 1.3.6.1.4.1.50977.1.2.420 |
| Time Stamping Certificate | 1.3.6.1.4.1.50977.1.2.500 |
| 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 a secure facility 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, subordinate CAs, including CAs owned by third parties. All such issuing CAs and subordinate CAs are required to operate in conformance with this CP/CPS.

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 CAs may be operated by emSign PKI or other organizations that have been authorized by emSign PKI to participate within the emSign PKI to carry out the above functions. Issuing CAs are required to act in accordance with their respective Issuing CA Agreements and to be bound by the terms of this CP/CPS. Generally, Issuing CAs will be authorised to issue and manage all types of Digital Certificates supported by this CP/CPS.

Issuing CAs, if authorised to do so by emSign PKI, may rely on third party Registration Authorities in the performance of Certificate Holder Identification and Authentication requirements. In circumstances where an Issuing CA has relied on a third-party Registration Authority to perform Identification and Authentication, the Issuing CA bears all responsibility and liability for the Identification and Authentication of its Certificate Holders.

### 1.3.2. Registration Authorities

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

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

emSign PKI may enter into contractual relationship with third party Issuing CAs, who may operate their own RA & authorize the issuance of certificates. Such third party issuing CAs and their RAs must comply with all the requirements of this CP/CPS and the terms of their contract. This may also refer to additional criteria as recommended by the CA Browser Forum. RAs may implement more restrictive vetting practices as per their internal policy.

Obligations of the Registration Authorities (RAs) 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 digital 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 utilise 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

### 1.3.4. Relying Parties

A Relying Party is an individual or entity that acts in reliance of a certificate and/or a digital signature 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 read 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 public-key certificate (e.g., through digital signature verification).
- Confirming that the subscriber uses the public-key in the Subscriber's certificate in compliance with this CP/CPS.
- Any other terms as per Relying Party Agreement.

Any party receiving a digitally signed electronic document may rely on that Digital Signature to the extent that they are authorized by contract with the Certificate Holder, or by legislation pursuant to which that Digital Certificate has been issued, or by commercial law in the jurisdiction in which that Digital Certificate was issued.

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 / Subordinates shall not Cross Certify / Bridge any Third-Party CAs, where such Third-Party CA would derive SSL/TLS and/or SMIME certificate issuing capabilities under emSign PKI.

## 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

emSign Certificates issued under this CP/CPS may be used as defined by certificate extensions on key usage and extended usage. The scope of use of the certificates include all legal authentication, encryption, access control and signing.

### 1.4.2. Prohibited Applications and Certificate Uses

emSign certificates are not for use and entities or subscribers may not use emSign certificates in circumstances where:

1) Usage of certificate is inconsistent with the certificate extensions in key usage and extended key usage
2) Usage of certificate is above the designated reliance limits indicated in the emSign Warranty Policy
3) Usage of certificate is for any equipment operated in hazardous conditions or under fail proof conditions (eg. Nuclear facilities, aircraft navigation, medical devices, direct life support devices, other systems where any failure could lead to injury, death or environmental damage etc.)
4) Usage of certificates is in connection with fraud, pornography, obscenity, hate, defamation, harassment and other activity that is contrary to public policy.

emSign Certificates do not guarantee that the Subject is trustworthy, operating a reputable business or that the equipment into which the Certificate has been installed is free from defect, malware or virus. In the case of code signing, Certificates do not guarantee that signed code is free from bugs or vulnerabilities.

emSign Certificates shall not be used for man-in-the-middle (MITM) or traffic management of domain names or IPs that the certificate holder does not legitimately own or control. Such certificate usage is expressly prohibited.

emSign's certificates should be used only for the designated purposes, in addition to specific types and categories. An end subscriber certificate should not be used for CA function, like, to issue/sign a certificate under it. Similarly, the CA certificates are to be used only for CA function, and not to perform any end subscriber usages like document signing, etc.

More generally, certificates shall be used only to the extent where use is consistent with all applicable laws, statute, order, decree, rules, regulations and court judgements of competent jurisdiction or governmental order.

In emSign PKI's CA and end subscriber certificates, the key usage extension is intended to limit the technical purposes for which a private key corresponding to the public key in a certificate may be used.

## 1.5. Policy Administration

This 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)
3rd Floor, Sai Arcade, Outer Ring Road, Devarabeesanahalli,
Bangalore - 560103, Karnataka, India
Phone: +91 80 42275300
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)
3rd Floor, Sai Arcade, Outer Ring Road, Devarabeesanahalli,
Bangalore - 560103, Karnataka, India
Phone: +91 80 42275300
Email: info@emsign.com
Website: www.emsign.com

**Certificate Problem Reporting**
Attn: Revocation Support
Email: problem-reporting@emsign.com

### 1.5.3. 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.

### 1.5.4. CPS Approval Procedures

The CP/CPS shall be reviewed/revised from time to time, as and when needed by the CA, or at a minimum of once a year, upon approval from the policy authority. The changes in CP/CPS are also made based on review of latest Baseline Requirements of CA Browser Forum, as and when published, which may need the policy or practices to be amended.

## 1.6. 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**: 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.

**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.

**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.

**CAA**: From RFC 6844 (http:tools.ietf.org/html/rfc6844): "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**: 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.

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

**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.

**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.

**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 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.

**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).

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

**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.).

**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.

**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.

**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.

**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**: 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.

**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.

**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**: 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**: 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**: The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.

**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.

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

**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.

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

**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.

**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.

# 2. Publication and Repository Responsibilities

## 2.1. Repositories

The emSign PKI online repositories are available at http://repository.emsign.com.

Repositories shall ensure that emSign PKI's Root Certificate and the revocation data for issued Certificates are available through their repository 24 hours a day, 7 days a week with a minimum of 99% availability overall per year with a scheduled down-time that does not exceed 0.5% annually.

Other external Issuer CAs shall publish emSign PKI's Root Certificate, all publicly trusted CA Certificates and Cross-Certificates, issued to and from the Issuer CA, revocation data for issued digital Certificates, CP/CPS, and standard Relying Party Agreements and Subscriber Agreements in their online repositories, and comply with above uptime requirements.

**Publication and Repository Obligations**
emSign and other Issuer CAs shall maintain an online repository of information relevant to the operations of PKI services under emSign PKI hierarchy on best effort basis. The information in the CA repository is subject to change and published periodically and also on need basis.

emSign PKI shall reserve rights to not to publish any information that it considers as confidential or not to be disclosed due to the sensitivity of the information.

In providing Repository services, obligations of the emSign PKI include:

- Storing and distributing public-key certificates (where relevant).
- Storing and distributing certificate status information (such as CRLs and/or online certificate status).
- Storing and distributing this CP/CPS and subsequent updates.
- Storing and distributing the Relying Party and Subscriber 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 (CRL).
- Test websites for the roots (wherever applicable).
- CP/CPS.

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 emSign and other Issuer CA online repository is publicly accessible information and, emSign and other Issuer CA provide unrestricted read only access to the contents of the repository. emSign and Other Issuer CA have put in place sufficient safeguards, logical and physical, to prevent any unauthorized write access or alteration/modification of repository entries.

# 3. Identification and Authentication

Issuing CAs or RAs may perform the Identification and Authentication required in connection with the issue of Digital Certificates. The level of Identification and Authentication depends on the class and/or type of Digital Certificate being issued and this may include face-to-face / video / biometric identity verification at the beginning of the Digital Certificate request procedure or at some point prior to Digital Certificate delivery to the Certificate Holder.

## 3.1. Naming

### 3.1.1. Types of Names

All names issued by emSign PKI conform to X.500 Distinguished Names standards. Each Digital signature certificate shall contain an X.501 distinguished name in the Subject name field. The Digital Certificates issued by emSign PKI shall use Distinguished Names (DN) to facilitate the identification of subscribers. Distinguished Name may comprise of the fields as required by the Certificate Profile of respective type and/or class of the certificate.

### 3.1.2. Need for Names to be Meaningful

The subject distinguished names in a digital signature certificate must be meaningful and must be able to determine the identity of the entity/subject. The common name in a certificate shall refer to the generally accepted personal name for individuals, a fully qualified domain name for devices, legal name of the organization, a unit within an organization, any other name identifying the device or any name legally owned or assigned to the organization. Requests for internationalized domain names (IDNs) in Certificates will be flagged for additional manual review and any necessary risk analysis procedures

The organization name (O) attribute type, when present in the subject distinguished name, represents the legal name of the Subscriber organization. Such information provided is for identity purposes only and shall not be construed to constitute any power of attorney or other rights.

If a certificate carries an empty Subject field, the information contained in the SAN (Subject Alternative Name) extension may or may not be meaningful depending on the type and intended use of the certificate.

### 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

The Subscriber names are unique within emSign CA / Issuing CA for a specific class and/or type of Certificate. It is possible for a Subscriber to have two or more certificates with the same Subject Distinguished Name (DN). emSign CA / Issuing CA may, if necessary, insert additional numbers or letters to the Certificate Holder's Subject Common Name, or other attribute, in order to distinguish between two Digital Certificates that would otherwise have the same Subject Name.

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

Certificate Applicants are prohibited from using names in their Certificate Applications that infringe upon others' Intellectual Property Rights. However, unless otherwise specifically stated in this CP/CPS, emSign PKI does not verify whether a Certificate Applicant has Intellectual Property rights in the name appearing in a Certificate Application nor does emSign PKI arbitrate, mediate, prosecute, or otherwise resolve any dispute concerning the ownership of any domain name, trade name, trademark, or service mark. emSign PKI may, without liability to any Certificate applicant, reject any Certificate application or suspend/revoke any Certificate because of such dispute.

For EV SSL/TLS Certificates, emSign shall implement a process that prevents such Certificates from including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific person or Legal Entity unless the CA has verified this information in accordance with the Identity Validation requirements of this document, and the Extended Validation SSL/TLS Certificate Guidelines of CAB Forum.

## 3.2. Initial Identity Validation

Issuing CAs may perform identification of the Applicant for issuance of certificate, or for services including CA chaining services, using any legal means of communication or investigation necessary to identify the Legal Entity or individual.

Issuing CAs may use the result of a successful Subject DN initial identity validation process to create alternative product offerings by effectively combining elements of previously verified information with alternative, newly verified, information. A suitable account based challenge response mechanism must be used to authenticate any previously verified information for any returning Applicant provided that the re-verification requirements of this CP/CPS are complied with.

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

The possession of the Private key, corresponding to the public key (which has to be listed in the Certificate), must be demonstrated by the certificate applicant, by submitting a PKCS #10 (CSR) request signed using the private key, or another approved method by emSign PKI.

For signature keys, this requirement shall not apply where the key pair is generated by emSign PKI on behalf of the Subscriber. Like:

(1) Where pre-generated keys are placed on smart cards / crypto token / any other crypto devices, or

(2) A key pair is generated on-behalf of the certificate applicant within secure emSign PKI environment, after due authentication by the certificate applicant. Such authentication may be performed using shared secret, or any other authentication mechanism approved by emSign PKI.

emSign PKI shall not generate the key pairs for end-entity certificates that have an EKU extension containing the KeyPurposeIds id-kp-serverAuth or anyExtendedKeyUsage.

### 3.2.2. Authentication of Organization Identity

If a Certificate asserts identity of an Organization, emSign or an RA validates the individual identity as per the applicable verification process for specific class or type of certificate. This shall be referred in Appendix A.

### 3.2.3. Authentication of Individual Identity

If a Certificate asserts individual identity, emSign or an RA validates the individual identity as per the applicable verification process for specific class or type of certificate. This shall be referred in Appendix A.

### 3.2.4. Non-Verified Certificate Holder Information

The Issuing CA may accept any form of Non-Verified Holder Information for the issuance of Digital Certificates used solely for demonstration or testing purposes. This will be allowed only in specific type of certificate uniquely identified as Test / Demonstration certificate.

SSL/TLS Certificates shall not have any Test / Demonstration certificate under the scope of this CP/CPS. For Live Certificates, in case of SSL/TLS certificate, self-declared values of the applicant shall not be allowed. emSign PKI may add additional OU fields to provide CA disclaimers or additional content given by the subscriber, as separate OU fields to the certificate.

### 3.2.5. Validation Of Authority

Where an Applicant's Name is to be associated with an Organisational Name to indicate his / her association as an employee or an authorisation person to act on behalf of an Organisation, Issuing CA / RA / Trusted Agents or LRA (if applicable) will validate the Applicant's Authority by reference to business records maintained by / submitted to the Issuing CA / RA.

### 3.2.6. Criteria for interoperation

Interoperation is permitted pursuant to the CP/CPS.

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

For CA Certificates, Certificate renewal is allowed by the way of new certificate with an extended validity period for an existing Distinguished Name.

For Subscriber Certificates, renewal is permitted by reuse of a previous certificate request to replace an expiring or expired Certificate. Where the initial Subscriber identification & authentication process as per this CP/CPS has been performed within the previous 825 days for DV and OV SSL certificates or as per EV stipulation or any other applicable guideline based on type or class of certificate, and the certificate is not revoked, emSign PKI may authenticate a renewal certificate request using a passphrase or any kind of shared secret or any other form of subscriber authentication mechanism.

### 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. Re-keyed 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 has been performed within the previous 825 days for DV and OV SSL certificates or as per EV stipulation or any other applicable guideline based on type or class of certificate, emSign PKI may authenticate re-key request using a passphrase or any kind of shared secret or any other form of subscriber authentication mechanism.

#### 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 and Digital Certificates may be submitted by the subscribers / persons authorised to do so under relevant contractual documentation. Revocation requests from subscribers may be granted following a suitable challenge response such as logging into an account with a username and password, or proving possession of unique elements incorporated into the Certificate, like Domain Name, email address, etc

Issuing CAs may also perform revocation on behalf of Subscribers in accordance with the requirements of the applicable Subscriber Agreement, or based on any instruction received from a competent authority.

## 4. Certificate Life-Cycle Operation Requirements

### 4.1. Certificate Application

Digital Certificate applications are subject to various evaluation criteria depending upon the type and class of Digital Certificate applied for.

#### 4.1.1. Who Can Submit a Certificate Application

An application for issuance of Digital Certificate in a procedure prescribed by the Issuing CA must be completed by Applicants (either in writing or electronically), which includes all registration information as described by this CP/CPS (including, without limitation, that information set out in Appendix A) and the relevant Certificate Holder Agreement or other terms and conditions upon which the Digital Certificate is to be issued. All applications are subject to review, approval, and acceptance by the Issuing CA in its discretion.

EV Certificate requests shall be submitted by an authorized Certificate Requester and approved by a Certificate Approver. The certificate request shall be accompanied by a signed Subscriber Agreement (either in writing or electronically) from a Contract Signer.

Globally accepted practices shall be followed for accepting documents electronically.

No individual or entity listed on a government denied list, list of prohibited persons or persons listed in other internationally recognized denied person list which are applicable to the jurisdictions in which the Issuing CA operates, shall submit an application for a certificate.

#### 4.1.2. Enrolment Process and Responsibilities

Certain information concerning applications for Digital Certificates is set out in this emSign PKI CP/CPS. However, the issuance of Digital Certificates by Issuing CAs will be pursuant to forms and documentation required by that Issuing CA.

Notwithstanding the foregoing, the following steps are required in any application for a Digital Certificate:

(i) Identity of the Holder or Device is to be established in accordance with Appendix A
(ii) A Key Pair for the Digital Certificate is to be generated in a secure fashion

(iii) The binding of the Key Pair to the Digital Certificate shall occur as set forth in this CP/CPS, and
(iv) The Issuing CA shall have a contractual relationship with emSign PKI.
(v) The issuing CA shall enter into contractual relations with the Certificate Holder for the use of that Digital Certificate.

Issuing CAs shall maintain systems and processes that sufficiently authenticate the Applicant's identity for all Certificate types that present the identity to Relying Parties. Applicants should submit sufficient information to allow Issuing CAs and/or RAs to successfully perform the required verification. Issuing CAs and RAs shall protect communications and securely store information presented by the Applicant during the application process.

Each Issuing CA may adopt its own application procedures, which Applicants will be required to satisfy. Each Holder of a Digital Certificate is required to be bound by contract with respect to the use of that Digital Certificate. These contracts may be directly between the Issuing CA and the Holder or imposed upon that Holder through terms and conditions binding upon him or her. All agreements concerning the use of, or reliance upon, Digital Certificates issued within the emSign PKI must incorporate by reference, the requirements of this emSign PKI CP/CPS, as may be amended from time to time.

## 4.2. Certificate Application Processing

### 4.2.1. Performing Identification And Authentication Functions

emSign CA or Issuing CAs shall maintain systems and processes to sufficiently authenticate the Applicant's identity in compliance with its CP/CPS. Initial identity validation shall be performed by an Issuing CAs validation team or by Registration Authorities under contract as set forth in this CP/CPS. All communications shall be securely stored along with all information presented by the Applicant during the application process.

Identification and Authentication requirements for each Digital Certificate profile is given in Appendix A.

Future identification of repeat Applicants and subsequent authentication checks may be addressed using a passphrase or any kind of shared secret or any other form of subscriber authentication mechanism.

However, use of the documents and data provided to verify certificate information in accordance to Appendix A shall be valid for a period no more than a specific period, prior to issuing the Certificate. This specific period shall not be more than the maximum validity period of the digital certificates limited under section 6.3.2 of this CP/CPS. Any issuance exceeding such period, shall undergo the requirements specified under Appendix A of this CP/CPS.

For SSL/TLS Certificates, emSign PKI's Issuing CAs shall also verify the existence of CAA record (RFC 6844) in applicant's DNS. If any CAA record exists in applicant's DNS, then the issuance shall be made only of the CAA record value contains the expected value for emSign PKI. The CAA records authorizing emSign PKI shall contain 'emsign.com' as the issuer domain names for 'issue' and 'issuewild' entries.

### 4.2.2. Approval or Rejection Of Certificate Applications

A Registration Authority will approve or reject Certificate Holder applications based upon the Certificate Holders meeting the requirements of this CP/CPS in Appendix A.

The Issuer CA shall reject any certificate application that cannot be verified. The Issuer CA may also reject a certificate application on any reasonable basis, including if the Certificate could damage the Issuer CA's business or reputation. Issuer CAs are not required to provide a reason for rejecting a certificate application.

### 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.

## 4.3. Certificate Issuance

### 4.3.1. Certification Authority Actions During Certificate Issuance

During Digital Certificate issuance, Issuing CA must comply with the practices described in and any requirements imposed by the emSign PKI CP/CPS.

#### 4.3.1.1. emSign Root Certification Authority

The Root Certification Authority Certificate has been self-generated and self-signed. All root certifying authorities are operated offline.

emSign PKI publishes all Root CA Certificates along with its subordinates in its repository available at http://repository.emsign.com

#### 4.3.1.2. emSign Issuing Certification Authority Certificates

emSign PKI creates and operates its own Issuing CAs under this CP/CPS.

Issuing Certifying Authorities are issued out of offline root certificates. However, on a need basis, emSign PKI may create and operate issuing CAs under a subordinate under Root CA.

emSign PKI publishes all Issuing CA Certificates along with its Hierarchy to its Root CA, in its repository available at http://repository.emsign.com

emSign PKI may also appoint external Issuing CAs upon accepting the terms and conditions of the emSign Issuing CA Agreement by the Issuing CA as prescribed by emSign CA, and final approval of the application by the emSign Policy Authority. The emSign PKI issues the Issuing CA Digital Certificate to the relevant Issuing CA.

#### 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.

### 4.3.2. 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

Digital Certificate acceptance is governed by and should comply with the practices described in, and any requirements imposed by, this CP/CPS.

By accepting a certificate, the Subscriber:

- Agrees to be bound by the continuing responsibilities, obligations and duties imposed by this CP/CPS,
- Agrees to be bound by the Subscriber Agreement, and
- Represents and warrants that to its knowledge no unauthorized person has had access to the private key associated with the certificate, and
- Represents and warrants that the certificate information it has supplied during the registration process is truthful and has been accurately and fully published within the certificate.
- ASSUMES A DUTY TO RETAIN CONTROL OF THE PRIVATE KEY CORRESPONDING TO THE PUBLIC KEY CONTAINED IN THE CERTIFICATE, TO USE A TRUSTWORTHY SYSTEM AND TO TAKE REASONABLE PRECAUTIONS TO PREVENT THE PRIVATE KEY'S LOSS, EXCLUSION, MODIFICATION, OR UNAUTHORISED USE.

Until a Digital Certificate is accepted, it is not published in any Repository or otherwise made publicly available. Without limitation to the generality of the foregoing, the use of a Digital Certificate or the reliance upon a Digital Certificate signifies acceptance by that person, of the terms and conditions of this emSign PKI CP/CPS and Subscriber Agreement (as the same may, from time to time, be amended or supplemented) by which they irrevocably agree to be bound.

### 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, including to Certificate Transparency Logs (optional).

### 4.4.3. Notification Of Certificate Issuance By The Certification Authority To Other Entities

Issuing CAs and Registration Authorities within the emSign PKI may choose to notify other Entities of Digital Certificate Issuance.

## 4.5. Key Pair And Certificate Usage

### 4.5.1. Subscriber private key and certificate usage

By accepting the Digital Certificate a Certificate Holder unconditionally agrees to use the Digital Certificate in a manner consistent with the Key-Usage field extensions included in the Digital Certificate Profile. All Certificate Holders shall protect their Private Keys from unauthorized use or disclosure to third parties and shall use their Private Keys only for their intended and lawful purpose.

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

Any party receiving a signed electronic document may rely on that Digital Signature to the extent that they are authorised by contract with the Certificate Holder, or by legislation pursuant to which that Digital Certificate has been issued, or by commercial law in the jurisdiction in which that Digital Certificate was issued.

For SSL/TLS:

- emSign PKI assumes that all user software will be compliant with X.509, the SSL/TLS protocol, and other applicable standards that enforce the requirements set forth in this CP/CPS.
- emSign PKI does not warrant that any third party's software will support or enforce such controls or requirements, and all Relying Parties are advised to seek appropriate technical or legal advice.
- Parties relying on a Certificate must adhere to the SSL/TLS protocol and verify a digital signature at all times by checking the validity of the associated Certificate against the relevant CRL or OCSP resource provided by emSign PKI.

Relying on a digital signature or SSL/TLS session without proper verification may result in risks that the Relying Party assumes in whole and which emSign PKI does not assume in any way.

Relying Party seeking to rely on a Digital Certificate issued within the emSign PKI is deemed to have accepted the Relying Party Agreement by seeking to place or by placing reliance upon the Digital Certificate or by the way of querying the existence or validity of the certificate.

Relying Parties are solely responsible for performing the risk assessment prior to relying on the Certificate or any assurances made. If the circumstances indicate that additional assurances are required, the Relying Party must obtain such assurances before using the Certificate. Relying Parties are obliged to seek further independent assurances before any act of reliance is deemed reasonable.

Relying Parties must also at the minimum must assess:

- The use of digital certificate is not prohibited by this CP/CPS.
- The appropriateness of the use of the Digital Certificate for any given purpose
- That the Digital Certificate is being used in accordance with its Key-Usage field extensions.
- That the Digital Certificate is valid at the time of reliance by reference to Online Certificate Status Protocol or Certificate Revocation List Checks.

Warranties are only valid if the steps detailed above have been carried out.

## 4.6. Certificate Renewal

### 4.6.1. Circumstances for Certificate Renewal

An Issuer CA may renew a Certificate if:

1. The associated public key has not reached the end of its validity period

2. The associated private key has not been compromised
3. The subscriber and attributes remain consistent
4. No new or additional validation is required

#### 4.6.2. Who may request renewal

Certificate Renewal means the issuance of a new Certificate without changing the Public Key or any other information in the Certificate, except the validity period.

An Issuing CA may accept a renewal request provided that it is authorized by the original subscriber using a passphrase or any kind of shared secret or any other form of subscriber authentication mechanism. A Certificate Signing request is not mandatory, however if one is used, then it must contain the same public key.

#### 4.6.3. Processing Certificate Renewal Requests

An Issuing CA may request additional information before processing a renewal request

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

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

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

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

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

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

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

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

### 4.7. Certificate Re-Key

Certificate Re-Key consists of creating a new Certificate with a different public key and validity period while retaining all the identifying information from the old Digital Certificate. Due diligence, Key Pair generation, delivery and management are performed in accordance with this CP/CPS.

#### 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 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

Certificate Holders or PKI Sponsors may request Digital Certificate Re-Keys.

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

Digital Certificate Re-Key requests are processed in the same manner as requests for new Digital Certificates and in accordance with the provisions of this CP/CPS. In order to process a Re-Key request,

the Certificate Holder or PKI Sponsor is required to authenticate themselves as per the requirements laid down in this CP/CPS for re-keying of certificate.

If the Private Key and any identity and domain information in a certificate have not changed, then emSign PKI can issue a replacement certificate using a previously issued certificate or previously provided Certificate Signing 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

Issuance of a Digital Certificate because of changes in details in an existing Digital Certificate is termed as Certificate Modification. emSign PKI does not offer certificate modification. Issuing CAs shall treat the modification requests in the same manner as a new Certificate Issuance and process the modification requests accordingly.

#### 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 changes or becomes obsolete.

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

- When such revocation is requested by the Subscriber
- Any information appearing in the Certificate was or became inaccurate or misleading;
- Private Key associated with or used to sign the Certificate was compromised or misused;
- When the original certificate request was not authorized by the Subscriber either prior to issuance or retroactively
- The Applicant has lost its rights to a trademark or the domain name listed in the Certificate;
- The subscriber breached a material obligation under the CP/CPS or Subscriber Agreement
- The Certificate was not issued in accordance with the CP/CPS, or applicable industry standards;
- Issuing CA is compromised.
- Issuing CA ceases operations or its right to manage Certificates under applicable industry standards was terminated and Issuing CA does not arrange for another CA to provide revocation support
- A government or regulatory order is received by the Issuing CA to revoke a Certificate
- The technical content or format of the Certificate presents an unacceptable security risk to application software vendors, Relying Parties, or others;
- The Subscriber was added as a denied party or prohibited person to a blacklist
- If the Certificate was used to sign, publish, or distribute malware or other harmful content
- If 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.
- Certificate Holder bankruptcy or liquidation
- Certificate Holder death

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;
- 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.)

### 4.9.2. Who Can Request Revocation

Issuing CA or RA shall accept authenticated requests for revocation from Subscriber or affiliated organization named in the Certificate. Issuing CAs may also at their own discretion revoke Certificates in the circumstances indicated in this CP/CPS.

**Certificate Problem Reporting**

Any party including Security Researchers, Anti-Malware Organizations, Subscribers, Relying Parties, Application Software Suppliers, or any other third parties may report suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates by sending email to the contact as provided in Section 1.5.2 of the CP/CPS. The reporter shall preferably indicate "Certificate Problem Report" in the subject line of such communication. The communication shall also include the Identity and Contact of such party reporting, along with the explanation of the problem / reason for revocation request. Necessary action will be taken up, subject to provisions mentioned in Section 4.9.3 of the 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 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. However, such duration shall not exceed 24 hours after successful validation of a revocation request.

### 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 uses commercially reasonable efforts to inform Subscribers about their private key compromise if it discovers or believes the compromise of such Private Key. This includes cases where new vulnerabilities have been discovered or where emSign at its own discretion decides that evidence suggests a possible Key Compromise has taken place.

Any party reporting of key compromise to emSign must include the proof of key compromise in either of the following formats:

- The private key itself, OR,
- A CSR signed by the compromised private key with the Common Name "Proof of Key Compromise for emSign".

The reporting party is recommended to provide description of the vulnerability and/or references to vulnerability and/or security incident sources from which the compromise is verifiable.

The reports shall be sent by email to the contact as provided in Section 1.5.2 of the CP/CPS (Certificate Problem Reporting section). The reporter shall preferably indicate "Certificate Problem Report" in the subject line of such communication. The communication shall also include the Identity and Contact of such party reporting, along with the explanation of the problem / reason for revocation request. This is necessary to receive confirmation of the problem report and any associated certificate revocations

The reporting party is required to use above method of reporting. emSign may accept any other acceptable method of submission in future, at its own discretion which may imply future revisions to this section of this document.

Necessary action will be taken up, subject to provisions mentioned in Section 4.9.3 of the 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 Certificate Holder may end a subscription by:
- Allowing a Digital Certificate to expire.
- Revoking a Digital Certificate.

### 4.12. Key escrow and recovery
Issuer CA Private Keys shall not be escrowed. An Issuing CA may offer key archival services to Subscribers to archive Subscriber Private Keys. Any Private Keys that are archived must be held in at least the same of level of security as when the Key Pair was originally created.

Private Keys pertaining to Signature Certificates and SSL/TLS Certificates shall not be archived.

#### 4.12.1. Key escrow and recovery policy and practices
Subscribers and other authorized entities may request recovery of an escrowed Private Key under the following circumstances
- Private Key has been lost or damaged
- The Subscriber is not available or is no longer part of the organization that contracted with the Issuer CA for Private Key escrow,
- A legal or governmental or other competent authority conducting investigation or audit requires access to the Private Key
- Law or governmental regulation mandates key recovery
- If the entity contracting with the Issuer CA for escrow of the Private Key indicates that key recovery is mission critical or mission essential.

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.

### 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 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 utilise 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 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 utilise 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 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 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 for all Issuing CAs of emSign PKI shall be as under:

1. Logs of CA key management activity 30 years
2. CA system logs of certificate management activity 30 years
3. Operating system logs 7 years
4. Physical access system logs 7 years
5. Manual logs of physical access 7 years
6. Video recording of CA facility access 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 authorised 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. Are Generated by the Subscriber in a secure manner either in hardware or software prior to submitting a Digital Certificate request.
2. Differ in its Key generation methods according to the class or type of Digital Certificate requested.
3. For certain types of certificates like Adobe signing, etc, be generated in a medium that meets FIPS 140-1 Level 2+ certification standards and also prevents exporting or duplication of keys.

emSign PKI retains the right to generate Subscriber Key Pairs, based on the type or class of the certificate, in the scenario which needs emSign PKI to generate such key pairs.

### 6.1.2. Private Key Delivery To Certificate Holder

As applicable in most of the cases, if the Subscriber or intended key holder generates the private key, then there is no need to deliver the Private Key. If someone other than the intended key holder is generating the key on behalf of the intended key holder, they must ensure that sufficient security is maintained within the key generation process and any onward issuance process to the Subscriber. At all time, access to private key must be protected by a PIN provided by Subscriber.

### 6.1.3. Public Key Delivery To Certificate Issuer

Public Keys must be delivered to the Issuing CA in a secure and trustworthy manner in a way that it binds the Subscriber's verified identity to the Public Key. The request process must ensure that the public key has not been modified during transit and that the sender possesses the private key corresponding to the transferred public key.

### 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

Key lengths and Key Algorithms within the emSign PKI are determined by Certificate Profiles.

The minimum key size of RSA 3072-bit or ECC NIST P-256 is ensured for:

1. New Root, new Subordinate CA Certificates created after 01-Jan-2021, which issue Code Signing and Timestamping Certificates.
2. New Codesigning and Timestamping Subscriber Certificates created after 01-Jun-2021.

For all other Subscriber certificates, emSign PKI ensures usage of minimum key length of 2,048-bit modulus certificates for RSA / DSA algorithms and minimum key length of 256bit for ECC algorithms. At all times, Issuing CA will ensure that key lengths align with Baseline Requirements and EV guidelines.

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 186-2, which ensures the proper parameters and their quality for Public Keys.

Reasonable techniques are used to validate the suitability of Subscriber Public Keys. Any known weak keys 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)

emSign PKI Root CA permits the "key usage" to sign its Subordinated CAs, the CRLs and other necessary purposes defined in Certificate Profiles section of this CP/CPS. Similarly, the Issuing CAs under emSign PKI permits the usage to sign subscriber certificates and other purposes defined in Certificate Profiles section of this CP/CPS.

Subscriber Keys shall be used for digital signature, key encipherment, data encryption and other purposes defined in 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
CA private keys are not escrowed.

Subscriber Signature Keys shall not be escrowed. However, Issuing CAs under emSign PKI may escrow subscriber encryption keys or other types of keys, in order to provide key recovery.

### 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.

Issuing CAs under emSign PKI may archive copies of Subscriber private keys. Any Private Keys that are archived must be held in at least the same of level of security as when the Key Pair was originally created. Signature keys shall not be archived.

### 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.

Subscriber Private Keys must be protected/activated with a PIN or Password.

### 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 | 397 Days |
| Other Subscriber Certificates | Not Applicable | Not Applicable | 39 Months (or maximum allowed as per applicable guidelines) |
| All other Digital Certificates | No stipulation | No stipulation | No Stipulation (or maximum allowed as per applicable guidelines) |

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 CA shall generate activation data that has sufficient strength to protect its Subscriber Private Keys including methods such as two-factor authentication.

emSign PKI Officers are also required to use strong passwords to further prevent unauthorized access to CA systems.

### 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.

In addition, a dedicated authority Time Stamp Authority (TSA) of emSign is operated to offer Time Stamping Services in accordance to RFC 3161, as well as for Microsoft Authenticode Time Stamps.

# 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 are X.509 version 3 Certificates.

### 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

An object identifier (OID) is a unique number that identifies an object or policy, unambiguously. The *CertificatePolicies* extension are populated with the OID for the policy identifiers defined in this CP/CPS. The criticality field of this extension shall be set to FALSE.

This may contain additional policy identifiers as required by CABF guidelines, Adobe Certificate requirements, etc in order to provide necessary information or assurance of meeting respective requirements.

**Reserved Certificate Policy Identifiers**

emSign Issuing CAs shall optionally use DV, OV and IV related policy IDs of CA Browser Forum baseline requirements, to assert the respective compliance. The subject field shall also contain the values in compliance to DV, OV and IV requirements, as may be applicable.

**Root CA Certificates**

emSign Root CA Certificates shall not contain this extension.

**Subordinate CA Certificates**

The own Subordinate CAs of emSign PKI contains “anyPolicy” identifier (2.5.29.32.0), or explicit policy identifier to confirm the policy compliance.

However, the external Subordinate CAs shall contain only explicit policy identifiers to confirm the policy compliance. It shall not contain “anyPolicy” identifier (2.5.29.32.0).

**Subscriber Certificates**
The Subscriber Certificates issued by Subordinate CAs shall contain one or more policy IDs.

- One of such Policy ID may indicate the CPS policy ID and URL, to confirm the adherence to and compliance of this CP/CPS.
- It shall also contain policy ID indicating compliance to verification, issuance and certificate compliance of respective certificate, as per Appendix A & B. Such Policy ID shall be referred from 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 20 bits of entropy.

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.

### 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. 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

The practices in this CP/CPS are designed to meet or exceed the requirements of generally accepted industry standards and all Issuing CAs of emSign PKI are annually audited for compliance to the latest version of AICPA/CICA WebTrust for Certification Authorities and the Extended Validation Program.

### 8.2. Identity and Qualifications of Assessor

The external audit services are performed by a “Qualified Auditor” that is independent, credible, recognized by AICPA/Webtrust with significant experience in performing Information Security Audits and PKI and Cryptographic technologies. The “Qualified Auditor” is bound by law, government regulation or professional code of ethics and maintains Professional Liability/Errors and Omissions insurance with policy limits of at least USD 1,000,000 in coverage

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 providing access to its certificate databases/repository.

#### 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 vis OCSP.

#### 9.1.4. Fees for Other Services
emSign PKI reserves the right to charge fee for timestamping 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, to the extent specified in this CP/CPS, emSign PKI complies, in all material aspects, with the CP/CPS, and all applicable laws and regulations.

emSign PKI further warrants that:

1. it has taken reasonable steps to verify that the information contained in any Certificate is accurate at the time of issue and are verified in accordance with this CP/CPS and the Baseline requirements and EV guidelines
2. Certificates shall be revoked if emSign believes or is notified that the contents of the Certificate are no longer accurate, or that the key associated with a Certificate has been compromised in any way.

emSign PKI also provides representations and warranties as specified in CA Browser Forum Baseline Requirements.

For EV SSL Certificates, emSign PKI also provides representations and warranties as specified in CA Browser Forum Guidelines for EV SSL.

emSign makes no other warranties, and all warranties, express or implied, statutory or otherwise, are excluded to the greatest extent permissible by applicable law, including without limitation all warranties as to merchantability or fitness for a particular purpose.

### 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 not

using code signing Certificates to sign malicious code or any code that is downloaded without a user's consent, 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 in order 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

emSign PKI accepts notices related to this CP/CPS, in paper or electronic form, at the location and/or email address specified in this CP/CPS. Notices are deemed effective after the sender receives a valid and signed acknowledgment of receipt from emSign PKI. If an acknowledgement of receipt is not received by the sender within seven days, the sender must resend the notice in paper form to the street address specified in this CP/CPS using a courier service that confirms delivery.

emSign PKI will provide any notices required under this CP/CPS by physical or electronic means, unless specifically agreed otherwise.

## 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>1. Validating the request by sending a Random Value to a Domain Contact via email and then receiving a confirming response utilizing the Random Value. (Baseline Requirements Section 3.2.2.4.2)<br>2. 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>3. 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>4. 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>5. 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>6. Validating the request by calling the Domain Contact's phone number and obtaining a response confirming the Applicant's request for validation of the FQDN. (Baseline Requirements Section 3.2.2.4.15)<br>7. 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>8. 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>9. Validating the request by using the ACME HTTP Challenge method in accordance to RFC 8555 (Baseline Requirements Section 3.2.2.4.19)<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, by means of (i) change in agreed information in an URL containing the IP address, OR (ii) IP assignment document of IANA or Regional Internet Registry, OR (iii) |

| | |
|---|---|
| | performing r-DNS lookup resulting in a domain name verified by above procedure. |

### 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>1. Validating the request by sending a Random Value to a Domain Contact via email and then receiving a confirming response utilizing the Random Value. (Baseline Requirements Section 3.2.2.4.2)<br>2. 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>3. 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>4. 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>5. 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>6. Validating the request by calling the Domain Contact's phone number and obtaining a response confirming the Applicant's request for validation of the FQDN. (Baseline Requirements Section 3.2.2.4.15)<br>7. 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>8. 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>9. Validating the request by using the ACME HTTP Challenge method in accordance to RFC 8555 (Baseline Requirements Section 3.2.2.4.19)<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>**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, by means of (i) change in agreed information in an URL containing the IP address, OR (ii) IP assignment document of IANA or Regional Internet Registry, OR (iii) performing r-DNS lookup resulting in a domain name verified by above procedure. |
| **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>1. Validating the request by sending a Random Value to a Domain Contact via email and then receiving a confirming response utilizing the Random Value. (Baseline Requirements Section 3.2.2.4.2)<br>2. 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>3. 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>4. 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>5. 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>6. Validating the request by calling the Domain Contact's phone number and obtaining a response confirming the Applicant's request for validation of the FQDN. (Baseline Requirements Section 3.2.2.4.15)<br>7. 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>8. 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>9. Validating the request by using the ACME HTTP Challenge method in accordance to RFC 8555 (Baseline Requirements Section 3.2.2.4.19) |
| **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 |

## 10.4. Code Signing - OV

| | |
|---|---|
| **Usage/Purpose** | Secure Application / Objects |
| **Individual Verification** | For Individual validated, 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 be 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** | 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 the 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. |
| **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. |

## 10.5. Code Signing - EV

| | |
|---|---|
| **Usage/Purpose** | Secure Application / Objects |
| **Physical Verification** | As per EV requirements, mentioned below. |
| **Individual Verification** | As per EV requirements, mentioned below. |
| **Organization Verification** | As per EV requirements, mentioned below. |
| **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 |
| **Key Storage Verification** | Verification of key storage in Crypto Hardware (FIPS 140-2 Level 2+) by the form of IT audit (attested letter) by the organization, or site visit, or any other form of verification to satisfactorily validate the compliance. |

## 10.6. Device Certificates

| | |
|---|---|
| **Usage/Purpose** | Secure Device Communications. Includes certificates for internal use, Domain Controller certificates, Gateway certificates. |
| **Individual Verification** | The human sponsor of Device certificate shall provide necessary proof of ownership or responsibility or control of the device. This may be provided by any one or many of following options:<br>1. Equipment identification information, along with ownership/purchase information.<br>2. Identification letter from the Organization along with device and sponsor information.<br>3. Any other reasonable or point-in-time modes of verification made by emSign CA, RA or trusted agents. |
| **Organization Verification** | 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 the 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.<br>6. By documentation from the organization that is sufficient to confirm that the individual has an affiliation with the organization named in the Certificate. |
| **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. |

## 10.7. Client Certificates - Class 1

| | |
|---|---|
| **Usage/Purpose** | Email Signing Certificate with / without Identity Information |

| | |
|---|---|
| **Physical Verification** | No Stipulation |
| **Individual Verification** | For Individual validated, 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).<br>6. As an alternate or additional validation, information on identity and address from a pre-verified source, including national ID, government ID, bank or telecom verified information, or any other equivalent trusted source shall be considered. |
| **Organization Verification** | If Organization is to be present in O value of the certificate, Verification of the identity & address of the applicant shall be made using, any one or more the following:<br>1. By documentation from the organization that is sufficient to confirm that the individual has an affiliation with the organization named in the Certificate.<br>2. A Reliable Data Source including the 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>3. A site visit verification by CA or RA.<br>4. An attestation letter that is signed by a practicing/qualified accountant, lawyer, government official, or any other reliable third party.<br>5. 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>6. 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. |
| **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, shall be verified in the form of delivery and acceptance of the email. |

## 10.8. Client Certificates - Class 2

| | |
|---|---|
| **Usage/Purpose** | Document Signing/Encryption/Both<br>For Individual / Organizational Individual / Organization<br>(Document Signer Certificate) |
| **Physical Verification** | Face-to-Face in the form of Physical Verification Letter by Trusted Agents like Accountants, Lawyers, Public Notary, gazetted Officer.<br>OR, Face-to-Face / Video verification by CA / RA |
| **Individual Verification** | For Individual validated, 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).<br>6. As an alternate or additional validation, information on identity and address from a pre-verified source, including national ID, government ID, bank or telecom verified information, or any other equivalent trusted source shall be considered. |
| **Organization Verification** | If Organization is to be present in O value of the certificate, Verification of the identity & address of the applicant shall be made using, any one or more the following:<br>1. By documentation from the organization that is sufficient to confirm that the individual has an affiliation with the organization named in the Certificate.<br>2. A Reliable Data Source including the 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>3. A site visit verification by CA or RA.<br>4. An attestation letter that is signed by a practicing/qualified accountant, lawyer, government official, or any other reliable third party.<br>5. 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>6. 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. |
| **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. |
| **Key Storage Verification** | Verification of key storage in Crypto Hardware (FIPS 140-2 Level 2+ or equivalent Common Criteria or QSCD specifications) by the form of attested letter by the organization, or site visit, or hardware managed/operated by CA or Trusted Third party. Key control with the subscriber may also be verified in such means. |

## 10.9. Client Certificates - Class 3

| | |
|---|---|
| **Usage/Purpose** | Document Signing/Encryption/Both<br>For Individual / Organizational Individual / Organization<br>(Document Signer Certificate) |
| **Physical Verification** | Face-to-Face / Video verification by CA / RA |
| **Individual Verification** | For Individual validated, 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).<br>6. As an alternate or additional validation, information on identity and address |

| | |
|---|---|
| | from a pre-verified source, including national ID, government ID, bank or telecom verified information, or any other equivalent trusted source shall be considered. |
| **Organization Verification** | If Organization is to be present in O value of the certificate, Verification of the identity & address of the applicant shall be made using, any one or more the following:<br>1. By documentation from the organization that is sufficient to confirm that the individual has an affiliation with the organization named in the Certificate.<br>2. A Reliable Data Source including the 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>3. A site visit verification by CA or RA.<br>4. An attestation letter that is signed by a practicing/qualified accountant, lawyer, government official, or any other reliable third party.<br>5. 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>6. 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. |
| **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. |
| **Key Storage Verification** | Verification of key storage in Crypto Hardware (FIPS 140-2 Level 2+ or equivalent Common Criteria or QSCD specifications) by the form of attested letter by the organization, or site visit, or hardware managed/operated by CA or Trusted Third party. Key control with the subscriber may also be verified in such means. |

# 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<br>or<br>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 2048 (OR)<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<br>or<br>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 2048 (OR)<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<br><br>In case the CA issues Code Signing certificates:<br>Code Signing<br><br>In other cases, it will not be present or limits to other 'key usage types' with critical=false. |
| 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<br>or<br>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 2048 (OR)<br>ECC curves NIST P-256, P-384, or P-521 |
| Subject: CommonName | FQDN or Single IP |
| Subject: OrganizationalUnitName | Variable Information |
| 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, Client 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<br>or<br>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 2048 (OR)<br>ECC curves NIST P-256, P-384, or P-521 |
| Subject: CommonName | FQDN or Single IP |
| Subject: OrganizationName | Legal Name of the Organization with allowed variations |
| Subject: OrganizationalUnitName | Variable Information |
| 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, Client 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)<br>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<br>or<br>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 2048 (OR)<br>ECC curves NIST P-256, P-384, or P-521 |
| 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, Client 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<br>CRL HTTP URL = http://crl.emsign.com?<IssuerName>.crl |

### 11.6. Code Signing - 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<br>or<br>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 2048 (OR)<br>ECC curves NIST P-256, P-384, or P-521 |
| Subject: CommonName | Legal Name of the Organization |
| Subject: OrganizationName | Legal Name of the Organization with allowed variations |
| Subject: OrganizationalUnitName | Variable Information (optional) |
| 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) |
| Key Usage | Critical=TRUE<br>Digital Signature |
| Enhanced Key Usage | Critical=FALSE<br>CodeSigning |
| Certificate Policies | Critical=FALSE<br>1. Policy ID=1.3.6.1.4.1.50977.1.2.200 (User Notice, Code Sign Certificate)<br>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 |

### 11.7. Code Signing - 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<br>or<br>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 2048 (OR)<br>ECC curves NIST P-256, P-384, or P-521 |
| Subject: CommonName | Legal Name of the Organization |
| Subject: OrganizationName | Legal Name of the Organization with allowed variations |
| Subject: StreetAddress | Verified Street Address (Optional) |
| Subject: LocalityName | Verified Locality |
| 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 |
| Key Usage | Critical=TRUE<br>Digital Signature |
| Enhanced Key Usage | Critical=FALSE<br>CodeSigning |
| Certificate Policies | Critical=FALSE<br>1. Policy ID=1.3.6.1.4.1.50977.1.2.210 (User Notice, Extended Validated Code Sign Certificate)<br>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 |

## 11.8. Device 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<br>or<br>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 2048 (OR)<br>ECC curves NIST P-256, P-384, or P-521 |
| Subject: CommonName | Subject Common Name |
| Subject: GivenName | First name (Optional if Organization name provided) |
| Subject: Surname | Last name (Optional if Organization name provided) |
| Subject: OrganizationName | Organization name (Optional if Individual name provided) |
| Subject: OrganizationalUnitName | Variable Information (optional) |
| Subject: LocalityName | Verified Locality |
| Subject: StateOrProvinceName | Verified State/Province |
| Subject: CountryName | Verified Country |
| Subject Alternative Name | Critical=FALSE<br>RFC822Name = EmailAddress |
| Key Usage | Critical=TRUE<br>Digital Signature, (in case of RSA algorithm, it shall also contain Key Encipherment, Data Encipherment) |
| Enhanced Key Usage | Critical=FALSE<br>Client Authentication, Secure Email |
| Certificate Policies | Critical=FALSE<br>1. Policy ID=1.3.6.1.4.1.50977.1.2.300 (User Notice, Device Certificate)<br>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 |

### 11.9. Client Certificates - Class 1

| | |
|---|---|
| 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<br>or<br>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 2048 (OR)<br>ECC curves NIST P-256, P-384, or P-521 |
| Subject: CommonName | Common Name |
| Subject: GivenName | First name (Optional if Organization name provided) |
| Subject: Surname | Last name (Optional if Organization name provided) |
| Subject: OrganizationName | Organization name (Optional if Individual name provided) |
| Subject: OrganizationalUnitName | Variable Information (optional) |
| Subject: StreetAddress | Verified Steet address (optional) |
| Subject: LocalityName | Verified Locality (optional) |
| Subject: StateOrProvinceName | Verified State/Province (optional) |
| Subject: CountryName | Verified Country (optional) |
| Subject: PostalCode | Verified Postal Code (optional) |
| Subject: TelephoneNumber | Verified Telephone in SHA256 Hash (optional) |
| Subject: EmailAddress | Verified Email Address |
| Subject Alternative Name | Critical=FALSE<br>RFC822Name = EmailAddress |
| Key Usage | Critical=TRUE<br>digitalSignature, nonRepudiation<br>OR<br>keyEncipherment (in case of RSA)<br>OR<br>digitalSignature, nonRepudiation, keyEncipherment (in case of RSA) |
| Enhanced Key Usage | Critical=FALSE<br>smartcardlogon, clientAuth, emailProtection<br>OR<br>emailProtection<br>OR<br>smartcardlogon, clientAuth, emailProtection |

| | |
|---|---|
| Certificate Policies | Critical=FALSE<br>1. Policy ID=1.3.6.1.4.1.50977.1.2.400 (User Notice, Class 1 Client Certificate)<br>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 |

## 11.10. Client Certificates - Class 2

| | |
|---|---|
| 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<br>or<br>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 2048 (OR)<br>ECC curves NIST P-256, P-384, or P-521 |
| Subject: CommonName | Common Name |
| Subject: GivenName | First name (Optional if Organization name provided) |
| Subject: Surname | Last name (Optional if Organization name provided) |
| Subject: OrganizationName | Organization name (Optional if Individual name provided) |
| Subject: OrganizationalUnitName | Variable Information (optional) |
| Subject: StreetAddress | Verified Steet address (optional) |
| Subject: LocalityName | Verified Locality |
| Subject: StateOrProvinceName | Verified State/Province |
| Subject: CountryName | Verified Country |
| Subject: PostalCode | Verified Postal Code (Optional) |
| Subject: TelephoneNumber | Verified Telephone in SHA256 Hash (Optional) |
| Subject: EmailAddress | Verified Email Address (Optional) |
| Subject Alternative Name | Critical=FALSE<br>RFC822Name = EmailAddress |
| Key Usage | Critical=TRUE<br>digitalSignature, nonRepudiation<br>OR<br>keyEncipherment (in case of RSA) |

| | |
|---|---|
| | OR<br>digitalSignature, nonRepudiation, keyEncipherment (in case of RSA) |
| Enhanced Key Usage | Critical=FALSE<br>smartcardlogon, clientAuth, emailProtection<br>OR<br>emailProtection<br>OR<br>smartcardlogon, clientAuth, emailProtection |
| Certificate Policies | Critical=FALSE<br>1. Policy ID=1.3.6.1.4.1.50977.1.2.410 (User Notice, Class 2 Client Certificate)<br>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 |

### 11.11. Client Certificates - Class 3

| | |
|---|---|
| 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<br>or<br>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 2048 (OR)<br>ECC curves NIST P-256, P-384, or P-521 |
| Subject: CommonName | Common Name |
| Subject: GivenName | First name (Optional if Organization name provided) |
| Subject: Surname | Last name (Optional if Organization name provided) |
| Subject: OrganizationName | Organization name (Optional if Individual name provided) |
| Subject: OrganizationalUnitName | Variable Information (optional) |
| Subject: StreetAddress | Verified Steet address (optional) |
| Subject: LocalityName | Verified Locality |
| Subject: StateOrProvinceName | Verified State/Province |
| Subject: CountryName | Verified Country |

| | |
|---|---|
| Subject: PostalCode | Verified Postal Code (Optional) |
| Subject: TelephoneNumber | Verified Telephone in SHA256 Hash (Optional) |
| Subject: EmailAddress | Verified Email Address (Optional) |
| Subject Alternative Name | Critical=FALSE<br>RFC822Name = EmailAddress |
| Key Usage | Critical=TRUE<br>digitalSignature, nonRepudiation<br>OR<br>keyEncipherment (in case of RSA)<br>OR<br>digitalSignature, nonRepudiation, keyEncipherment (in case of RSA) |
| Enhanced Key Usage | Critical=FALSE<br>smartcardlogon, clientAuth, emailProtection<br>OR<br>emailProtection<br>OR<br>smartcardlogon, clientAuth, emailProtection |
| Certificate Policies | Critical=FALSE<br>1. Policy ID=1.3.6.1.4.1.50977.1.2.420 (User Notice, Class 3 Client Certificate)<br>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 |

# 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 : 10-Nov-2017**

- Base Version

**Version 1.01 : 15-Feb-2018**

- Policy ID update for SSL-DV, SSL-IV, SSL-OV, SSL-EV, CS-Non-EV, CS-EV in Section 1.2
- Inclusion of Internationalised Domain name (IDN) procedure in section 3.1.2
- Key Archival sentence corrections to be in sync between section 4.12 and section 6.2.5
- Root and Issuing CA Information and repository URL update in Section 4.3.1.1 and 4.3.1.2

- CRL update frequency has been updated in line with BR specifications, in section 4.9.7
- Root certificate and usage term reduced from 30 to 25 years, in Section 6.3.2.
- Explicit statement to limit subscriber certificates to 825 days, in Section 6.3.2.
- Security controls related update in section 6.5, 6.6 and 6.7.
- Details about Certificate Policy Extension is elaborated in Section 7.1.4.1 to Section 7.1.4.4.
- Self-audit sample size is explicitly added as part of CP-CPS in section 8.7.
- Domain Verification procedure for IP addresses & wildcard domain in Section 10.1, 10.2 and 10.3 of Appendix A.
- CRL URL correction (special character) in all certificate profiles of Appendix B

**Version 1.02 : 05-Jun-2018**

- In section 1.1, last paragraph, the word 'not' is removed to avoid contradiction with CP/CPS applicability on cross certified CAs under emSign PKI.
- In section 1.6, the definition of 'Reliable Data Source' is amended to include the accuracy of the data source. Accordingly, all references to third party databases in Appendix A is modified to a Reliable Data Source.
- In section 2.1.3, test websites related information is mentioned as part of the repository.
- In section 2.1.3, CP/CPS update frequency is specified.
- In section 4.2.1, definition added to limit the validity of initial identification and authentication for a specified period.
- In section 4.2.4, CAA domain names are explicitly defined.
- In section 4.9.1, more information added towards providing reasons for revocation of subordinate CA.
- In section 4.9.10, more definition is added defining OCSP service.
- In section 5.7.1, information specified about applicability and coverage of audit on Business Continuity Plan.
- In section 6.2.5, the erroneous phrase "shall may" is changed to "may" and now provides clarity of the sentence.
- In section 6.5, information added for multi-factor authentication.
- In Appendix A, the domain verification requirements under SSL-DV, SSL-OV and SSL-EV are updated to incorporate the following changes:
    - As Domain Authorization Document is deprecated and not valid for processing after August 01, 2018 (as per Baseline Requirements), this provision is omitted.
    - The process of DNS based on file-based domain verification with 'an agreed upon change in website' has been explained.
    - The process of 'Any other method' is omitted.
- All certificates profiles in Appendix B is updated for the 'serial number' definition, to include the statement 'and is greater than zero'.
- In Appendix C, Change History section updated to include date against each version.

**Version 1.03: 26-Jun-2018**

- In section 1.1, amended the statement on Baseline requirement version reference to "The latest versions (as on date of this CP/CPS) of the CA/Browser Forum (CABF) requirements…".
- Inserted statement in section 1.5.1 "The changes in CP/CPS are also made based on review of latest Baseline Requirements of CA Browser Forum, as and when published, which may need the policy or practices to be amended."
- In section 4.9.1, amended the subscriber revocation statement to "Issuing CA shall revoke a Digital Certificate of Subscriber within 24 Hours when…".
- In section 6.1.5, the conditional statement is removed, which was referring to 'SHA-1 usage subject to provisions allowed by Baseline Requirements'.

- In section 6.3.2, the statement referring to 'applicability of 825 days with effect from 01-Mar-2018' is removed and made changes to generalize the definition with applicability of 825 days limit to Subscriber Certificates.

**Version 1.04: 09-Oct-2018**

- In Section 10.8 of Appendix A, the "physical verification" requirements under Client Certificates - Class 2, it is now added with option of 'Face-to-Face or Video Verification by CA/RA'. This is already permitted in higher assurance class (Class 3) and hence now is permitted for Class 2 also.
- In Section 10.9 of Appendix A, the "physical verification" requirements under Client Certificates - Class 3, it is now removed with the option to permit 'Face-to-Face or Video Verification by Trusted Agents'. This is permitted in Class 2 only.
- In Section 11.2 of Appendix B (Subordinate CA Certificates), defined the conditional presence of 'Enhanced Key Usage' field. The Subordinate CA Certificates generated prior to this change in the document were containing this field, but the CP/CPS definition was not clear. It is therefore updated.
- In Section 4.2.4, statement to override CAA record with additional authorization is removed.
- In Section 10.1, 10.2 and 10.3 of Appendix A, option 2 under 'domain verification' is omitted, which specified the option of "Relying on publicly available records from the Domain Name Registrar, such as WHOIS or other DNS record information."
- In section 10.6 of Appendix A, the word 'TLS/SSL' is removed. It may also be noted that, Device certificates are never issued with 'server authentication EKU'.
- In section 10.7, 10.8 and 10.9 of Appendix A, the phrase 'any other reliable means' is removed under 'Email Verification'.
- In Section 10.1, 10.2 and 10.3 of Appendix A, the phrase 'OR (iv) any other equivalent procedure, which proves the applicant's right to use the IP' is removed under 'domain verification'.
- In section 3.2.1, added the sentence "emSign PKI shall not generate the key pairs for end-entity certificates that have an EKU extension containing the KeyPurposeIds id-kp-serverAuth or anyExtendedKeyUsage."
- In section 3.2.8, time limit (of 825 days, or as may be applicable) is now specified for re-key request authentication.

**Version 1.05: 25-Oct-2018**

- In Section 10.2, 10.4 and 10.6 of Appendix A, the phrase 'any other reliable means' is removed under 'Email Verification'. These certificates do not contain EKU 'Email Protection'. However, this change is approved to remove the ambiguity in email verification mechanisms.
- New section 1.5.4 introduced for "CPS Approval Procedures". The information was earlier covered under section 1.5.1, and has been separated now to adhere to the structure of RFC 3647.
- New section 3.1.3 and 3.1.4 are inserted, and accordingly existing sections in that position are renumbered to 3.1.5, 3.1.6 and 3.1.7. These new sections are introduced to adhere to the structure of RFC 3647 on 'anonymous or pseudonymous names' and 'Rules for interpreting various name forms'. This is a text addition to CP/CPS and there is no change in practice due to this effect. emSign practices prior to this change adhered to the definition given in these sections.
- In section 1, it promises to adhere to latest CA Browser Forum requirements. For an easy reference, now the statement also contains the URL to CA Browser forum website, which helps the reader to navigate the same.

- Version number has been removed from header of all the pages, and retained in first page of the document, as a single point of reference.

**Version 1.06: 25-Aug-2019**

- In Section 1.2, the Code Signing Policy OID is updated from 2.23.140.1.4 to 2.23.140.1.4.1. This is in line with Microsoft Root Program Requirements. The earlier one was a typo error, and there were no live certificates issued with past OID.
- In Section 7.1.6, the statement included clarifying the Baseline Requirements amendment of not to use underscore in dNSNames of Subject Alternative Name extension.

**Version 1.07: 20-Aug-2020**

- Changes to document structure to fully adhere to RFC 3647 structure. The Mozilla root store policy requires "Effective for versions dated April 1, 2020 or later, CPs and CPSes MUST be structured according to RFC 3647 and MUST include at least every section and subsection defined in RFC 3647". While the content of the document has been suitably merged / changed due to re-ordering of sections, it has been ensured that there is no change in the meaning that impacts the practice of emSign PKI, unless that the change is notified under this version change history log. The changes impacted thereby are as under:
    - Heading text changes across the document in line with RFC, without change in the meaning. (eg: Section 1.1 heading changed from "Objective" to "Overview")
    - Section 2 has been renumbered, and content has been suitably moved within the section. The obligations present in earlier version under this section has been taken out / moved under PKI participants section of Section 1.
    - In Section 3, the old sub section 3.1.7 is merged to 3.1.6.
    - In Section 3, the new sections 3.3 (and its sub-sections) and 3.4 are renumbered from old 3.2.7 to 3.2.10.
    - Old Section 4.2.4 is merged with Section 4.2.1.
    - Old Section 4.3.1.6 renumbered to 4.3.2.
    - Rearrangement of Section 4.8, with relevant new sub-sections.
    - Rearrangement of Section 5.7, with relevant new sub-sections.
    - Inserted Section 6.5.1, and accordingly renumbered subsequent section(s).
    - Rearrangement of Section 7, with relevant new sub-sections.
    - The Sub-sections of Section 9.2 are reorganized.
    - Old Section 9.8.1 is merged with Section 9.8.
    - Table of Contents have been updated according to latest sections and page numbers.
- New section 3.1.6 is added with a statement on specific checks made for EV SSL/TLS with regards to trademarks, etc.
- Typographic error correction in Appendix B (section 11.1 to 11.11). The bracket closure was missing for the text in Certificate Policies explanation.
- In Section 6.3.2, explicit statement added to limit subscriber certificates to 398 days, with effect from 01-Sep-2020. A subsequent version of this document may generalize this requirement and remove the explicit statement.
- In Section 4.9.1, the sentence breaks in a few bullet points had typographic errors which have been corrected.
- The newly inserted sections 7.1.5 to 7.1.9 are provided with relevant policy & practice statement.
- In Section 9.12.2, the sentence has been rephrased to remove the statement on "no change to version numbers", which caused the ambiguity about version numbering.

**Version 1.08: 26-Apr-2021**

- In Section 1.3.5, an exclusive statement added to avoid ambiguous definition on Not permitting Cross Certified / Bridged CA on SSL/TLS & SMIME Certificates.
- In Section 3.2.4, an exclusive statement added to avoid ambiguous definition on Not providing Test/Demonstration Certificates of SSL/TLS Certificates.
- In Section 4.12, an exclusive statement / modification made to avoid ambiguous definition on Not Escrowing Private Keys of SSL/TLS Certificates.
- In Section 4.9.2, additional paragraph added on "Certificate Problem Reporting" to make it easier for third parties to report problems / request revocation of problematic certificates.
- In Section 6.3.2, separate statement provided earlier to limit subscriber certificates to 398 days has been generalized without date condition, as all certificates complying hereafter are issued only with latest time limit.
- In Section 10.1, 10.2 and 10.3 of Appendix A, Domain Verification Methods has been redrafted for the following changes:
    - Providing Baseline Requirements Section reference numbers for each method.
    - Adopting new methods of validation in accordance to Baseline Requirements Section numbers 3.2.2.4.13, 3.2.2.4.14, 3.2.2.4.15, 3.2.2.4.16, 3.2.2.4.17, and 3.2.2.4.19.
- In Section 10.3 of Appendix A, the erroneous reference to IP Address verification is removed.

**Version 1.09: 26-Jul-2021**

- In Section 4.9.12, it has been fully modified to cover the details of problem reporting on key compromise.
- In Section 6.1.5, the explicit key size limits for code signing and time stamping certificates are incorporated.