Verasys Technologies Pvt. Ltd.
CERTIFICATION PRACTICE STATEMENT

VERSION 1.0

Date of Publication:

Verasys Technologies Pvt. Ltd.
2nd Floor, Bhavna Building, V.S, Marg,
Prabhadevi, Mumbai -400025

Phone: +91 43156000
Email: admin@vsign.in
Website: www.vsign.in

CERTIFICATION PRACTICE STATEMENT

Document Name	Verasys CPS
Release	Version 1.0
Status	
Issue Date	

AMENDMENT CERTIFICATE

RELEASE				
Version	**Description**	**Approved by**	**Approval Date**	**CCA Approved Date**

DEFINITIONS

The following definitions are to be used while reading this CPS. The following terms bear the meanings assigned to them hereunder and such definitions are applicable to both the singular and plural forms of such terms:

- “CA” refers to certification and trust services offered by Verasys Technologies Pvt. Ltd. which is licensed by Controller of Certifying Authorities (CCA), Govt. of India under Information Technology Act 2000
- “Act” means Information Technology Act, 2000.
- “Digital Certificate Applicant” or “User” means a person that has applied for, but has not yet been issued a digital certificate by CA.
- “Auditor” means any internationally accredited computer security professional or agency appointed by Certifying Authority (CA) and recognized by Controller of Certifying Authorities (CCA) for conducting audit of operation of CA.
- “Controller” means Controller of Certifying Authorities appointed under subsection (1) of Section 17 of the Act.
- ‘ESP’ means the e-Sign Service Provider, Verasys.
- “CPS” means the CA’s Certification Practice Statement.
  "Digital signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3 of the IT Act;
  “Private Key” means the key of a key pair used to create a digital signature.
- “Registration Authority” or “RA” is an entity engaged by CA to collect DSC Application Forms (along with supporting documents) and to facilitate verification of applicant’s credentials
- “Subscriber” means a person in whose name the Digital Signature Certificate is issued by CA

Note: Words and expressions used herein and not defined have the meaning respectively assigned to them in the IT Act.

LIST OF ACRONYMS AND ABBREVIATIONS USED IN THIS CPS

Acronym	Term
CA	Certifying Authority
CCA	Controller Of Certifying Authorities
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DN	Distinguished Name
ESP	ESign Service Provider
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol With SSL
IETF	Internet Engineering Task Force
ITU	International Telecommunications Union
OID	Object Identifier
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standard
PKI	Public Key Infrastructure
RA	Registration Authority
RCAI	Root Certifying Authority Of India
RFC	Request For Comment
SSL	Secure Sockets Layer
URL	Uniform Resource Locator

Table of Contents

1. INTRODUCTION

This document states the practices that CA employs in providing Digital Signature Certificates and related services that include, but are not limited to, the digital certificate lifecycle management process of Certificate Application, Approval, Issuance, Revocation and Renewal. The CPS is the principal practice statement governing the services provided by CA and establishes conformance to the requirements of the Indian Information Technology Act – 2000 (IT Act).

1.1 SERVICES OFFERED

The following services are being offered by the CA:

1.1.1 CERTIFICATE SERVICES

The CA issues Certificates as per India CP. viz. Class 1, Class 2, Class 3, AADHAAR e-KYC OTP and AADHAAR e-KYC Biometric. Special types of Certificates- System Certificate, Document Signer, Encryption etc. These would be issued to Individuals or individual representing organizations based on the validation requirements specified by Identity Verification Guidelines of the CCA.

1.1.2 OCSP (Online Certificate Status Protocol) Validation Services

OCSP Validation Services provided by the CA using the OCSP technology facilitates accurate, scalable and real time status of Digital Certificates.

1.1.3 ESIGN SERVICES

CA is empanelled as ESP to offers eSign online Digital Signature Service as per the e-authentication guidelines of CCA published on the CCA website, http://www.cca.gov.in/cca/sites/default/files/files/ESIGN/CCA-EAUTH.pdf

1.2 CERTIFYING AUTHORITY

The term “Certifying Authority” or CA as used in this CPS, refers to Verasys Technologies Pvt. Ltd. as the entity that holds the CA license from the Controller of Certifying Authorities (CCA), Govt. of India.

1.3 ROLE OF CPS AND OTHER DOCUMENTS

This CPS explains specific practices of the CA with respect to issuance and management of the certificates vis-à-vis the policies specified in the corresponding CP. It covers the following areas:

- Appropriate application for various classes of certificates.
- Assurance level associated with each class.
- Obligation of CA, Legal matters that are covered in subscriber agreements and relying party agreements.
- Audit and related security and practices

- Methods used for identification and verification of subscriber for various certificates.
- Operational procedures for certificate applications, issuance, acceptance, revocation, and renewal.
- Physical, personnel, cryptographic private key and logical security controls
- Operational security procedures for audit logging, records retention and disaster recovery.
- Certificate and certificate revocation list (CRL) content
- Administration of CPS, including methods of updating it

1.4 COMPLIANCE WITH IT ACT 2000

The practices specified in this certification practice statement (CPS) have been designed to meet the requirements of Indian IT Act 2000, the interoperability guidelines (IOG) and the Identity Verification Guidelines (IVG) issued by CCA and published on CCA website, www.cca.gov.in

1.5 POLICY OVERVIEW

The CA issues certificates as per the classes defined by the India CP published by CCA on its website, http://www.cca.gov.in/cca/sites/default/files/files/Guidelines/CCA-CP.pdf

1.6 IDENTIFICATION

This CPS is called Verasys Certification Practice Statement. The contact details are mentioned in section 1.8 of this CPS.

Serial No.	Product	OID
1	Verasys CA	2.16.356.100.1.x
2	Verasys CA CPS	2.16.356.100.1.x.2

1.7 APPLICABILITY

The scope of this CPS is applicable to Verasys CA, entities that functions as RAs, entities that are certified as Subscriber(s) and entities that rely on the certificates i.e. relying party.

1.7.1 Certifying Authority and Hierarchy

The term Certifying Authority (“CA”) is an umbrella term that refers to all entities signing certificates within CA.

1.7.2 Registration Authorities

Registration authority (RA) is an entity engaged by CA to collect DSC Application Forms (along with supporting documents) and to facilitate verification of subscriber credentials. RA interacts with the CA and submit the applicant’s request for certificate issuance to CA. RA should have legally enforceable agreement with CA.

1.7.3 End Entities

The end entities / end users of the Digital Certificates in business and other communication applications are:

Applicants - An applicant is a person that has applied for, but has not yet been issued a Digital Certificate.

Subscribers - A Subscriber is a person that has been issued a Digital Signature Certificate.

Relying parties – A Relying Party is a person, entity, or organization that relies on or uses Digital Certificates and/or any other information provided in the repository to verify the identity and public key of a subscriber and/or use such public key to send or receive encrypted communications to or from a subscriber.

1.8 CONTACT DETAILS

This CPS is administered by CA and is revised with the approval of CCA from time to time as and when needed by the CA with sufficient notification to the end users.

The contact details of the CA are:

Verasys Technologies Pvt. Ltd..,
21, 2nd floor, Bhavna Building,
V. S. Marg, Prabhadevi,
Mumbai – 400025,India
Phone: +91 43156000
Email: info@vsign.in
Website: www.vsign.in

2. GENERAL PROVISIONS

This section sets forth general provisions of obligations and defines and allocates specific responsibilities among various parties participating in the Public Key Infrastructure established by this CPS.

2.1 OBLIGATIONS

2.1.1 CA Obligations

The CPS specifies obligations for the CA throughout this document.

Broadly the CA has the following obligations:

- Acting in accordance with policies and procedures designed to safeguard the certificate management process (including certificate issuance, suspension, activation, revocation, and audit trails) and to protect the CA private key from compromise.
- Issuing a Digital Signature Certificate to the applicants that have been verified by the CA
- Physical & Logical Security of Verasys CA
- Assurance level associated with each class
- Audit & related security & practices reviews
- Revocation of the Digital Signature Certificate upon the request from the subscriber as per the terms and conditions in CPS.
- Issuing and publishing the CRL regularly as mentioned in this CPS

- Maintaining this CPS with revisions as and when changes are made.
- Creating and maintaining an accurate audit trail of all CA operations& records retention.
- Ensure that all aspects of CA services, operations and infrastructure related to certificate issuance are performed in accordance with the requirements, representations and warranties of this CPS.
- Submission of certificate/CRL issued to the CCA
- Legal matters relating to Subscriber agreements and Relying Party Agreements

2.1.2 RA obligations

RA facilitate verification of subscriber credentials, entering subscriber information and verifies correctness and securely communicating requests to and responses from the CA. RA Collect the relevant documents for the corresponding class of certificates from applicant as mentioned in the Identity Verification Guidelines of the CCA.

2.1.3 Subscriber Obligations

The Subscriber has the following obligations:

- Providing the correct information without any errors, omissions or misrepresentations in the application.
- Generating the key pair (except in case of Encryption Certificate) on a secure medium as specified in this CPS.
- Using the certificate only for the authorized purposes as specified in this CPS.
- Protecting the private key in a secure medium.
- Demonstrate acceptance of the Digital Certificate generated by CA when all information contained in the Digital Certificate is as applied for and validated as true.
- Notifying immediately any change in the information included in the Subscriber's Digital Signature Certificate that makes the information in the Certificate inaccurate or misleading.
- Notifying immediately any suspected or actual compromise of the Subscriber's private key.
- Terminating the use of the Certificate if the information in the Certificate is found to be inaccurate and misleading.
- Additional obligations as mentioned in the Subscriber agreement.
- Safeguarding of the private key.

2.1.4 Relying Party Obligations

Relying Party obligations apply to Relying Parties by way of the CA's Relying Party Agreement.

- Relying Parties must independently assess the appropriateness of the use of a Digital Certificate for any given purpose.
- Relying parties must use appropriate utilities or tools to perform digital signature verification or other operations. The utilities/ tools should be able to identify the certificate chain and verifying the digital signature on all certificates in the chain and only on successful verification should rely on the certificate.
- Relying party must consent to the Relying Party Agreement before proceeding with relying on certificates.
- The relying parties have to determine the appropriateness of the use of a certificate.

2.1.5 Repository obligations

The CA publishes the Certificates issued by it in its repository which are updated whenever there is any change in any of them. The CRL is published and updated in Repository, once every business working day and whenever a certificate is revoked

2.2 LIABILITY

2.2.1 Certifying Authority Liability

The CA disclaims any liability that may arise from use of any certificate issued by the CA
The CA has no responsibility for any delays or damages due to force majeure such as warfare or a natural disaster or reasons beyond provisions of the IT Act, the rule and regulations.

The warranties, disclaimers of warranty, and limitations of liability among CA's Intermediaries and their respective customers are set forth and governed by the agreements among them.

2.2.1.1 Disclaimers of Warranties

To the extent permitted by applicable law, the subscriber agreement and relying party agreement disclaim any warranty of merchantability or fitness for a particular purpose.

2.2.1.2 Limitations of liability

The CA shall not be liable in any way, for any inaccuracy, error, delay or omission in the issuance or validation of any Digital Signature Certificate, or for non-performance including suspension, activation and revocation or the failure to suspend, activate or revoke, due to any cause beyond the CA reasonable control.

The CA shall have no liability to a Subscriber, arising from or relating to issuance, administration or use of a Digital Signature Certificate under the CA that is issued or continued in force in reliance upon or as a result of any false or misleading information provided by the Subscriber or any material omission in any information provided by the Subscriber in connection with their application for Digital Signature Certificate under the CA or otherwise.

The CA will not be responsible for failures that may take place during the Aadhaar based authentication and eSign process, including but not limited to, failures as a result of, false reject, network, or connectivity failure, device failure, software failure, OTP not received by end-user, possible down time or rejection of Aadhaar authentication by UIDAI due to technical problem of CIDR.

Unless otherwise specifically stated in this CPS, CA including its affiliates, shareholders, officers, directors, employees, agents, representatives etc. is not responsible and liable for any direct, indirect, exemplary, special, punitive, incidental, and consequential losses, damages, claims, liabilities including loss of data, revenue, profits, business and for any claims of Subscribers or other third parties including Relying parties except as mentioned in section 2.2.1.3

2.2.1.3 CA Liability Caps

CA's liability is as per the IT Act, other governing Indian laws and Agreement. It includes the following caps limiting CA's damages concerning a specific Certificate.

Class of Certificate	Liability Cap per Certificate (Rs.)
Class 1	1000
Class 2	1000
Class 3	5000

With respect to Class eKYC OTP / Biometric (eSign services) , CA's liability under any circumstances/situations shall not exceed the net surplus generated by it out of the particular transaction resulting into alleged loss to claimant user of CA service. Net Surplus will be the positive balance amount arrived at after deducting total expenditure from the fees collected in respect of the particular transaction.

2.2.1.4 Force Majeure

To the extent permitted by applicable law, CA's subscriber agreements, Registration Authority agreement and Relying Party agreements include, and other subscriber agreements are subject to the conditions of force majeure clause. CA, Registration Authority and Relying party are not responsible for any delay/default/inadequate performance/ non-performance / failure in its performance under the Subscribers Agreement, Relying Party Agreement or Registration Authority Agreement if the same is caused by extraordinary weather conditions or other natural catastrophes, war, riots, strikes, lockouts or other industrial disturbances or acts of any governmental agencies.

2.3 FINANCIAL RESPONSIBILITY

2.3.1 Indemnification by Subscribers

To the extent permitted by applicable law, subscriber agreement requires Subscribers to indemnify CA for:

- False and misrepresentation of fact by the subscriber on the subscriber's certificate application,
- Suppression of a material fact on the certificate application, if the omission was made negligently or with intent to deceive any party,
- The subscriber's failure to protect the subscriber's private key, to use a trustworthy system, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the subscriber's private key, or
- The subscriber's use of a name (including without limitation within a common name, domain name, or e-mail address) that infringes upon the Intellectual Property Rights of a third party.

2.3.2 Indemnification by relying parties

To the extent permitted by applicable law, relying party agreement requires, relying parties to indemnify CA for:

- The relying party's failure to perform the obligations of a relying party as outlined in this section 2.1.4 of this CPS. The relying party's reliance on a certificate that is not reasonable under the circumstances, or
- The relying party's failure to check the status of such certificate to determine if the certificate is expired or revoked.

2.4 INTERPRETATION AND ENFORCEMENT

In the event of any conflict between the provisions of the IT Act and Rules and Guidelines issued there under and the provisions of the CPS, the provisions of such Act, Rules and Guidelines will prevail over the provisions of the CPS, except where the provision in such Act, Rules and Guidelines provide that the CPS can have provisions which are inconsistent with the provisions of such Act, Rules and Guidelines and such inconsistent provisions are made in the CPS.

2.4.1 Governing Law

The laws of India and more particularly the Information Technology Act, 2000, The Information Technology (Certifying Authorities) Rules, 2000 and Information Technology (Certifying Authority) Regulations, 2001, and the guidelines issued and clarifications made from time to time by the Controller of Certifying Authorities, Ministry of Electronics and Information Technology governs the construction, validity, enforceability and performance of this CPS.

2.4.2 Severability, Survival, Merger, Notice

To the extent permitted by applicable law, the CA's subscriber agreements and relying party agreements contain, and other subscriber agreements contains, severability, survival, merger, and notice clauses. A severability clause in an agreement prevents any determination of the invalidity or unenforceability of a clause in the agreement from impairing the remainder of the agreement. A survival clause specifies the provisions of an agreement that continue in effect despite the termination or expiration of the agreement. A merger clause states that all understandings concerning the subject matter of an agreement are incorporated in the agreement. A notice clause in an agreement sets forth how the parties are to provide notices to each other.

2.4.3 Dispute Resolution Procedures

To the extent permitted by applicable law, the CA subscriber agreements and relying party agreements contain a dispute resolution clause.

2.4.4 Role of the CCA

Under the IT Act 2000, the Controller of Certifying Authorities (CCA) is authorized to resolve disputes arising out of CA services.

2.5 FEES

The fees for various types of Digital Certificates are available on the CA's website at www.vsign.in and are updated from time to time.

CA is entitled to charge subscribers fees for management and issuance of certificates. The current fees for various types of certificates are listed in the website.

CA updates and make the CRL accessible free of charge to relying parties (www.vsign.in/repository/crl). However any OCSP validation services would be charged based on the specific agreement between the parties.

CA provides access to policy information documents such as CPS/ CP free of charge (www.vsign.in/repository/cps). This is however limited to the specific purpose of viewing. Any reproduction, derivative work creation, modification etc, would be subject to license agreement with the CA.

The refund policy and other payments terms would be governed as per the terms in the subscriber agreement. The terms and fee structure are subject to change at the sole discretion of the CA.

2.6 PUBLICATION AND REPOSITORY

The CA maintains the repository to store information relevant to the operations of the CA's services. This includes the Digital Certificate trust chain of the CA. All the information and modifications are published in the repository to provide access to the updated information. This information is subject to changes and any such change are published in the repository as detailed in other relevant sections of this CPS.

2.6.1 Publication of CA Information

The following information is published in the repository and is publically available,

- Certification Practice Statement.
- The Digital Signature Certificates issued by the CA
- The public keys corresponding to private keys of the CA.
- The CRL for the revoked or suspended Certificates.
- Fee structures of the various services.
- Search facility for Digital Signature Certificates.
- Subscriber agreement & Relying party agreement

2.6.2 Frequency of Publication

The CA publishes the CPS and its CA Certificate in its repository which is updated whenever there is any change in them. The CRLs is published and updated in the repository, once every business working day or whenever a certificate is revoked.

2.6.3 Repositories

The repositories are maintained by CA and are accessible to the authorized personnel. The repositories are a collection of databases for storing and retrieving certificates and other information related to certificates and contain certificates, CRLs, current and prior versions of this CPS and other information as prescribed by CA from time to time.

2.7 COMPLIANCE AUDIT

Compliance audits conducted by a CCA empanelled auditor is as per the specifications of the IT Act 2000 and its associated rules, regulations and amendments.

2.7.1 Frequency of Audit

Compliance audits are performed on an annual basis. Internal audits are performed on a half-yearly basis.

2.7.2 Identity of Auditor

The audit is performed by a CCA empanelled auditor.

2.7.3 Auditors relationship to audited party

The Audit firm would be independent of CA and will not have other business dealings with the CA.

2.7.4 Topics covered by Audit

The scope of audit is as per IT Act 2000 and its associated rules and regulations and includes physical controls, environmental controls, key management, personnel, security compliance, CPS and its adherence, regulation prescribed by controller and any other items deemed necessary by the CA.

2.7.5 Actions taken as result of deficiency

Significant exceptions and non-conformance as reported by the auditors are reviewed by the CA. If the exceptions are deemed to provide immediate risk to the security of the system corrective actions is planned and implemented by the CA within a reasonable commercially viable time frame.

2.7.6 Communication of results

Results of the compliance audit of CA operations is submitted to the CCA and any other parties as per CCA orders.

2.8 CONFIDENTIALITY AND PRIVACY

2.8.1 Types of Information to be kept Confidential and Private

The following records of Subscribers are kept confidential and private ("Confidential/Private Information"):

- Information pertaining to digital certificate applications, whether approved or rejected is kept confidential. Digital Certificate information collected from the subscriber as part of registration and verification records but not included in the information contained in the Digital Certificate are kept confidential.
- Transactional records (both full records and the audit trail of transactions).
- Audit results and information are considered sensitive and are not disclosed to anyone other than CA authorized and trusted personnel and the CCA. This information is not used for any purpose other than audit purposes or where required by law.
- Audit trail records created or retained by CA.

- Contingency planning and disaster recovery plans.
- Security measures controlling the operations of CA's hardware and software and the administration of Certificate services and designated enrolment services.
- Any other records / data / information mandated to be kept confidential and private by the IT Act 2000, its associated rules and regulations

2.8.2 Disclosure of Certificate Revocation/Suspension Information

The CA publishes the Digital Certificate revocation / suspension details of all the Digital Certificates revoked or suspended by the CA. The reasons for the revocation is disclosed only to the Subscriber or to the agencies having the power to compel the disclosure.

2.8.3 Release to Law Enforcement Officials

The CA shall release the confidential information to law enforcement officials in compliance to an order from a Court or Tribunal as per the provisions of IT ACT.

3. IDENTIFICATION AND AUTHENTICATION

3.1 INITIAL REGISTRATION

The initial registration process by the applicant includes the submission of the online application or an offline application for issuing Digital Certificate along with the supporting documents by the applicant and the applicable verification by the CA/RA of the information submitted by the applicant.

3.1.1 Authentication of Organization Identity

The CA is responsible for verifying the identity of the organization as per the Identity Verification Guidelines of the CCA for the organization certificates. For the CA to establish the identity of the organization, the organization submitting the application must submit proof of ownership of the name, such as:

- Company Registration
- Society Registration
- Memorandum of Understanding
- Article of Association
- Documents pertaining to Shops & Establishments Act
- Bank details for a Current Account
- Partnership Deed / Agreement etc.

In addition, proof that the person representing the organization is duly authorized to do so, is also required. The details of the documents to be verified are as per the Identity Verification guidelines of CCA published on the website of CCA.
http://www.cca.gov.in/cca/sites/default/files/files/Guidelines/CCA-IVG.pdf

3.1.2 Authentication of Individual Identity

The process of identification of a subscriber differs based on the class of certificate that the subscriber is applying for and may include any or all of the following: verification of e-mail, face to face authentication and verification of stipulated documents, real time video verification & mobile number verification. An application for a certificate must be made (i) personally by an individual or, (ii) by the duly authorized representative of the organization in the case of Organization certificates. The details of the documents to be verified are as per the identity verification guidelines of CCA published on the website of CCA
http://www.cca.gov.in/cca/sites/default/files/files/Guidelines/CCA-IVG.pdf

3.1.3 Verification documents required

The CA issues certificates to Individuals and Authorized Individuals of Organizations for Class1, Class 2 and Class 3 certificates as per India CP as mentioned in Section 2.2.1.4

The document requirement for certificates mentioned above is governed by Identity Verification Guidelines issued by CCA and published on the website of CCA, http://www.cca.gov.in/cca/sites/default/files/files/Guidelines/CCA-IVG.pdf

3.2 REKEY AND RENEWAL PROCESS

Prior to the expiry of the existing certificate, if there is a compromise with the existing certificate then the subscriber has to apply for a new certificate. In this case the subscriber has to go through the entire process of obtaining a certificate as mentioned earlier in this CPS. This process is called REKEY as the subscriber is allocated new set of keys to continue using the CA's service.

3.3 REKEY AFTER REVOCATION

The CA does not renew the digital certificates that have been revoked for any subscriber. The subscriber, who further wants to use the Digital Certification Services of the CA, has to apply for a new digital certificate and complete the registration process again as specified in this CPS.

3.4 REVOCATION REQUEST

Prior to revocation of any certificate, CA verifies that the revocation has in fact been requested by the certificate's subscriber. The certificate can also be revoked by CA if it has sufficient reason to believe that the certificate has been obtained by providing fraudulent information

4. OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

The initial registration process by the applicant includes the submission of the application for issuing Digital Certificate along with the supporting documents.

For certificates, all end-user certificate applicants undergo an enrollment process consisting of:

- Completing and submitting a certificate application form and providing the required information,
- Generating a key pair.
- Delivering his/ her, or its public key to CA
- Demonstrating to CA that the certificate applicant has possession of the private key corresponding to the public key delivered to CA.
- Manifesting assent to the relevant subscriber agreement.

Certificate Applications submitted to the RA or CA for processing could result in either approval or denial.

4.2 CERTIFICATE ISSUANCE

After a certificate applicant submits a certificate application, the CA validates or refutes the information in the certificate application. Upon successful performance of all required authentication procedures based on various classes of certificates, the RA receiving the certificate application forwards the certificate application to CA for approval. The applicant's request for certificate issuance is reviewed by a CA trusted person which may result in approval or denial of certificate.

A certificate is created and issued based on the information in the certificate application following the approval of a certificate application by CA.

4.3 CERTIFICATE ACCEPTANCE

A notification is sent to subscriber that the certificate is ready to be downloaded. Along with this notification, a PIN / passcode or authentication number to download certificate is sent to subscriber. Certificates are made available to subscribers by allowing them to download them from CA web site, www.vsign.in . Downloading the certificate constitutes the subscriber's acceptance of the certificate. In case there is a failure during the download process and the certificates are not sent by the CA server, the subscriber is allowed to download again. In case the subscriber claims that he has not been able to download the certificate though the server has sent it, the subscriber sends in a new certificate application request and the old certificate is revoked. The charges are at the discretion of the CA.

4.4 CERTIFICATE SUSPENSION AND REVOCATION

4.4.1 Circumstances for Revocation

CA revokes a subscriber certificate if:

- The subscriber requests revocation of the certificate, or
- The information within the certificate is incorrect or has changed,
- In the case of organizational certificates, the subscriber's organization name changes or the relationship between the organization and the organizational representative has terminated,
- The subscriber has materially breached a material obligation, representation, or warranty under the applicable Subscriber Agreement,
- The Subscriber Agreement with the subscriber has been terminated,
- CA has reason to believe that a material fact in the certificate application is false or the information presented at the time of certificate creation is incorrect or has changed.

4.4.2 Who Can Request Revocation

The parties permitted to request revocation of a certificate are the individual subscribers for their own individual certificate, a duly authorized representative of the organization for organizational certificates. CA can initiate revocation of a subscriber's certificate.

4.4.3 Procedure for Revocation Request

Subscriber or duly authorized representative, as applicable, requesting revocation is required to communicate the request to CA. The request is online through a challenge phrase or in an offline mode through signed revocation request. Upon receiving a valid revocation request CA promptly revokes the certificate, publish the CRL and notify the subscriber about the certificate revocation.

4.4.4 Revocation Request Grace Period

Revocation requests are to be verified on receipt and action taken within 2 working days. .

4.4.5 Certificate Suspension

CA offer suspension services for subscriber certificates upon subscriber's request.
Subscriber can electronically send a suspension request to CA from CA's website, www.vsign.in. The certificate is suspended upon successful validation of this request.

4.4.6 CRL Issuance Frequency

CA publishes CRLs showing the revocation of certificates and offers status checking services through CA's repository. CA updates and publishes the CRLs for subscriber Certificates at least every 24 hours, even if no changes to the CRLs have been made. The CRL is published immediately in case a certificate is revoked.

4.4.7 Certificate Revocation List Checking Requirements

Relying Parties must check the status of certificates on which they wish to rely by referring to the most recent CRL. The CRL is available in CA's repository www.vsign.in/repository/crl.

4.4.8 On-Line Revocation/Status Checking Availability

In addition to publishing the CRL, CA also provides a web query mechanism to check the status of CRL in the repository. In addition CA also provides OCSP service to relying parties who require such services. This is a charged service and the exact mode will be communicated with the relying parties.

4.5 SECURITY AUDIT PROCEDURES

4.5.1 Types of Events Recorded

CA manually or automatically logs the following significant events:

SECURITY AUDIT

- Any changes to the Audit parameters, e.g., audit frequency, type of event audited
- Any attempt to delete or modify the Audit logs

IDENTITY-PROOFING

- Successful and unsuccessful attempts to assume a role
- The value of maximum number of authentication attempts is changed
- The number of unsuccessful authentication attempts exceeds the maximum authentication attempts during user login
- An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts
- An Administrator changes the type of authenticator, e.g., from a password to a biometric

ROOT KEY GENERATION

- Whenever the Component generates a key (not mandatory for single session or one-time use symmetric keys)

ROOT CA CREATION

- All CA creation parameters including trusted roles

LICENCED CA CERTIFICATE SIGINING

- All certificate PKCS#10 requests signing

CERTIFICATE REVOCATION

- All certificate revocation requests

ACCOUNT ADMINISTRATION

- Roles and users are added or deleted
- The access control privileges of a user account or a role are modified

CERTIFICATE PROFILE MANAGEMENT

- All changes to the certificate profile

REVOCATION PROFILE MANAGEMENT

- All changes to the revocation profile

CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT

- All changes to the certificate revocation list profile

MISCELLANEOUS

- Creation of a Trusted Role
- Designation of personnel for multiparty control
- Installation of the Operating System
- Installation of the PKI Application
- Installation of hardware cryptographic modules
- Removal of hardware cryptographic modules
- Destruction of cryptographic modules
- Logon attempts to PKI Application
- Receipt of hardware / software
- Attempts to set passwords

- Attempts to modify passwords
- Restoration from back up of the internal CA database
- Posting of any material to a PKI Repository
- Access to the internal CA database
- All certificate compromise notification requests

CONFIGURATION CHANGES
- Hardware
- Software
- Operating System
- Patches
- Security Profiles

PHYSICAL ACCESS / SITE SECURITY
- Personnel Access to room housing Components
- Access to the Components
- Known or suspected violations of physical security

ANOMALIES
- Software error conditions
- Software check integrity failures
- Equipment failure
- Electrical power outages
- Uninterruptible Power Supply (UPS) failure

CA AND SUBSCRIBER CERTIFICATE LIFE CYCLE MANAGEMENT EVENTS
- Certificate Applications, renewal, rekey, and revocation
- Successful or unsuccessful processing of requests
- Generation and issuance of Certificates and CRLs.

RAs LOG CERTIFICATE APPLICATION INFORMATION
- Kind of identification document(s) presented by the certificate applicant
- Record of unique identification data, numbers, or a combination thereof (e.g. Certificate Applicant's driver license number) of identification documents, if applicable
- Storage location of copies of applications and identification documents
- Identity of entity accepting the application
- Method used to validate identification documents, if any
- Name of submitting RA

4.5.2 Frequency of Processing Log

Audit logs are examined for key security and operational events on at least a weekly basis. In addition, CA reviews its audit logs as required in the event of any suspicious or unusual activity based on irregularities and incidents within CA and RA systems.

The processing of audit logs includes a review of the audit logs and recording of significant events in an audit log summary. It includes a verification that the log has not been tampered

with, a brief inspection of all log entries, and a detailed investigation of any irregularities in the logs. Actions taken based on audit log reviews is recorded.

4.5.3 Retention Period for Audit Log

Audit logs are retained onsite at least two (2) months after processing and thereafter archived

4.5.4 Protection of Audit Log

Only authorized CA personnel have access to view and process audit log files. Electronic and manual audit log files are protected from unauthorized viewing, modification, deletion, or other tampering through the use of physical and logical access controls.

4.5.5 Audit Log Backup Procedures

Incremental backups of audit logs on physical removable media are created daily and full backups weekly. The backup media is stored in a safe storage. In addition, audit logs and audit summaries are backed up or copied if in manual form

4.5.6 Audit Collection System

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

4.5.7 Notification to Event-Causing Subject

Where an event is logged by the audit collection system, no notice is required to be given to the individual, organization, device, or application that caused the event.

4.5.8 Vulnerability Assessments

Events in the audit log are recorded, in part, to monitor system vulnerabilities. A vulnerability assessment is performed, reviewed, and revised following an examination of these monitored events.

4.6 RECORDS ARCHIVAL

4.6.1 Types of Events Recorded

CA retains an archive of information and actions that are material to each certificate application and to the creation, Issuance, revocation, expiration, and renewal of each certificate issued by the CA. These records include all relevant evidence regarding:

- The identity of the subscriber named in each certificate including documentary evidence in support of the certificate application,
- The identity of persons requesting certificate revocation
- Other facts represented in the certificate, and
- Certain foreseeable material facts related to issuing certificates including, but not limited to, information relevant to successful completion of a compliance audit
- Records are kept in the form of either computer-based messages and paper-based documents. It is ensured that the indexing, storage, preservation, and reproduction of records are accurate and complete.

4.6.2 Retention Period for Archive

Records associated with certificates are archived for a period of 7 years.

4.6.3 Protection of Archive

CA protects its archived records so that only authorized persons can access the archived data. CA protects the archive against unauthorized viewing, modification, deletion, or other tampering, by storage within a trustworthy system. The media holding the archive data and the systems required to process the archive data are maintained to ensure that the archive data can be accessed for the time period

4.6.4 Archive Backup Procedures

CA creates back-up copies of archives compiled as and when the archives are created. Backup copies of the archive and copies of paper-based records are maintained in an off-site disaster recovery/ warehouse facility. CA has implemented a process to scan and digitize the physical documents to ensure tracking and easy retrieval.

4.6.5 Requirements for Time-Stamping Of Records

Certificates, CRLs, other revocation databases and usage entries contain time and date information provided by System time, which is synchronized with IST

4.6.6 Archive Collection System

The archive collection system is internal to the CA.

4.6.7 Procedures to Obtain and Verify Archive Information

Only CA trusted personnel are permitted to access the archived data. Additionally, the archive information may be made available to the CCA upon request.

4.7 KEY CHANGEOVER

CA keys are changed periodically as stipulated by the IT Act and the key change are processed as per key generation specified in this CPS. CA provides reasonable notice to the subscriber's relying parties of any change to a new key pair used by CA to sign digital certificates under its trust hierarchy. There is no key change of the subscriber's Certificate unless in the case of a compromise.

The subscribers is issued digital certificate for a specified period of time. The subscribers generates a new private-public key pair and submit the public key along with the new application to the corresponding RA for generating a new Certificate, preferably before the existing certificate expires.

4.8 DISASTER RECOVERY AND KEY COMPROMISE

CA maintains off-site backups of the application logs, certificate application data, audit data, and records for all certificates and CRLs issued. Backup of CA and Sub-CA private keys are generated and maintained. These backups are made available in the event of a compromise

or disaster. CA is also implementing a Disaster Recovery center as per the guidelines of IT Act. The disaster recovery center is a warm site which can become operational within 24 hours by means of offsite backup data upload. Once operational the Disaster Recovery site can handle at a minimum, revocation of certificates, publishing of CRL and certificate validation services.

In the event of CA key compromise, the key management and operations personnel of CA including the security, cryptographic operations, administration and management representatives will devise an action plan and implement it after approval from Verasys executive management. The action plan could include:

- Additional reasonable effort to notify relying parties of the compromise
- New key generation of CA and procedure for revocation and re-issue of all certificates issued under the old key.

4.9 CA TERMINATION

CA has a termination plan that reasonably minimizes disruption to customers, subscribers, and relying parties. The termination plan covers issues including:

- Providing notice to parties affected by the termination, such as subscribers, relying Parties, customers, and the CCA,
- The revocation of the certificate issued by CA,
- The preservation of the archives and records for the time periods required in CPS
- The continuation of subscriber and customer support services,
- The continuation of revocation services, such as the issuance of CRLs,
- The Revocation of certificates of subscribers and Sub-CAs, if necessary,
- The payment of compensation (if necessary) to subscribers whose certificates are revoked under the termination plan or provision for the Issuance of substitute certificates by a successor CA,
- Disposition of the CA's private key and the hardware token containing such private key, and
- Provisions needed for the transition of services to a successor CA.

5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1 PHYSICAL CONTROLS

5.1.1 Site Location and Construction

The system components and operation of CA is contained within a physically protected environment to deter, detect and prevent unauthorized use of, access to, or disclosure of sensitive information. The physical security standards are modeled as per the physical and operational security guidelines mentioned in the Information Technology Act.

CA's primary site consists of seven physical security tiers comprising of:

Tier 1: The common area in the vicinity of the CA operations set-up where in physical access check is performed. This is the area where common facilities are incorporated.

Tier 2: This is the first level where CA operations commence. This is manned by physical security personnel and also enforces physical proximity access control restricting entries only to CA authorized personnel.
Tier 3: Enables two factor authentication (biometrics and physical proximity). The RA validation, receiving and dispatch are carried out in this area.
Tier 4: This is where the core CA operations are housed.
Tier 5: Servers are installed in this area.
Tier 6: Certificate issuance and revocation is done in this area which houses the Certificate Manager server. The Key Ceremony is also done here.
Tier 7: The HSM module is housed in this area.

5.1.2. Physical Access

CA operation premises are actively monitored with redundant power and notification methods. Sensitive areas within the facility, such as power and network connection are also be controlled within the protected facility.

The operation site has multiple tiers of security enforced through Photo ID badges, proximity cards and biometric access devices. All visitors are escorted by the trusted persons and every visitor signs the visitor's log.

The facility is continually staffed (24x7), either by trusted persons or by an on-site guard service during non-business hours.

5.1.3. Power and Air Conditioning

CA's secure facilities are equipped with primary and backup power systems to ensure continuous, uninterrupted access to electric power and also these secure facilities are equipped with air conditioning systems to control temperature and relative humidity.

5.1.4. Water Exposures

CA locations are reasonably protected against floods and other damaging exposure to water.

5.1.5 Fire Prevention and Protection

CA facility is equipped to prevent and extinguish fires. Appropriate procedures have also been implemented to minimize the damage due to smoke and fire exposure. These measures also meet all applicable fire safety regulations.

5.1.6 Media Storage

All media containing production software and data, audit, archive, or backup information are stored within CA facilities or in a secure off-site storage facility with appropriate physical and logical access controls designed to limit access to authorized personnel and protect such media from accidental damage (e.g., water, fire, and electromagnetic exposure).

5.1.7. Waste Disposal

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Cryptographic devices are physically destroyed or zeroed in accordance the manufacturer's guidance prior to disposal. Other waste is disposed of in accordance with the CA's normal waste disposal requirements.

5.1.8. Off-Site Backup

All critical data is incrementally backed up and the backup copies are stored at an offsite location. The data is properly secured based on the classification of data, which is defined by the Certifying Authority in the security policy.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

The trusted roles pertain to CA personnel handling the following functions:

- The validation of information in certificate applications;
- The acceptance, rejection, or other processing of certificate applications, revocation requests, or renewal requests, or enrollment information;
- The issuance, or revocation of certificates, including personnel having access to restricted portions of its repository
- Handling of subscriber information or requests.

Trusted Persons include, but are not limited to:

- Cryptographic business operations personnel
- Security personnel
- System administration personnel
- Designated engineering personnel
- Executives that are designated to manage infrastructural trustworthiness

5.2.2 Number of Persons Required Per Task

Separate individuals are identified for each trusted role to ensure the integrity of the CA operations. In addition sensitive CA operations like operations of the cryptographic units, certificate manager requires the m out of n control to handle the operations of these sensitive functions. Also split control is implemented to ensure segregations between physical and logical access to systems. Personnel having secret shares do not have physical access and vice-versa.

5.2.3 Identification and Authentication for Each Role

For all personnel seeking to become trusted persons, verification of identity is performed through the personal (physical) presence of such personnel before Operations Review Committee and a check of well recognized forms of identification document issued by government. Identity is further confirmed through the background checking procedures in section 5.3.1.

CA ensures that personnel have achieved trusted status and departmental approval has been given before such personnel are:

- Issued access devices and granted access to the required facilities
- Issued electronic credentials to access and perform specific functions on CA's IT systems.

5.3 PERSONNEL CONTROLS

5.3.1 Background, Qualifications, Experience, and Clearance Requirements

Personnel seeking to become trusted persons must present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily, as well as proof of any government clearances, if any,

necessary to perform certification services under government contracts. Background checks are repeated at least every 2 years for personnel holding Trusted Positions.

5.3.2 Background Check Procedures

CA conducts background checks, which include the following:

- Confirmation of previous employment,
- Search of criminal records,
- Search of PAN & Aadhaar records or any one other government issued ID.

The factors revealed in a background check that may be considered grounds for rejecting candidates for trusted positions or for taking action against an existing trusted person generally include the following:

- Misrepresentations made by the candidate or trusted person,
- Highly unfavorable or unreliable personal references and
- Certain criminal convictions

Reports containing such information are evaluated by human resources and security personnel, who determine the appropriate course of action in light of the type, magnitude, and frequency of the behavior uncovered by the background check. Such actions may include measures up to and including the cancellation of offers of employment made to candidates for trusted positions or the termination of existing trusted persons.
The use of information revealed in a background check to take such actions is subject to the applicable state, and local laws.

5.3.3 Training Requirements

CA provides adequate training to the personnel selected for each trusted role to perform their job responsibilities ably and satisfactorily.

- Comprehensive training with respect to the duties they have to perform.
- Awareness of the relevant aspects of Information Technology Security Policy and
- Security Guidelines framed for carrying out CA operations.
- Training in disaster recovery and business continuity procedures of the CA.
- Technical training on operations of the relevant PKI software and associated platforms

5.3.4 Retraining Frequency and Requirements

CA provides refresher training and updates to its personnel to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily. Periodic security awareness and any new technology changes training is provided on an ongoing basis based on the newer versions or releases of the products.

5.3.5 Sanctions for Unauthorized Actions

Appropriate disciplinary actions are taken for unauthorized actions or other violations of CA policies and procedures. Disciplinary actions may include measures up to and including termination and are commensurate with the frequency and severity of the unauthorized actions.

5.3.6 Contracting Personnel Requirements

Independent contractors and consultants are permitted access to CA secure facilities only to the extent they are escorted and directly supervised by trusted persons.

5.3.7 Documentation Supplied to Personnel

All the personnel involved in CA services are required to read this CPS and other policy documents.

Adequate training materials and relevant documents is provided to all the personnel in trusted roles to perform their job responsibilities ably and satisfactorily.

6. TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

CA key pair, is generated by multiple trained and trusted personnel in pre-planned key generation ceremonies. This procedure is documented, recorded and signed by all the individuals entrusted with this activity and is stored for audit requirements for a period of time deemed appropriate by the CA. Key pairs for CA is generated in a hardware security module (HSM) certified to meet the requirements of FIPS 140-1 level 3 or higher.

Subscribers are required to use key pairs that are 2048 bits long, generated on a secure medium preferably on smartcard/token. The subscribers generate their own key pairs.

6.1.1 Private Key Delivery to Entity

End subscriber private key is generated by the end subscriber and hence there is no delivery to the end subscribers. In the case of hardware based tokens or smart cards, pre-formatted tokens are sent to the subscribers and the associated PIN is sent by an out of band process. The end user then uses the token and the client software provided to him to generate and store the private key and also initiates an online session with the CA server for certificate generation

6.1.2 Public Key Delivery to Certificate Issuer

End user subscribers generate a PKCS#10 request containing their public key and send it to the CA. This is accomplished using the client software which initiates an online session with the CA server and deliver the signed certificates to the subscriber. The online session is secured by SSL.

6.1.3 CA Public Key Delivery to Users

CA makes its Public Keys available to relying parties in repository available at www.vsign.in/repository/cacerts

6.1.4 Key Sizes

The key length of CA, is equivalent to 2048-bit RSA key pair. RA and subscribers are required to use key pairs that are 2048 bits long.

6.1.5 Hardware/Software Key Generation

CA generates key pairs on in FIPS 140-1 Level 3 compliant hardware security modules.

6.1.6 Key Usage Purposes

The purposes for which a key can be used is restricted by CA through Key Usage extension in the certificate (Refer section 7.1.2 of this CPS).

6.2 PRIVATE KEY PROTECTION

CA has put into practice a combination of physical, logical and procedural controls to ensure the security of private keys. Logical and procedural controls are described in this section. Physical access controls are described in section 5.1 of this CPS.

6.2.1 Standards for Cryptographic Modules

CA performs all cryptographic operations with its own private keys on hardware cryptographic modules rated at a minimum of FIPS 140-1 level 3.
All RAs perform cryptographic operations with their own private keys on hardware cryptographic modules. Subscribers have the option of protecting their private keys in a smart card or other hardware token.

6.2.2 Private Key (N out of M) Multi-Person Control

CA has implemented multi-person control to protect the activation data needed to activate CA private keys. It uses 'secret sharing' to split the private key or activation data needed to operate the private key into separate parts called 'secret shares'. Each 'secret share' is held by a distinct CA trusted personnel referred to as the Custodian. A threshold number of secret shares (n) out of the total number of secret shares (m) are required to operate the private key. CA also uses secret sharing to protect the activation data needed to activate private keys located at its disaster recovery site.

6.2.3 Private Key Backup

CA creates backup of its private keys. These are stored in encrypted form in a hardware cryptographic module

6.2.4 Private Key Archival

At the end of the validity period, **CA private key is be archived for a period of 7 years**. These are archived in the hardware cryptographic module meeting the FIPS 140-1 level 3 standards. Procedural controls prevent the archived CA keys pairs from being returned to production use. After completion of the archive period, these keys are destroyed as per requirements specified in section 6.2.9 of this CPS.

6.2.5 Private Key Entry into Cryptographic Module

CA key pairs is generated on the hardware cryptographic modules. CA makes copies of such key pairs for routine recovery and disaster recovery purposes and the copies are transferred in an encrypted form.

6.2.6 Method of Activating Private Key

CA activation of private key requires m out of n secret shares as mentioned in section 6.2.2 and is from the cryptographic hardware device that follows FIPS 140-1level 3 standards.

In case of RA and subscriber, private keys are activates by the client application either by a PIN or password.

6.2.7 Method of Deactivating Private Key

CA private keys are deactivated upon removal from the token reader. RA private keys (used for authentication to the RA application) are deactivated upon system log off or removal from card/token reader. Subscriber private keys may be deactivated after each operation, upon logging off their system, or upon removal of a smart card/token from the reader depending upon the authentication mechanism employed by the user. In all cases, subscribers have an obligation to adequately protect their private key(s).

6.2.8 Method of Destroying Private Key

At the conclusion of CA's operational lifetime, one or more copies of the **private key are archived.** Remaining copies of the CA private key are securely destroyed. In addition, archived CA private keys are securely destroyed at the conclusion of their archive periods. CA key destruction activities require the participation of multiple trusted individuals.

CA destroys its private keys in a manner that reasonably ensures that there are no residuals remains of the key that could lead to the reconstruction of the key.
CA utilizes the zeroization function of its hardware cryptographic modules and other appropriate means to ensure the complete destruction of CA private keys. When performed, CA key destruction activities are logged.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1. Public Key Archival

All certificate containing public keys (including CA and Subscribers) are archived upon expiry as part of CA's routine backup procedures and kept for a period of seven (7) years as per the IT Act.

6.3.2. Usage Periods for the Public and Private Keys

The maximum operational periods for certificates are set forth in table below :

Certificate	Validity
CA	10 years
All certificates issued including RA, Subscriber	Maximum 3 years

6.4 ACTIVATION DATA

6.4.1. Activation Data Generation and Installation

After personalization or initialization of HSM/Smart card/token, no activation data other that access control mechanisms (PIN) are required to operate cryptographic modules.

6.4.2. Activation Data Protection

Passwords or PIN is notaccessible to anyone except the authorized personnel or certificate holder.

6.5 COMPUTER SECURITY CONTROLS

CA ensures that the systems maintaining CA software and data files are trustworthy systems secure from unauthorized access. In addition, CA limits access to production servers to trusted persons and those individuals with a valid business reason for such access. General application users do not have accounts on production servers. CA production network is logically separated from other components. This separation prevents network access except through defined application processes. CA use firewalls to protect the production network from internal and external intrusion and limit the nature and source of network activities that may access production systems. Direct access to databases supporting CA's repository is limited to trusted persons in its operations group having a valid business reason for such access.

The CA systems used for issuance of eSigns are separate from the CA systems used for issuance of other type of Digital Signatures as prescribed by CCA.

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

Applications are developed and implemented by CA in accordance with CA's systems development and change management standards.

6.6.2 Security Management Controls

CA has mechanisms and/or policies in place to control and monitor the configuration of its CA systems. Upon installation and periodically thereafter, CA validates the integrity of its systems.

6.7 NETWORK SECURITY CONTROLS

CA performs all its functions using networks secured in accordance with the security and audit requirements to prevent unauthorized access and other malicious activity. CA protects its communications of sensitive information through the use of encryption and digital signatures.

6.8 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

CA uses hardware cryptographic modules rated FIPS 141-level 3 to perform all digital signing operations.

7. CERTIFICATE PROFILE& CRL PROFILE

CA issues Certificates & CRLs with profiles as per the Interoperability Guidelines (IOG) of CCA published on the website of CCA,
http://www.cca.gov.in/cca/sites/default/files/files/Guidelines/CCA-IOG.pdf

8. SPECIFICATION ADMINISTRATION

8.1 SPECIFICATION CHANGE PROCEDURES

Amendments to this CPS made by CAneed to be approved by the CCA before they become effective. Updates are in the form of a document containing a revised CPS.

8.1.1. Items that Can Change Without Notification

The CA reserves the right to amend the CPS without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URLs, and changes to contact information.

8.1.2. Items that Can Change with Notification

8.1.2.1 List of Items

All updates, except those covered in section 8.1.1, to the CPS require notification prior to becoming effective.

8.1.2.2 Notification Mechanism

Except as noted under section 8.1.1, CA submits the updates in electronic and/or paper form to the CCA for approval. After obtaining the CCA's approval the updates to the CPS is posted in CA's repository, which is located at www.vsign.in/repository/cps

8.1.2.3 Comment Period

Except as noted under section 8.1.2.2, the comment period for any material amendments to this CPS is be fifteen (15) days, starting on the date on which the amendments are posted on CA's repository. Any PKI participant is entitled to file comments with CA up until the end of the comment period.

8.1.2.4 Mechanism to Handle Comments

CA will consider any comments on the proposed amendments. CA will either (a) allow the proposed amendments to become effective without amendment, (b) amend the proposed amendments and republish them as a new amendment under section 8.1.2.2, or (c) withdraw

the proposed amendments. CA is entitled to withdraw proposed amendments by providing notice in the Revision History section of this CPS.

Unless proposed amendments are amended or withdrawn, they become effective upon the expiration of the comment period under section 8.1.2.3.

8.2 PUBLICATION AND NOTIFICATION PROCEDURES

8.2.1 Items not published in the CPS

Security documents considered confidential by CA are not disclosed to the public.

8.2.2 Distribution of the CPS

This latest version of this CPS is available for viewing in electronic form within CA's repository at www.vsign.in/repository/cps

CA also makes the CPS available upon request sent to: info@vsign.in

The paper copy of the CPS is available from CA upon requests sent to:

Verasys Technologies Pvt. Ltd.,
2nd floor, Bhavna Building,
V.S. Marg, Prabhadevi
Mumbai- 400025
Phone: +91 43156000

Email: info@vsign.in
Website: www.vsign.in

8.3 CPS APPROVAL PROCEDURES

CA must sanction CPS intended for use, however the final approval to the CPS is made by the CCA.

9. ESIGN ONLINE ELECTRONIC SIGNATURE SERVICE

9.1 INTRODUCTION

eSign is an online electronic signature service which can be integrated with service delivery applications via an API to facilitate an eSign user to digitally sign a document. Using authentication of the eSign user through e-KYC service, online electronic signature service is facilitated

The eSign service is governed by e-authentication guidelines. While authentication of the signer is carried out using e-KYC services, the signature on the document is carried out on a backend server of the e-Sign provider. eSign services are facilitated by trusted third party service providers - currently Certifying Authorities (CA) licensed under the IT Act. To enhance security and prevent misuse, eSign user's private keys are created on Hardware Security Module (HSM) and destroyed immediately after one time use.

9.2 REQUIREMENTS AND SECURITY CONTROLS

- The communication between Application service provider and ESP is in accordance with eSign API Specifications published by the CCA.
- The CA system used for issuing e-KYC class based DSCs are independent of CA systems used for other classes of DSCs.
- The CA system used for eSign accept only digitally signed Certificate Signing Request (CSR) from designated ESP systems over a secure link.
- CA system used for eSign are configured to issue only e-KYC class end entity individual digital signature certificates.
- ESP is allowed access to CA systems only for submitting CSR for issuance of e-KYC classes of DSCs to be used for eSign.
- The ESP systems used for e-KYC service request and response is different from ESP systems used to communicate with CA servers.
- The eSign user key generation and management systems of ESP is separate from CA systems in use for issuing end user certificate for other classes of DSCs.

9.3 KEY VALIDITY

The validity of DSC does not exceed 30 minutes. After one time usage private key of the applicant is deleted.

9.4 AUDIT LOGS

Audit Logs such as type of events, security procedures, retention period, audit frequency, backup and archival are performed as per requirements specified in the e-Authentication Guidelines.

*****